Funzioni della release 1.0.1 per i modelli WAP125 e WAP581

Obiettivo

Lo scopo di questo articolo è evidenziare e fornire una panoramica delle funzioni più recenti di questo aggiornamento del firmware per i punti di accesso wireless (WAP).

Dispositivi interessati

- WAP125
- WAP581

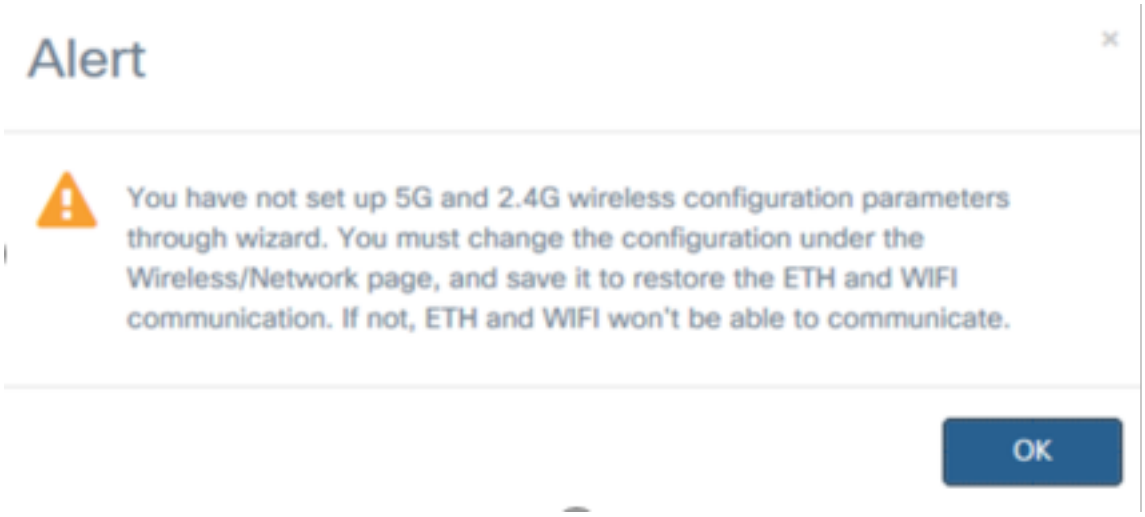
Versione del software

- 1.0.1

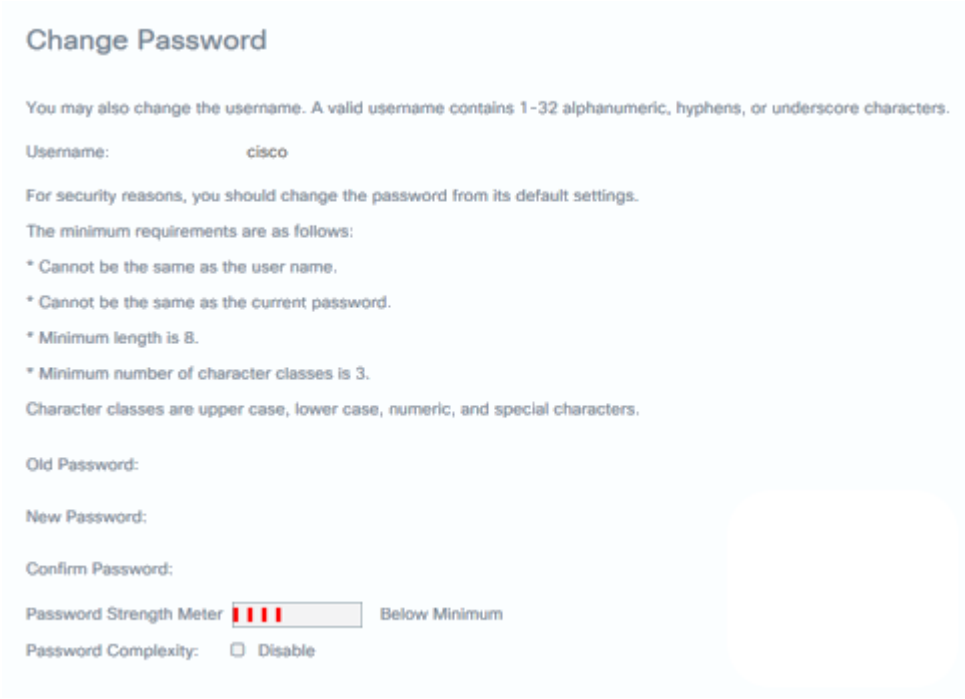
Installazione guidata

Nelle versioni precedenti di WAP125 e WAP581, se si annulla l'Installazione guidata, si verrà disconnessi da WAP.

Il firmware 1.0.1 consente di annullare l'installazione guidata. Verrà inviato un avviso.



