Konfigurieren von PEAP und EAP-FAST mit ACS 5.2 und WLC

Inhalt

Einleitung

In diesem Dokument wird erläutert, wie der Wireless LAN Controller (WLC) für die EAP-Authentifizierung (Extensible Authentication Protocol) mithilfe eines externen RADIUS-Servers wie Access Control Server (ACS) 5.2 konfiguriert wird.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie die folgenden Anforderungen erfüllen, bevor Sie diese Konfiguration vornehmen:

- Grundkenntnisse der WLC und Lightweight Access Points (LAPs)
- Besitzen funktionale Kenntnisse des AAA-Servers

- Umfassende Kenntnisse über Wireless-Netzwerke und Sicherheitsprobleme bei Wireless-Netzwerken

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco 5508 WLC mit Firmware-Version 7.0.220.0
- Cisco Serie 3502 - LAP
- Microsoft Windows 7 Native Komponente mit Intel 6300-N Treiber, Version 14.3
- Cisco Secure ACS mit Version 5.2
- Cisco Switch der Serie 3560

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

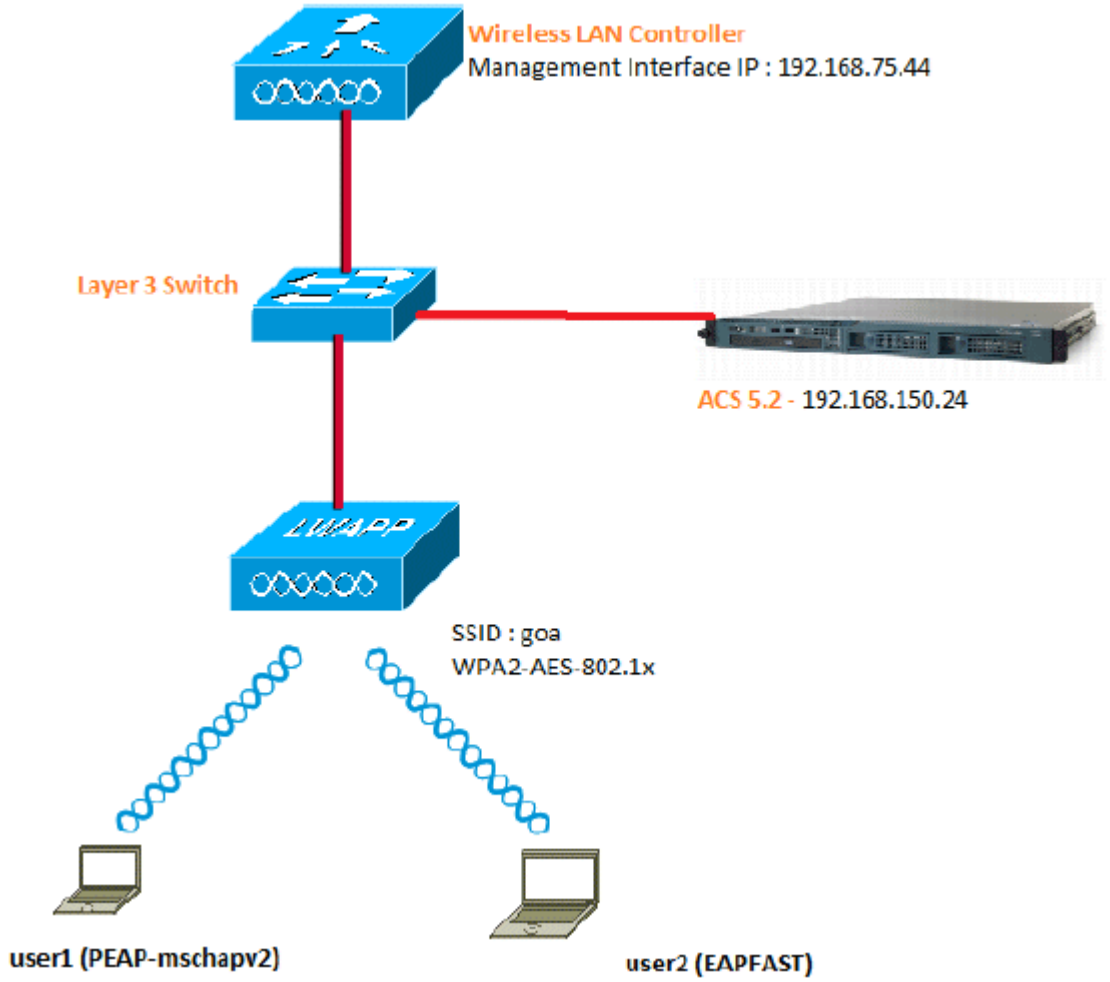
Konfigurieren

In diesem Abschnitt erfahren Sie, wie Sie die in diesem Dokument beschriebenen Funktionen konfigurieren können.

Hinweis: Verwenden Sie das Tool für die Suche nach Befehlen (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Nachfolgend sind die Konfigurationsdetails der in diesem Diagramm verwendeten Komponenten aufgeführt:

- Die IP-Adresse des ACS (RADIUS)-Servers lautet 192.168.150.24.
- Die Management- und AP-Manager-Schnittstellenadresse des WLC lautet 192.168.75.44.
- Die DHCP-Server-Adresse lautet 192.168.150.25.
- In dieser Konfiguration wird VLAN 253 verwendet. Beide Benutzer stellen eine Verbindung zum gleichen SSID-Ziel her. user1 ist jedoch für die Authentifizierung mithilfe von PEAP-MSCHAPv2 und user2 mithilfe von EAP-FAST konfiguriert.
- Benutzer werden in VLAN 253 zugewiesen:
  - VLAN 253: 192.168.153.x/24 Gateway: 192.168.153.1
  - VLAN 75: 192.168.75.x/24 Gateway: 192.168.75.1

Annahmen

- Switches werden für alle Layer-3-VLANs konfiguriert.
- Dem DHCP-Server wird ein DHCP-Bereich zugewiesen.
- Zwischen allen Geräten im Netzwerk bestehen Layer-3-Verbindungen.

- Die LAP ist bereits mit dem WLC verbunden.
- Jedes VLAN hat eine /24-Maske.
- In ACS 5.2 ist ein selbstsigniertes Zertifikat installiert.

Konfigurationsschritte

Diese Konfiguration ist in drei Hauptschritte unterteilt:

1. Konfigurieren des RADIUS-Servers
2. Konfigurieren des WLC
3. Konfigurieren des Dienstprogramms für den Wireless-Client

Konfigurieren des RADIUS-Servers

Die Konfiguration des RADIUS-Servers ist in vier Schritte unterteilt:

1. Netzwerkressourcen konfigurieren
2. Konfigurieren Sie Benutzer.
3. Definieren Sie Richtlinienelemente.
4. Wenden Sie Zugriffsrichtlinien an.

ACS 5.x ist ein richtlinienbasiertes Zugriffskontrollsystem. ACS 5.x verwendet also ein regelbasiertes Richtlinienmodell anstelle des in Version 4.x verwendeten gruppenbasierten Modells.

Das regelbasierte ACS 5.x-Richtlinienmodell bietet im Vergleich zum älteren gruppenbasierten Ansatz eine leistungsstärkere und flexiblere Zugriffskontrolle.

Im älteren gruppenbasierten Modell definiert eine Gruppe eine Richtlinie, da sie drei Informationstypen enthält und miteinander verknüpft:

- Identitätsinformationen - Diese Informationen können auf der Mitgliedschaft in AD- oder LDAP-Gruppen oder einer statischen Zuweisung für interne ACS-Benutzer basieren.
- Andere Einschränkungen oder Bedingungen - Zeitbeschränkungen, Gerätebeschränkungen usw.
- Berechtigungen - VLANs oder Cisco IOS®-Berechtigungsebenen

Das ACS 5.x-Richtlinienmodell basiert auf folgenden Regeln:

- Wenn Bedingung dann Ergebnis

Wir verwenden z. B. die für das gruppenbasierte Modell beschriebenen Informationen:

- Wenn Identität-Bedingung, Restriktionsbedingung dann Autorisierungsprofil.

Dies gibt uns die Flexibilität, zu begrenzen, unter welchen Bedingungen der Benutzer auf das Netzwerk zugreifen darf und welche Autorisierungsstufe erlaubt ist, wenn bestimmte Bedingungen erfüllt sind.

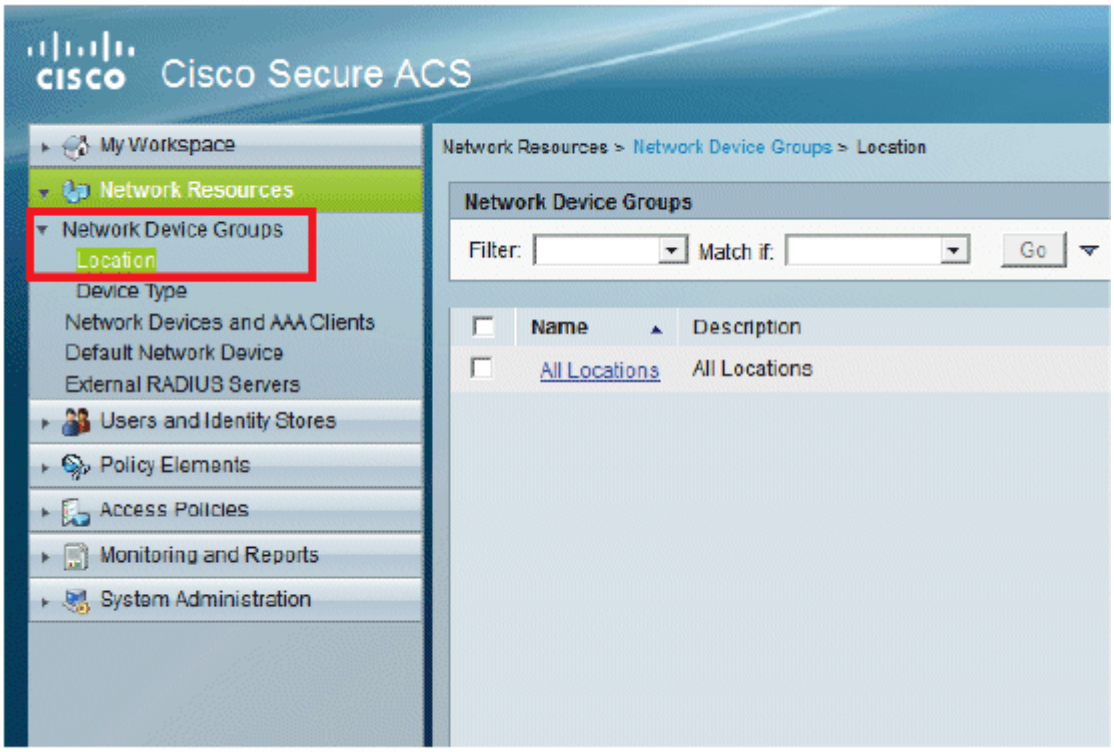
Netzwerkressourcen konfigurieren

In diesem Abschnitt wird der AAA-Client für den WLC auf dem RADIUS-Server konfiguriert.

In diesem Verfahren wird erläutert, wie der WLC als AAA-Client auf dem RADIUS-Server hinzugefügt wird, damit der WLC die Benutzeranmeldeinformationen an den RADIUS-Server weitergeben kann.

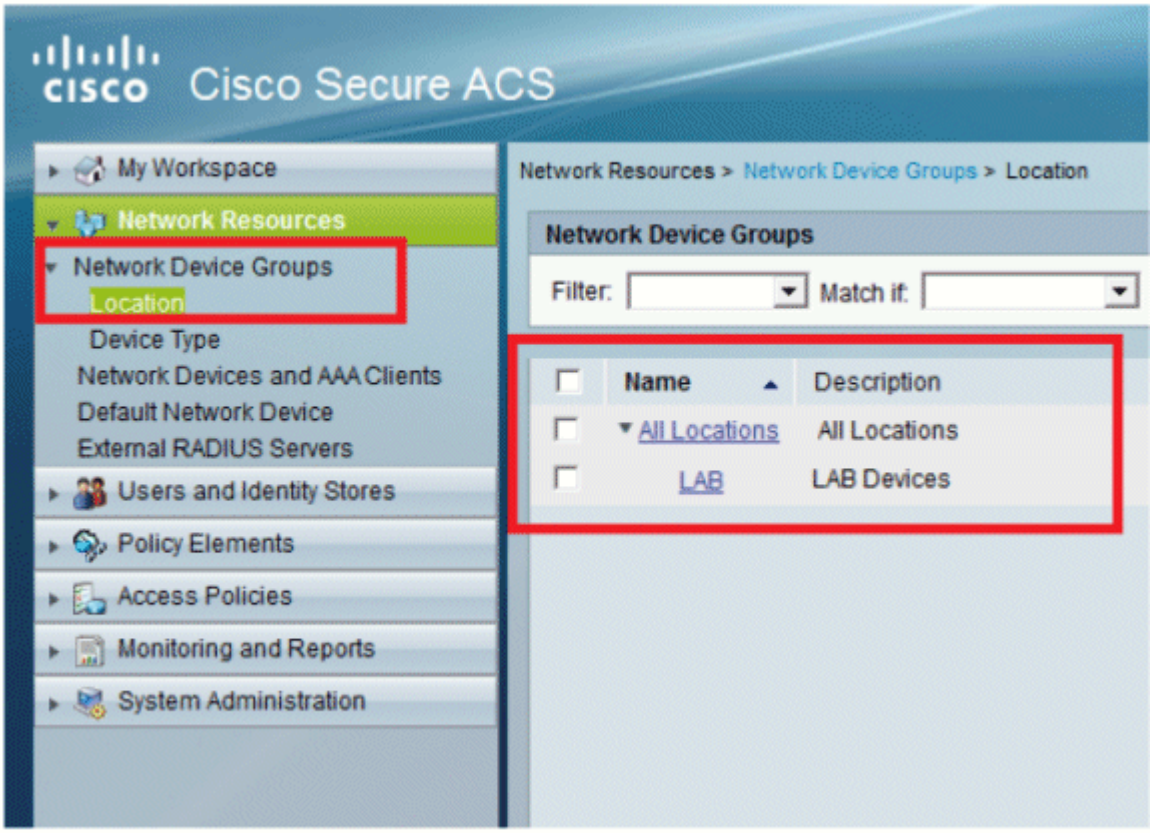
Führen Sie diese Schritte aus:

1. Wechseln Sie in der ACS-GUI zu **Netzwerkressourcen** > **Netzwerkgerätegruppen** > **Standort**, und klicken Sie unten auf **Erstellen**.

