

Configurare l'autenticazione guest di Active Directory su WAP571 o WAP571E

Obiettivo

L'obiettivo di questo documento è mostrare come configurare l'autenticazione guest di Active Directory su WAP571 o WAP571E.

Introduzione

Microsoft fornisce il servizio Active Directory di Windows, un servizio Active Directory interno (AD). Memorizza tutte le informazioni essenziali per la rete, inclusi utenti, dispositivi e policy. Gli amministratori utilizzano Active Directory come un'unica posizione per creare e gestire la rete. L'autenticazione guest di Active Directory consente a un client di configurare un'infrastruttura di portale vincolata utilizzando AD per l'autenticazione. Captive Portal (CP) è una funzione che consente a un amministratore di concedere l'accesso a utenti predefiniti che si connettono a un punto di accesso wireless (WAP). I client vengono indirizzati a una pagina Web per l'autenticazione e le condizioni di accesso prima di potersi connettere alla rete. La verifica CP è per guest e utenti autenticati della rete. Questa funzionalità utilizza il browser Web e lo trasforma in un dispositivo di autenticazione.

Le istanze CP sono un set definito di configurazioni utilizzate per autenticare i client sulla rete WAP. È possibile configurare le istanze in modo che rispondano agli utenti in modi diversi quando tentano di accedere ai punti di accesso virtuali (VAP) associati che simulano più punti di accesso all'interno di un dispositivo WAP fisico. Per ulteriori informazioni su VAP e sui passaggi necessari per configurarlo, fare clic [qui](#).

I portali vincolati vengono spesso utilizzati presso gli hotspot Wi-Fi per garantire che gli utenti accettino i termini e le condizioni e forniscano credenziali di sicurezza prima di ottenere l'accesso a Internet. Per alcune organizzazioni offrono all'utente la possibilità di essere contattato in futuro sul marchio. Una funzionalità di questo tipo può essere utilizzata in molti casi nel marketing. Per supportare l'autenticazione di Active Directory, il punto di accesso Windows dovrà comunicare con uno o tre controller di dominio Windows (noti anche come server) per consentire l'autenticazione. Può supportare più domini per l'autenticazione scegliendo controller di dominio da domini AD diversi.

Dispositivi interessati

WAP571

WAP571E

Versione del software

1.1.0.3

Configura autenticazione Guest di Active Directory

Passaggio 1. Accedere all'utility di configurazione Web di WAP immettendo il nome utente e la password. Il nome utente e la password predefiniti sono cisco/cisco. Se il nome utente o la password sono stati modificati, immettere le nuove credenziali. Fare clic su **Login**.

Nota: In questo articolo, il protocollo WAP571E viene utilizzato per dimostrare la configurazione dell'autenticazione guest di Active Directory. Le opzioni del menu possono variare leggermente a seconda del modello del dispositivo.



Wireless Access Point

Username

1

Password

2

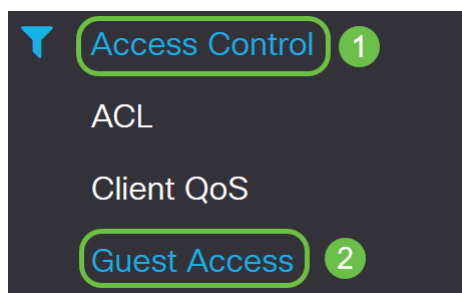
English



Login

3

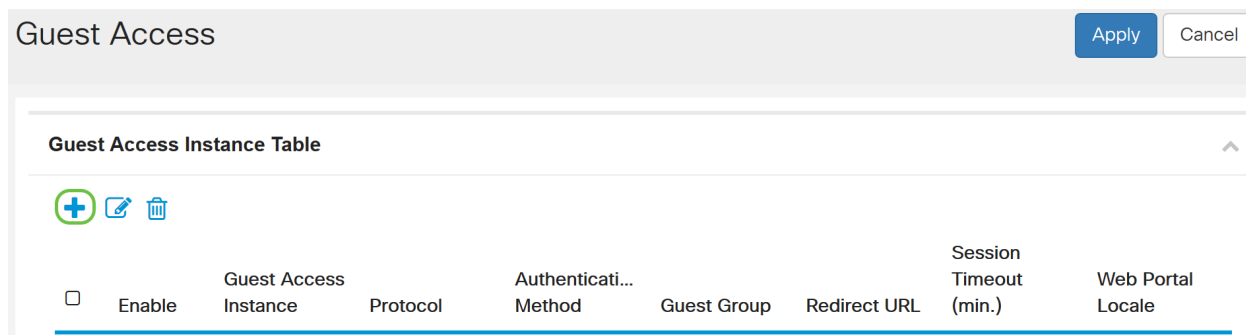
Passaggio 2. Scegliere **Controllo accesso > Accesso guest**.



