

# Configura reindirizzamento HTTPS su Web-auth

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Errore certificato](#)

[Configurazione](#)

[Configurare il WLC per il reindirizzamento HTTPS](#)

[Verifica](#)

[Risoluzione dei problemi](#)

## Introduzione

In questo documento viene descritta la configurazione del reindirizzamento dell'autenticazione Web su HTTPS. Questa funzionalità è stata introdotta in Cisco Unified Wireless Network (CUWN) versione 8.0.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base dell'autenticazione Web di Wireless LAN Controller (WLC)
- Come configurare il WLC per l'autenticazione Web.

### Componenti usati

Le informazioni di questo documento si basano sul WLC Cisco serie 5500 con firmware CUWN versione 8.0.

**Nota:** La configurazione e la spiegazione della web-auth fornite in questo documento sono applicabili a tutti i modelli WLC e a tutte le immagini CUWN uguali o successive alla versione 8.0.100.0.

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

L'autenticazione Web è una funzione di sicurezza di livello 3. Blocca tutto il traffico IP/dati, ad eccezione dei pacchetti correlati a DHCP/DNS, da un client specifico fino a quando un client wireless non ha fornito un nome utente e una password validi. L'autenticazione Web viene in genere utilizzata dai clienti che desiderano distribuire una rete ad accesso guest. L'autenticazione Web viene avviata quando il controller intercetta il primo pacchetto TCP HTTP (porta 80) GET dal client.

Affinché il browser Web del client arrivi a questo punto, il client deve prima ottenere un indirizzo IP ed eseguire una conversione dell'URL in indirizzo IP (risoluzione DNS) per il browser Web. Questo consente al browser Web di sapere quale indirizzo IP inviare HTTP GET. Quando il client invia il primo HTTP GET alla porta TCP 80, il controller reindirizza il client a `https:<IP virtuale>/login.html` per l'elaborazione. Questo processo apre la pagina Web di login.

Nelle versioni precedenti a CUWN 8.0 (ovvero fino a 7.6), se il client wireless presenta una pagina HTTPS (TCP 443), la pagina non viene reindirizzata al portale di autenticazione Web. Poiché sempre più siti Web iniziano a utilizzare HTTPS, questa funzionalità è inclusa in CUWN 8.0 e versioni successive. Con questa funzione, se un client wireless tenta di eseguire `https://<sito Web>`, viene reindirizzato alla pagina di accesso Web-auth. Questa funzione è molto utile anche per i dispositivi che inviano richieste https con un'applicazione (ma non con un browser).

## Errore certificato

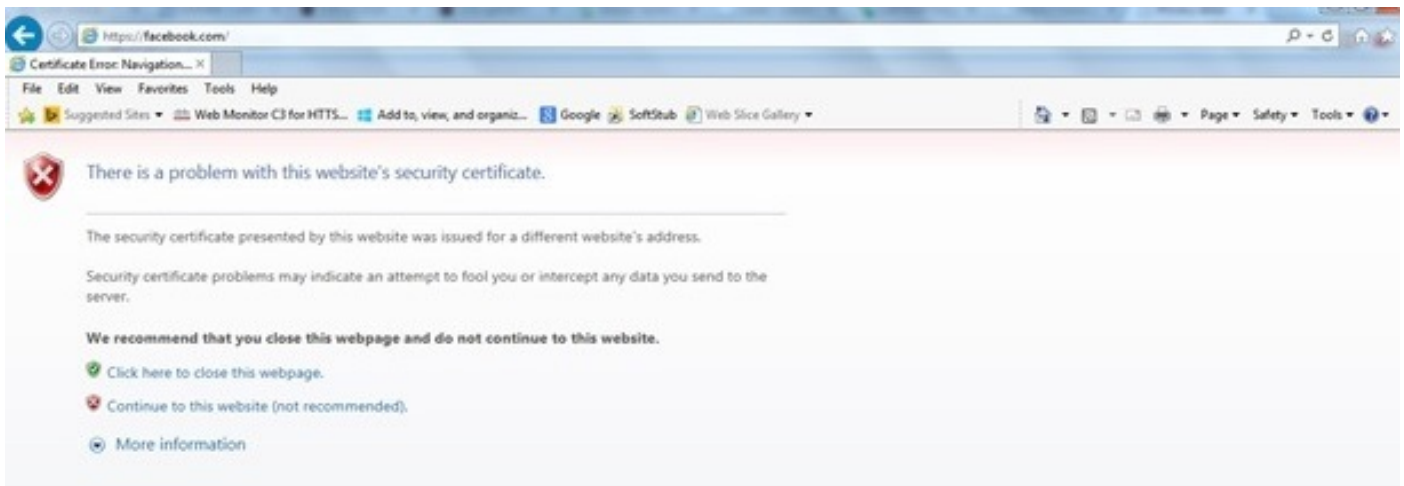
Viene visualizzato il messaggio di avviso "il certificato non è rilasciato da un'autorità di certificazione attendibile". viene visualizzato nel browser dopo aver configurato la funzionalità di reindirizzamento https. Questo messaggio viene visualizzato anche se si dispone di un certificato radice o concatenato valido sul controller, come mostrato nella Figura 1 e nella Figura 2. Il motivo è che il certificato installato sul controller è stato rilasciato all'indirizzo IP virtuale.

**Nota:** Se si prova un reindirizzamento HTTP e si dispone di questo certificato sul WLC, non viene visualizzato questo errore di avviso del certificato. Tuttavia, nel caso di HTTPS-redirect, viene visualizzato questo errore.