Dopo aver confermato l'avviso, è possibile impostare la password locale per il WAP.



Èpossibile configurare manualmente tutte le impostazioni in un secondo momento.

Installazione guidata Mobile Optimized

I dispositivi WAP125 e WAP581 ora includono pagine di gestione, pagine Captive Portal e procedure guidate di installazione ottimizzate per i dispositivi mobili.

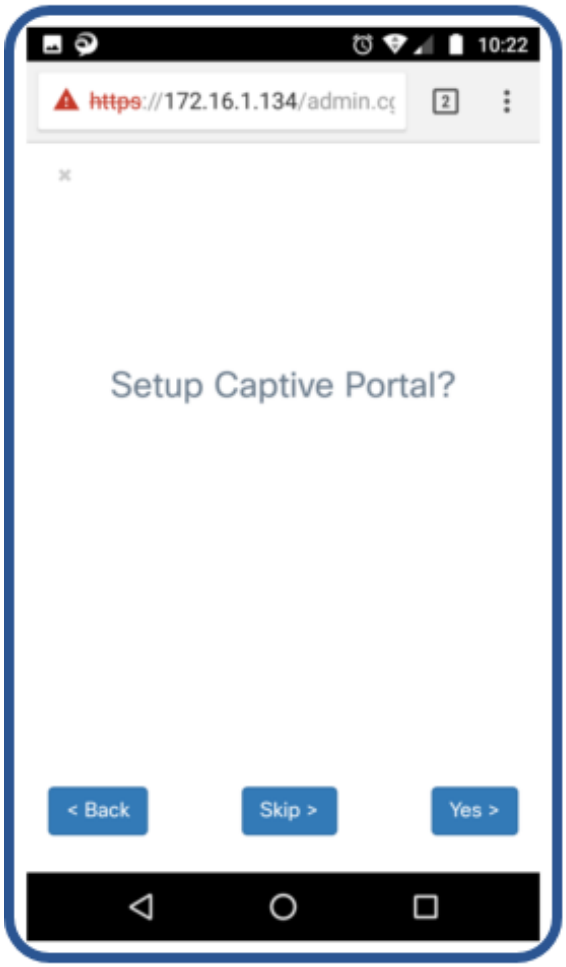
Èpossibile configurare un WAP eseguendo l'Installazione guidata tramite un dispositivo mobile utilizzando la nuova pagina di configurazione ottimizzata per dispositivi mobili.

