

Risoluzione dei problemi di autenticazione Web su un controller WLC

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Prodotti correlati](#)

[Autenticazione Web sui WLC](#)

[Risoluzione dei problemi di autenticazione Web](#)

[Informazioni correlate](#)

Introduzione

In questo documento vengono forniti suggerimenti per risolvere i problemi di autenticazione Web in un ambiente WLC (Wireless LAN Controller).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Controllo e provisioning dei punti di accesso wireless (CAPWAP).
- Come configurare un Lightweight Access Point (LAP) e un WLC per le operazioni di base.
- Conoscenze base dell'autenticazione Web e di come configurare l'autenticazione Web sui WLC.

Per informazioni su come configurare l'autenticazione Web sui WLC, fare riferimento all'[esempio di configurazione dell'autenticazione Web del controller LAN wireless](#).

Componenti usati

Per questo documento, è stato usato uno switch WLC 5500 con firmware versione 8.3.121.

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.

Prodotti correlati

Questo documento può essere utilizzato anche per questo hardware:

- Cisco serie 5500 Wireless Controller
- Cisco serie 8500 Wireless Controller
- Cisco serie 2500 Wireless Controller
- Cisco Airespace serie 3500 WLAN Controller
- Cisco Airespace serie 4000 Wireless LAN Controller
- Cisco Flex serie 7500 Wireless Controller
- Cisco Wireless Services Module 2 (WiSM2)

Autenticazione Web sui WLC

L'autenticazione Web è una funzione di sicurezza di livello 3 che impedisce al controller di autorizzare il traffico IP, ad eccezione dei pacchetti correlati a DHCP/DNS (Domain Name System), da un determinato client fino a quando il client non ha fornito correttamente un nome utente e una password validi, con un'eccezione del traffico consentito tramite un elenco di controllo di accesso (ACL) di preautenticazione. L'autenticazione Web è l'unico criterio di protezione che consente al client di ottenere un indirizzo IP prima dell'autenticazione. Si tratta di un semplice metodo di autenticazione senza la necessità di un supplicant o di un'utility client. L'autenticazione Web può essere eseguita localmente su un WLC o su un server RADIUS. L'autenticazione Web viene in genere utilizzata dai clienti che desiderano distribuire una rete di 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. In questo modo il browser Web può sapere quale indirizzo IP inviare HTTP GET.

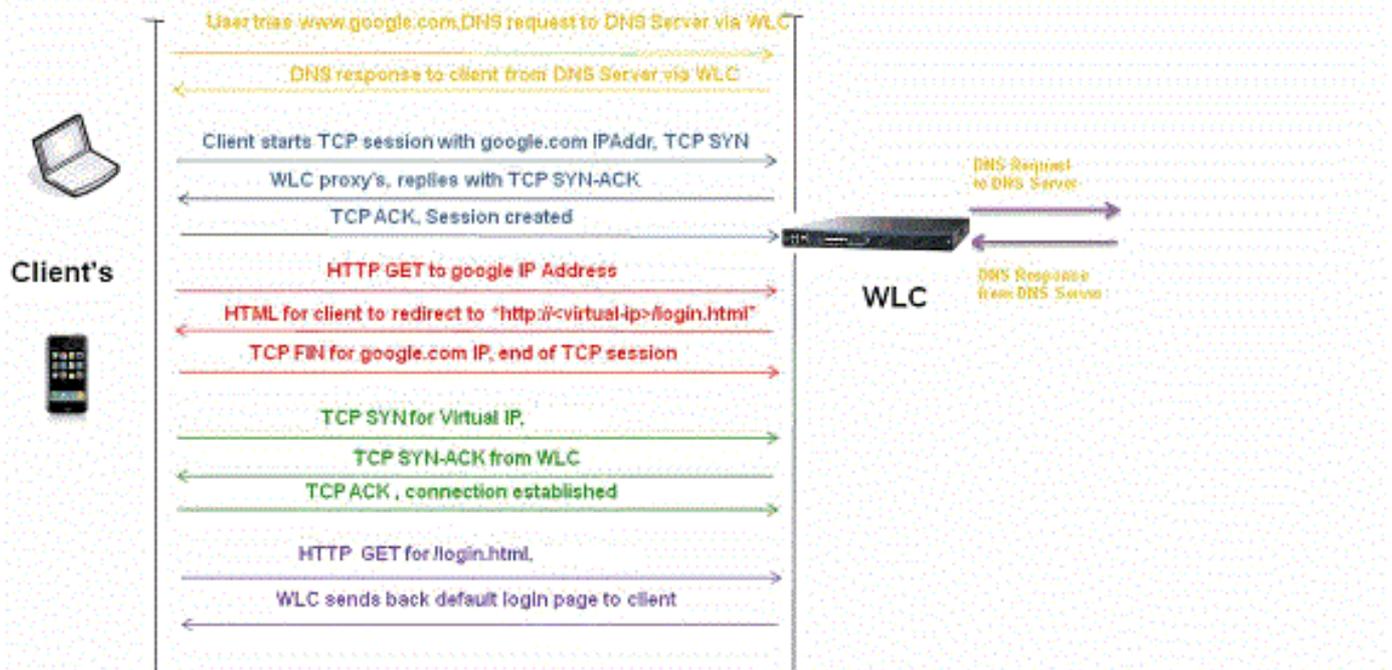
Quando l'autenticazione Web è configurata sulla WLAN, il controller blocca tutto il traffico (fino al completamento del processo di autenticazione) proveniente dal client, ad eccezione del traffico DHCP e DNS. Quando il client invia il primo HTTP GET alla porta TCP 80, il controller reindirizza il client a <https://192.0.2.1/login.html> (se si tratta dell'IP virtuale configurato) per l'elaborazione. Questo processo apre la pagina Web di login.