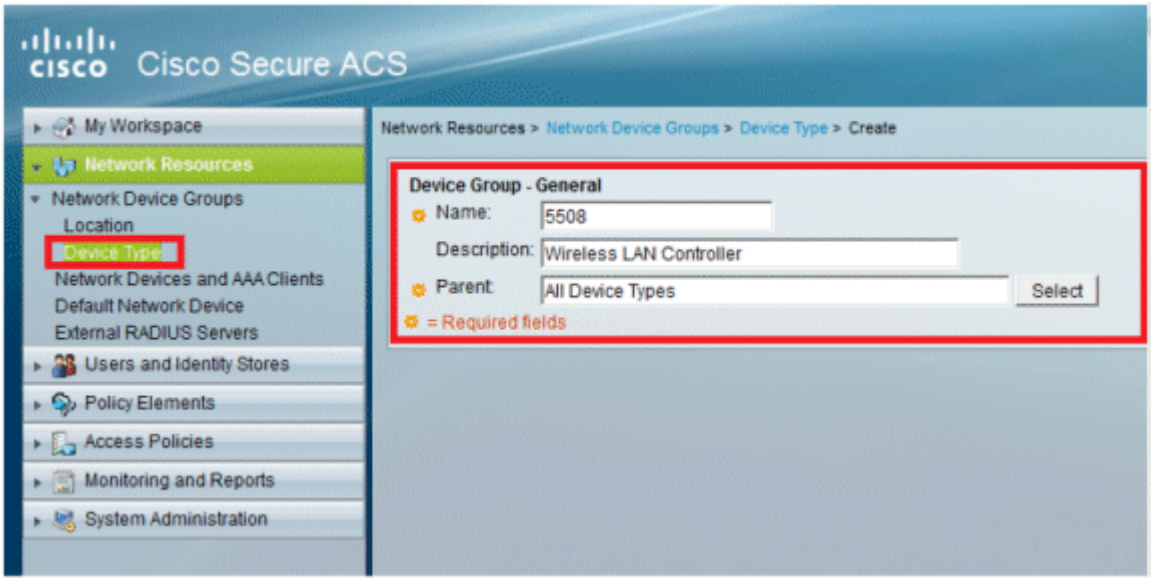


2. Fügen Sie die erforderlichen Felder hinzu, und klicken Sie auf **Senden**.

Sie sehen nun diesen Bildschirm:



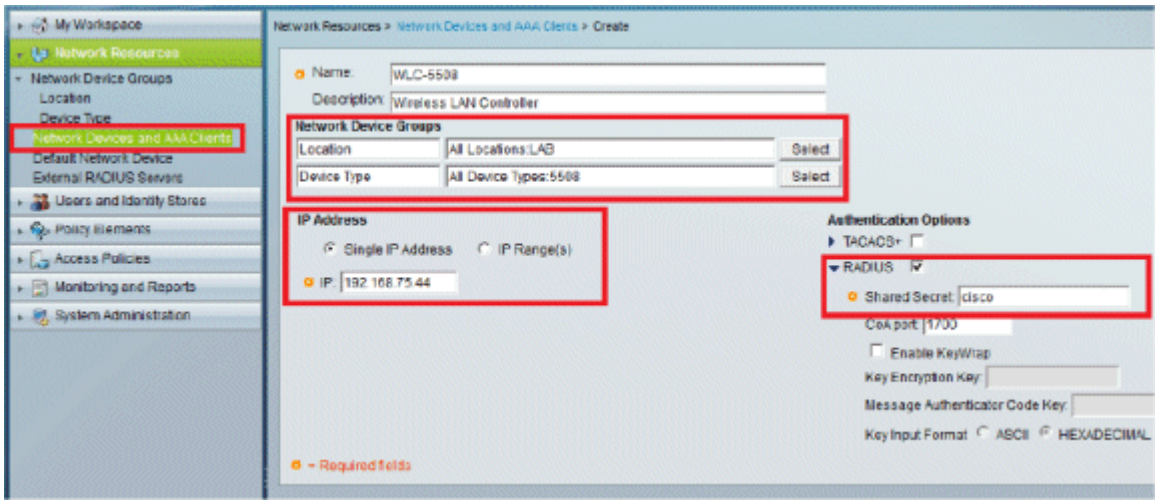
3. Klicken Sie auf **Gerätetyp** > **Erstellen**.



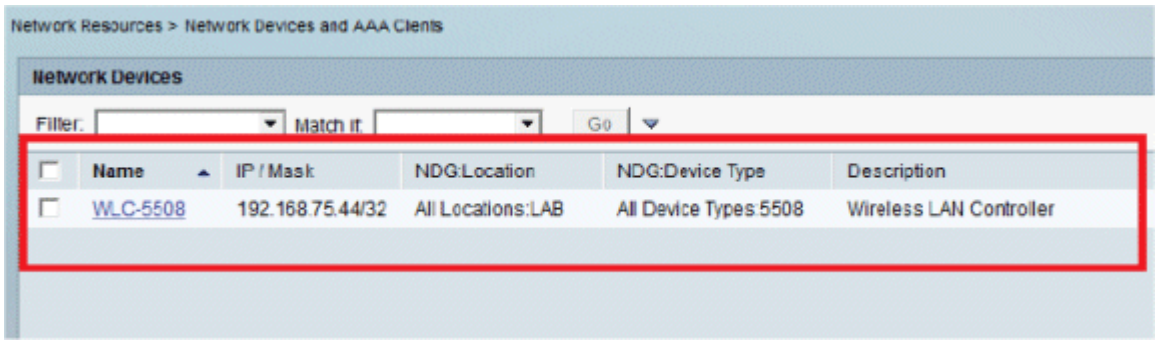
4. Klicken Sie auf **Senden**. Sie sehen nun diesen Bildschirm:

5. Gehen Sie zu **Network Resources** > **Network Devices and AAA Clients**.

6. Klicken Sie auf **Erstellen**, und geben Sie die Details wie folgt ein:



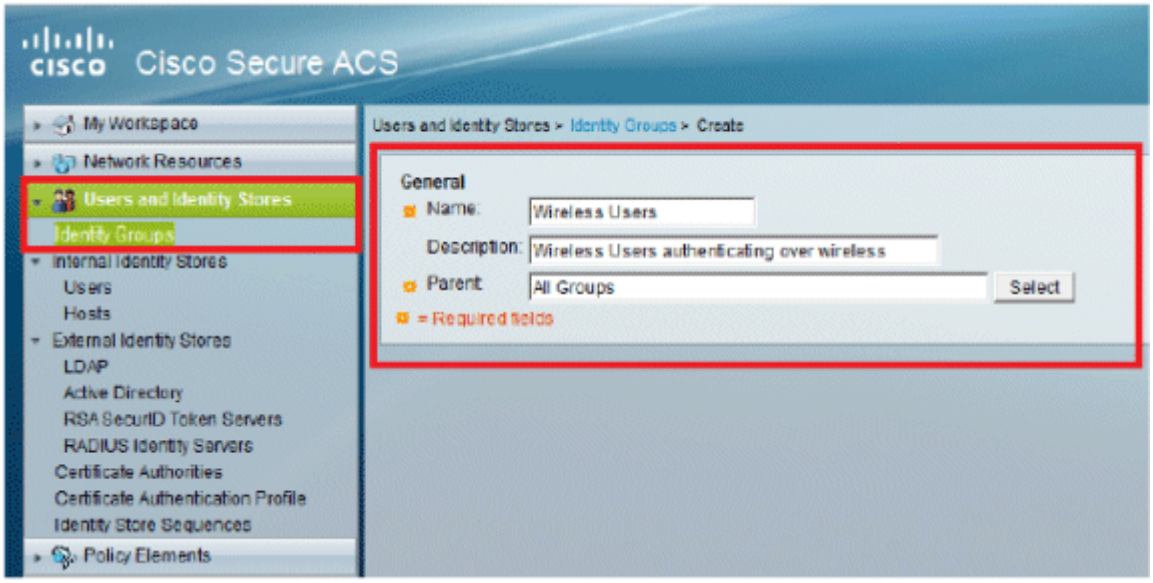
7. Klicken Sie auf **Senden**. Sie sehen nun diesen Bildschirm:



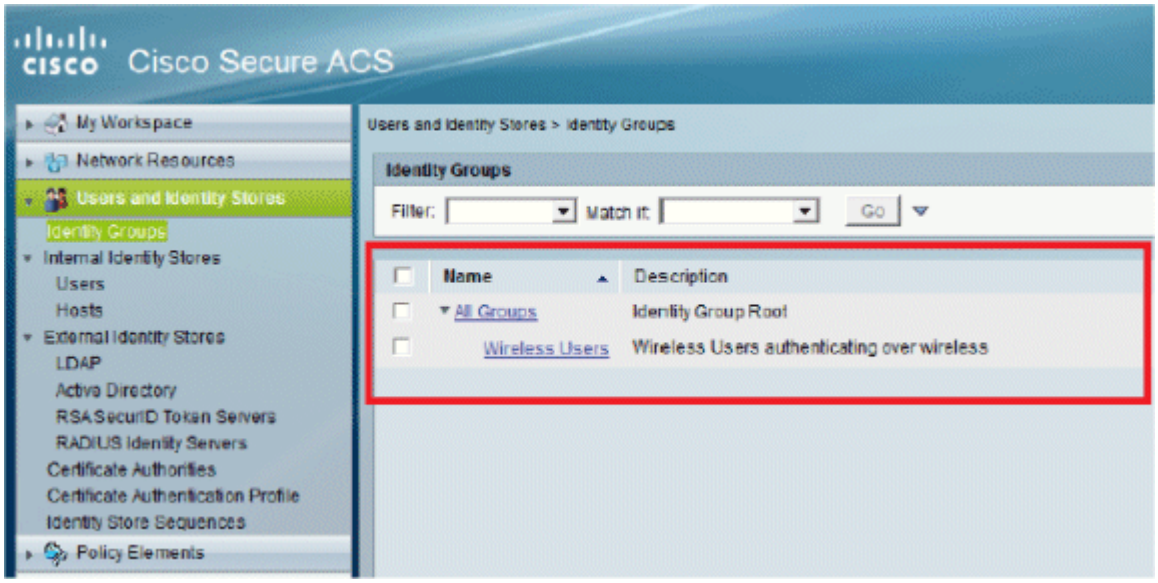
Benutzer konfigurieren

In diesem Abschnitt erstellen wir lokale Benutzer auf dem ACS. Beide Benutzer (user1 und user2) werden in der Gruppe "Wireless-Benutzer" zugewiesen.

1. Gehen Sie zu **Benutzer und Identitätsdaten** > **Identitätsgruppen** > **Erstellen**.

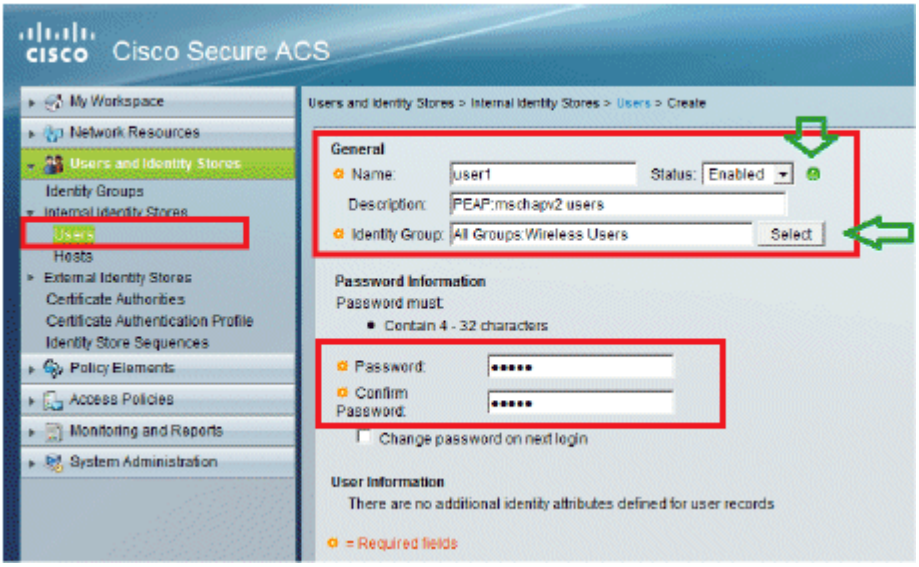


2. Wenn Sie auf **Senden** klicken, sieht die Seite wie folgt aus:

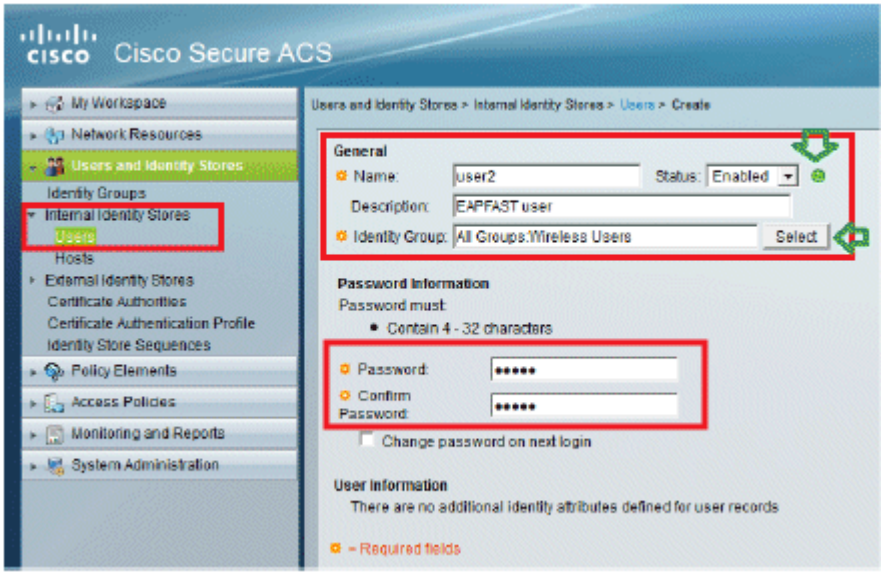


3. Erstellen Sie **user1** und **user2**, und weisen Sie sie der Gruppe "Wireless-Benutzer" zu.

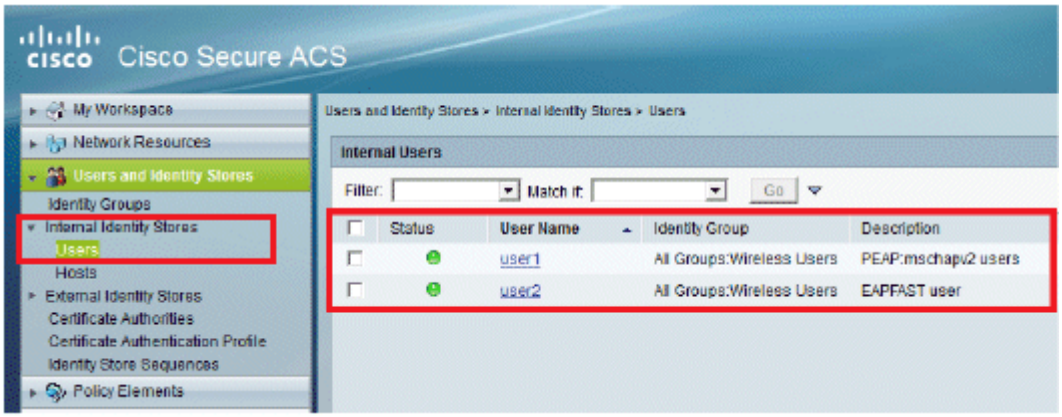
    a. Klicken Sie auf **Benutzer und Identitätsdaten** > **Identitätsgruppen** > **Benutzer** > **Erstellen**.



b. Erstellen Sie auf ähnliche Weise user2.

