Funktionen der Version 1.0.1 für WAP125 und WAP581

Ziel

In diesem Artikel werden die neuesten Funktionen dieses Firmware-Updates für die Wireless Access Points (WAP) vorgestellt und erläutert.

Anwendbare Geräte

- WAP125
- WAP581

Softwareversion

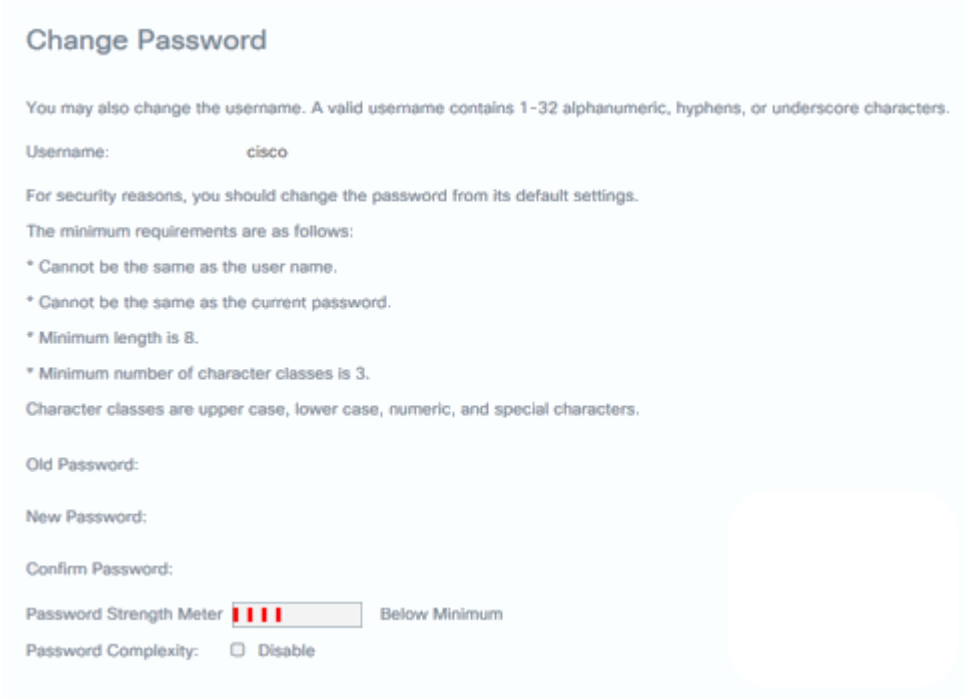
- 1,0/1

Einrichtungsassistent

Bei früheren Versionen des WAP125 und WAP581 werden Sie beim Abbrechen des Installationsassistenten vom WAP abgemeldet.

Mit der Firmware 1.0.1 können Sie den Setup-Assistenten abbrechen. Sie werden benachrichtigt.

Nachdem Sie die Warnmeldung bestätigt haben, können Sie das lokale Kennwort für den WAP festlegen.



Sie können alle Einstellungen zu einem anderen Zeitpunkt manuell konfigurieren.

Mobile Optimized Setup-Assistent

Die Geräte WAP125 und WAP581 umfassen jetzt Managementseiten, Captive Portal-Seiten und Setup-Assistenten, die für Mobilgeräte optimiert sind.

