

Konfigurieren der Active Directory-Gastauthentifizierung auf WAP571 oder WAP571E

Ziel

In diesem Dokument wird erläutert, wie Sie die Active Directory-Gastauthentifizierung auf dem WAP571 oder WAP571E konfigurieren.

Einführung

Microsoft stellt Windows Active Directory-Dienst bereit, ein internes Active Directory (AD). Sie speichert alle wichtigen Informationen für das Netzwerk, einschließlich Benutzer, Geräte und Richtlinien. Administratoren verwenden das AD als einen zentralen Ort zum Erstellen und Verwalten des Netzwerks. Mithilfe der AD-Gastauthentifizierung kann ein Client eine Captive Portal-Infrastruktur konfigurieren, die das AD für die Authentifizierung verwendet. Captive Portal (CP) ist eine Funktion, mit der ein Administrator vordefinierten Benutzern, die mit einem Wireless Access Point (WAP) verbunden sind, Zugriff gewähren kann. Clients werden auf eine Webseite zur Authentifizierung und zu Zugriffsbedingungen geleitet, bevor sie eine Verbindung zum Netzwerk herstellen können. Die CP-Verifizierung ist sowohl für Gäste als auch für authentifizierte Benutzer des Netzwerks vorgesehen. Diese Funktion nutzt den Webbrowser und verwandelt ihn in ein Authentifizierungsgerät.

CP-Instanzen sind ein definierter Satz von Konfigurationen zur Authentifizierung von Clients im WAP-Netzwerk. Instanzen können so konfiguriert werden, dass sie auf verschiedene Arten auf Benutzer reagieren, wenn sie versuchen, auf die zugehörigen virtuellen Access Points (VAPs) zuzugreifen, die mehrere Access Points innerhalb eines physischen WAP-Geräts simulieren. Weitere Informationen zu VAP und den Konfigurationsvorgängen finden Sie [hier](#).

Captive Portale werden häufig an Wi-Fi-Hotspots eingesetzt, um sicherzustellen, dass die Benutzer die Nutzungsbedingungen akzeptieren und Sicherheitszertifikate vorlegen, bevor sie Zugang zum Internet erhalten. Für einige Unternehmen bieten sie dem Benutzer die Möglichkeit, sich zukünftig über die Marke zu informieren. Es gibt viele Anwendungsfälle für Marketing-Zwecke für eine solche Funktion. Zur Unterstützung der AD-Authentifizierung muss der WAP mit einem bis drei Windows-Domänencontrollern (auch als Server bezeichnet) kommunizieren, um die Authentifizierung bereitzustellen. Es kann mehrere Domänen für die Authentifizierung unterstützen, indem Domänen-Controller aus verschiedenen AD-Domänen ausgewählt werden.

Anwendbare Geräte

WAP571

WAP571E

Softwareversion

1,1/0,3

Active Directory-Gastauthentifizierung konfigurieren

Schritt 1: Melden Sie sich beim Webkonfigurations-Dienstprogramm des WAP an, indem Sie den Benutzernamen und das Kennwort eingeben. Der Standardbenutzername und das Standardkennwort sind *cisco/cisco*. Wenn Sie einen neuen Benutzernamen oder ein neues Kennwort konfiguriert haben, geben Sie diese stattdessen ein. Klicken Sie auf **Anmelden**.

Hinweis: In diesem Artikel wird der WAP571E verwendet, um die Konfiguration der AD-Gastauthentifizierung zu veranschaulichen. Die Menüoptionen können je nach Gerät leicht variieren.