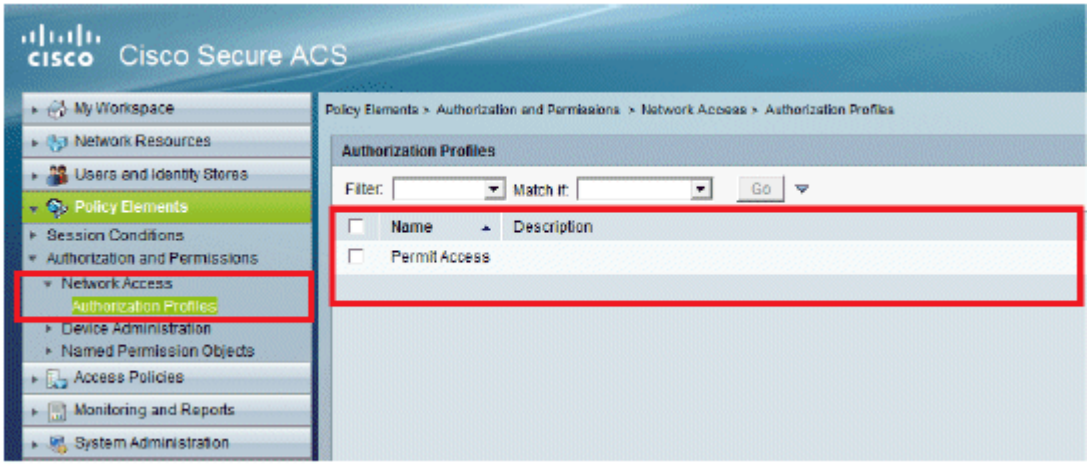


Der Bildschirm sieht wie folgt aus:



Definieren von Richtlinienelementen

Überprüfen Sie, ob **Zugriffsberechtigung** festgelegt ist.

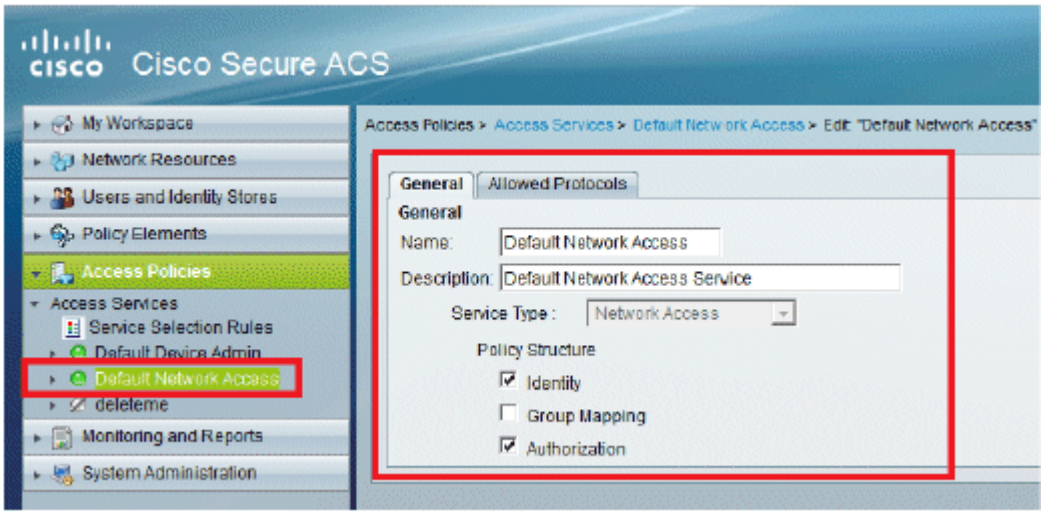


Zugriffsrichtlinien anwenden

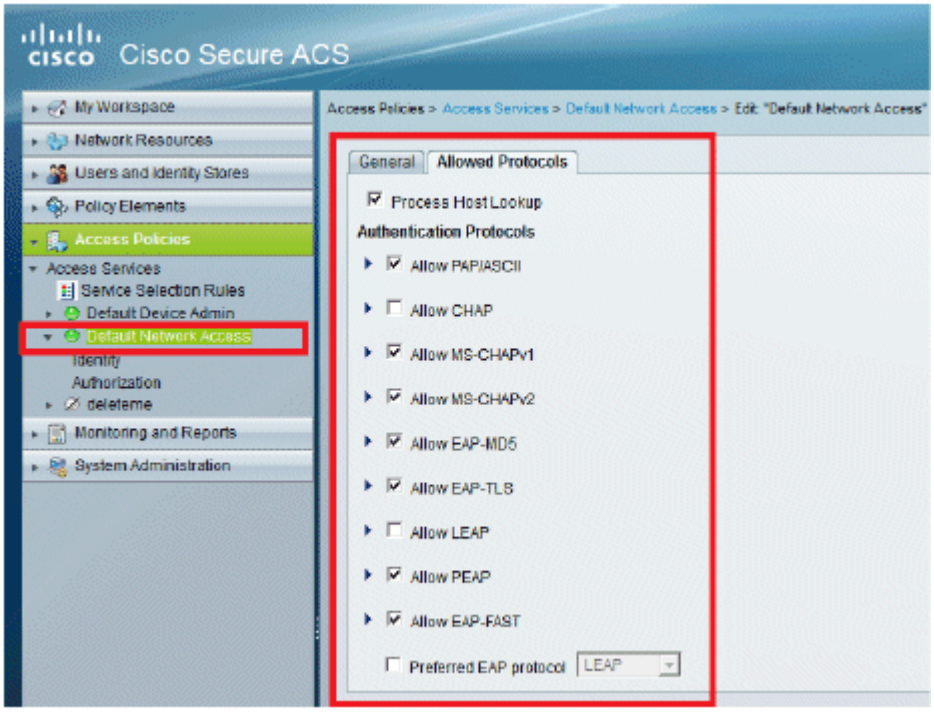
In diesem Abschnitt wählen wir die zu verwendenden Authentifizierungsmethoden und die Art der Konfiguration der Regeln aus. Wir werden Regeln erstellen, die auf den vorherigen Schritten basieren.

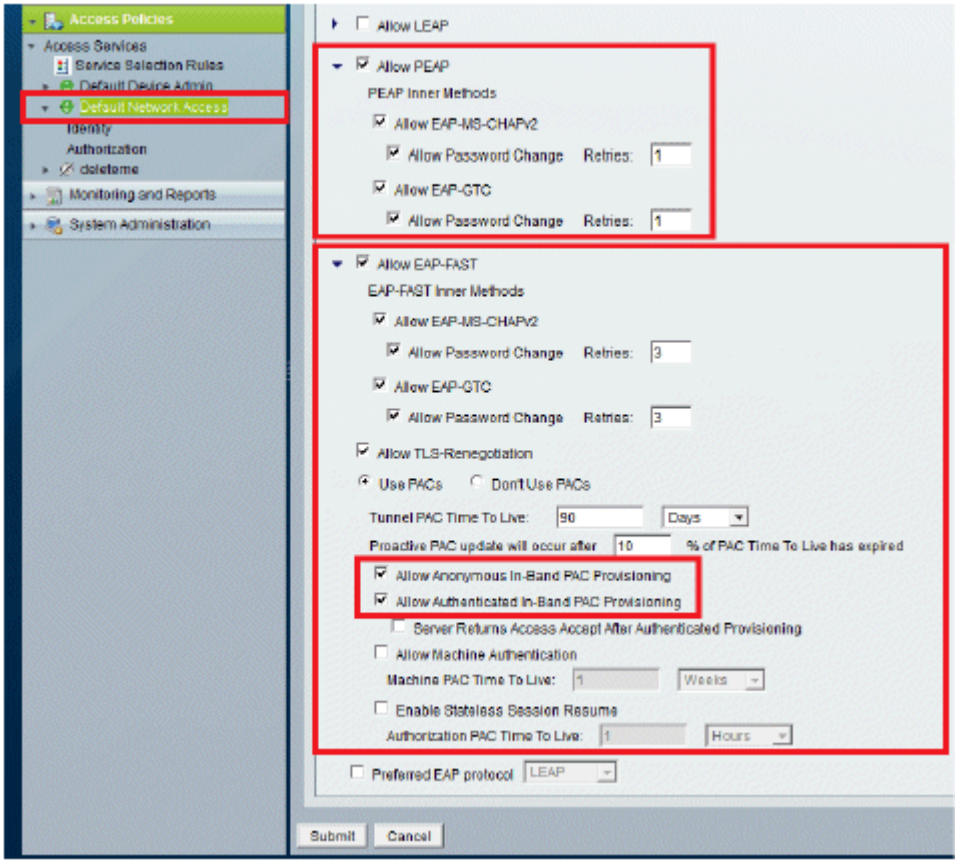
Führen Sie diese Schritte aus:

1. Gehen Sie zu **Zugriffsrichtlinien** > **Zugriffsdienste** > **Standard-Netzwerkzugriff** > **Bearbeiten: "Standard-Netzwerkzugriff"**.



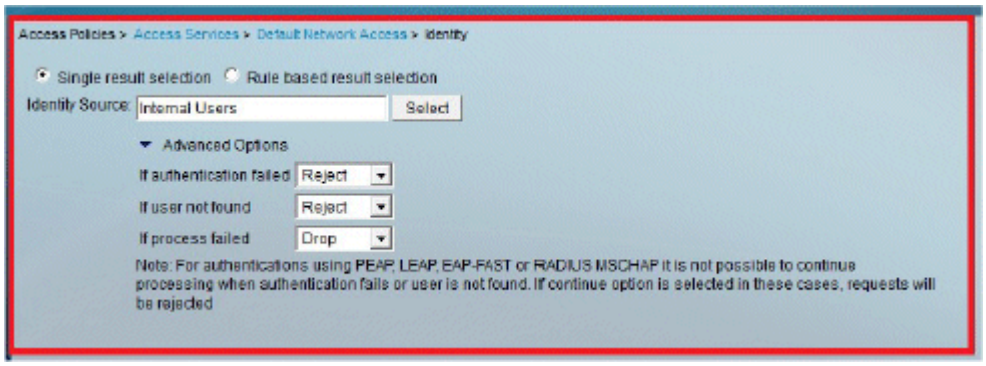
2. Wählen Sie aus, welche EAP-Methode die Wireless Clients authentifizieren sollen. In diesem Beispiel verwenden wir **PEAP- MSCHAPv2** und **EAP-FAST**.





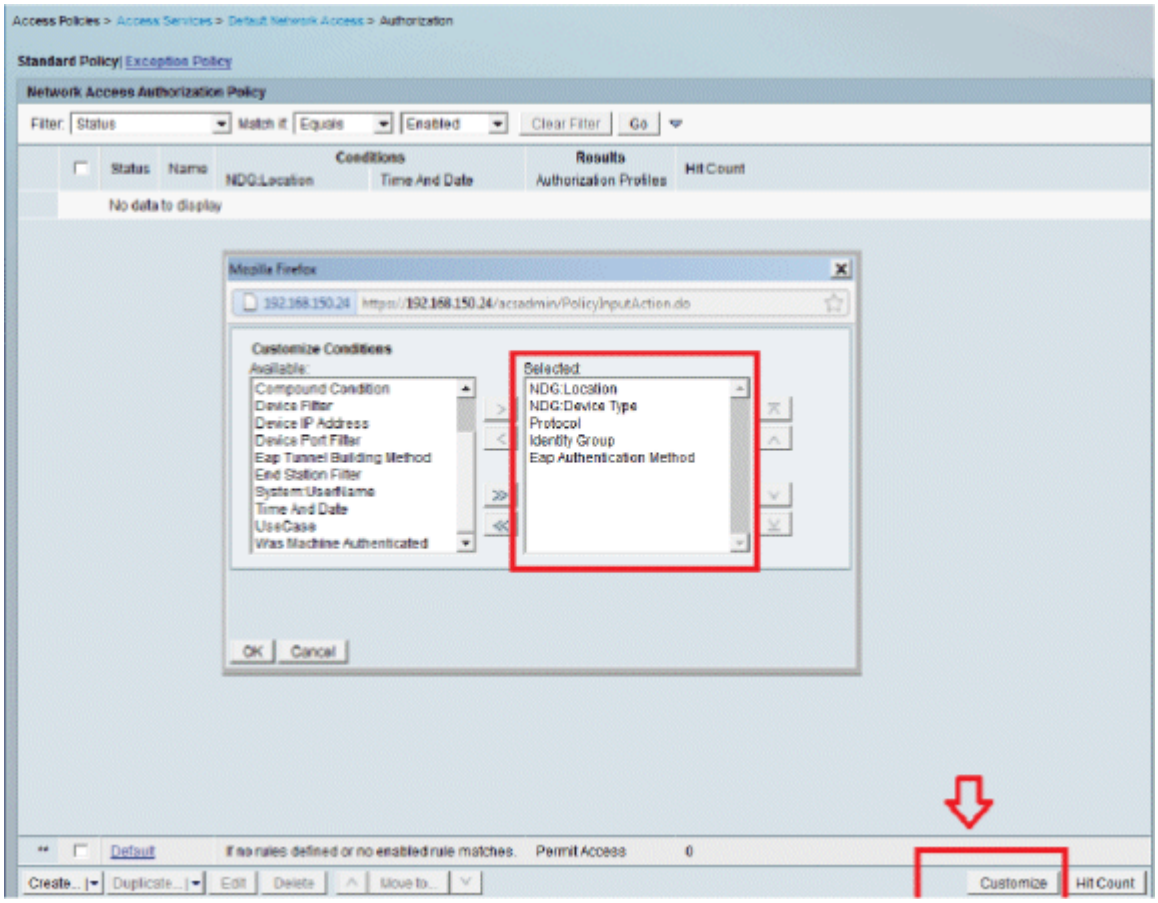
3. Klicken Sie auf **Senden**.

4. Überprüfen Sie die ausgewählte Identitätsgruppe. In diesem Beispiel werden **interne Benutzer** verwendet, die auf ACS erstellt wurden. **Speichern Sie** die Änderungen.



5. Um das Autorisierungsprofil zu überprüfen, gehen Sie zu **Zugriffsrichtlinien** > **Zugriffsdienste** > **Standard-Netzwerkzugriff** > **Autorisierung**.

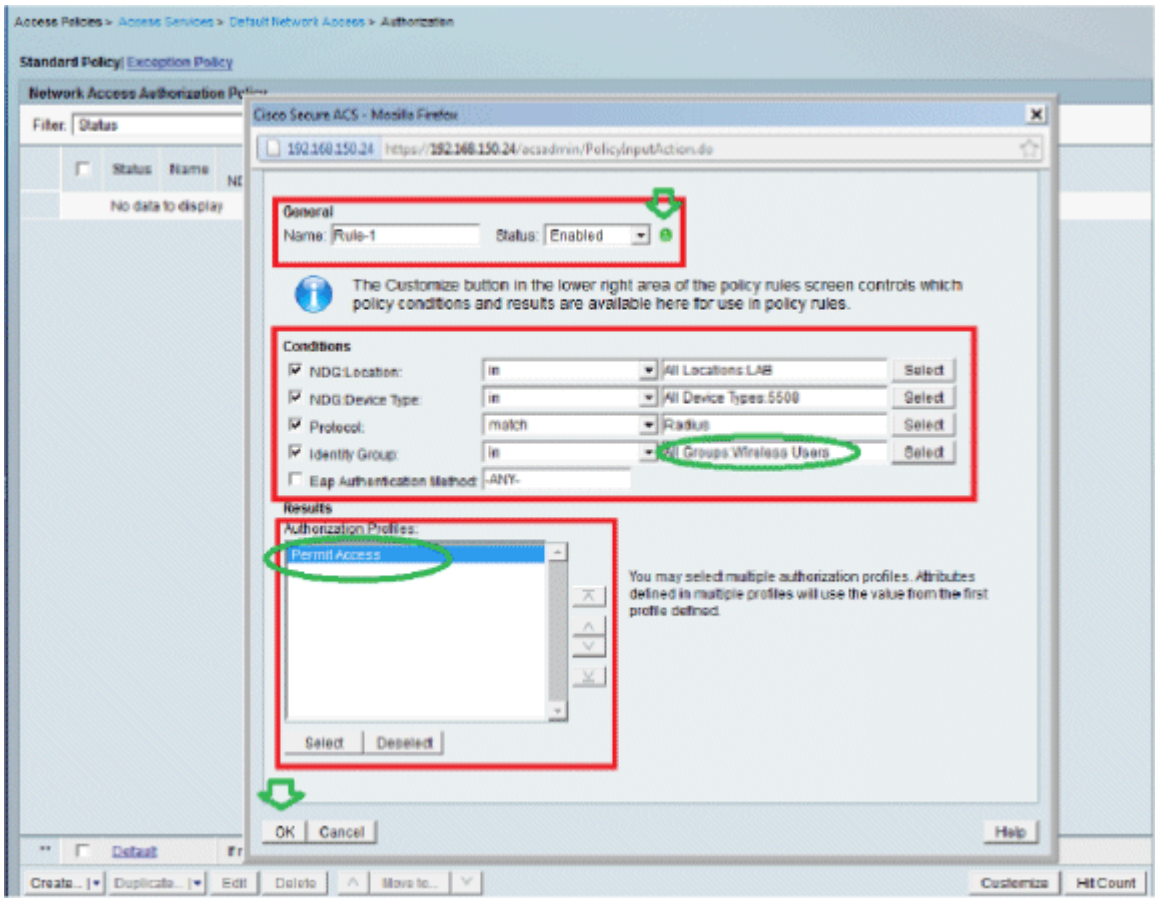
   Sie können festlegen, unter welchen Bedingungen Sie den Benutzerzugriff auf das Netzwerk zulassen und welches Autorisierungsprofil (Attribute) Sie nach der Authentifizierung weitergeben. Diese Granularität ist nur in ACS 5.x verfügbar. In diesem Beispiel haben wir Standort, **Gerätetyp**, **Protokoll**, **Identitätsgruppe** und **EAP-Authentifizierungsmethode** ausgewählt.