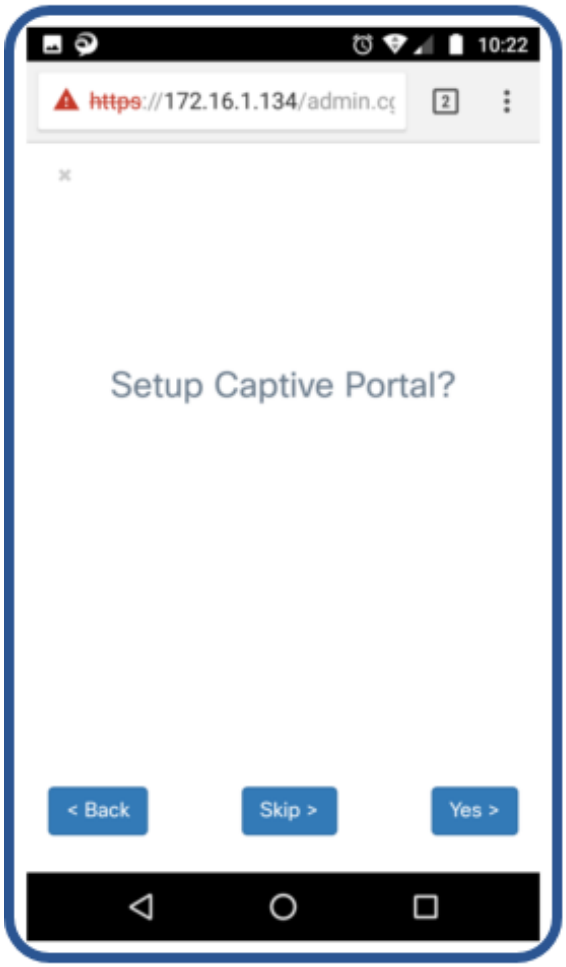
Sie können einen WAP konfigurieren, indem Sie den Setup-Assistenten über ein Mobilgerät über die neue, für Mobilgeräte optimierte Einrichtungsseite ausführen.

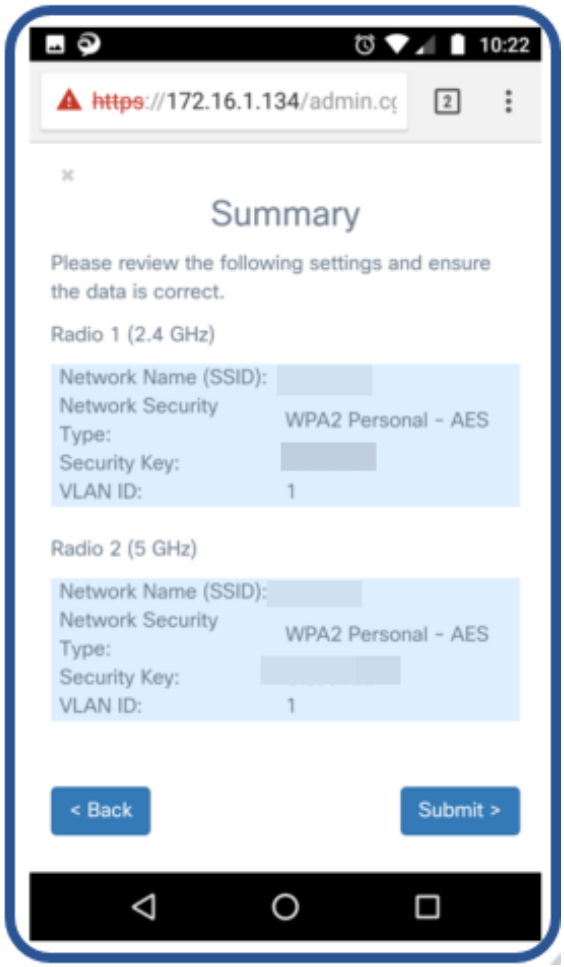
Stellen Sie eine Verbindung zum CiscoSB-Setup SSID her, und gehen Sie zur Konfiguration des Geräts entweder zur IP-Adresse des WAP oder zur Standard-IP-Adresse 192.168.1.245.

Der Setup Wizard (Installationsassistent) ist auf der für Mobilgeräte optimierten Seite identisch mit dem auf der Standardseite.


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 >

Gastauthentifizierung von Drittanbietern

Mithilfe der Gastauthentifizierung von Drittanbietern können Sie ein Gastnetzwerk mithilfe der Facebook- oder Google-Authentifizierung konfigurieren. Dies ist eine von einem Drittanbieter validierte sichere Authentifizierung. Der WAP125 ermöglicht eine Gastzugriffsinstanz, während der WAP581 mehrere Instanzen zulässt.