 Nota: quando si utilizza un server Web esterno per l'autenticazione Web, le piattaforme WLC richiedono un ACL di preautenticazione per il server Web esterno.

In questa sezione viene illustrato in dettaglio il processo di reindirizzamento dell'autenticazione

Web.

Web-Auth Redirection Process



- Aprire il browser Web e digitare un URL, ad esempio <http://www.example.com>. Il client invia una richiesta DNS per questo URL per ottenere l'IP per la destinazione. WLC passa la richiesta DNS al server DNS e il server DNS risponde con una risposta DNS, che contiene l'indirizzo IP della destinazione www.example.com, che a sua volta viene inoltrata ai client wireless.
- Il client tenta quindi di aprire una connessione TCP con l'indirizzo IP di destinazione. Invia un pacchetto TCP SYN destinato all'indirizzo IP di www.example.com.
- Il WLC ha delle regole configurate per il client e può quindi fungere da proxy per www.example.com. Invia un pacchetto TCP SYN-ACK al client con origine come indirizzo IP di www.example.com. Il client restituisce un pacchetto TCP ACK per completare l'handshake TCP a tre vie e la connessione TCP viene stabilita completamente.
- Il client invia un pacchetto HTTP GET destinato a www.example.com. Il WLC intercetta questo pacchetto e lo invia per la gestione del reindirizzamento. Il gateway applicazioni HTTP prepara un corpo HTML e lo invia come risposta al comando HTTP GET richiesto dal client. Con questo codice HTML il client passa all'URL predefinito della pagina Web del WLC, ad esempio <http://<Virtual-Server-IP>/login.html>.
- Il client chiude la connessione TCP con l'indirizzo IP, ad esempio www.example.com.
- A questo punto il client desidera andare su <http://<virtualip>/login.html> e quindi cerca di aprire una connessione TCP con l'indirizzo IP virtuale del WLC. Invia un pacchetto TCP SYN per 192.0.2.1 (ossia il nostro IP virtuale qui) al WLC.
- Il WLC risponde con un TCP SYN-ACK e il client restituisce un TCP ACK al WLC per

completare l'handshake.

- Il client invia una richiesta HTTP GET per /login.html destinata alla versione 192.0.2.1 per richiedere la pagina di accesso.
- Questa richiesta è consentita fino al server Web del WLC e il server risponde nuovamente con la pagina di accesso predefinita. Il client riceve la pagina di login nella finestra del browser dove l'utente può procedere ed effettuare il login.