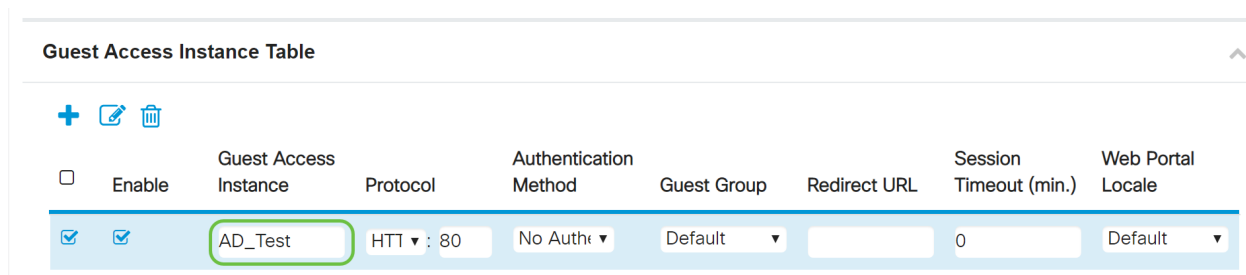
Passaggio 3. Nella *tabella Istanza di accesso guest*, è possibile selezionare l'**icona più** per aggiungere una nuova *istanza di accesso guest* oppure l'**icona a forma di matita e carta** per modificarne una esistente. La funzionalità di accesso guest del punto di accesso WAP571 o WAP571E fornisce connettività wireless ai client wireless temporanei entro la portata del dispositivo. Il punto di accesso trasmetterà l'SSID (Service Set Identifier) specifico della rete guest. Gli ospiti vengono quindi reindirizzati a un PC dove è necessario immettere le credenziali. In questo modo la rete principale è al sicuro e gli utenti possono accedere a Internet.

Le impostazioni di CP vengono configurate nella tabella delle istanze di accesso guest dell'utility basata sul Web di WAP. La funzione Guest Access è particolarmente utile nelle hall di hotel e uffici, nei ristoranti e nei centri commerciali.

In questo esempio, viene aggiunta una nuova *istanza di Guest Access* facendo clic sull'**icona più**.



Passaggio 4. Assegnare un nome all'*istanza di Accesso guest*. In questo esempio, il nome è **AD_Test**.



Passaggio 5. Scegliere il *protocollo* per l'istanza CP da utilizzare durante il processo di verifica dal menu a discesa.

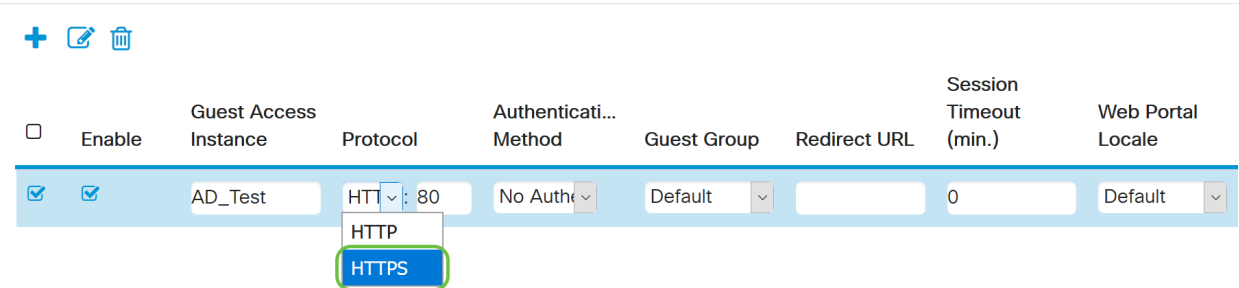
HTTP - Non utilizza la crittografia durante la verifica.

HTTPS - Utilizza SSL (Secure Sockets Layer), che richiede un certificato per fornire la

crittografia. Il certificato viene presentato all'utente al momento della connessione.

Nota: È molto importante che un client configuri la pagina del portale vincolato in modo che utilizzi HTTPS e non HTTP, in quanto il primo è più sicuro. Se un client sceglie HTTP, può inavvertitamente esporre nomi utente e password trasmettendoli in testo non crittografato. È consigliabile utilizzare una pagina del portale captive HTTPS.