Anforderungen:

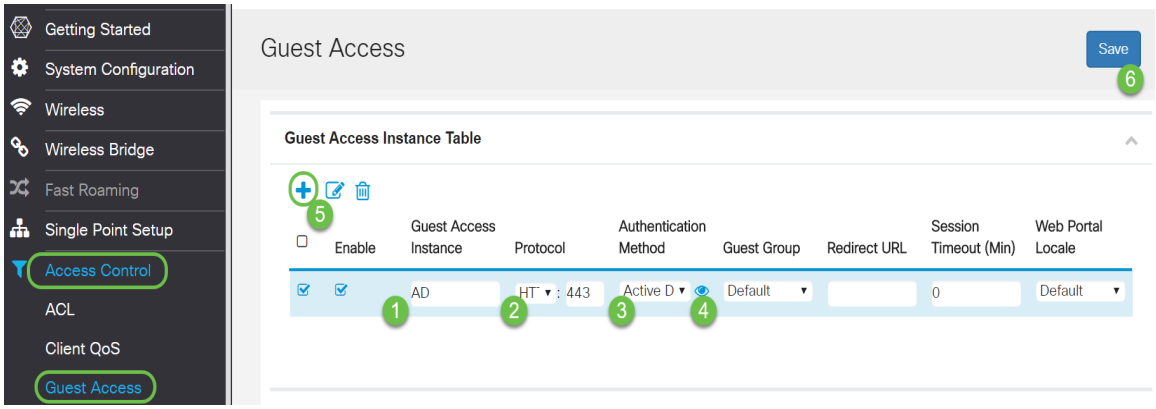
- Internetverbindung zu Facebook oder Google
- Benutzer müssen über ein Facebook- oder Google-Konto verfügen oder ein solches Konto erstellen und über Wireless-Zugriff auf ihr öffentliches Profil verfügen.
- Facebook oder Google müssen vor Abschluss der Authentifizierung verfügbar sein, damit sich ein Endbenutzer anmelden und seine Anmeldeinformationen validieren kann.

Ein Unternehmen kann auch andere Sites, wie z. B. die geschäftliche Website, vor der Authentifizierung zur Verfügung stellen.

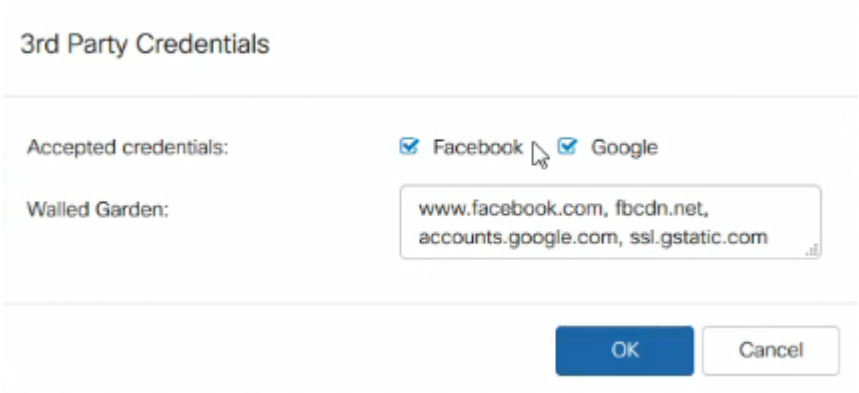
Klicken Sie auf **Zugriffskontrolle > Gastzugriff** und anschließend auf das *Pluszeichen*.

Eine kurze Erklärung für jede der unten angegebenen Zahlen:

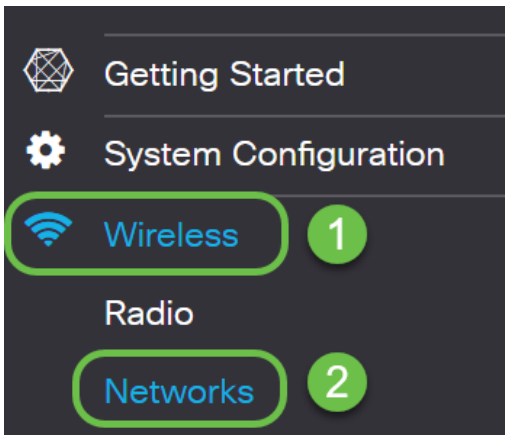
1. Fügen Sie den Namen für das Active Directory hinzu.
2. Sie sollten die Captive Portal-Seite so konfigurieren, dass sie **HTTPS** verwendet, nicht HTTP. Wenn Sie HTTP auswählen, können Sie Benutzernamen und Kennwörter versehentlich verfügbar machen, indem Sie sie in unverschlüsseltem Klartext durch die Luft übertragen. Die Seite Secure HTTPS Captive Portal wird empfohlen.
3. Wählen Sie **Anmeldeinformationen von Drittanbietern aus**.
4. Klicken Sie auf die Grafik des **Auges**, um akzeptierte Anmeldeinformationen und die richtigen Websites auszuwählen.
5. Klicken Sie hier, wenn Sie eine weitere Gastzugriffsinstanz hinzufügen möchten.
6. Stellen Sie sicher, dass Sie **speichern**.