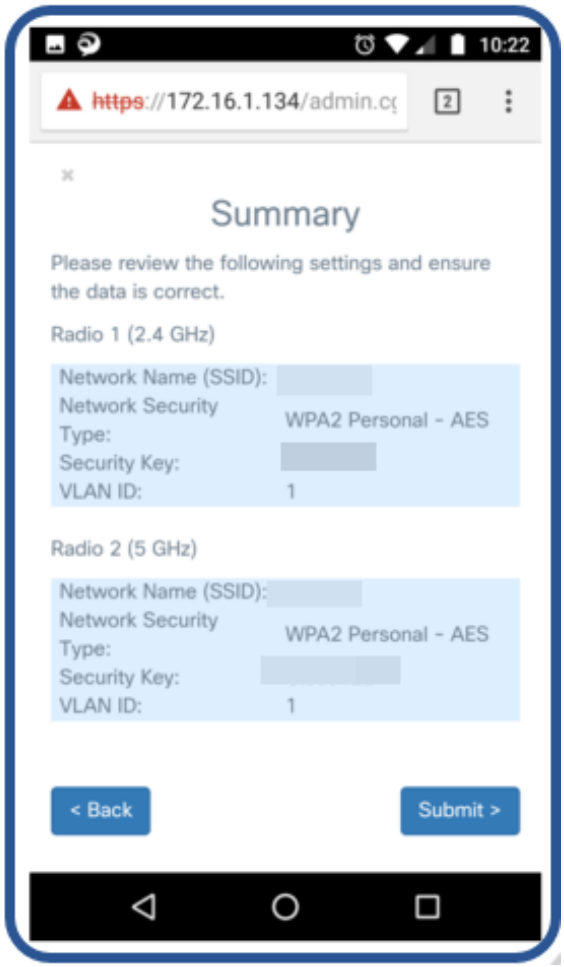
Collegarsi al SSID ciscoSB-Setup e selezionare l'indirizzo IP del WAP o l'indirizzo IP predefinito 192.168.1.245 per configurare il dispositivo.

L'Impostazione guidata è la stessa sulla pagina ottimizzata per dispositivi mobili e sulla pagina standard.


10:21
https://172.16.1.134/admin.cg
Configure Your Wireless Network
Radio 1 (2.4 GHz)
Radio 2 (5 GHz)
Enter a name for your wireless network:
Network Security Type: WPA2 Personal - AES
Enter a security key with 8-63 characters.
Enter a VLAN ID for your wireless network:
1
Apply same configuration to Radio 2 (5 GHz)
< Back
Next >


10:22
https://172.16.1.134/admin.cg
Configure Your Wireless Network
Radio 1 (2.4 GHz)
Radio 2 (5 GHz)
Enter a name for your wireless network:
Network Security Type: WPA2 Personal - AES
Enter a security key with 8-63 characters.
Enter a VLAN ID for your wireless network:
1
Apply same configuration to Radio 1 (2.4 GHz)
< Back
Next >


10:22
https://172.16.1.134/admin.cg
Setup Captive Portal?
< Back
Skip >
Yes >


10:22
https://172.16.1.134/admin.cg
Summary
Please review the following settings and ensure the data is correct.
Radio 1 (2.4 GHz)
Network Name (SSID):
Network Security Type:
WPA2 Personal - AES
Security Key:
VLAN ID:
1
Radio 2 (5 GHz)
Network Name (SSID):
Network Security Type:
WPA2 Personal - AES
Security Key:
VLAN ID:
1
< Back
Submit >

Autenticazione Guest Di Terze Parti

L'autenticazione guest di terze parti consente di configurare una rete guest utilizzando l'autenticazione di Facebook o Google, un'autenticazione sicura convalidata da terze parti. WAP125 consente una sola istanza di accesso guest, mentre WAP581 consente più istanze.

Requisiti:

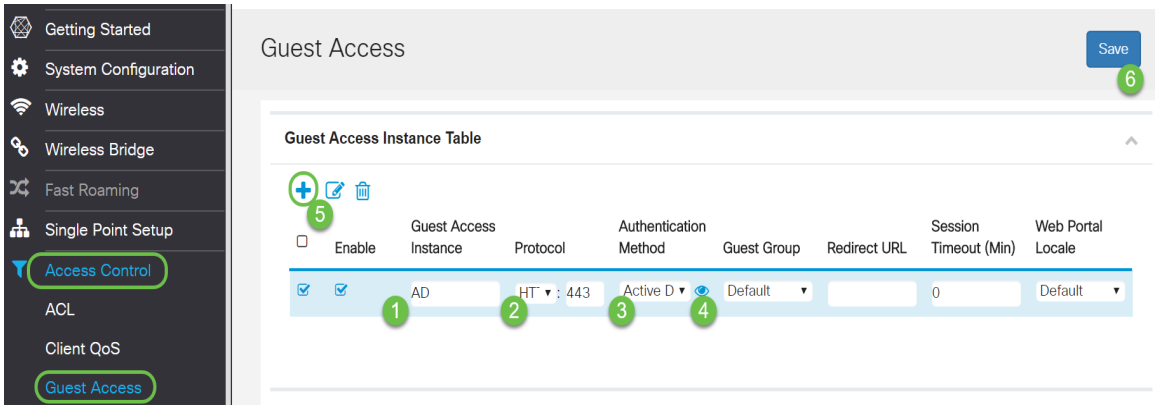
- Connettività Internet a Facebook o Google
- Gli utenti devono avere o creare un account Facebook o Google e l'accesso wireless al proprio profilo pubblico
- Facebook o Google devono essere accessibili prima del completamento dell'autenticazione in modo che un utente finale possa accedere per convalidare le proprie credenziali.

Un'azienda può inoltre scegliere di rendere disponibili altri siti, ad esempio il proprio sito Web aziendale, prima dell'autenticazione.

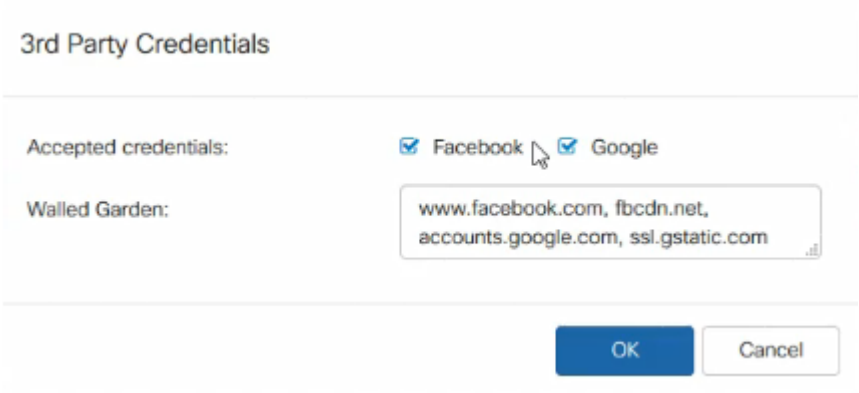
Fare clic su **Controllo accesso > Accesso guest** e fare clic sul segno *più*.

Breve spiegazione di ciascuno dei numeri seguenti:

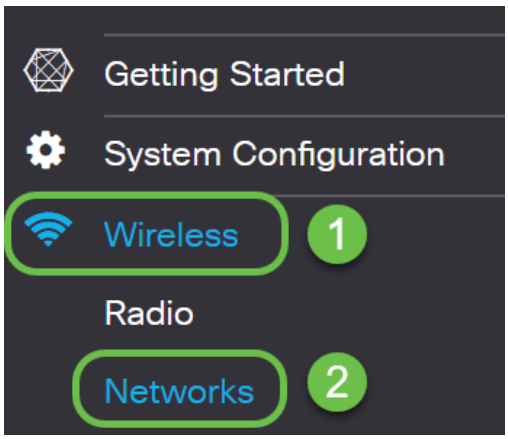
1. Aggiungere il nome per Active Directory
2. Ènecessario configurare la pagina Portale vincolato in modo che utilizzi **HTTPS** e non HTTP. Se si sceglie HTTP, è possibile esporre inavvertitamente nomi utente e password trasmettendoli via etere in testo non crittografato. Pagina Portale captive HTTPS protetto consigliata.
3. Scegliere **Credenziali di terze parti**.
4. Fare clic sull'immagine dell'**occhio** per selezionare le credenziali accettate e i siti Web corretti.
5. Fare clic qui se si sceglie di aggiungere un'altra istanza di Accesso guest.
6. Assicurarsi di **salvare**.