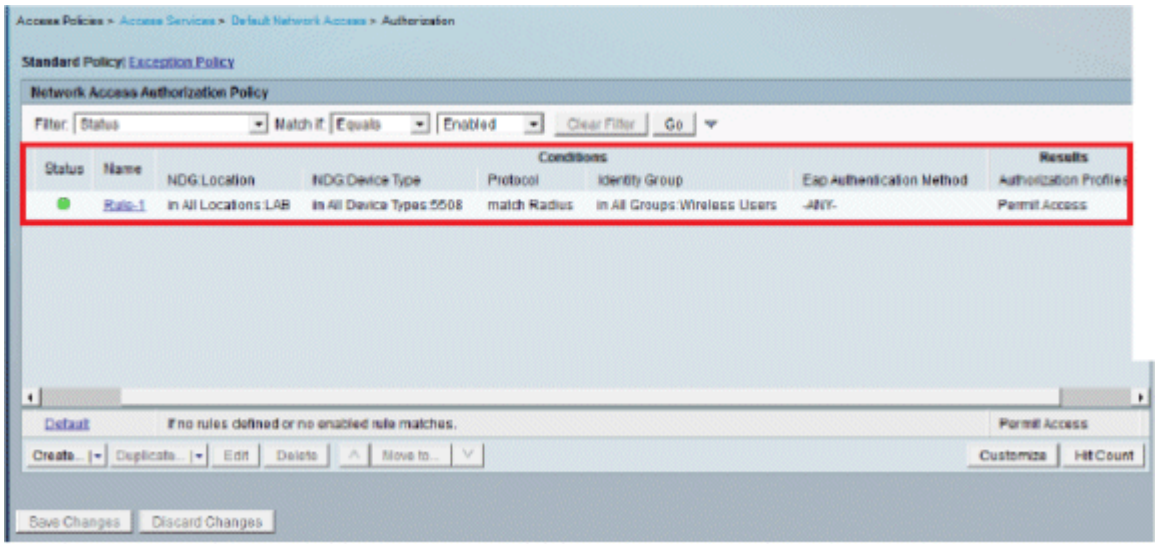
6. Klicken Sie auf **OK**, und **speichern Sie die Änderungen**.

7. Der nächste Schritt ist das Erstellen einer Regel. Wenn keine Regeln definiert sind, kann der Client ohne Bedingungen darauf zugreifen.

   Klicken Sie auf **Erstellen** > **Regel-1**. Diese Regel gilt für Benutzer in der Gruppe "Wireless-Benutzer".

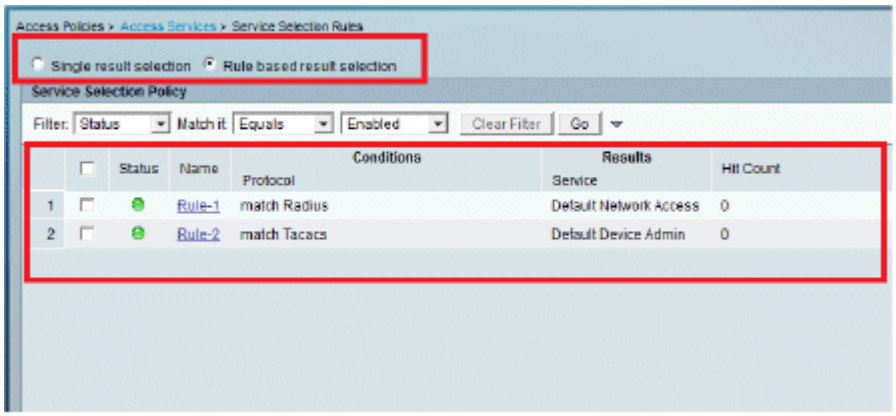


8. Speichern Sie die Änderungen. Der Bildschirm sieht wie folgt aus:



Wenn Benutzer, die nicht die Bedingungen erfüllen, abgelehnt werden sollen, ändern Sie die Standardregel so, dass "Zugriff verweigern" angezeigt wird.

9. Nun definieren Sie **Serviceauswahlregeln**. Auf dieser Seite können Sie eine einfache oder regelbasierte Richtlinie konfigurieren, um zu bestimmen, welcher Service auf eingehende Anfragen angewendet werden soll. In diesem Beispiel wird eine regelbasierte Richtlinie verwendet.



Konfigurieren des WLC

Für diese Konfiguration sind folgende Schritte erforderlich:

1. Konfigurieren Sie den WLC mit den Details des Authentifizierungsservers.
2. Konfigurieren der dynamischen Schnittstellen (VLANs)
3. Konfigurieren der WLANs (SSID)

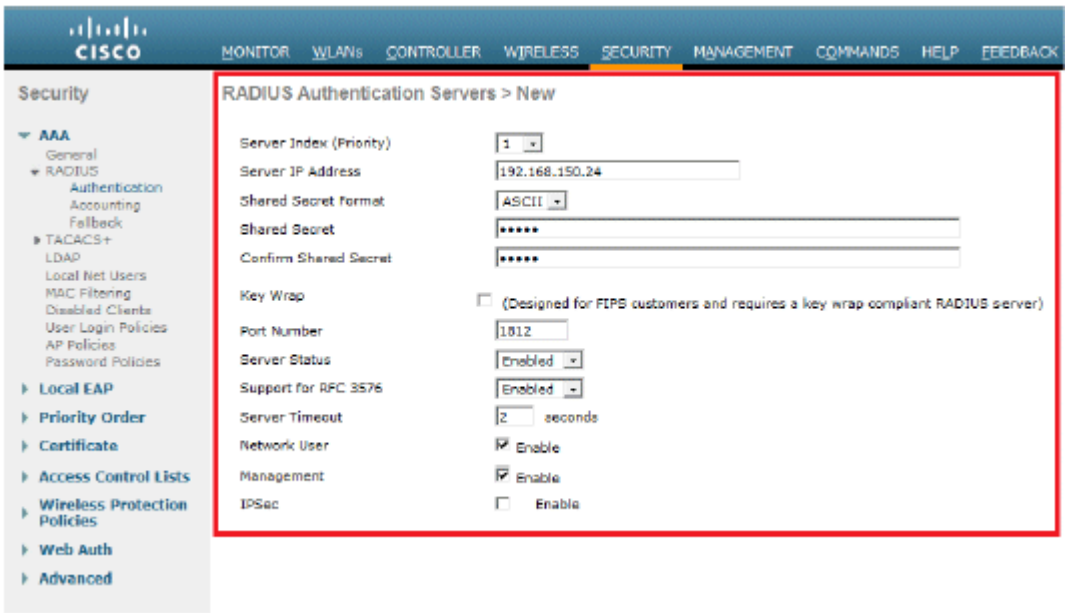
Konfigurieren des WLC mit den Details des Authentifizierungsservers

Der WLC muss so konfiguriert werden, dass er mit dem RADIUS-Server kommunizieren kann, um die Clients zu authentifizieren, und auch für alle anderen Transaktionen.

Führen Sie diese Schritte aus:

1. Klicken Sie in der Controller-GUI auf **Sicherheit**.
2. Geben Sie die IP-Adresse des RADIUS-Servers und den Schlüssel für den gemeinsamen geheimen Schlüssel ein, der zwischen dem RADIUS-Server und dem WLC verwendet wird.

   Dieser Schlüssel muss mit dem Schlüssel übereinstimmen, der im RADIUS-Server konfiguriert wurde.

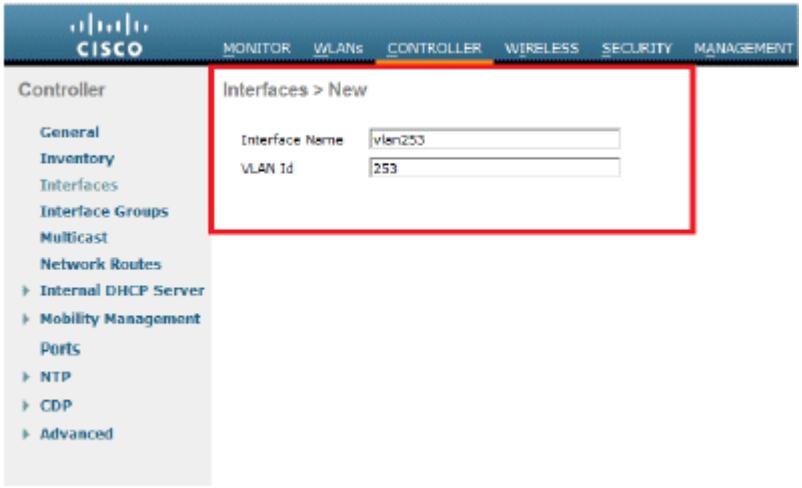


Konfigurieren der dynamischen Schnittstellen (VLANs)

In diesem Verfahren wird beschrieben, wie dynamische Schnittstellen auf dem WLC konfiguriert werden.

Führen Sie diese Schritte aus:

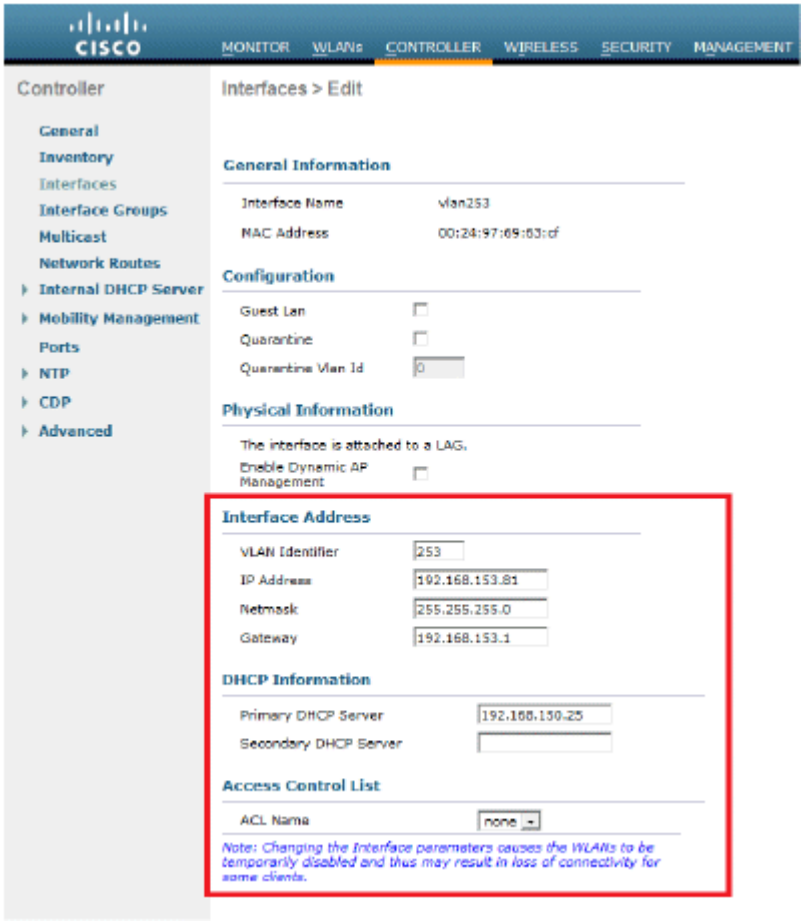
1. Die dynamische Schnittstelle wird über die Benutzeroberfläche des Controllers im Fenster **Controller > Interfaces (Controller > Schnittstellen)** konfiguriert.



2. Klicken Sie auf **Apply** (Anwenden).

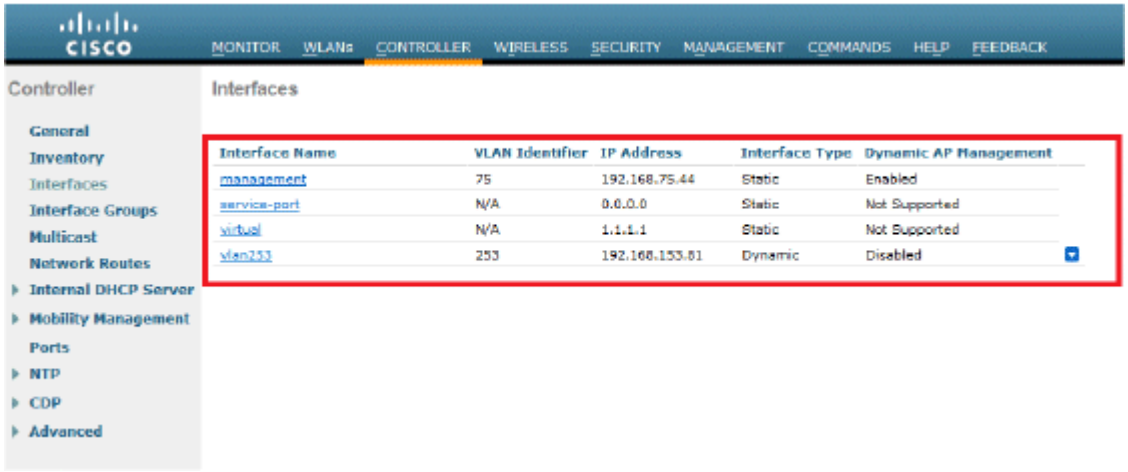
   Dadurch gelangen Sie zum Bearbeitungsfenster dieser dynamischen Schnittstelle (hier VLAN 253).

3. Geben Sie die IP-Adresse und das Standard-Gateway dieser dynamischen Schnittstelle ein.



4. Klicken Sie auf **Apply** (Anwenden).

5. Die konfigurierten Schnittstellen sehen wie folgt aus:



Konfigurieren der WLANs (SSID)

In diesem Verfahren wird erläutert, wie die WLANs im WLC konfiguriert werden.