Dieses Beispiel zeigt, wie Facebook und Google ausgewählt wurden. Die Websites sind für den Walled Garden aufgelistet.



Navigieren Sie dann im Navigationsbereich zu **Wireless > Networks**, um die Gastzugriffsinstanz zum Namen des Active Directory hinzuzufügen oder zu ändern.

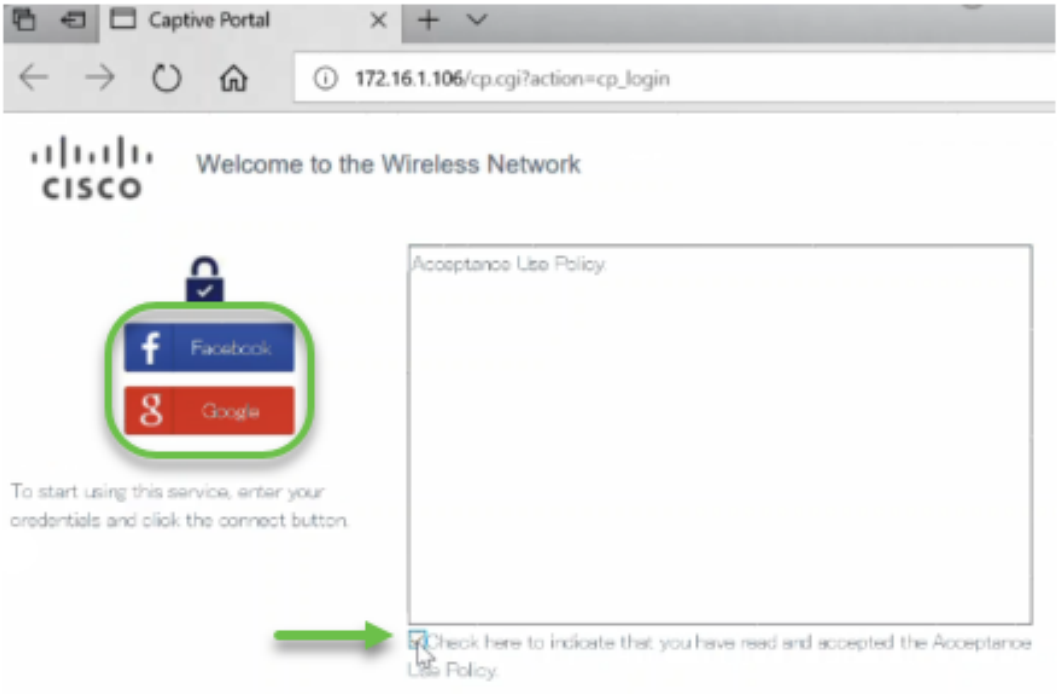


Hinweis: Der WAP125 ermöglicht Ihnen eine Gastzugriffsinstanz. Sie müssen also entscheiden, ob Sie die Konfiguration für die Authentifizierung von Drittanbietern oder die Active Directory-Authentifizierung vornehmen möchten. Der WAP581 ermöglicht mehrere Authentifizierungsverfahren.

