

# Esempio di configurazione dell'autenticazione Web locale del portale guest di Identity Services Engine

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Procedura LWA con ISE Guest Portal](#)

[Esempio di rete](#)

[Prerequisiti di configurazione](#)

[Configurare il WLC](#)

[Configurazione dell'ISE esterna come URL Webauth a livello globale](#)

[Configurazione degli Access Control Lists \(ACLs\)](#)

[Configurare SSID \(Service Set Identifier\) per LWA](#)

[Configurazione dell'ISE](#)

[Definire il dispositivo di rete](#)

[Configurare il criterio di autenticazione](#)

[Configura criteri di autorizzazione e risultato](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

## Introduzione

In questo documento viene descritto come configurare Local Web Authentication (LWA) con il portale guest Cisco Identity Services Engine (ISE).

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- ISE
- Cisco Wireless LAN Controller (WLC)

## Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- ISE versione 1.4
- WLC versione 7.4

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Premesse

Questo documento descrive la configurazione di LWA. Tuttavia, Cisco consiglia di utilizzare l'autenticazione Web centralizzata (CWA) con ISE quando possibile. Esistono alcuni scenari in cui LWA è preferibile o l'unica opzione, pertanto questo è un esempio di configurazione per tali scenari.

## Configurazione

LWA richiede alcuni requisiti e una configurazione principale sul WLC, oltre ad alcune modifiche necessarie sull'ISE.

Prima di illustrare questi argomenti, di seguito viene riportata una descrizione del processo LWA con ISE.

### Procedura LWA con ISE Guest Portal

1. Il browser tenta di recuperare una pagina Web.
2. Il WLC intercetta la richiesta HTTP(S) e la reindirizza all'ISE.  
Nell'intestazione di reindirizzamento HTTP sono memorizzate diverse informazioni chiave. Di seguito è riportato un esempio di URL di reindirizzamento:  
`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/`  
Dall'URL di esempio si può vedere che l'utente ha cercato di raggiungere "yahoo.com". L'URL contiene anche informazioni sul nome della rete WLAN (Wireless Local Area Network) (mlatosie\_LWA) e sugli indirizzi MAC del client e del punto di accesso (AP). Nell'URL di esempio, 1.1.1.1 è il WLC, e **mlatosieise.wlaaan.com** è il server ISE.
3. Viene visualizzata la pagina di accesso per i guest ISE in cui è possibile immettere nome utente e password.
4. L'ISE esegue l'autenticazione sulla base della sequenza di identità configurata.
5. Il browser viene reindirizzato di nuovo. Questa volta, invia le credenziali al WLC. Il browser fornisce il nome utente e la password che l'utente ha immesso nell'ISE senza ulteriori interazioni da parte dell'utente. Di seguito è riportato un esempio di richiesta GET al WLC.  
GET  
`/login.html?redirect_url=http://yahoo.com/&username=mlatosie%40cisco.com&password=ityh&buttonClicked=4&err_flag=0`