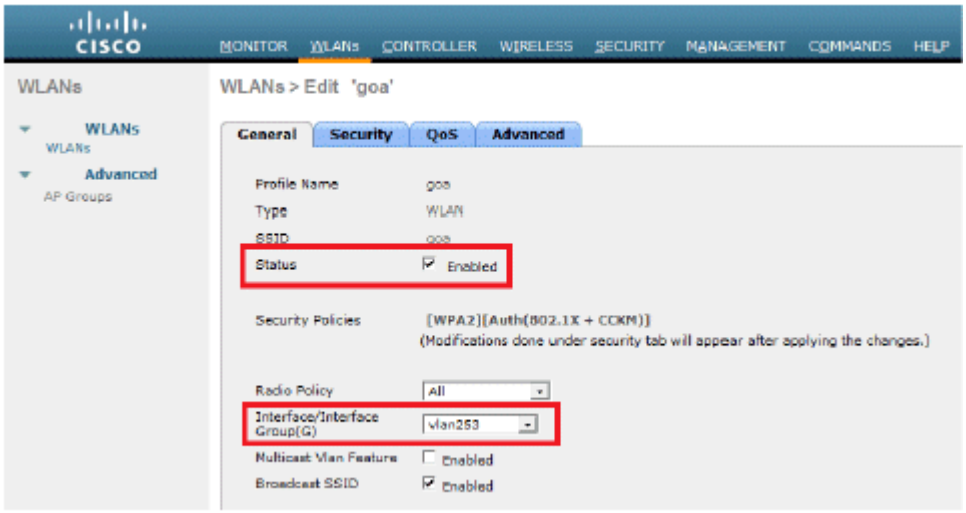
Führen Sie diese Schritte aus:

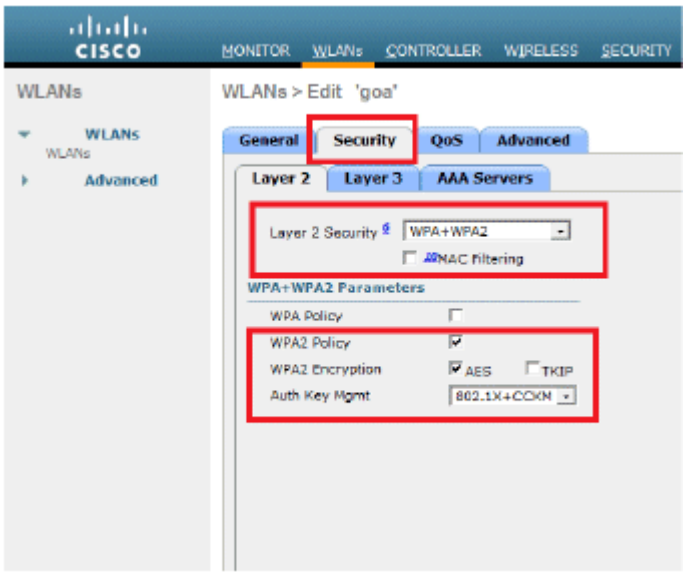
1. Gehen Sie in der Controller-GUI zu **WLANs** > **Create New**, um ein neues WLAN zu erstellen. Das Fenster Neue WLANs wird angezeigt.

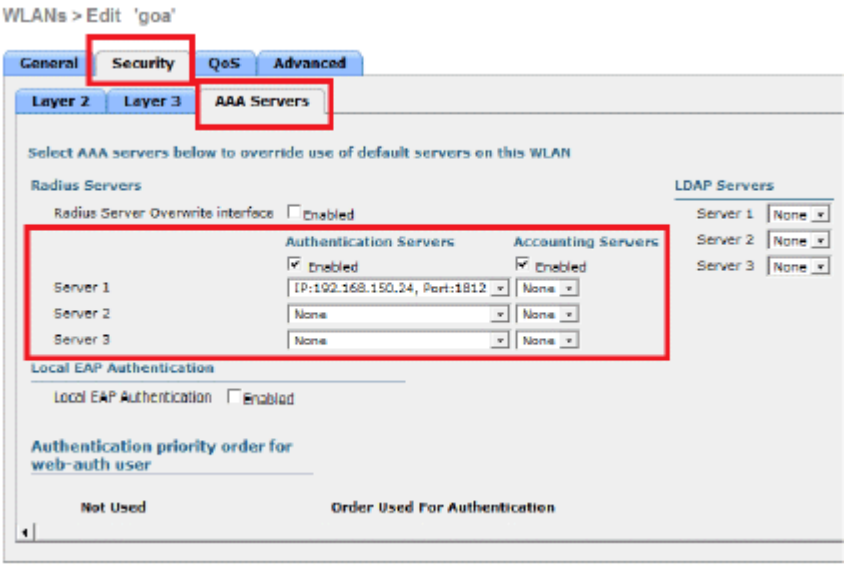
2. Geben Sie die WLAN-ID und die WLAN-SSID ein.

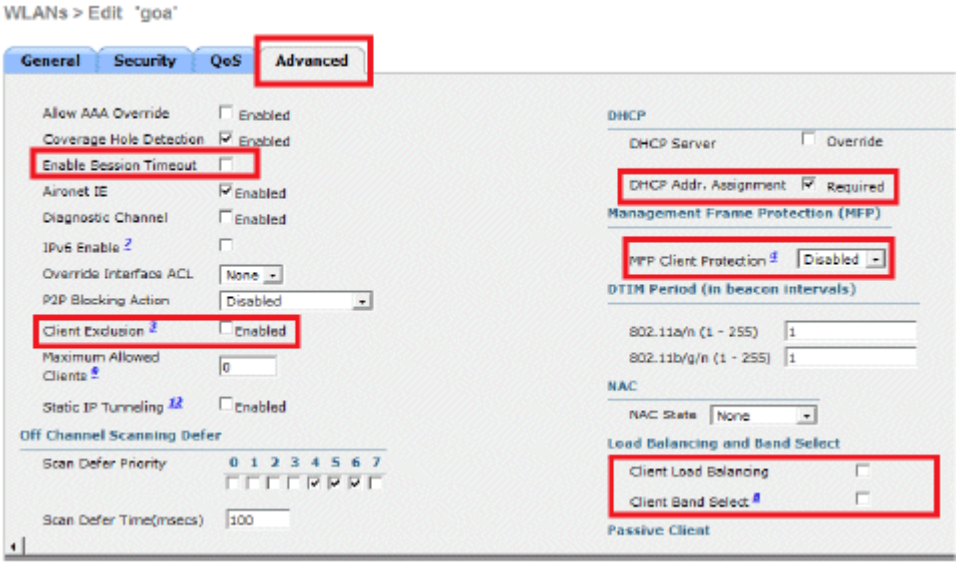
Sie können einen beliebigen Namen als WLAN-SSID eingeben. In diesem Beispiel wird **goa** als WLAN-SSID verwendet.

3. Klicken Sie auf **Apply** (Anwenden), um zum Fenster Edit (Bearbeiten) des WLAN-Ziels zu wechseln.









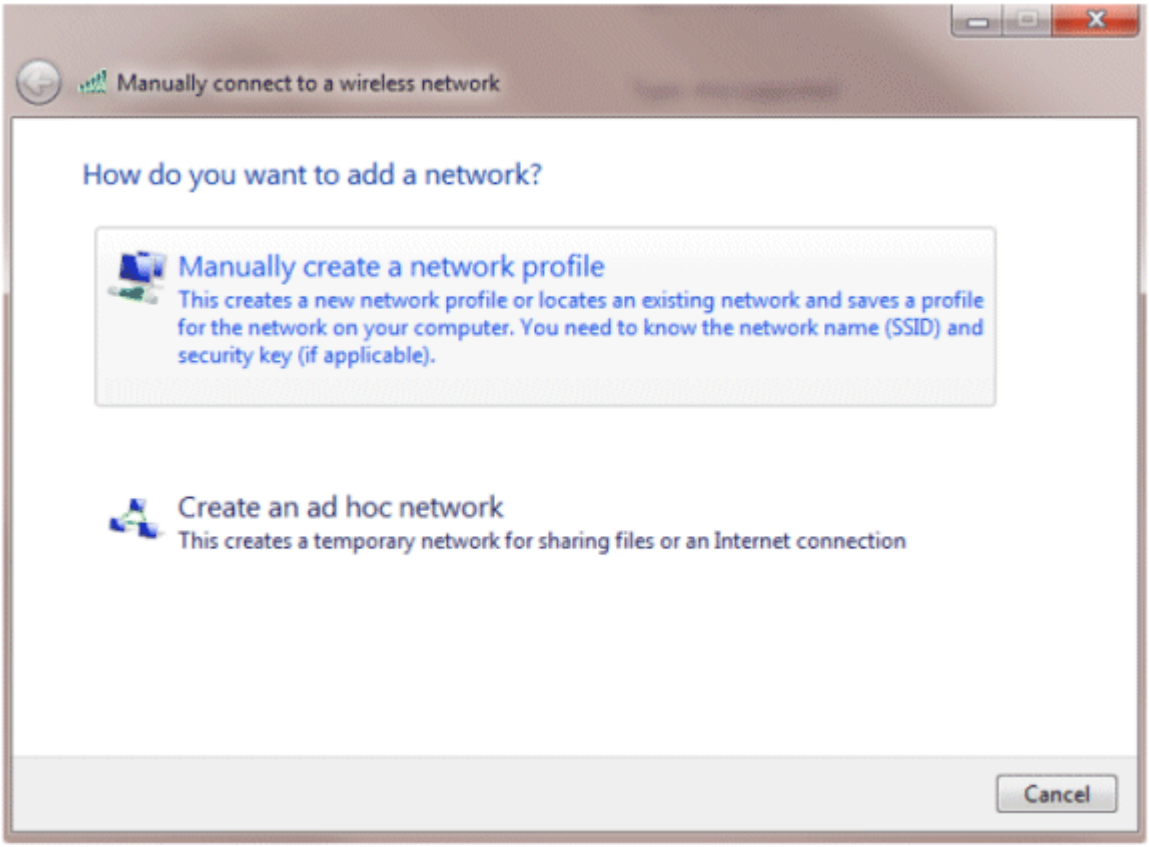
Konfigurieren des Dienstprogramms für den Wireless-Client

PEAP-MSCHAPv2 (Benutzer1)

In unserem Test-Client verwenden wir eine native Windows 7-Komponente mit einer Intel 6300-N-Karte, auf der die Treiberversion 14.3 ausgeführt wird. Es wird empfohlen, die neuesten Treiber von anderen Anbietern zu verwenden.

Gehen Sie wie folgt vor, um ein Profil in Windows Zero Config (WZC) zu erstellen:

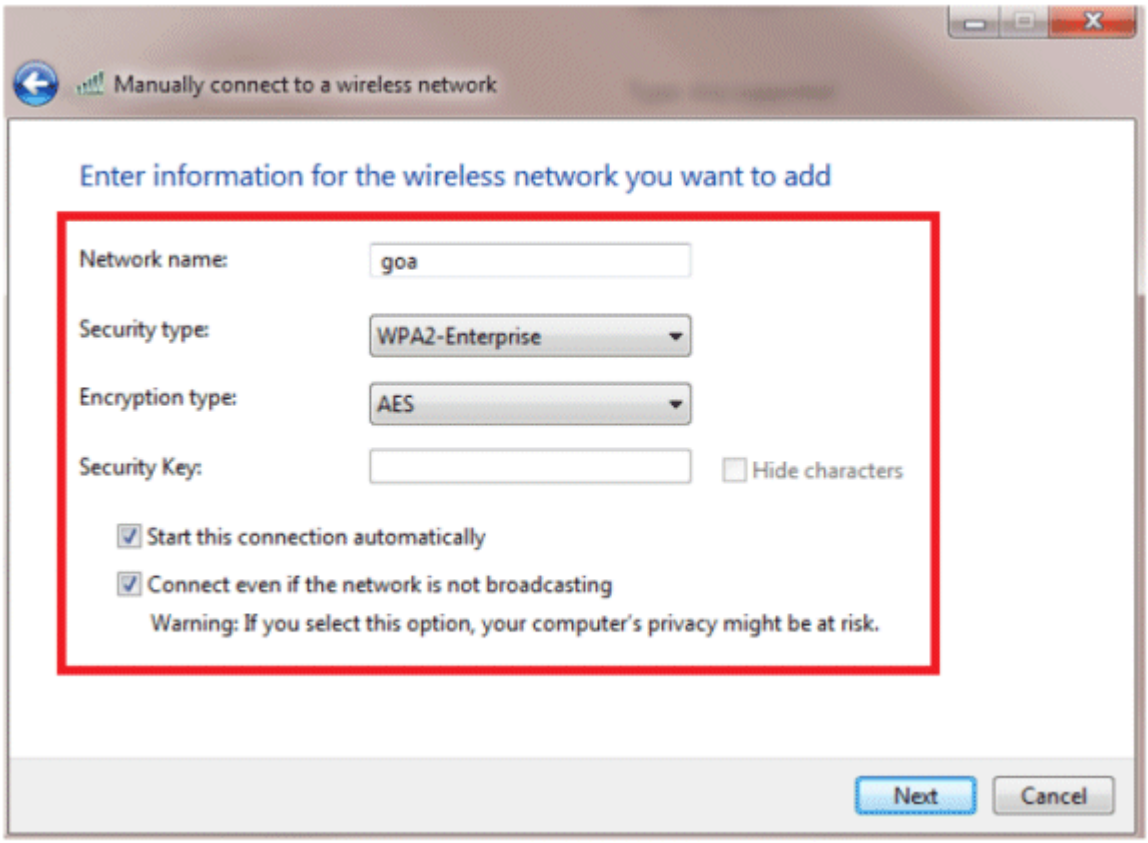
1. Gehen Sie zu **Systemsteuerung** > **Netzwerk und Internet** > **Drahtlose Netzwerke verwalten**.
2. Klicken Sie auf die Registerkarte **Hinzufügen**.
3. Klicken Sie auf **Netzwerkprofil manuell erstellen**.



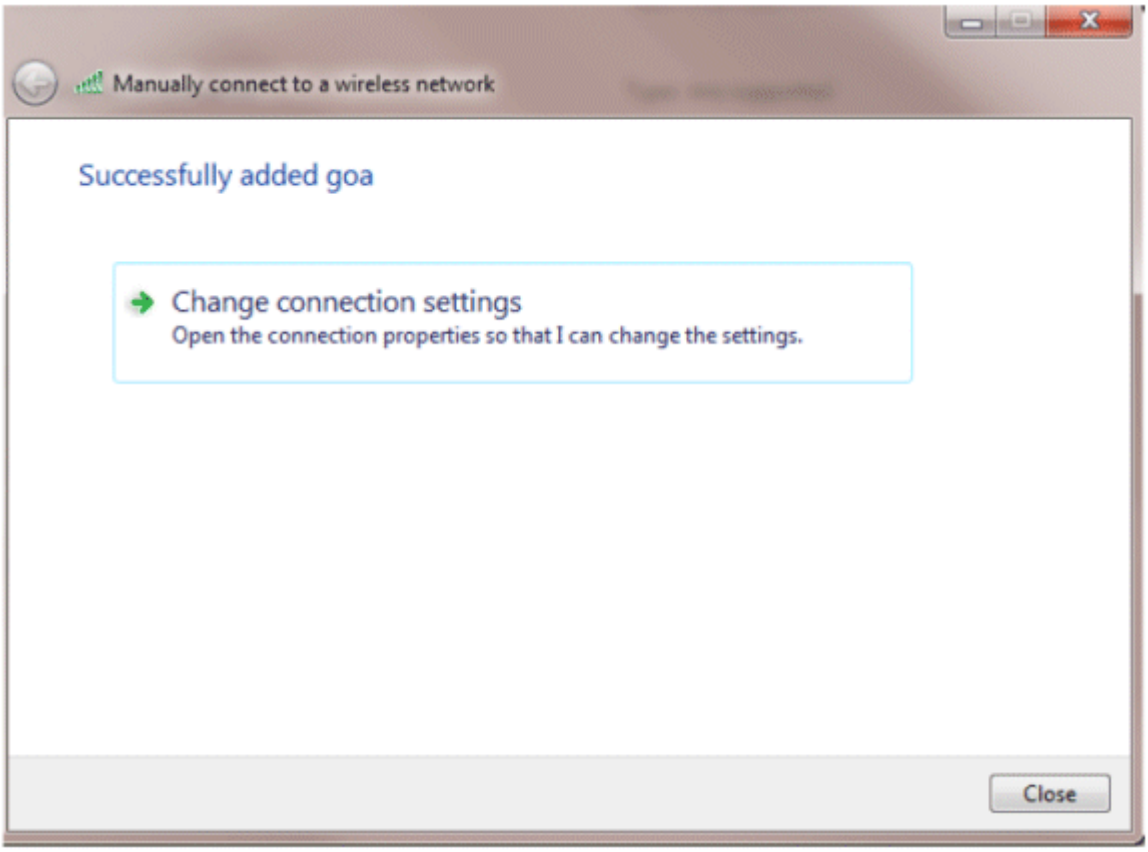
4. Fügen Sie die Details wie auf dem WLC konfiguriert hinzu.