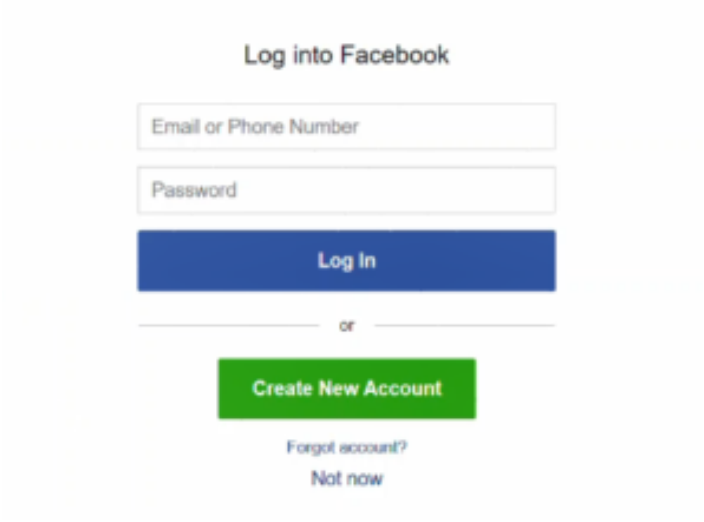
Client-Authentifizierung von Drittanbietern

Wenn ein Client auf eine Wireless-Verbindung klickt, wird das Captive Portal geöffnet. In diesem Beispiel sind Facebook und Google Optionen. Der Kunde muss das Kästchen markieren, um anzuzeigen, dass er die *Akzeptanzrichtlinie* gelesen und akzeptiert hat, und dann entweder die **Facebook-** oder **Google-**Option, sich anzumelden.

Hinweis: Bei der ersten Anmeldung beim Client wird eine Frage gestellt, ob der Kunde Captive Portal nutzen möchte. Sie müssen *Ja* auswählen.



Der Client kann dann Anmeldeinformationen eingeben. In diesem Beispiel wurde Facebook verwendet.



Der Kunde kann jetzt das Internet nutzen.

Active Directory-Gastauthentifizierung

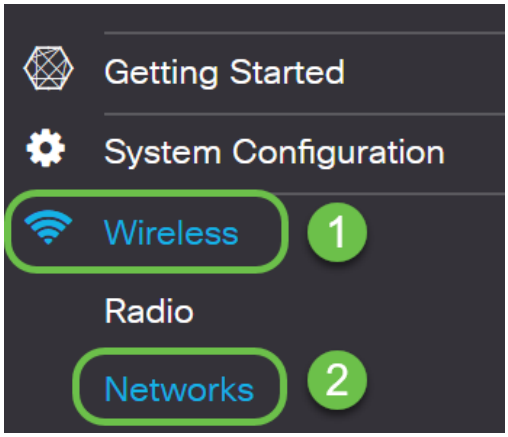
Zur Unterstützung der Active Directory-Authentifizierung muss der WAP mit einem Windows Domain Controller kommunizieren, um die Authentifizierung bereitzustellen. Als Administrator können Sie bis zu drei Windows-Domänencontroller für die Kommunikation mit dem WAP581 einrichten.

Klicken Sie auf **Zugriffskontrolle > Gastzugriff** und anschließend auf das **Pluszeichen** .

Eine kurze Erklärung für jede der unten angegebenen Zahlen:

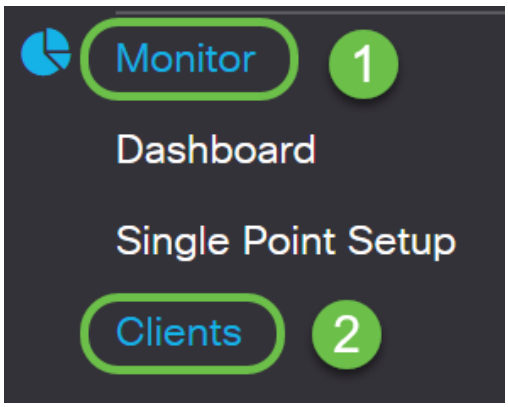
1. Fügen Sie den Namen für das Active Directory hinzu.
2. Sie sollten die Captive Portal-Seite so konfigurieren, dass sie **HTTPS** verwendet, nicht HTTP. Wenn Sie HTTP auswählen, können Sie Benutzernamen und Kennwörter versehentlich verfügbar machen, indem Sie sie in unverschlüsseltem Klartext durch die Luft übertragen. Die Seite Secure HTTPS Captive Portal wird empfohlen.
3. Wählen Sie **Active Directory-Dienst**
4. Klicken Sie auf die Grafik des **Auges**, um die IP-Adresse hinzuzufügen. Sie können von dort einen Test durchführen, um die Verbindung zu überprüfen.
5. Klicken Sie hier, wenn Sie eine weitere Gastzugriffsinstanz hinzufügen möchten.
6. Stellen Sie sicher, dass Sie speichern.