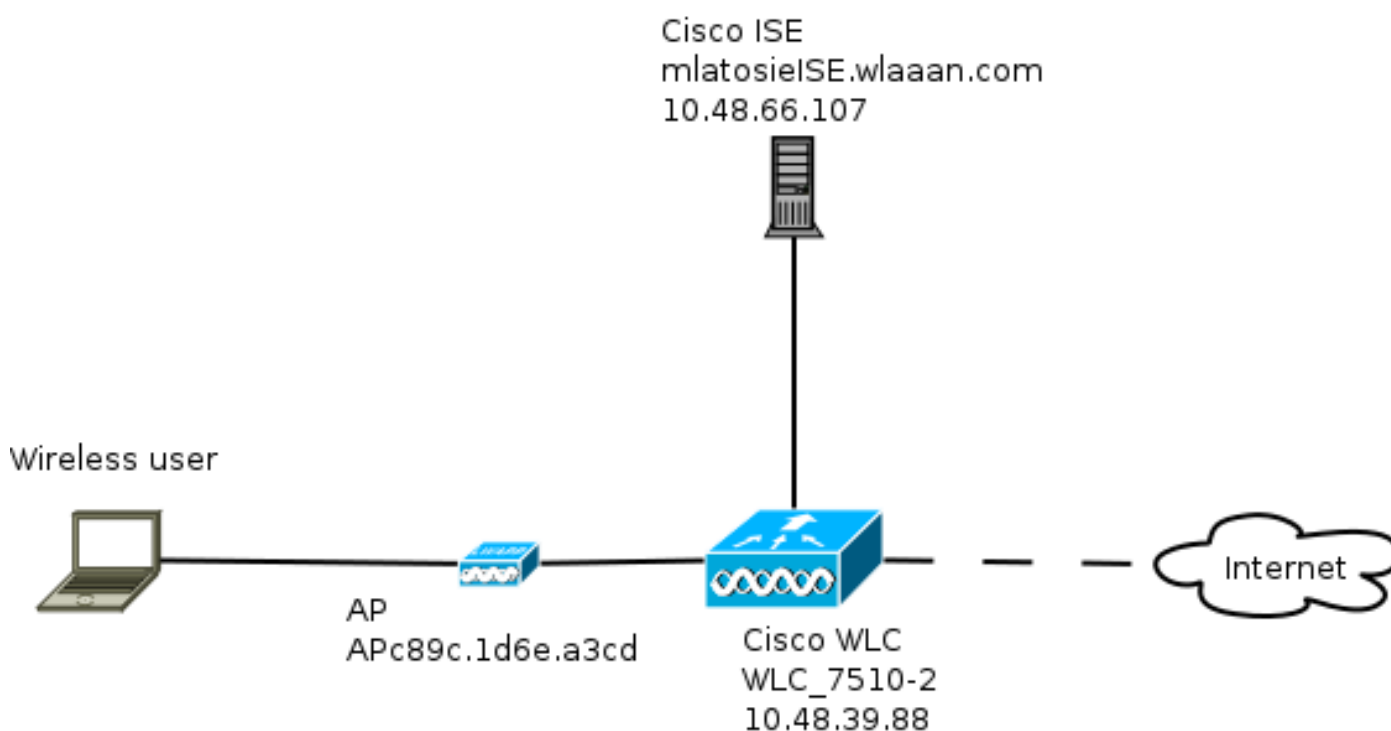
Anche in questo caso, l'URL originale (**yahoo.com**), il nome utente (**mlatosie@cisco.com**) e la password (**ityh**) sono tutti inclusi.

**Nota:** Sebbene l'URL sia visibile qui, la richiesta effettiva viene inviata tramite SSL (Secure Sockets Layer), indicato da HTTPS ed è difficile da intercettare.

6. Il WLC utilizza RADIUS per autenticare il nome utente e la password sull'ISE e consente l'accesso.
7. L'utente viene reindirizzato al portale specificato. Per ulteriori informazioni, consultare la sezione "**Configurazione dell'ISE esterna come URL webauth**" di questo documento.

## Esempio di rete

Nella figura viene descritta la topologia logica dei dispositivi utilizzati in questo esempio.



## Prerequisiti di configurazione

Affinché il processo LWA funzioni correttamente, il client deve essere in grado di ottenere:

- Configurazione dell'indirizzo IP e della maschera di rete
- Route predefinita
- Server DNS (Domain Name System)

Tutti questi elementi possono essere forniti con DHCP o con la configurazione locale. La risoluzione DNS deve funzionare correttamente affinché LWA funzioni.

## Configurare il WLC

### Configurazione dell'ISE esterna come URL Webauth a livello globale

In **Protezione > Web Auth > Pagina di accesso Web**, è possibile accedere a queste informazioni.