Nell'esempio, l'indirizzo IP del client è 192.168.68.94. Il client ha risolto l'URL del server Web a cui ha avuto accesso, 10.1.0.13. Come si può vedere, il client ha eseguito l'handshake a tre vie per avviare la connessione TCP e quindi ha inviato un pacchetto HTTP GET iniziato con il pacchetto 96 (00 è il pacchetto HTTP). Questo non è stato attivato dall'utente, ma dal sistema operativo sono stati attivati i trigger di rilevamento automatico del portale (come si può intuire dall'URL richiesto). Il controller intercetta i pacchetti e risponde con il codice 200. Il pacchetto del codice 200 contiene un URL di reindirizzamento:

```
<HTML><HEAD>
<TITLE> Web Authentication Redirect</TITLE>
<META http-equiv="Cache-control" content="no-cache">
<META http-equiv="Pragma" content="no-cache">
<META http-equiv="Expires" content="-1">
<META http-equiv="refresh" content="1; URL=https://192.0.2.1/login.html?redirect=http://captive.apple.c
</HEAD></HTML>
```

Quindi chiude la connessione TCP tramite l'handshake a tre vie.

Il client avvia quindi la connessione HTTPS all'URL di reindirizzamento che lo invia a 192.0.2.1, che è l'indirizzo IP virtuale del controller. Il client deve convalidare il certificato del server o ignorarlo per attivare il tunnel SSL. In questo caso, si tratta di un certificato autofirmato, quindi il client lo ha ignorato. La pagina Web di accesso viene inviata tramite questo tunnel SSL. Il pacchetto 112 inizia le transazioni.

No.	Time	Source	Destination	Protocol	Length	TID	Time delta from previous	Info
97	13:15:33.845038	17.253.21.208	192.168.68.94	TCP	74		0.003616000	80 - 50755 [SYN, ACK, ECN] Seq=0 Ack=1 Win=28960 Len=0 MSS=1250 SACK_PERM=1 TSval=1450324338
98	13:15:33.845100	192.168.68.94	17.253.21.208	TCP	66		0.000002000	50755 - 80 [ACK] Seq=1 Ack=1 Win=131200 Len=0 TSval=1585208304 TSecr=1450324338
99	13:15:33.845711	192.168.68.94	17.253.21.208	HTTP	197		0.000611000	GET /hotspot-detect.html HTTP/1.0
100	13:15:33.847912	17.253.21.208	192.168.68.94	TCP	66		0.002281000	80 - 50755 [ACK] Seq=1 Ack=132 Win=30080 Len=0 TSval=1450324342 TSecr=1585208304
101	13:15:33.847915	17.253.21.208	192.168.68.94	TCP	565		0.000003000	HTTP/1.1 200 OK (text/html)
102	13:15:33.847916	17.253.21.208	192.168.68.94	TCP	66		0.000001000	80 - 50755 [FIN, ACK] Seq=500 Ack=132 Win=30080 Len=0 TSval=1450324342 TSecr=1585208304
103	13:15:33.847972	192.168.68.94	17.253.21.208	TCP	66		0.000056000	50755 - 80 [ACK] Seq=132 Ack=500 Win=130720 Len=0 TSval=1585208306 TSecr=1450324342
104	13:15:33.847973	192.168.68.94	17.253.21.208	TCP	66		0.000001000	50755 - 80 [ACK] Seq=132 Ack=501 Win=130720 Len=0 TSval=1585208306 TSecr=1450324342
105	13:15:33.849232	192.168.68.94	17.253.21.208	TCP	66		0.001259000	50755 - 80 [FIN, ACK] Seq=132 Ack=501 Win=131072 Len=0 TSval=1585208307 TSecr=1450324342
106	13:15:33.850572	17.253.21.208	192.168.68.94	TCP	66		0.001340000	80 - 50755 [ACK] Seq=501 Ack=133 Win=30080 Len=0 TSval=1450324345 TSecr=1585208307
107	13:15:33.914358	192.168.68.94	192.168.68.1	UDP	46		0.063786000	58461 - 192 Len=4
108	13:15:33.934929	192.168.68.94	224.0.0.251	IGMP	46		0.020571000	Leave Group 224.0.0.251
109	13:15:33.934929	192.168.68.94	224.0.0.251	IGMP	46		0.000000000	Membership Report group 224.0.0.251
110	13:15:34.004031	192.168.68.94	224.0.0.251	MDNS	491		0.149102000	Standard query 0x0000 PTR _airport._tcp.local, "QM" question PTR _raop._tcp.local
111	13:15:34.418127	192.168.68.94	192.168.68.1	UDP	46		0.334096000	58461 - 192 Len=4
112	13:15:34.886433	192.168.68.94	192.0.2.1	TCP	78		0.468306000	50756 - 443 [SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=1585209337
113	13:15:34.889448	192.0.2.1	192.168.68.94	TCP	74		0.003015000	443 - 50756 [SYN, ACK, ECN] Seq=0 Ack=1 Win=20960 Len=0 MSS=1250 SACK_PERM=1 TSval=1450325384
114	13:15:34.889525	192.168.68.94	192.0.2.1	TCP	66		0.000077000	50756 - 443 [ACK] Seq=1 Ack=1 Win=131200 Len=0 TSval=1585209337 TSecr=1450325384
115	13:15:34.890281	192.168.68.94	192.0.2.1	TLS	264		0.000756000	Client Hello
116	13:15:34.891777	192.0.2.1	192.168.68.94	TCP	66		0.001496000	443 - 50756 [ACK] Seq=1 Ack=199 Win=30080 Len=0 TSval=1450325387 TSecr=1585209337
117	13:15:34.895783	192.0.2.1	192.168.68.94	TLS	1014		0.004006000	Server Hello
118	13:15:34.895787	192.0.2.1	192.168.68.94	TCP	1014		0.000004000	443 - 50756 [ACK] Seq=949 Ack=199 Win=30080 Len=948 TSval=1450325390 TSecr=1585209337
119	13:15:34.895788	192.0.2.1	192.168.68.94	TLS	425		0.000001000	Certificate, Server Hello Done
120	13:15:34.895851	192.168.68.94	192.0.2.1	TCP	66		0.000063000	50756 - 443 [ACK] Seq=199 Ack=1897 Win=129312 Len=0 TSval=1585209343 TSecr=1450325384