In questo esempio vengono mostrati Facebook e Google selezionati. I siti web sono elencati per il Giardino murato.



Sarà quindi necessario passare a **Wireless > Reti** nel riquadro di spostamento per aggiungere o modificare l'istanza di accesso guest nel nome di Active Directory.

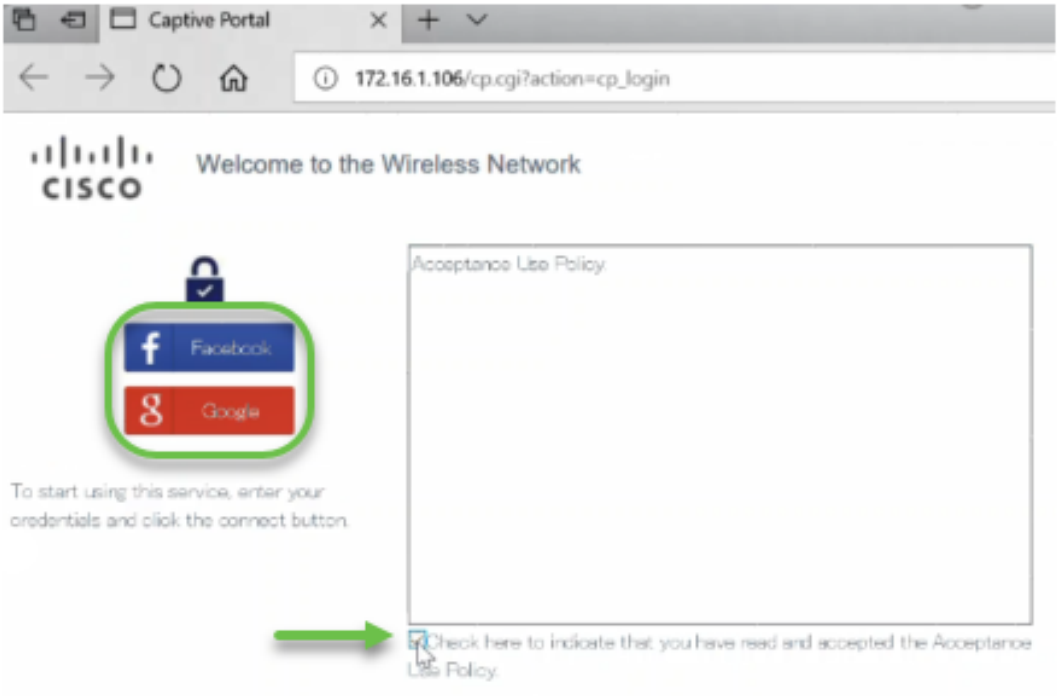


Nota: Il protocollo WAP125 consente di utilizzare un'istanza di accesso guest, pertanto è necessario decidere se si desidera configurare l'autenticazione di terze parti o l'autenticazione di Active Directory. Il protocollo WAP581 consente l'utilizzo di più metodi di autenticazione.