Wireless Access Point

Username

1

Password

2

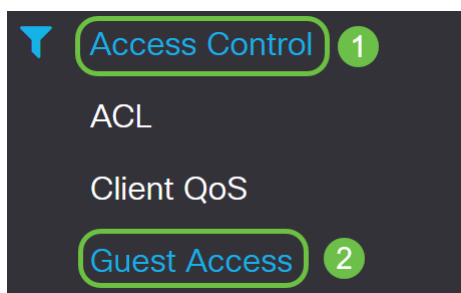
English



Login

3

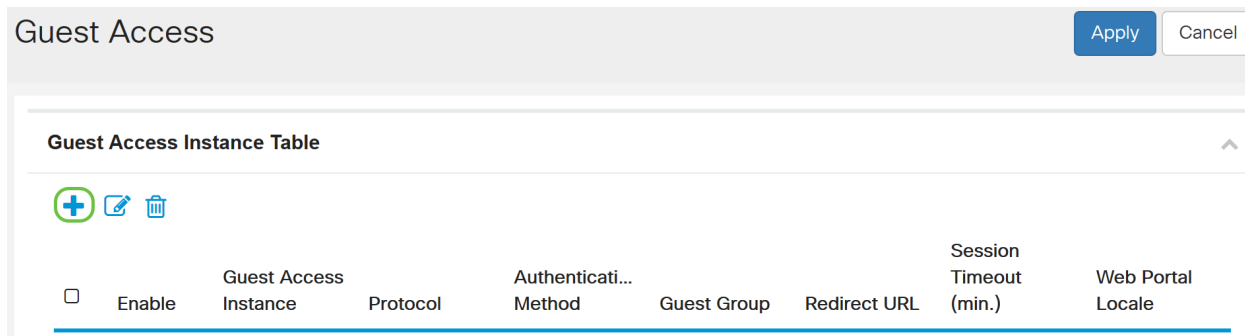
Schritt 2: Wählen Sie **Zugriffskontrolle > Gastzugriff** aus.



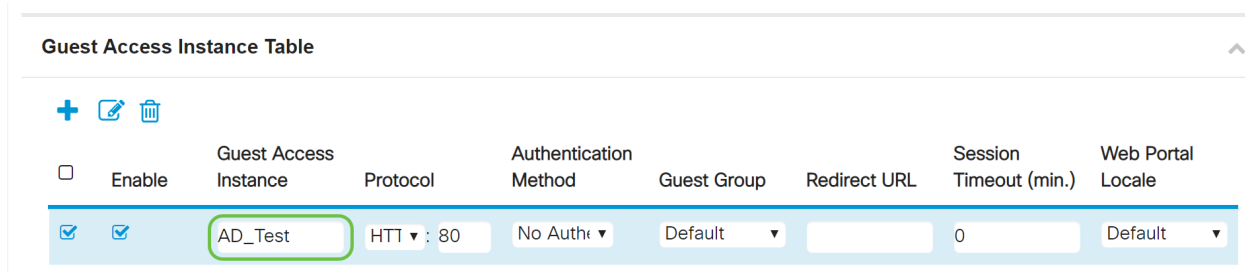
Schritt 3: In der *Gastzugriffs-Instanztabelle* können Sie entweder das **Pluszeichen** auswählen, um eine neue *Gastzugriffsinstanz* hinzuzufügen, oder das **Bleistift- und Papiersymbol**, um eine vorhandene Instanz zu bearbeiten. Die Gastzugangsfunktion des WAP571 oder WAP571E Access Points ermöglicht die drahtlose Verbindung mit temporären Wireless-Clients im Bereich des Geräts. Der Access Point sendet den für das Gastnetzwerk spezifischen Service Set Identifier (SSID). Die Gäste werden dann an einen PC weitergeleitet, auf dem sie ihre Anmeldeinformationen eingeben müssen. So bleibt das Hauptnetzwerk sicher, während die Gäste weiterhin auf das Internet zugreifen können.

Die Einstellungen des CP werden in der Guest Access Instance Table des webbasierten Dienstprogramms des WAP konfiguriert. Die Gastzugangsfunktion ist besonders in Hotel- und Bürolobbys, Restaurants und Einkaufszentren nützlich.

In diesem Beispiel wird eine neue *Gastzugriffsinstanz* durch Klicken auf das **Pluszeichen** hinzugefügt.



Schritt 4: Benennen Sie die *Gastzugriffsinstanz*. In diesem Beispiel wird sie **AD_Test** genannt.



Schritt 5: Wählen Sie im Dropdown-Menü das *Protokoll* für die CP-Instanz aus, die während des Verifizierungsprozesses verwendet werden soll.