È possibile configurare il nome di dominio per l'indirizzo IP virtuale del WLC. Se si configura il nome di dominio per l'indirizzo IP virtuale, questo nome di dominio viene restituito nel pacchetto HTTP OK dal controller in risposta al pacchetto HTTP GET del client. È quindi necessario

eseguire una risoluzione DNS per questo nome di dominio. Una volta ottenuto un indirizzo IP dalla risoluzione DNS, tenta di aprire una sessione TCP con tale indirizzo IP, che è un indirizzo IP configurato su un'interfaccia virtuale del controller.

Alla fine, la pagina Web viene passata attraverso il tunnel al client e l'utente restituisce il nome utente e la password tramite il tunnel SSL (Secure Sockets Layer).

L'autenticazione Web viene eseguita tramite uno dei tre metodi seguenti:

- Utilizza una pagina Web interna (impostazione predefinita).
- Utilizzare una pagina di accesso personalizzata.
- Utilizzare una pagina di accesso da un server Web esterno.



Note:

- Il pacchetto di autenticazione Web personalizzato prevede un limite massimo di 30 caratteri per i nomi dei file. Assicuratevi che i nomi di file all'interno del fascio non siano più lunghi di 30 caratteri.

- A partire dalla versione WLC 7.0, se l'autenticazione Web è abilitata sulla WLAN e si dispone anche di regole ACL della CPU, le regole di autenticazione Web basate sul client hanno sempre la precedenza, purché il client non sia autenticato nello stato WebAuth_Reqd. Quando il client passa allo stato RUN, vengono applicate le regole ACL della CPU.

- Pertanto, se gli ACL della CPU sono abilitati nel WLC, è richiesta una regola di autorizzazione per l'IP dell'interfaccia virtuale (in QUALSIASI direzione) nelle seguenti condizioni:

- Quando l'ACL della CPU non dispone di una regola allow ALL per entrambe le direzioni.
- Quando esiste una regola Allow ALL, ma esiste anche una regola DENY per la porta 443 o 80 con precedenza superiore.