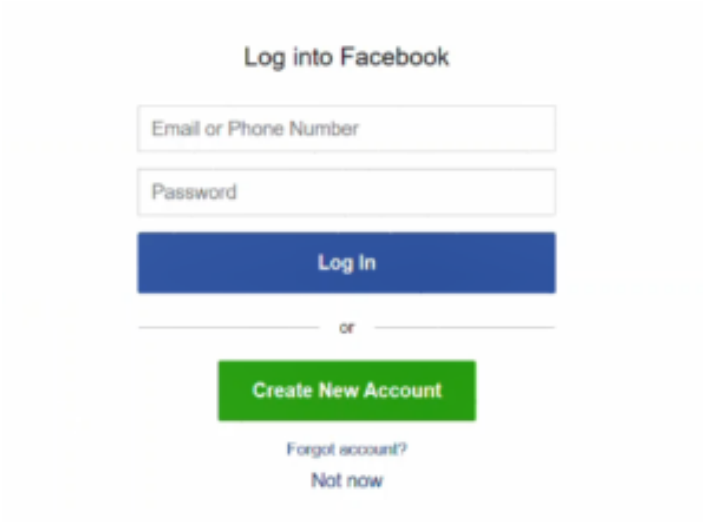
Autenticazione client di terze parti

Quando un client fa clic per accedere a una connessione wireless, viene aperto il Captive Portal. In questo esempio, Facebook e Google sono opzioni. Il cliente deve selezionare la casella per indicare di aver letto e accettato la *politica sull'utilizzo* dell'*accettazione*, quindi l'**opzione di accesso Facebook** o **Google**.

Nota: La prima volta che si accede al client, verrà chiesto se si desidera utilizzare Captive Portal. Selezionare *Sì.*



Il client può quindi immettere le credenziali. Nell'esempio è stato usato Facebook.



Il client è ora in grado di utilizzare Internet.

Autenticazione Guest Active Directory

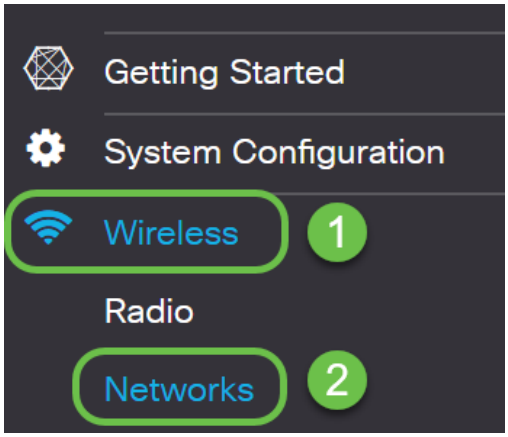
Per supportare l'autenticazione di Active Directory, il punto di accesso Windows dovrà comunicare con un controller di dominio di Windows per fornire l'autenticazione. In qualità di amministratore, è possibile configurare fino a tre controller di dominio Windows per la comunicazione su WAP581.

Fare clic su **Controllo accesso > Accesso guest** e fare clic sul segno **più**.

Breve spiegazione di ciascuno dei numeri seguenti:

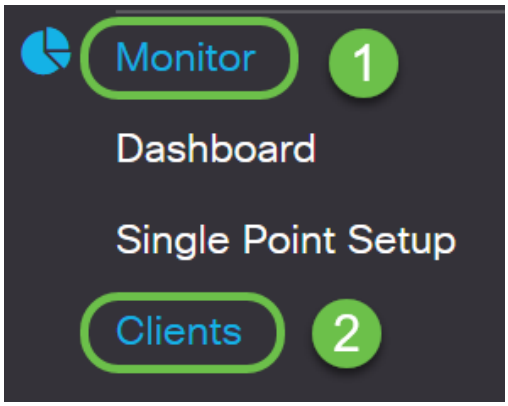
1. Aggiungere il nome per Active Directory
2. Ènecessario configurare la pagina Portale vincolato in modo che utilizzi **HTTPS** e non HTTP. Se si sceglie HTTP, è possibile esporre inavvertitamente nomi utente e password trasmettendoli via etere in testo non crittografato. Pagina Portale captive HTTPS protetto consigliata.
3. Scegli **servizio Active Directory**
4. Fare clic sull'immagine dell'**occhio** per aggiungere l'indirizzo IP. È possibile eseguire un test per verificare la connettività.
5. Fare clic qui se si sceglie di aggiungere un'altra istanza di Accesso guest.
6. Assicurarsi di salvare.