Navigieren Sie dann im Navigationsbereich zu **Wireless > Networks**, um die Gastzugriffsinstanz zum Namen des Active Directory hinzuzufügen oder zu ändern.



Um Clients im Netzwerk anzuzeigen, klicken Sie im Navigationsbereich auf **Monitor > Clients** .

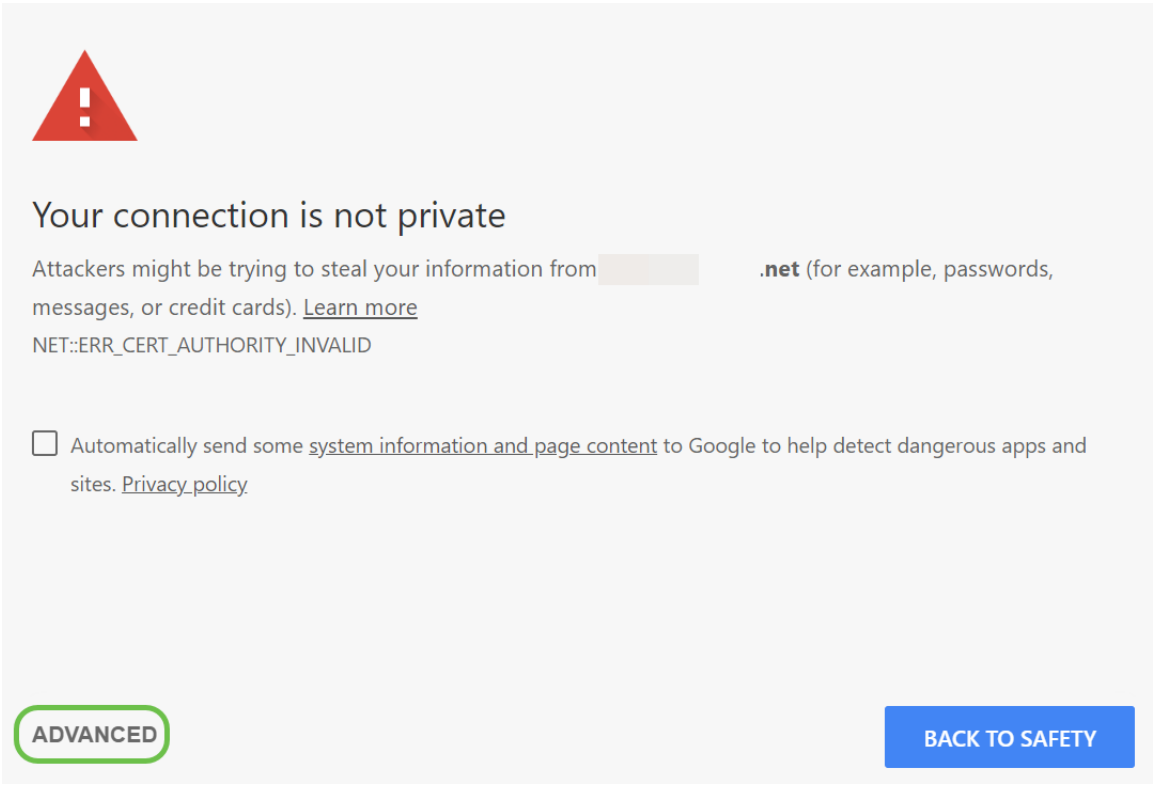
1. *Monitor* zeigt die Anzahl der angeschlossenen Clients an
2. *Clients* zeigen die Details des Clients an. Sie können diese exportieren, wenn Sie eine Aufzeichnung der verbundenen Personen speichern möchten.