- La regola di autorizzazione per l'IP virtuale deve essere impostata per il protocollo TCP e la porta 80 se secureweb è disabilitato oppure la porta 443 se secureweb è abilitato. Questa operazione è necessaria per consentire l'accesso del client all'indirizzo IP dell'interfaccia virtuale dopo l'autenticazione riuscita quando sono presenti ACL della CPU.

Risoluzione dei problemi di autenticazione Web

Dopo aver configurato l'autenticazione Web e se la funzionalità non funziona come previsto, attenersi alla seguente procedura:

1. Verificare se il client ottiene un indirizzo IP. In caso contrario, gli utenti possono deselezionare la casella di controllo DHCP Required sulla WLAN e assegnare al client wireless un indirizzo IP statico. Ciò presuppone l'associazione con il punto di accesso.
2. Il passaggio successivo del processo è la risoluzione DNS dell'URL nel browser Web.

Quando un client WLAN si connette a una WLAN configurata per l'autenticazione Web, ottiene un indirizzo IP dal server DHCP. L'utente apre un browser Web e immette l'indirizzo di un sito Web. Il client esegue quindi la risoluzione DNS per ottenere l'indirizzo IP del sito Web. Ora, quando il client tenta di raggiungere il sito Web, il WLC intercetta la sessione HTTP GET del client e reindirizza l'utente alla pagina di accesso per l'autenticazione Web.

3. Verificare pertanto che il client sia in grado di eseguire la risoluzione DNS per il corretto funzionamento del reindirizzamento. In Microsoft Windows, scegliere Start > Esegui, immettere CMD per aprire una finestra di comando ed eseguire una ricerca nslookup www.cisco.com per verificare se l'indirizzo IP viene restituito.

In Macintosh/Linux aprire una finestra del terminale ed eseguire una ricerca nslookup www.cisco.com e verificare se l'indirizzo IP viene restituito.

Se si ritiene che il client non ottenga la risoluzione DNS, è possibile:

- Immettere l'indirizzo IP dell'URL (ad esempio, <http://www.cisco.com> è <http://192.168.219.25>).
- Provare a digitare qualsiasi indirizzo IP (anche non esistente) che deve essere risolto tramite la scheda wireless.

Quando immetti questo URL, la pagina Web viene visualizzata? Se sì, è molto probabile che si tratti di un problema DNS. Può anche trattarsi di un problema relativo al certificato. Per impostazione predefinita, il controller utilizza un certificato autofirmato e la maggior parte dei browser Web ne avvisa l'utente.

4. Per l'autenticazione Web con una pagina Web personalizzata, verificare che il codice HTML della pagina sia appropriato.

È possibile scaricare uno script di autenticazione Web di esempio da [Cisco Software Downloads](#). Ad esempio, per i controller 5508, scegliere Prodotti > Wireless > Wireless LAN Controller > Controller autonomi > Cisco Wireless LAN Controller serie 5500 > Cisco Wireless LAN Controller > Software sullo chassis > Wireless Lan Controller Web Authentication Bundle e scaricare il file webauth_bundle.zip.