Sarà quindi necessario passare a **Wireless > Reti** nel riquadro di spostamento per aggiungere o modificare l'istanza di accesso guest nel nome di Active Directory.



Per visualizzare i client sulla rete, fare clic su **Monitor > Client** nel riquadro di navigazione.

1. *Il monitoraggio* mostra il numero di client connessi
2. *Client* mostra i dettagli del client. È possibile esportarle se si desidera tenere traccia delle persone che hanno effettuato la connessione.

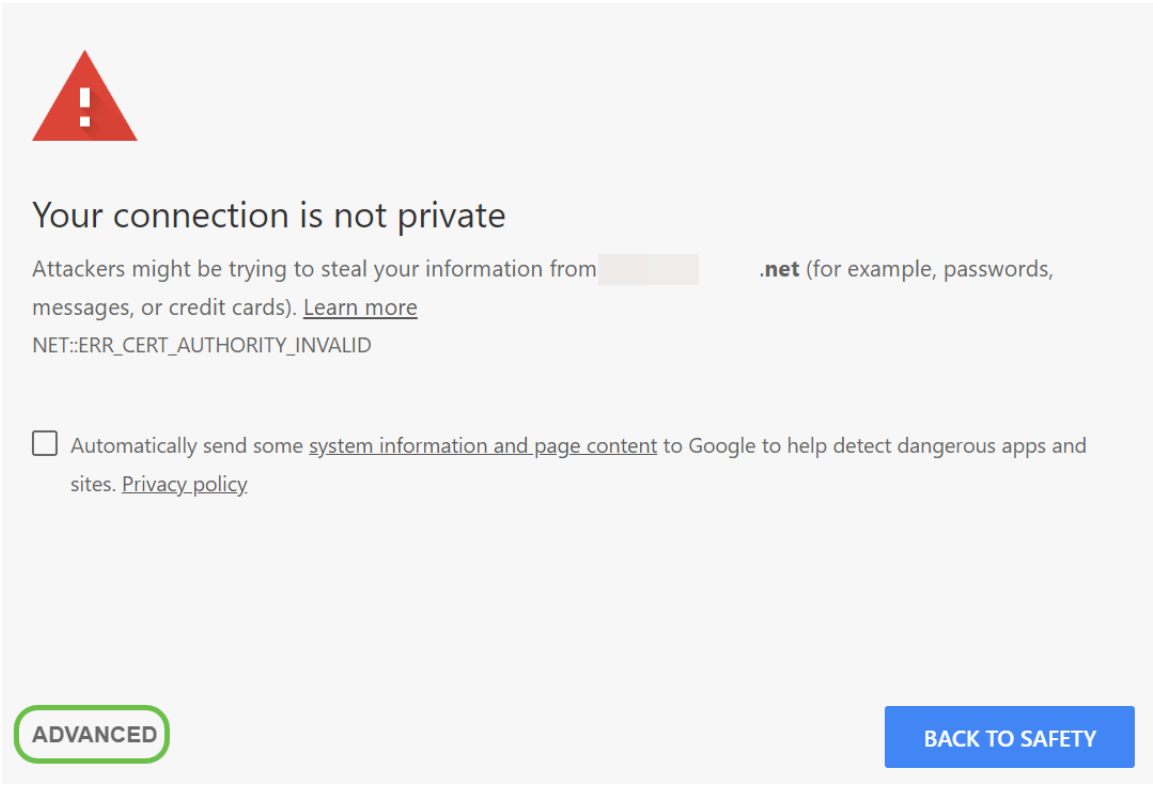


Per ulteriori informazioni su come monitorare gli ospiti, fare clic qui.