Quando il client tenta `HTTPS://<sito Web>`, il browser si aspetta il certificato rilasciato all'indirizzo IP del sito risolto dal DNS. Tuttavia, ciò che ricevono è il certificato che è stato rilasciato al server Web interno del WLC (indirizzo IP virtuale) che provoca l'emissione dell'avviso da parte del browser. Ciò è dovuto esclusivamente al modo in cui funziona HTTPS e si verifica sempre se si tenta di intercettare la sessione HTTPS per il funzionamento del reindirizzamento Web-auth.

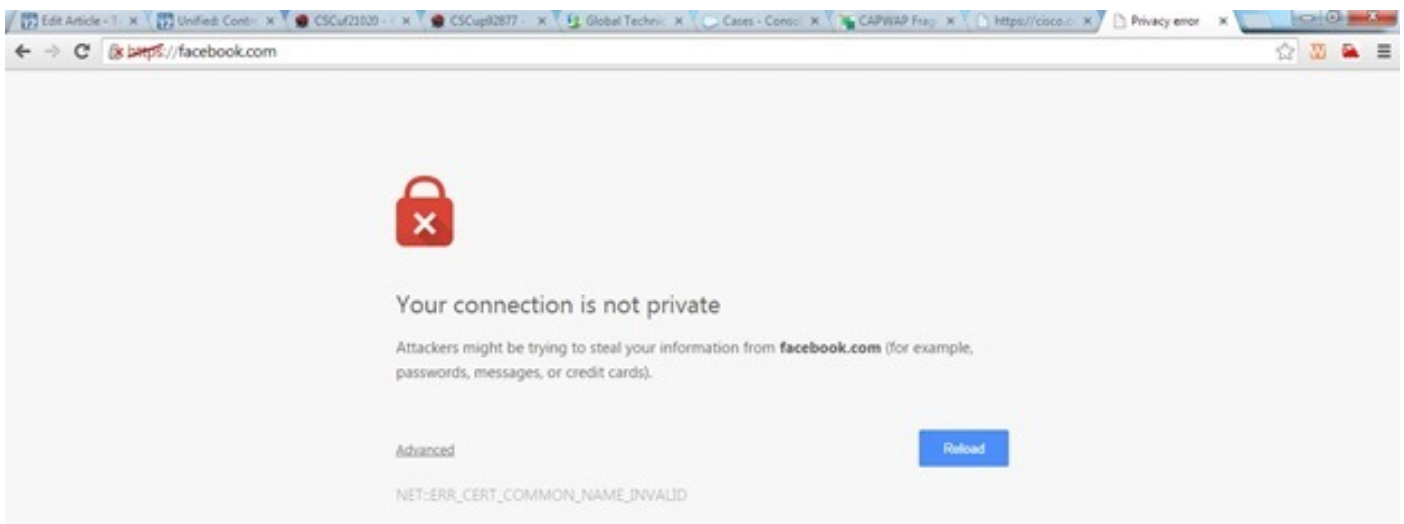
È possibile che in browser diversi vengano visualizzati messaggi di errore del certificato diversi, ma tutti sono correlati allo stesso problema descritto in precedenza.

## Figura 1



Questo è un esempio di come l'errore può apparire in Chrome:

Figura 2



## Configurazione

### Configurare il WLC per il reindirizzamento HTTPS

Questa configurazione presuppone che la rete LAN wireless (WLAN) sia già configurata per la sicurezza dell'autenticazione Web di layer 3. Per abilitare o disabilitare il reindirizzamento HTTPS su questa WLAN di autenticazione Web:

```
(WLC)>config wlan security web-auth enable 10
(WLC)>config network web-auth https-redirect enable
WARNING! - You have chosen to enable https-redirect.
This might impact performance significantly
```

Come mostrato nella configurazione di esempio, questo può influire sul throughput per un reindirizzamento HTTPS ma non sul reindirizzamento HTTP

Per ulteriori informazioni e una configurazione delle WLAN di autenticazione Web, vedere [Autenticazione Web sul controller WLAN](#).

# Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo [strumento Output Interpreter \(solo utenti registrati\) supporta alcuni comandi show](#). Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output del comando **show**.

```
(WLC)>show network summary
```

```
Web Auth Secure Web ..... Enable
Web Auth Secure Redirection ..... Enable
```

## 1. Abilita questi debug:

```
(WLC) debug client
```

```
(WLC)> debug web-auth redirect enable
```

## 2. Verificare i debug:

```
(WLC) >show debug
```

```
MAC Addr 1..... 24:77:03:52:56:80
```

```
Debug Flags Enabled:
webauth redirect enabled.
```

## 3. Associare il client al SSID abilitato per l'autenticazione Web.

## 4. Cercare i seguenti debug:

```
*webauthRedirect: Jan 16 03:35:35.678: 24:77:3:52:56:80- received connection.
client socket = 9
*webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- trying to read on socket 95
*webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- calling parser with bytes = 204
*webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- bytes parsed = 204
*webauthRedirect: Jan 16 03:35:35.679: captive-bypass detection enabled,
checking for wispr in HTTP GET, client mac=24:77:3:52:56:80
*webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- Preparing redirect
URL according to configured Web-Auth type
*webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- got the hostName
for virtual IP(wirelessguest.test.com)
*webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- Checking custom-web
config for WLAN ID:10
*webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- Global status is
enabled, checking on web-auth type
*webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- Web-auth type Customized,
using URL:https://wirelessguest.test.com/fs/customwebauth/login.html
```

**Nota:** Per il corretto funzionamento del reindirizzamento HTTPS, verificare che sia attivato Secure web (config network secureweb enable/disable) o web-auth secure (config network web-auth secureweb enable/disable). Si noti inoltre che quando si utilizza il reindirizzamento su HTTPS potrebbe verificarsi una leggera riduzione della velocità effettiva.

# Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.