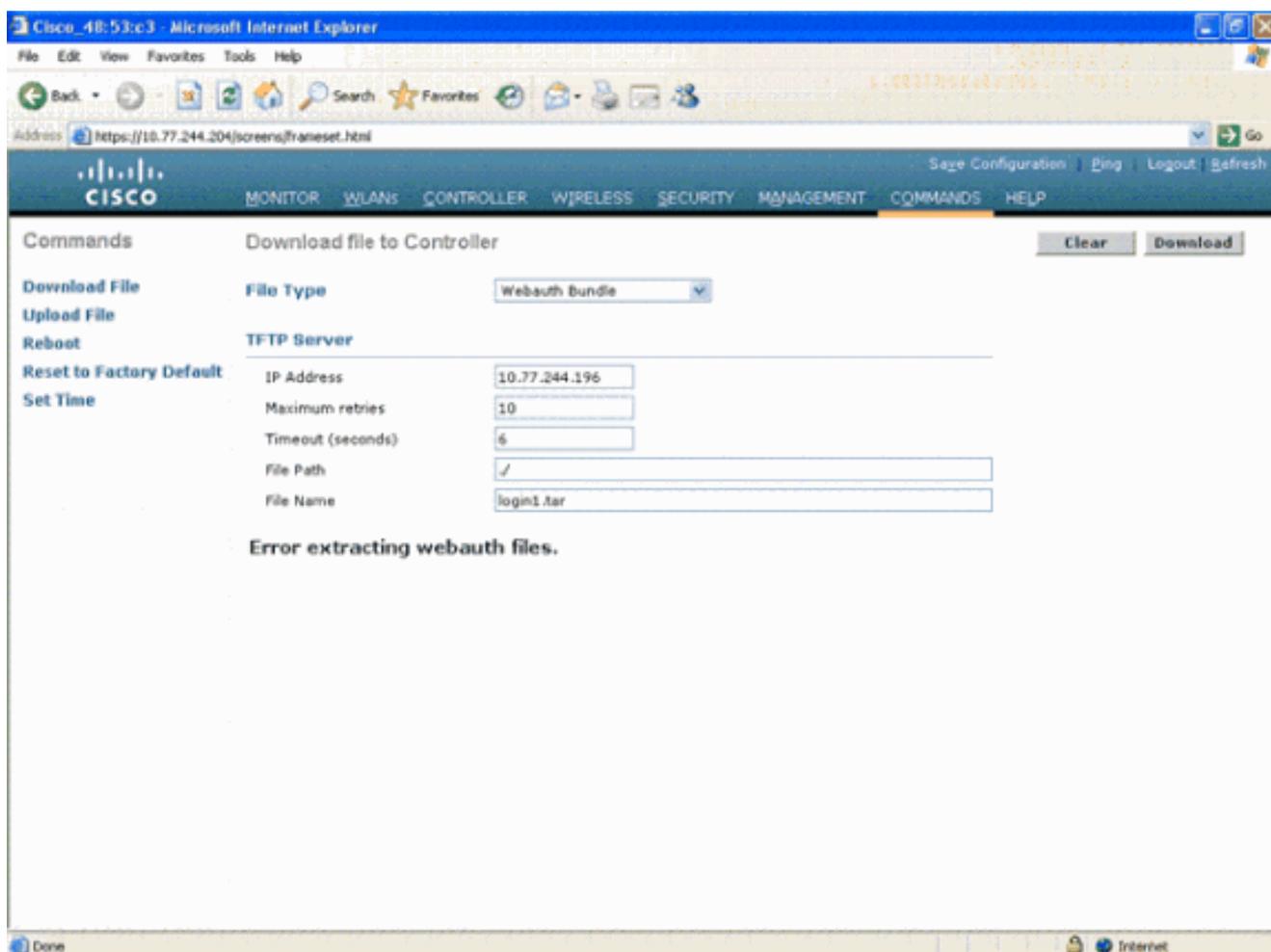
Questi parametri vengono aggiunti all'URL quando il browser Internet dell'utente viene reindirizzato alla pagina di accesso personalizzata:

- ap_mac - Indirizzo MAC del punto di accesso a cui è associato l'utente wireless.
- switch_url - URL del controller a cui devono essere inviate le credenziali utente.
- reindirizzamento: l'URL al quale l'utente viene reindirizzato dopo il completamento dell'autenticazione.
- statusCode: il codice di stato restituito dal server di autenticazione Web del controller.
- wlan: l'SSID WLAN a cui è associato l'utente wireless.

Di seguito sono riportati i codici di stato disponibili:

- Codice stato 1 - Accesso già effettuato. Non sono necessarie ulteriori azioni da parte vostra.

- Codice stato 2 - Non si è configurati per l'autenticazione sul portale Web. Non sono necessarie ulteriori azioni da parte vostra.
 - Codice di stato 3 - Impossibile utilizzare il nome utente specificato in questo momento. È possibile che il nome utente sia già connesso al sistema?
 - Codice stato 4 - Sei stato escluso.
 - Codice di stato 5 - La combinazione di nome utente e password immessa non è valida. Riprova.
5. Tutti i file e le immagini che devono apparire sulla pagina Web personalizzata devono essere inclusi in un file .tar prima di essere caricati sul WLC. Assicurarsi che uno dei file inclusi nel bundle .tar sia login.html. Se non si include il file login.html, viene visualizzato questo messaggio di errore:



Per ulteriori informazioni su come creare una finestra di autenticazione Web personalizzata, fare riferimento alla sezione [Linee guida per l'autenticazione Web personalizzata](#) di [Esempio di configurazione dell'autenticazione Web del controller LAN wireless](#).