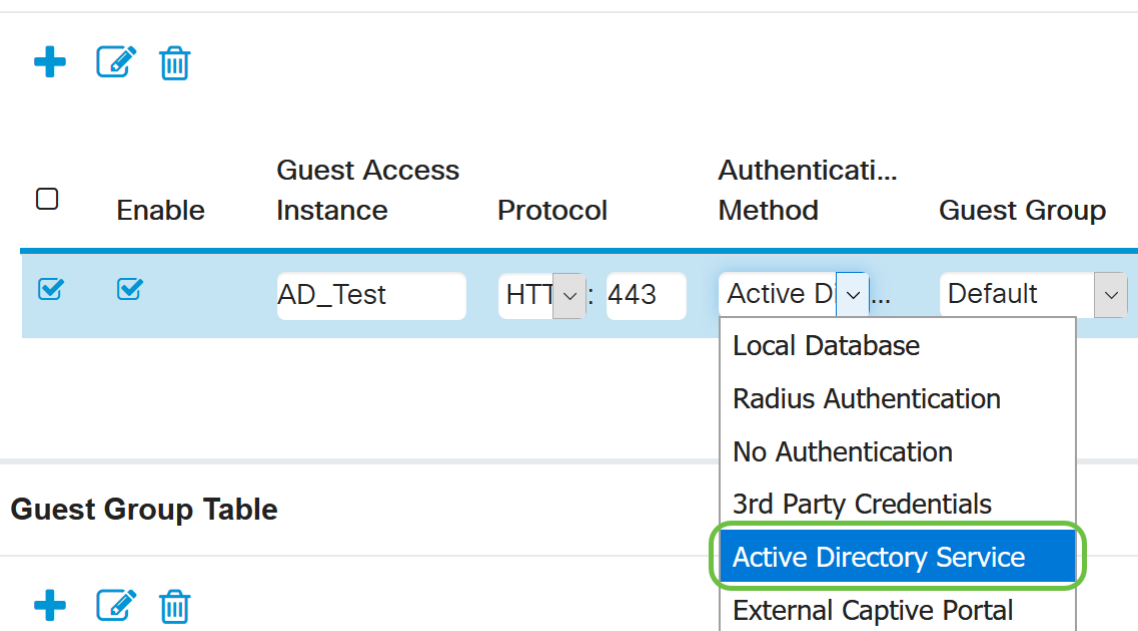
Guest Access Instance Table



<input type="checkbox"/>	Enable	Guest Access Instance	Protocol	Authenticati... Method	Guest Group	Redirect URL	Session Timeout (min.)	Web Portal Locale
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	AD_Test	HTT : 80	No Auth	Default		0	Default

Passaggio 6. Scegliere il *metodo di autenticazione* come **servizio Active Directory**.

Guest Access Instance Table



<input type="checkbox"/>	Enable	Guest Access Instance	Protocol	Authenticati... Method	Guest Group
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	AD_Test	HTT : 443	Active D ...	Default

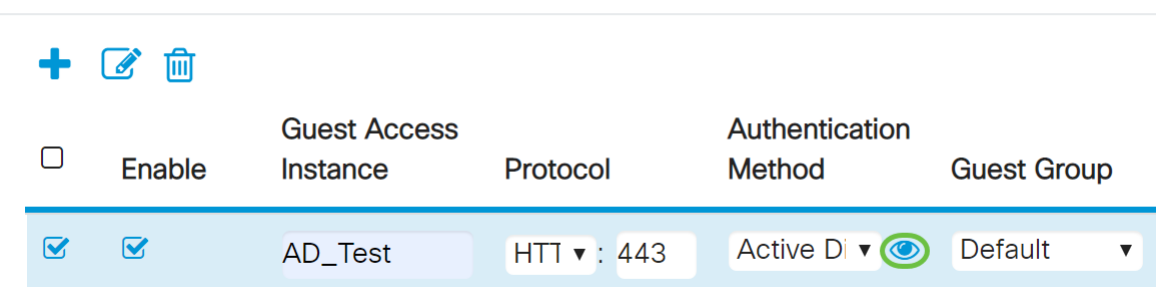
Guest Group Table




<input type="checkbox"/>	Enable	Guest Access Instance	Protocol	Authentication Method	Guest Group
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	AD_Test	HTT : 443	Active D 	Default

Passaggio 7. Configurare l'indirizzo IP del server AD facendo clic sull'icona con l'occhio blu accanto al servizio Active Directory nella colonna *Metodo di autenticazione*.

Guest Access Instance Table



<input type="checkbox"/>	Enable	Guest Access Instance	Protocol	Authentication Method	Guest Group
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	AD_Test	HTT : 443	Active D 	Default


Passaggio 8. Viene visualizzata una nuova finestra del browser. Immettere l'indirizzo IP del

server AD. Nell'esempio, l'indirizzo IP dell'host utilizzato è **172.16.1.35**. Fare clic su **OK**.