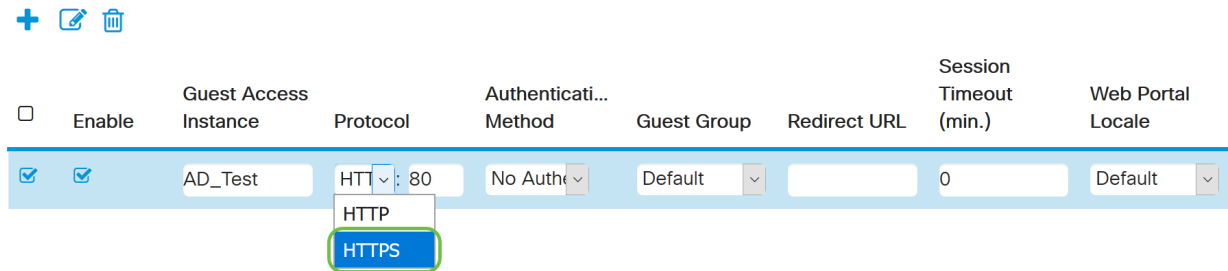
HTTP - Keine Verschlüsselung bei der Überprüfung.

HTTPS - Verwendet SSL (Secure Sockets Layer), für das ein Zertifikat zur Verschlüsselung

erforderlich ist. Das Zertifikat wird dem Benutzer zum Zeitpunkt der Verbindung angezeigt.

Hinweis: Es ist sehr wichtig, dass ein Client die Captive Portal-Seite so konfiguriert, dass HTTPS und nicht HTTP verwendet wird, da erstere sicherer ist. Wenn ein Client HTTP auswählt, kann er Benutzernamen und Kennwörter versehentlich verfügbar machen, indem er sie in unverschlüsseltem Klartext überträgt. Es empfiehlt sich, eine HTTPS-Seite für das Captive Portal zu verwenden.

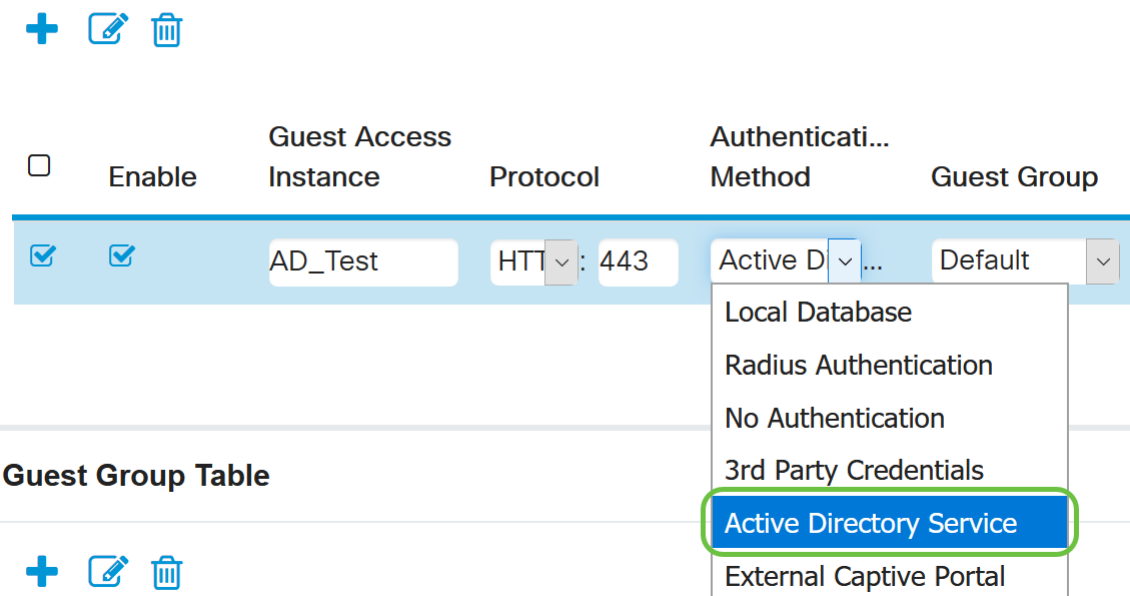
Guest Access Instance Table



<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

Schritt 6: Wählen Sie die *Authentifizierungsmethode* als **Active Directory-Dienst** aus.