 Nota: i file di grandi dimensioni e i file con nomi lunghi possono generare un errore di estrazione. È consigliabile che le immagini siano in formato jpg.

6. Verificare che l'opzione Scripting non sia bloccata nel browser client in quanto la pagina Web personalizzata nel WLC è fondamentalmente uno script HTML.

7. Se è stato configurato un nome host per l'interfaccia virtuale del WLC, verificare che la risoluzione DNS sia disponibile per il nome host dell'interfaccia virtuale.



Nota: passare al menu Controller > Interfacce dalla GUI del WLC per assegnare un nome host DNS all'interfaccia virtuale.

8. A volte il firewall installato nel computer client blocca la pagina di accesso per l'autenticazione Web. Disabilitare il firewall prima di tentare di accedere alla pagina di accesso. Una volta completata l'autenticazione Web, il firewall può essere riattivato.
9. Il firewall topologia/soluzione può essere posizionato tra il client e il server di autenticazione Web, che dipende dalla rete. Come per ogni progettazione/soluzione di rete implementata, l'utente finale deve assicurarsi che queste porte siano consentite sul firewall di rete.

Protocollo	Port
Traffico HTTP/HTTPS	porta TCP 80/443
Dati CAPWAP/Controllo traffico	porta UDP 5247/5246
Traffico di controllo/dati LWAPP (prima di rel 5.0)	porta UDP 1222/1223
Pacchetti EOIP	Protocollo IP 97
Mobilità	Porta UDP 16666 (non protetta) Porta UDP 16667 (tunnel IPSEC protetto)

10. per eseguire l'autenticazione Web, il client deve prima associarsi alla WLAN appropriata sul WLC. Per verificare se il client è associato al WLC, selezionare il menu Monitor > Clienti sull'interfaccia utente del WLC. Verificare che il client disponga di un indirizzo IP valido.
11. Disabilitare le impostazioni proxy nel browser client fino al completamento dell'autenticazione Web.
12. Il metodo di autenticazione Web predefinito è Password Authentication Protocol (PAP). Verificare che l'autenticazione PAP sia consentita sul server RADIUS affinché questa operazione funzioni. Per controllare lo stato dell'autenticazione del client, controllare i debug e i messaggi di registro provenienti dal server RADIUS. È possibile usare il comando debug aaa all sul WLC per visualizzare i debug del server RADIUS.
13. Aggiornare il driver hardware sul computer all'ultimo codice disponibile sul sito Web del produttore.
14. Verificare le impostazioni nel supplicant (programma sul laptop).
15. Quando si utilizza il supplicant Zero Config di Windows incorporato in Windows:
- Verificare che siano installate le patch più recenti.
 - Eseguire i debug sul supplicant.
16. Sul client, attivare i registri EAPOL (WPA+WPA2) e RASTLS da una finestra di comando. Scegliere Start > Esegui > CMD:

```
netsh ras set tracing eapol enable
netsh ras set tracing rastls enable
```

Per disabilitare i registri, eseguire lo stesso comando ma sostituire enable con disable. Per XP, tutti i registri si trovano in C:\Windows\tracing.

17. Se non si dispone ancora di una pagina Web di accesso, raccogliere e analizzare questo output da un singolo client:

```
debug client <mac_address in format xx:xx:xx:xx:xx:xx>
debug dhcp message enable
debug aaa all enable
debug dot1x aaa enable
debug mobility handoff enable
```

18. Se il problema non viene risolto dopo aver completato questi passaggi, raccogliere i debug e usare [Support Case Manager](#) per aprire una richiesta di servizio.

```
debug pm ssh-appgw enable
debug pm ssh-tcp enable
debug pm rules enable
debug emweb server enable
debug pm ssh-engine enable packet <client ip>
```

Informazioni correlate

- [Esempio di configurazione dell'autenticazione Web del controller LAN wireless](#)
- [Esempio di configurazione dell'autenticazione Web esterna con i controller LAN wireless](#)
- [Supporto tecnico Cisco e download](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).