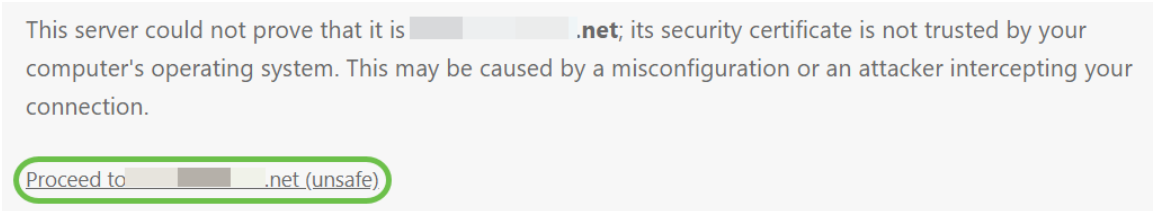
Autenticazione client Active Directory

Quando un client si trova in Active Directory, può accedere al WAP per accedere a Internet. Quando scelgono il punto di accesso wireless, potrebbero ricevere un messaggio di avviso simile a questo, a seconda del browser Web utilizzato. L'avviso viene visualizzato se non

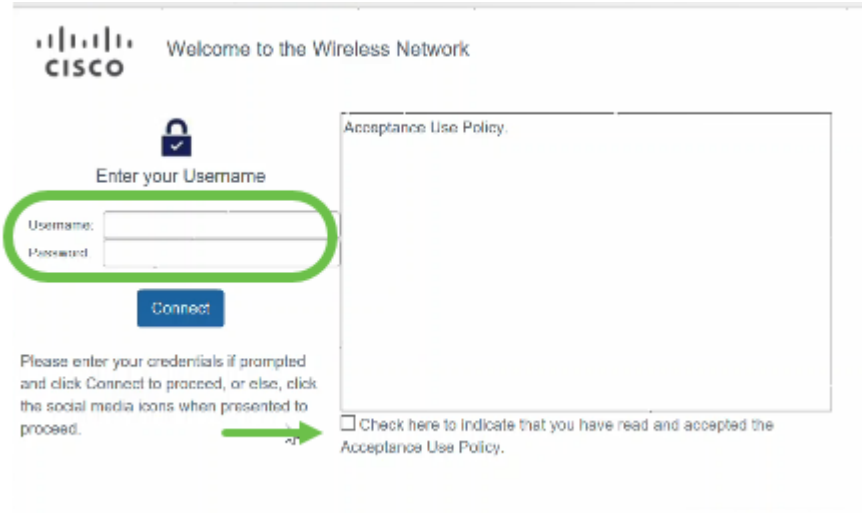
esiste un certificato assegnato alla pagina da un'Autorità di certificazione attendibile. Il client deve fare clic su **ADVANCED**.



Il client potrebbe ricevere un messaggio di avviso simile al seguente:



Èstata avviata una pagina del portale. In questa pagina devono immettere le credenziali e selezionare la casella per indicare che hanno letto e accettato la *politica sull'utilizzo* dell' *accettazione*.



Riceveranno un messaggio di benvenuto e potranno utilizzare Internet in modo sicuro.

Ora conoscete alcune delle funzioni più recenti fornite con gli ultimi aggiornamenti di WAP125 e WAP581.

Per ulteriori informazioni su queste e altre nuove funzioni, fare clic sui collegamenti agli articoli correlati riportati di seguito.

Utilizzo dell'Impostazione guidata su WAP125 o WAP581

Utilizzo della Configurazione guidata su un dispositivo mobile per WAP125 o WAP581

Procedura: Integrazione con Cisco Umbrella

Procedura: CISCO CloudShark Integration

Procedura: Configurazione delle impostazioni di autenticazione di terze parti su WAP125 o WAP581

Procedura: Autenticazione Guest Microsoft Active Directory

Procedura: Umbrella - Registrazione di un nuovo dispositivo se hai perso il segreto della chiave API

Per personalizzare l'aspetto del portale vincolato

Qui è disponibile un video relativo a questo articolo...

Fare clic qui per visualizzare altre Tech Talks di Cisco