   Hinweis: Bei der SSID wird zwischen Groß- und Kleinschreibung unterschieden.

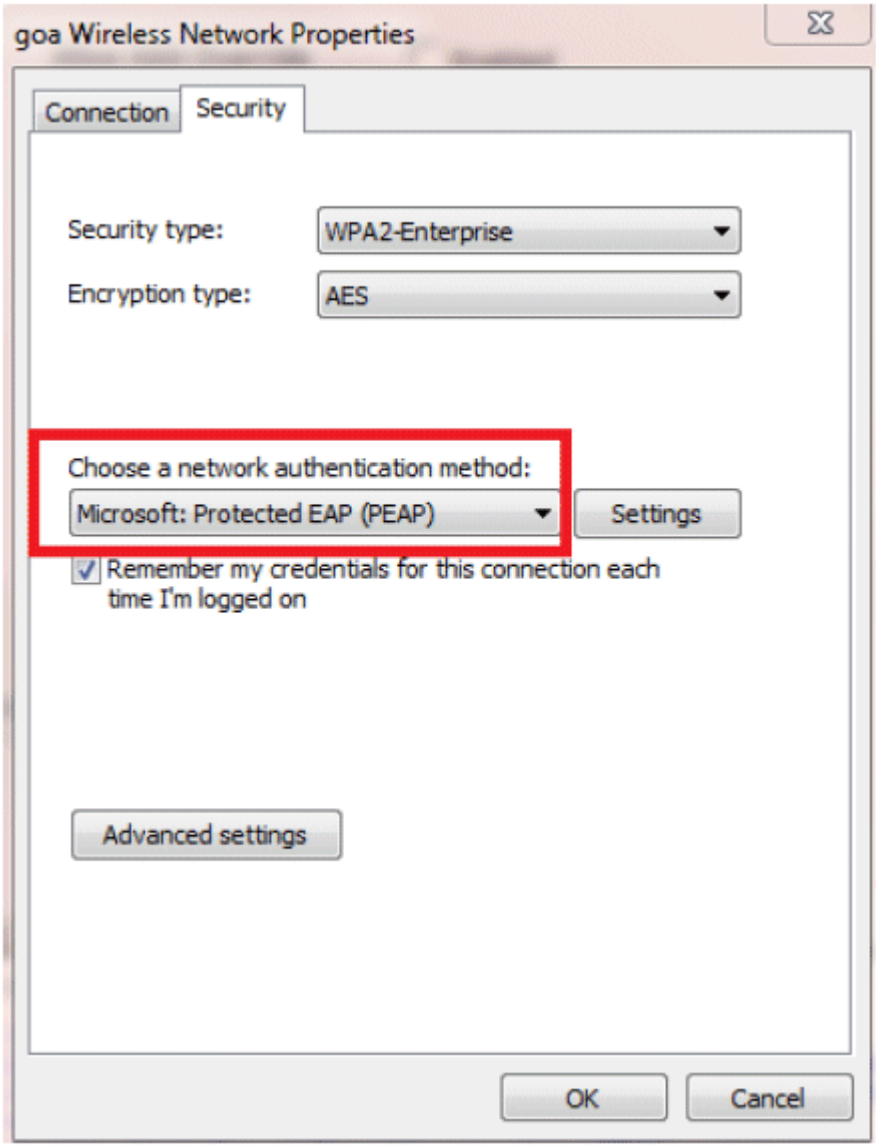
5. Klicken Sie auf **Next** (Weiter).

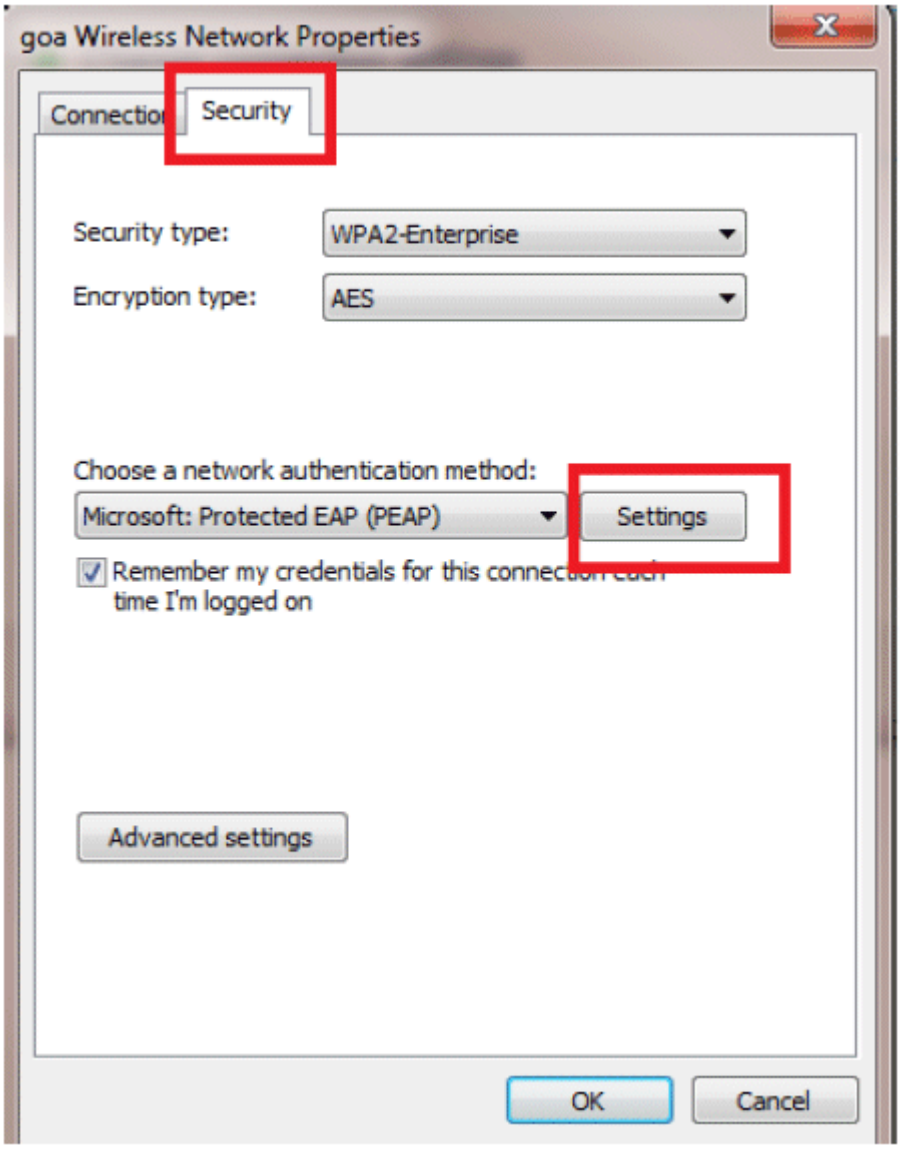


6. Klicken Sie auf **Verbindungseinstellungen ändern**, um die Einstellungen zu überprüfen.

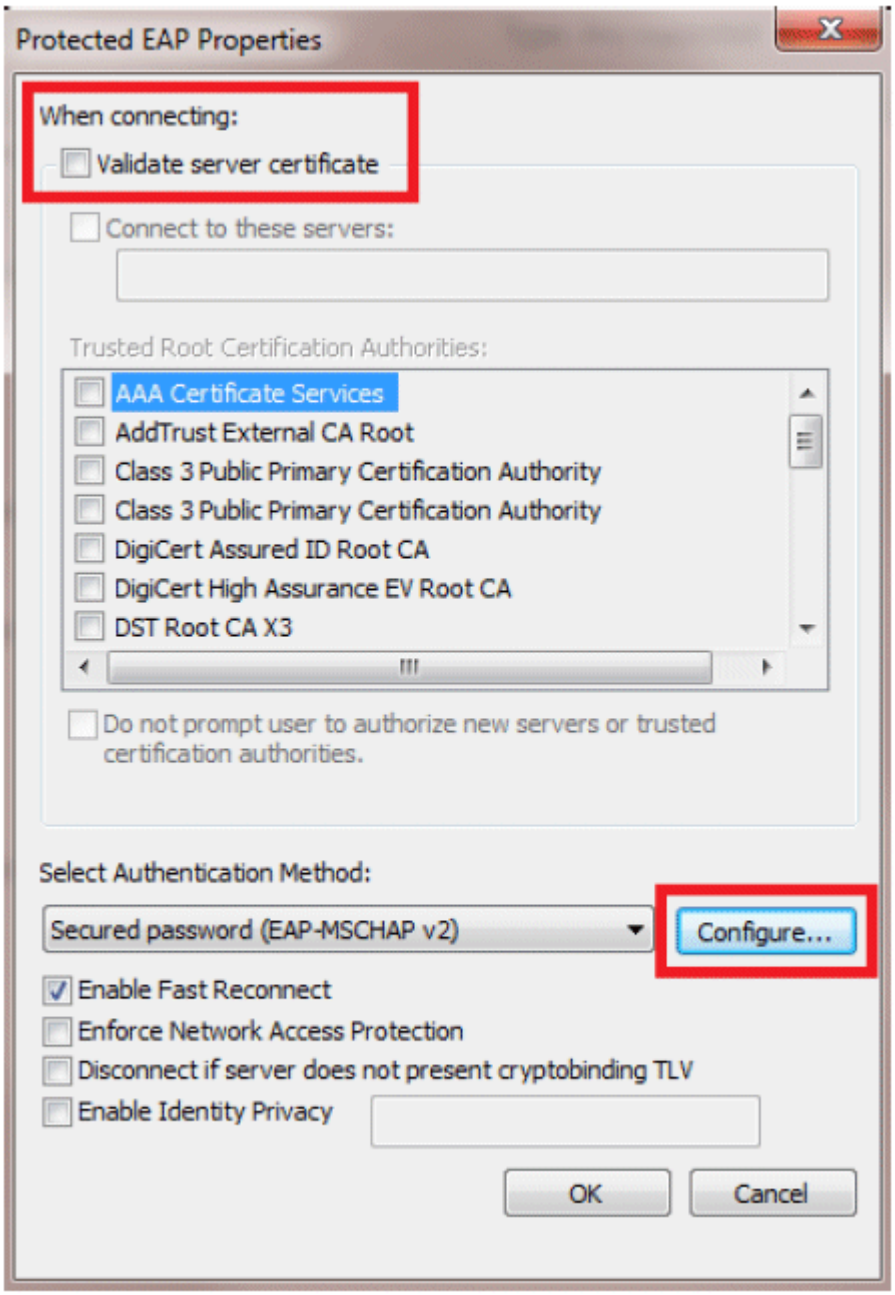


7. Stellen Sie sicher, dass **PEAP** aktiviert ist.

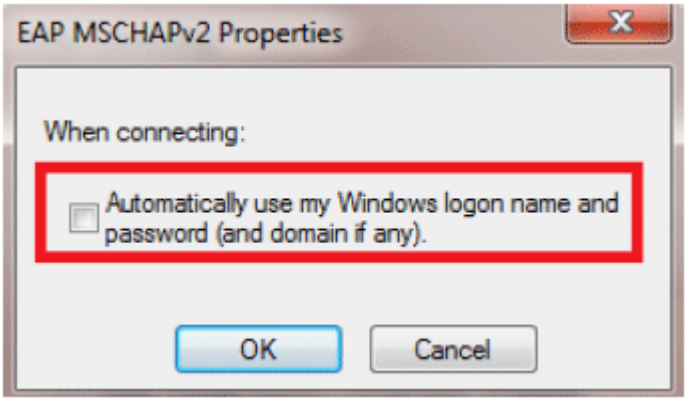

goa Wireless Network Properties
Connection
Security
Security type:
WPA2-Enterprise
Encryption type:
AES
Choose a network authentication method:
Microsoft: Protected EAP (PEAP)
Settings
Remember my credentials for this connection each time I'm logged on
Advanced settings
OK
Cancel



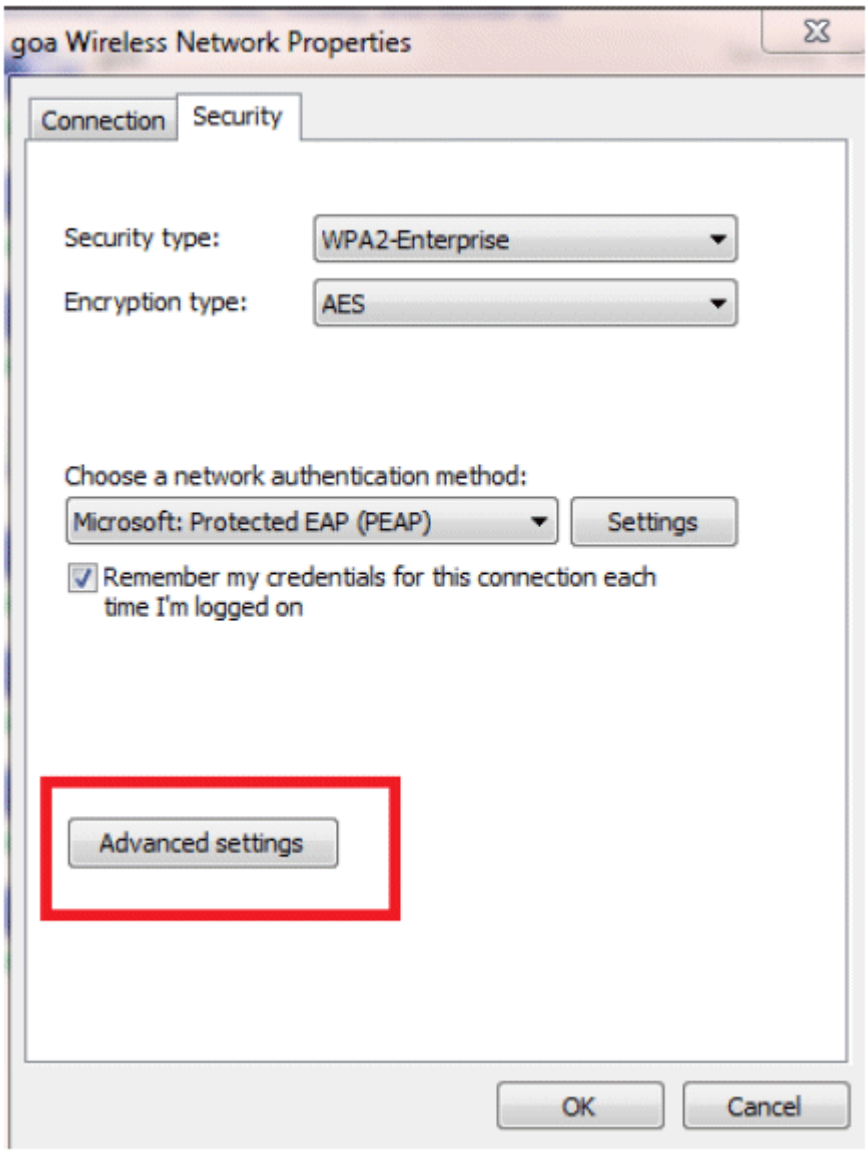
8. In diesem Beispiel wird das Serverzertifikat nicht validiert. Wenn Sie dieses Kontrollkästchen markieren und keine Verbindung herstellen können, deaktivieren Sie die Funktion, und testen Sie sie erneut.