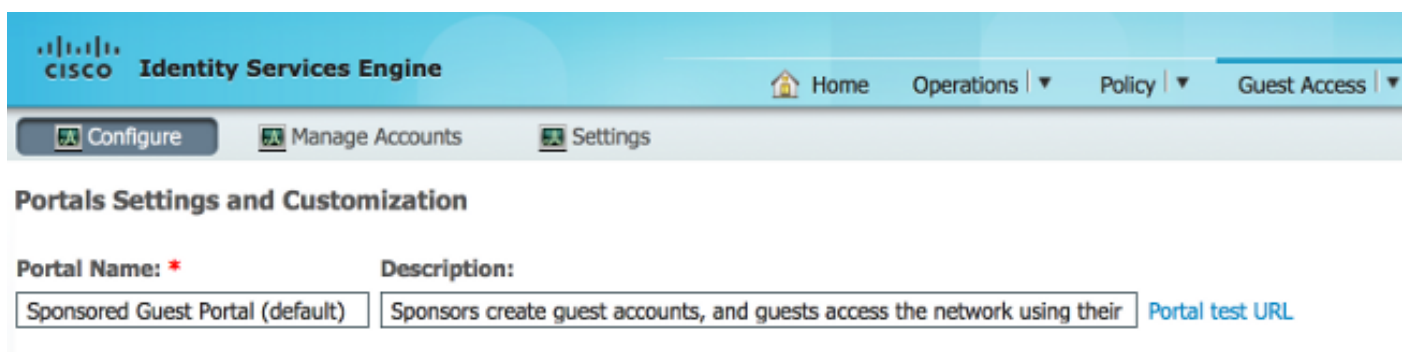
## Web Login Page

|                          |  |
|--------------------------|--|
| 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"/>                        |

**Nota:** Questo esempio utilizza un URL di autenticazione Web esterna ed è stato preso da ISE versione 1.4. Se si ha una versione diversa, consultare la guida alla configurazione per capire cosa deve essere configurato.

È possibile anche configurare questa impostazione per WLAN. e quindi nelle impostazioni di sicurezza WLAN specifiche. Queste sostituiscono l'impostazione globale.

Per individuare l'URL corretto per il portale specifico, scegliere **ISE > Criteri Guest > Configura > portale specifico**. Fare clic con il pulsante destro del mouse sul collegamento da "Portal test URL" (URL test portale) e scegliere **copy link location (copia percorso collegamento)**.



**Portals Settings and Customization**

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

Nell'esempio, l'URL completo è:

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

## Configurazione degli Access Control Lists (ACLs)

Per il corretto funzionamento dell'autenticazione Web, è necessario definire il traffico consentito. Determinare se utilizzare ACL FlexConnect o ACL normali. Gli AP FlexConnect utilizzano ACL FlexConnect, mentre gli AP che utilizzano la commutazione centralizzata utilizzano ACL normali.

Per capire in che modalità funziona un determinato access point, selezionare **Wireless > Access point** e selezionare la casella a discesa **Nome access point > Modalità AP**. Una distribuzione tipica è **locale** o **FlexConnect**.

In **Sicurezza > Access Control Lists**, scegliere **FlexConnect ACL** o **ACL**. Nell'esempio, tutto il traffico UDP è stato autorizzato per consentire specificamente lo scambio DNS e il traffico verso l'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"/> |

In questo esempio viene usato FlexConnect, quindi sono definiti sia FlexConnect che ACL standard.

Questo comportamento è documentato nell>ID bug Cisco [CSCue68065](#) per quanto riguarda i controller WLC 7.4. Non è più richiesto sul WLC 7.5, dove è sufficiente un FlexACL e non è più necessario un ACL standard

## Configurare SSID (Service Set Identifier) per LWA

In WLAN, scegliere l'ID WLAN da modificare.

## Configurazione autenticazione Web

Applicare gli stessi ACL definiti nel passaggio precedente e abilitare l'autenticazione Web.

WLANs > Edit 'mlatosie\_LWA'

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

**Nota:** Se si usa la funzionalità di commutazione locale di FlexConnect, è necessario aggiungere il mapping ACL a livello dell'access point. In **Wireless > Access Point**. Selezionare il nome dell'access point appropriato > **FlexConnect > ACL di autenticazione Web esterna**.

## 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

## Configurazione server di autenticazione, autorizzazione e accounting (AAA)

Nell'esempio, sia il server di autenticazione che il server di accounting puntano al server ISE definito in precedenza.

**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  Enabled

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

**Nota:** Le impostazioni predefinite nella scheda **Avanzate** non devono essere aggiunte.

## Configurazione dell'ISE

La configurazione ISE prevede diverse fasi.

Definire innanzitutto il dispositivo come dispositivo di rete.