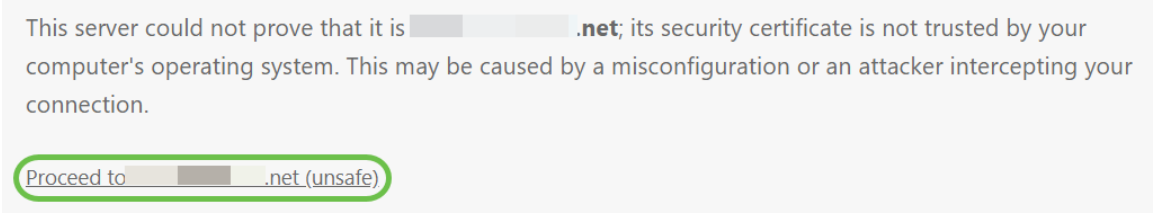
Weitere Informationen zur Gastüberwachung finden Sie hier.

Active Directory-Client-Authentifizierung

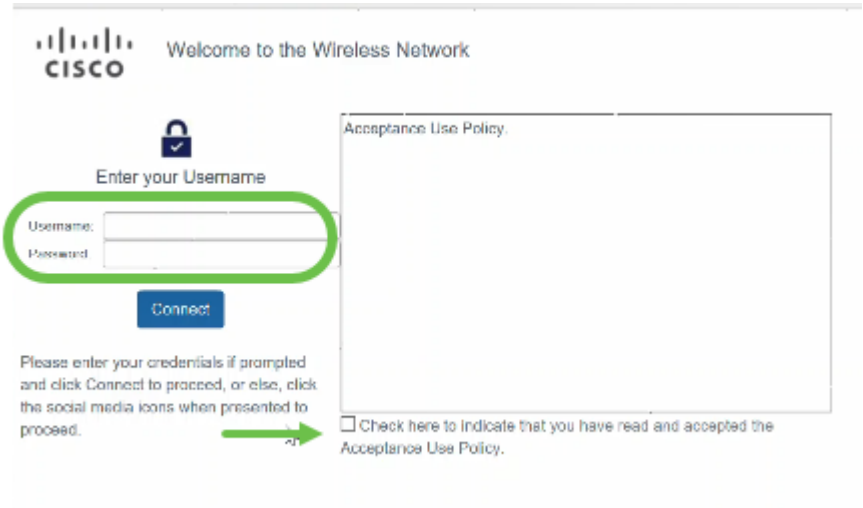
Wenn sich ein Client im Active Directory befindet, kann er sich beim WAP anmelden, um auf das Internet zuzugreifen. Wenn der Wireless Access Point ausgewählt wird, erhält er je nach verwendetem Webbrowser möglicherweise eine ähnliche Warnmeldung. Die Warnung tritt auf, wenn der Seite kein Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle zugewiesen wurde. Der Kunde muss auf **ERWEITERT** klicken.



Der Client kann dann eine Warnmeldung ähnlich der folgenden erhalten:



Eine Portalseite wurde gestartet. Auf dieser Seite sollten sie ihre Anmeldeinformationen eingeben und das Kontrollkästchen markieren, um anzugeben, dass sie die *Acceptance Use Policy* gelesen und akzeptiert haben.



Sie erhalten eine Begrüßungsnachricht und können das Internet sicher nutzen.

Sie kennen jetzt einige der neuesten Funktionen, die mit dem neuesten WAP125- und WAP581-Update ausgeliefert werden.

Weitere Informationen zu diesen und anderen neuen Features erhalten Sie, wenn Sie unten auf die Links zu den begleitenden Artikeln klicken.

Verwenden des Setup-Assistenten auf dem WAP125 oder WAP581

Verwenden des Setup-Assistenten auf einem Mobilgerät für den WAP125 oder WAP581

Vorgehensweise: Cisco Umbrella-Integration

Vorgehensweise: Cisco CloudShark-Integration

Vorgehensweise: Konfigurieren der Authentifizierungseinstellungen von Drittanbietern auf dem WAP125 oder WAP581

Vorgehensweise: Microsoft Active Directory-Gastauthentifizierung

Vorgehensweise: Umbrella - Registrieren eines neuen Geräts, wenn der Geheimschlüssel für die API verloren geht

Anpassung der Darstellung Ihres Captive Portals

Sehen Sie sich ein Video zu diesem Artikel an..

Klicken Sie hier, um weitere Tech Talks von Cisco anzuzeigen.