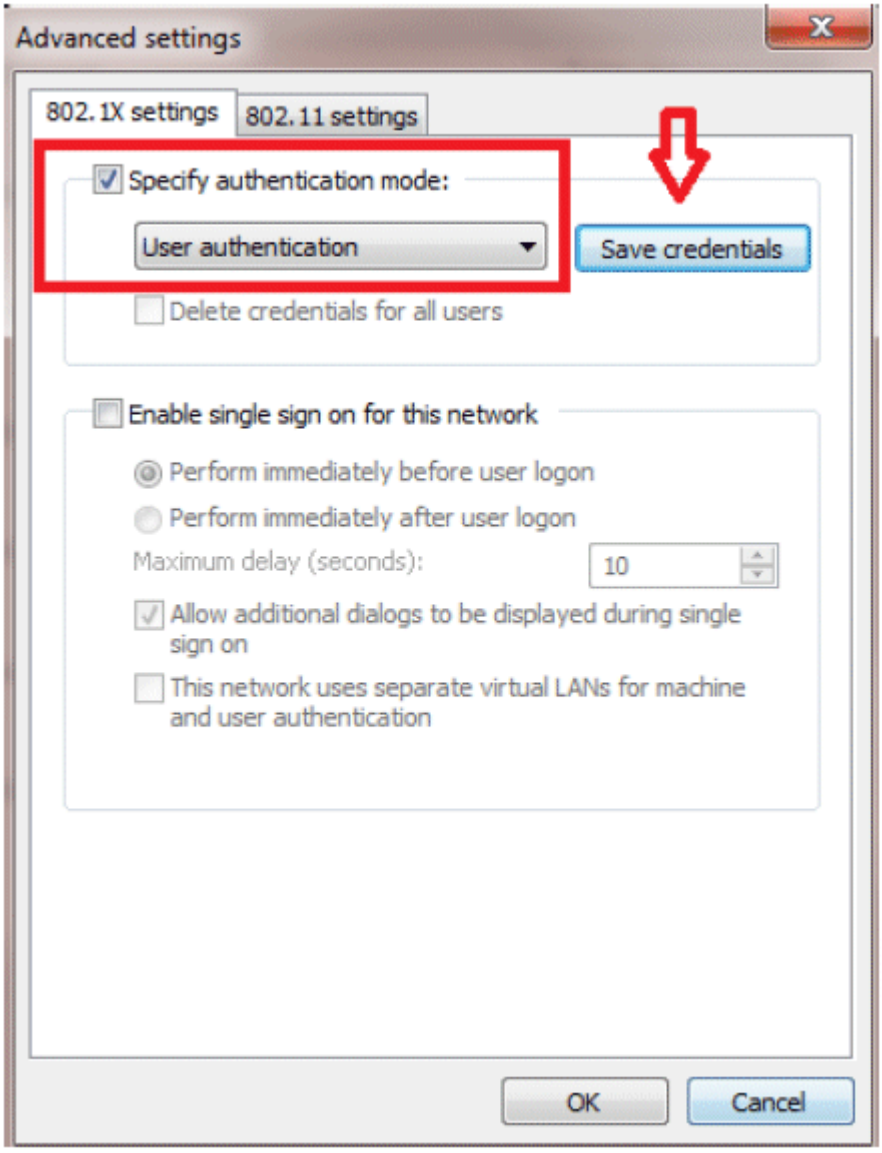


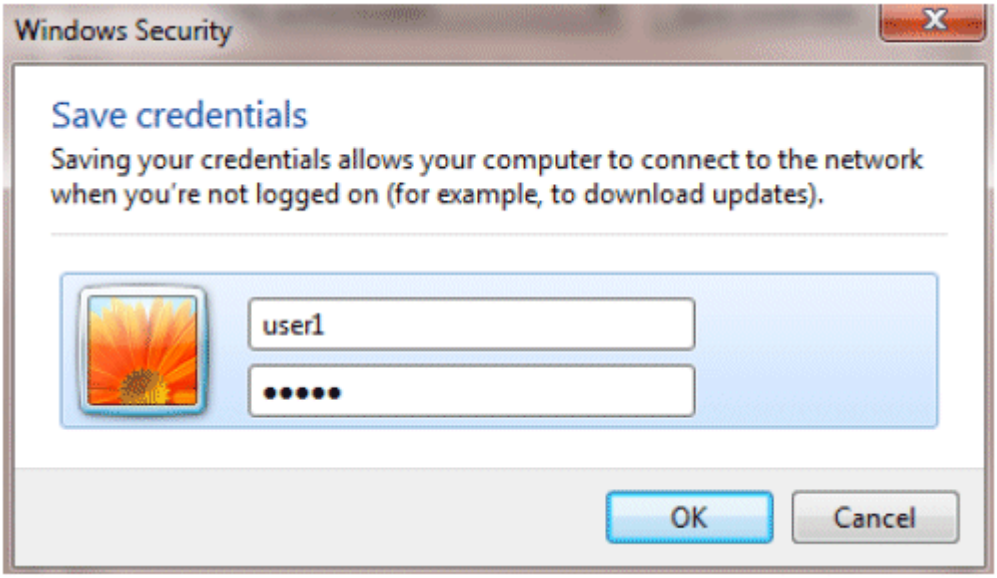
9. Alternativ können Sie Ihre Windows-Anmeldeinformationen verwenden, um sich anzumelden. In diesem Beispiel werden wir das jedoch nicht verwenden. Klicken Sie auf **OK**.



10. Klicken Sie auf **Erweiterte Einstellungen**, um Benutzername und Kennwort zu konfigurieren.


goa Wireless Network Properties
Connection
Security
Security type:
WPA2-Enterprise
Encryption type:
AES
Choose a network authentication method:
Microsoft: Protected EAP (PEAP)
Settings
Remember my credentials for this connection each time I'm logged on
Advanced settings
OK
Cancel





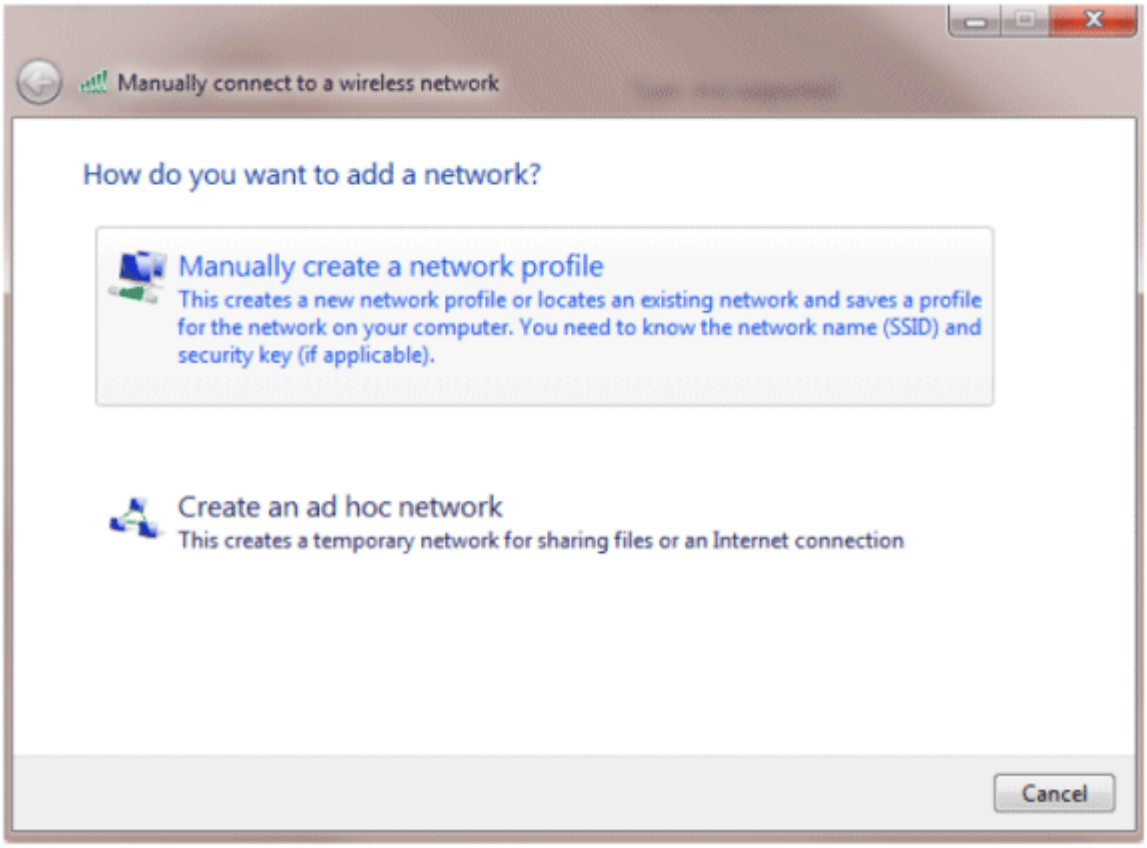
Das Client-Dienstprogramm kann jetzt eine Verbindung herstellen.

EAP-FAST (Benutzer 2)

In unserem Test-Client verwenden wir eine native Windows 7-Komponente mit einer Intel 6300-N-Karte, auf der die Treiberversion 14.3 ausgeführt wird. Es wird empfohlen, die neuesten Treiber von anderen Anbietern zu verwenden.

Gehen Sie wie folgt vor, um ein Profil in WZC zu erstellen:

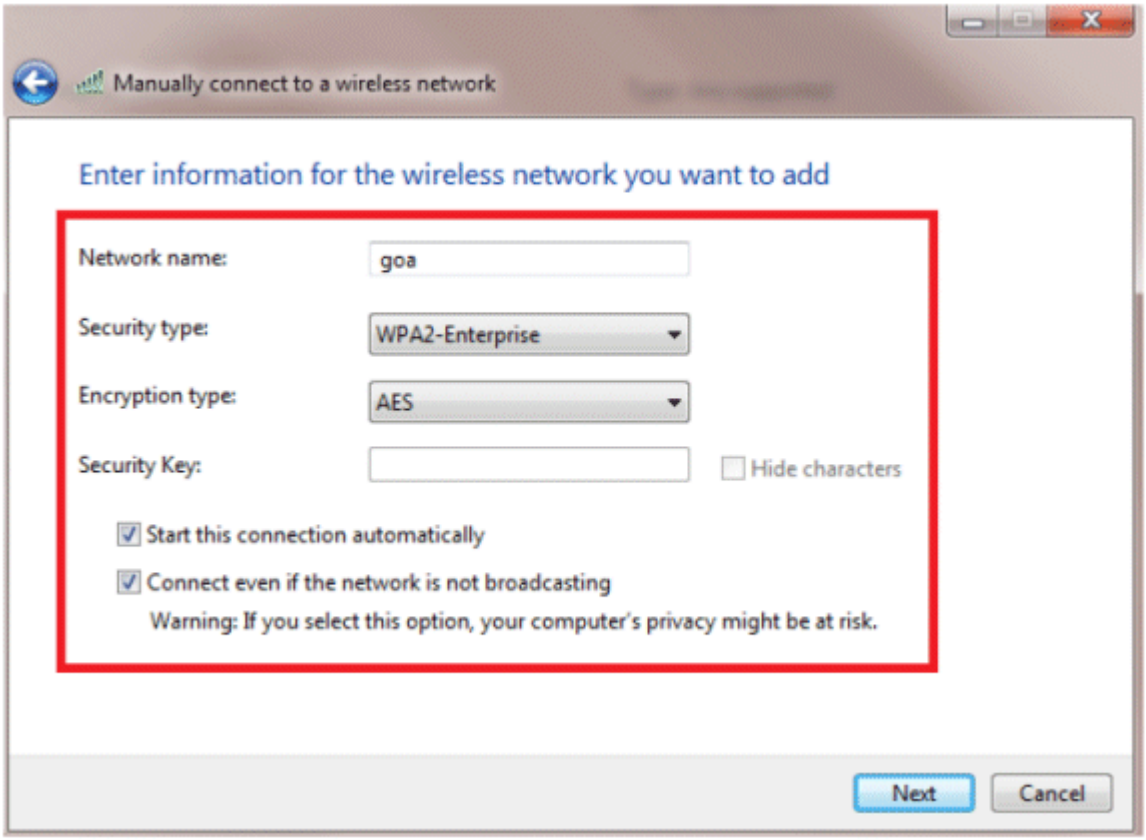
1. Gehen Sie zu **Systemsteuerung** > **Netzwerk und Internet** > **Drahtlose Netzwerke verwalten**.
2. Klicken Sie auf die Registerkarte **Hinzufügen**.
3. Klicken Sie auf **Netzwerkprofil manuell erstellen**.



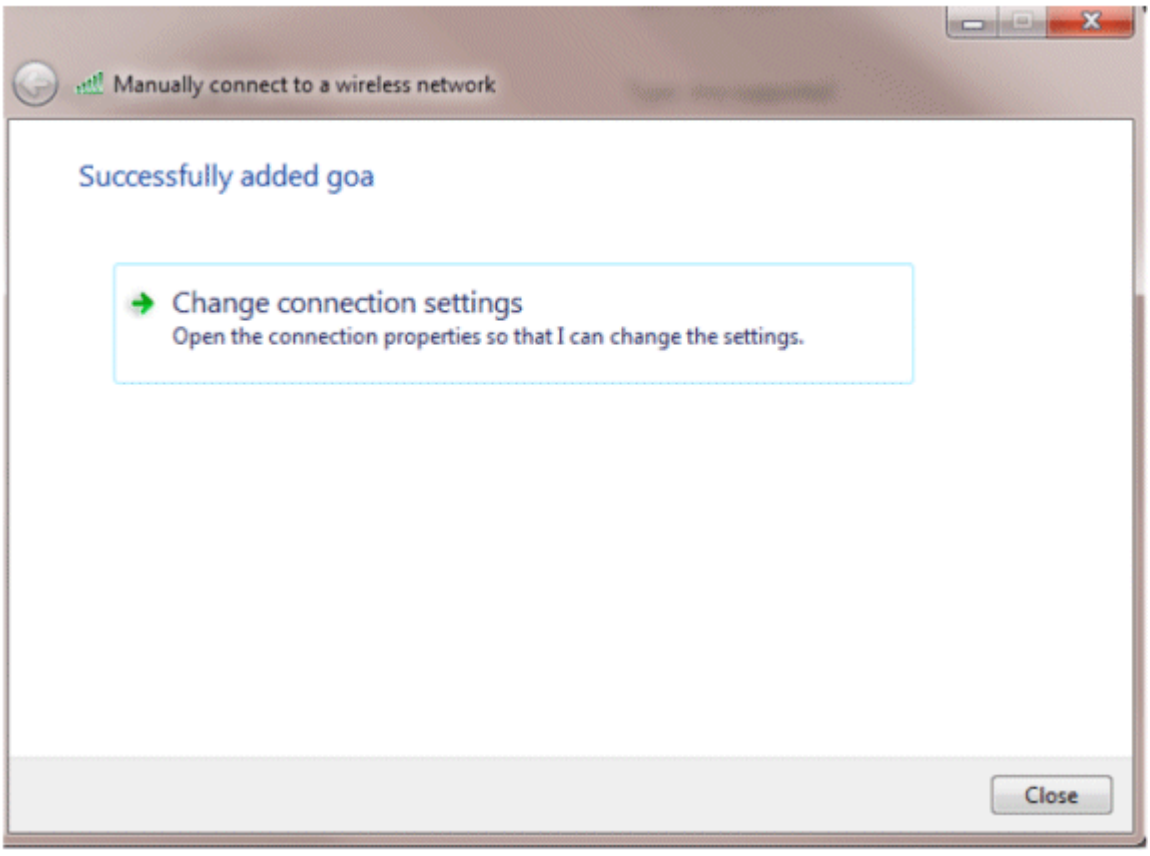
4. Fügen Sie die Details wie auf dem WLC konfiguriert hinzu.