Verificare quindi che esistano le regole di autenticazione e autorizzazione per questo scambio.

### Definire il dispositivo di rete

In **Amministrazione > Risorse di rete > Dispositivi di rete**, compilare i seguenti campi:

- Nome dispositivo
- Indirizzo IP dispositivo
- **Impostazioni autenticazione > Segreto condiviso**

#### 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"/> |

**Authentication Settings**

Enable Authentication Settings

Protocol **RADIUS**

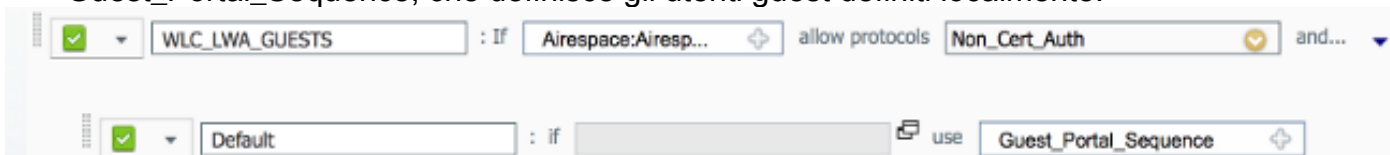
\* Shared Secret

### Configurare il criterio di autenticazione

In **Criteri > Autenticazione** aggiungere un nuovo criterio di autenticazione.

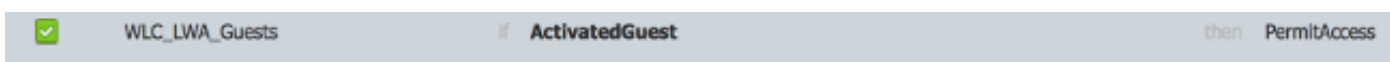
In questo esempio vengono utilizzati i seguenti parametri:

- Nome: **WLC\_LWA\_Guests**
- Condizione: **Airespace:Airespace-Wlan-Id**. Questa condizione corrisponde all'ID WLAN 3, che è l'ID della **variabile multisito\_LWA** WLAN precedentemente definita sul WLC.
- {facoltativo} Consente i protocolli di autenticazione che non richiedono il certificato **Non\_Cert\_Auth**, ma è possibile utilizzare le impostazioni predefinite.
- **Guest\_Portal\_Sequence**, che definisce gli utenti guest definiti localmente.



## Configura criteri di autorizzazione e risultato

In **Criterio > Autorizzazione** definire un nuovo criterio. Può trattarsi di una politica di base, come:



Questa configurazione dipende dalla configurazione generale di ISE. Questo esempio è stato intenzionalmente semplificato.

## Verifica

Sul sito ISE, gli amministratori possono monitorare e risolvere i problemi delle sessioni live in **Operazioni > Autenticazioni**.

Devono essere visualizzate due autenticazioni. La prima autenticazione viene effettuata dal portale guest all'ISE. La seconda autenticazione viene effettuata come richiesta di accesso dal WLC all'ISE.

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

Per verificare quali criteri di autorizzazione e criteri di autenticazione sono stati scelti, è possibile fare clic sull'icona **Authentication Detail Report**.

Sul WLC, un amministratore può monitorare i client in **Monitor > Client**.

Di seguito è riportato l'esempio di un client autenticato correttamente:

|                   |                   |              |              |                    |          |            |     |   |    |
|-------------------|-------------------|--------------|--------------|--------------------|----------|------------|-----|---|----|
| 28:cf:e9:13:47:cb | AP:c89c.1d6e.a3cd | mлатosie_LWA | mлатosie_LWA | mлатosie@cisco.com | 802.11bn | Associated | Yes | 1 | No |
|-------------------|-------------------|--------------|--------------|--------------------|----------|------------|-----|---|----|

## Risoluzione dei problemi

Cisco consiglia di eseguire i debug sul client, quando possibile.

Dalla CLI, questi debug forniscono informazioni utili:

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



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

```
debug aaa all enable
```

## Informazioni correlate

- [Guida alla configurazione di Cisco ISE 1.x](#)
- [Guida alla configurazione di Cisco WLC 7.x](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)