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

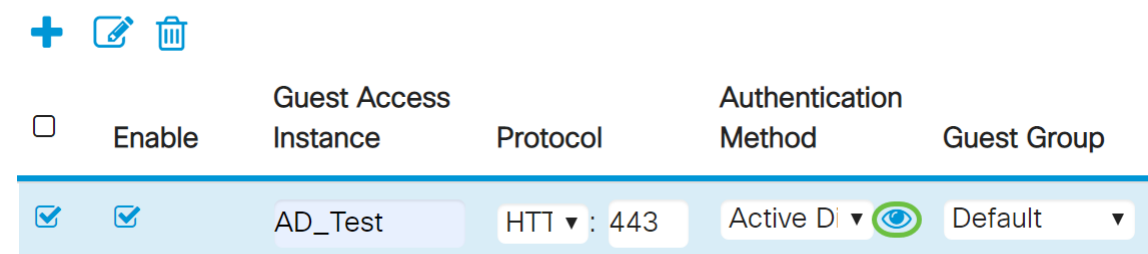
- Local Database
- Radius Authentication
- No Authentication
- 3rd Party Credentials
- Active Directory Service**
- External Captive Portal


Guest Group Table



Schritt 7: Konfigurieren Sie die IP-Adresse des AD-Servers, indem Sie in der Spalte *Authentifizierungsmethode* neben dem Active Directory-Dienst auf das **blaue Symbol** klicken.

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 Di 	Default

Schritt 8: Ein neues Browserfenster wird geöffnet. Geben Sie die IP-Adresse für den AD-Server ein. In diesem Beispiel wird die Host-IP-Adresse **172.16.1.35** verwendet. Klicken Sie auf **OK**.

Active Directory Service

Active Directory Servers

#	Host IP	Port	Action
1	172.16.1.35	3268	 Test

 Add a Server


 **OK**

Hinweis: Als optionalen Schritt können Sie auf **Test** klicken, um zu überprüfen, ob die IP-Adresse für den AD-Server gültig ist. Weitere Informationen zu den Überprüfungsschritten erhalten Sie [hier](#). Sie können bis zu 3 AD-Server hinzufügen.

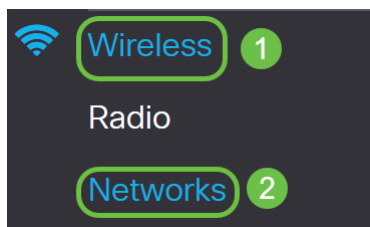
Schritt 9: Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern.

Guest Access

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

Schritt 10: Gehen Sie zum Menü, und wählen Sie **Wireless > Networks** aus.



Schritt 11: Wählen Sie das Netzwerk aus, und geben Sie an, dass **AD** als *Gastzugriffsinstanz* für die Authentifizierung ausgewählt wird. In diesem Beispiel ist das Netzwerk **WAP571_test**.

Networks Apply Cancel

Radio 1 (5 GHz) Radio 2 (2.4 GHz)

Virtual Access Points (SSIDs)

No..	Enable	VLAN ID	SSID Name	SSID Broadcast	WMF	Security	Client Filter	Channel Isolation	Band Steer	Scheduler	Guest Access Instance
0	<input checked="" type="checkbox"/>	1	WAP571-5G	<input checked="" type="checkbox"/>	<input type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	None	None
1	<input checked="" type="checkbox"/>	1	WAP571_test	<input checked="" type="checkbox"/>	<input type="checkbox"/>	None	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	None	AD_Test

Schritt 12: Klicken Sie auf **Übernehmen**.

Networks Apply Cancel

Radio 1 (5 GHz) Radio 2 (2.4 GHz)

Virtual Access Points (SSIDs)

No..	Enable	VLAN ID	SSID Name	SSID Broadcast	WMF	Security	Client Filter	Channel Isolation	Band Steer	Scheduler	Guest Access Instance
0	<input checked="" type="checkbox"/>	1	WAP571-5G	<input checked="" type="checkbox"/>	<input type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	None	None
1	<input checked="" type="checkbox"/>	1	WAP571_test	<input checked="" type="checkbox"/>	<input type="checkbox"/>	None	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	None	AD_Test

Schlussfolgerung

Sie haben jetzt die Active Directory-Gastauthentifizierung auf dem WAP571 oder WAP571E erfolgreich konfiguriert.

Schritte zum Herstellen einer Verbindung mit dem Wireless-Gastnetzwerk mithilfe der AD-Authentifizierung und zum Überprüfen seiner Funktionalität finden Sie im Artikel zum [Konfigurieren der Active Directory-Gastauthentifizierung für WAP125 oder WAP581](#).