Active Directory Service

Active Directory Servers

#	Host IP	Port	Action
1	172.16.1.35	3268	 Test

 Add a Server




2 **OK** Cancel

Nota: Come passaggio facoltativo, è possibile fare clic su **Test** per verificare che l'indirizzo IP del server AD sia valido. Per ulteriori informazioni sulle procedure di verifica, fare clic [qui](#). È possibile aggiungere fino a 3 server AD.

Passaggio 9. Fare clic su **Applica** per salvare le modifiche.

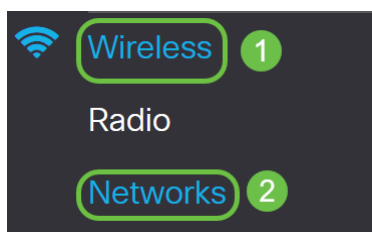
Guest Access **Apply** Cancel

Guest Access Instance Table ^

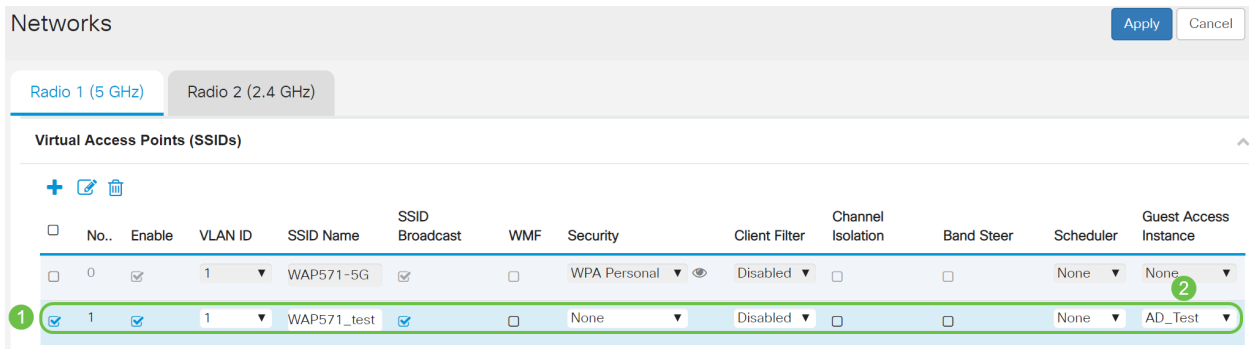
  

<input type="checkbox"/>	Enable	Guest Access Instance	Protocol	Authentication Method	Guest Group	Redirect URL	Session Timeout (min.)	Web Portal Locale
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	AD_Test	HTT : 443	Active D	Default		0	Default

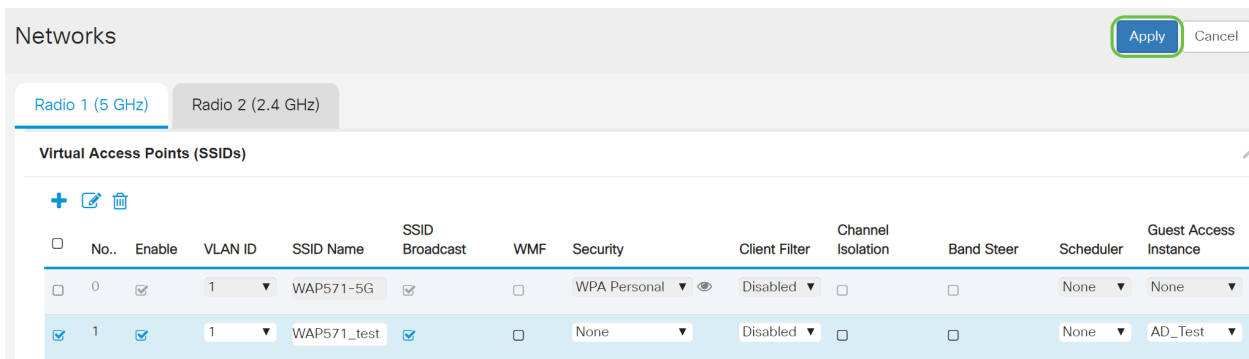
Passaggio 10. Andare al Menu e scegliere **Wireless > Reti**.



Passaggio 11. Scegliere la rete e specificare che **AD** verrà scelto come *istanza di accesso guest* per l'autenticazione. Nell'esempio, la rete è **WAP571_test**.



Passaggio 12. Fare clic su **Applica**.



Conclusioni

È stata completata la configurazione dell'autenticazione guest di Active Directory su WAP571 o WAP571E.

Per la procedura di connessione alla rete wireless guest tramite l'autenticazione AD e per verificarne la funzionalità, fare riferimento all'articolo [Configurazione dell'autenticazione guest di Active Directory su WAP125 o WAP581](#).