   Hinweis: Bei der SSID wird zwischen Groß- und Kleinschreibung unterschieden.

5. Klicken Sie auf **Next** (Weiter).



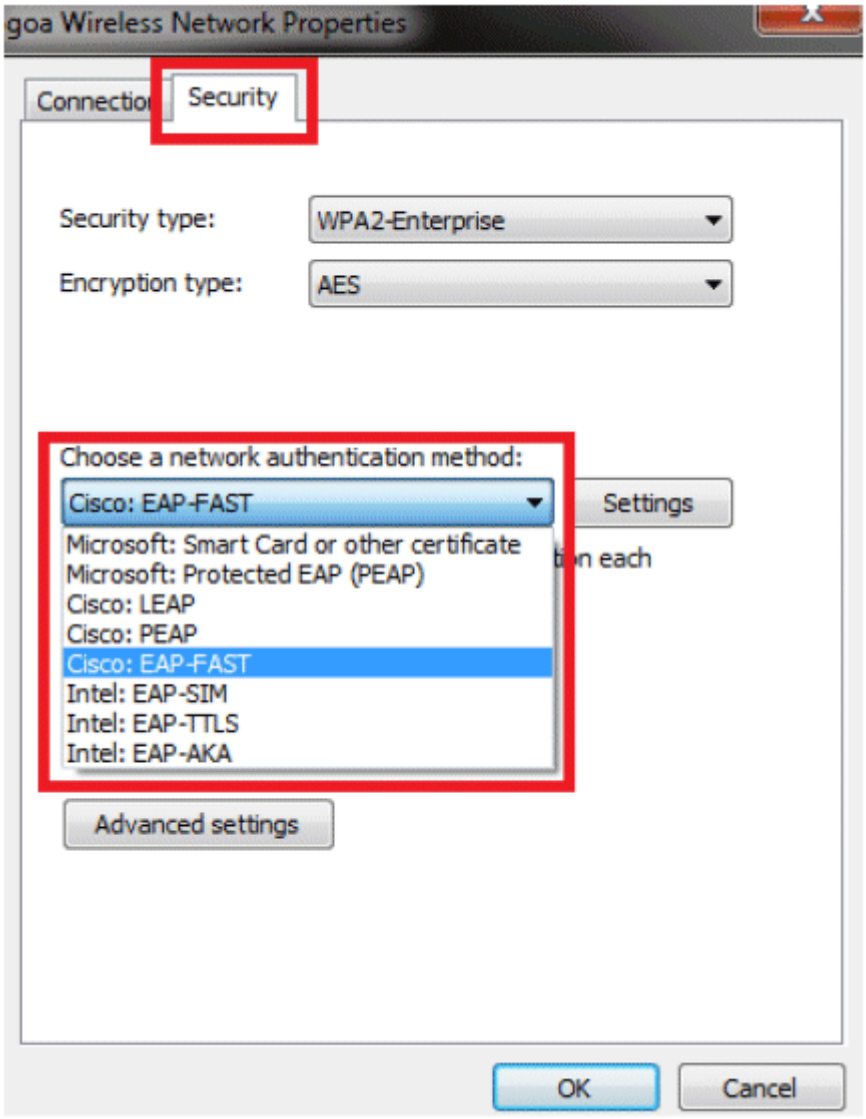
6. Klicken Sie auf **Verbindungseinstellungen ändern**, um die Einstellungen zu überprüfen.

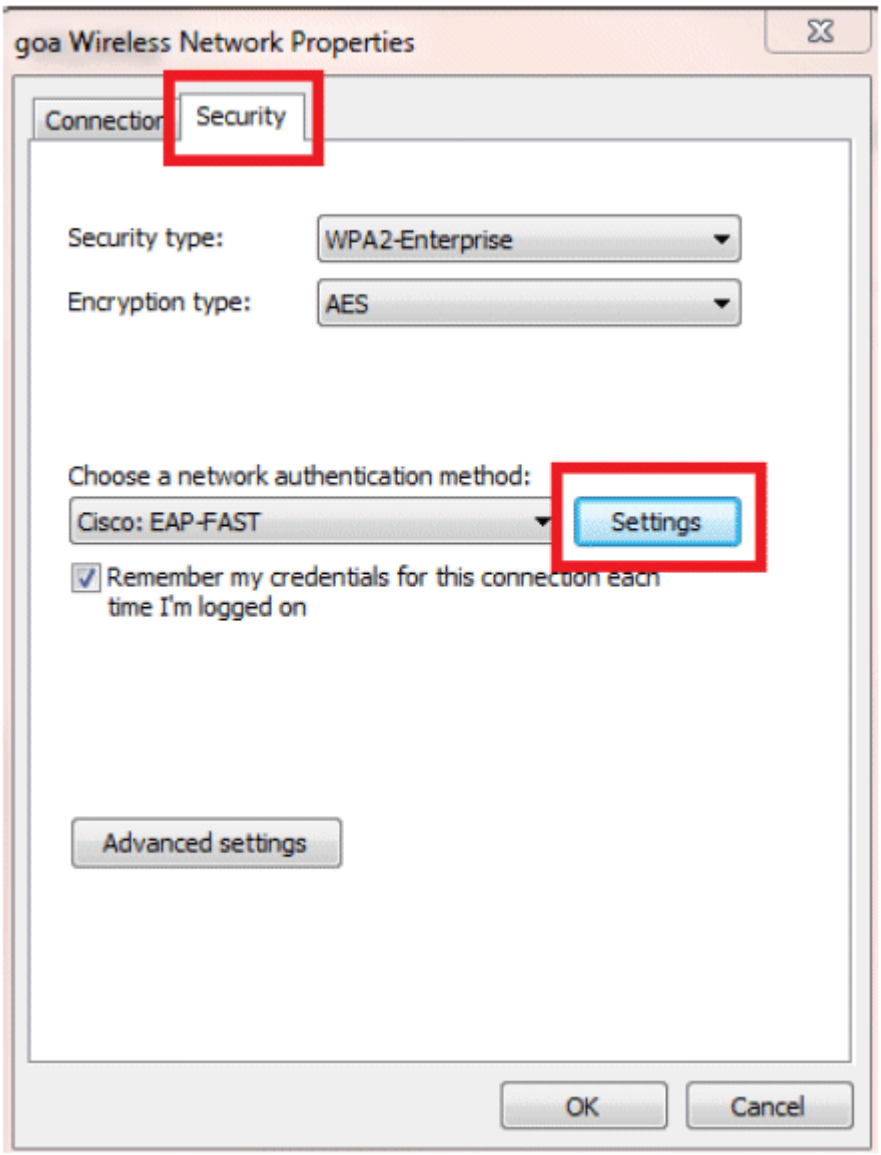


7. Stellen Sie sicher, dass EAP-FAST aktiviert ist.

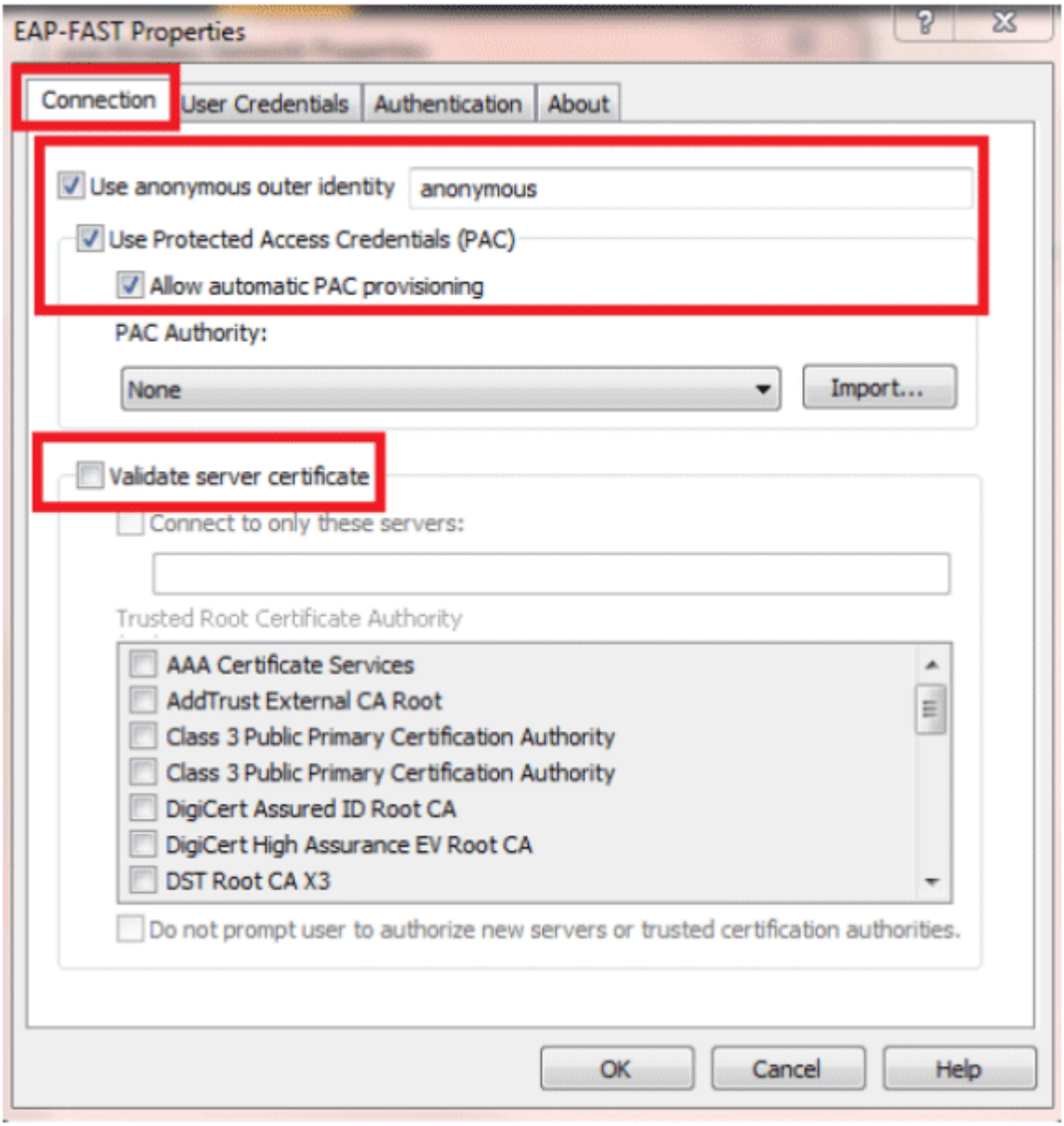
   Hinweis: Standardmäßig verfügt WZC nicht über EAP-FAST als Authentifizierungsmethode. Sie müssen das Dienstprogramm von einem Drittanbieter herunterladen. Da es sich in diesem Beispiel um

eine Intel-Karte handelt, ist Intel PROSet auf dem System installiert.

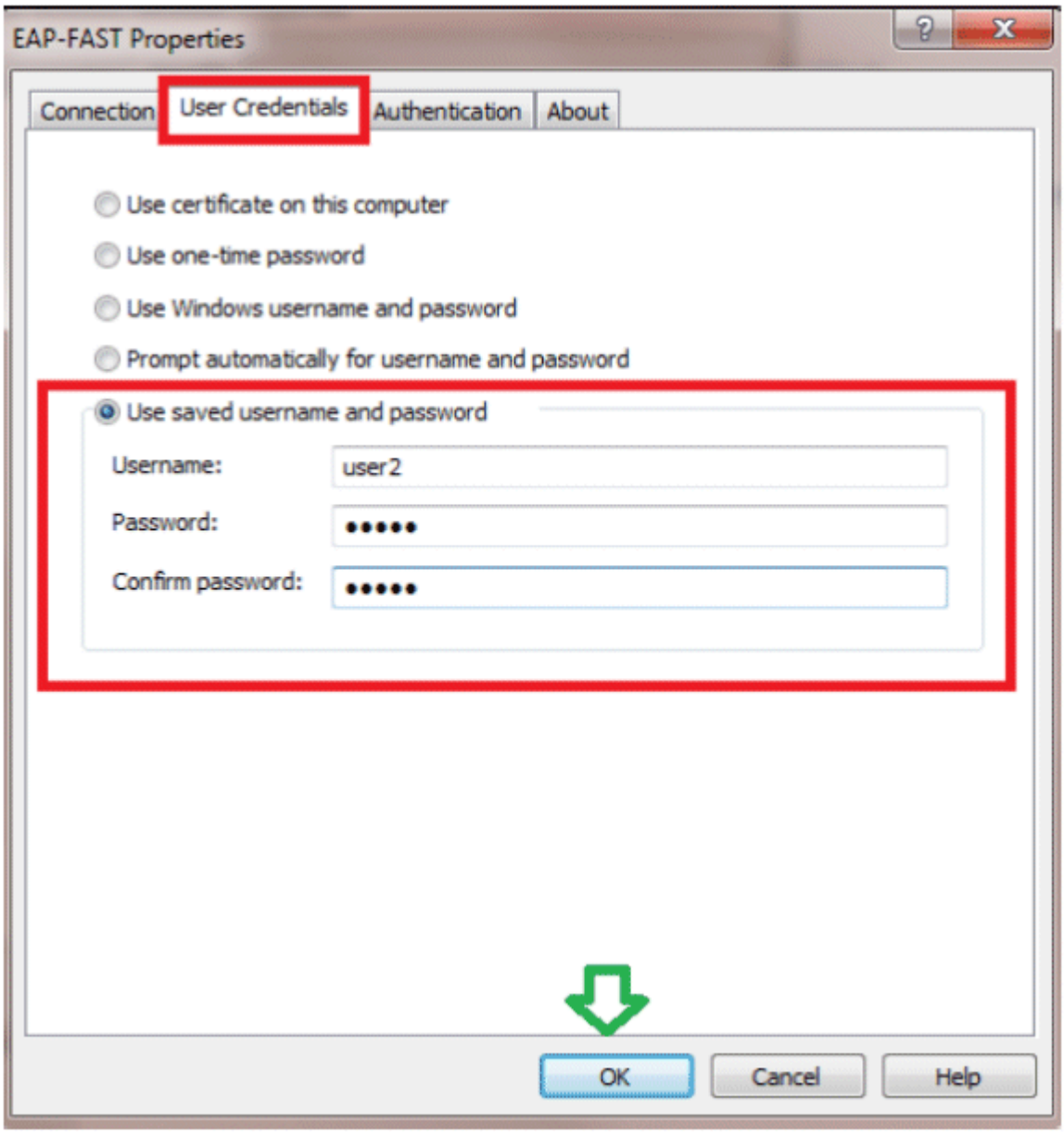




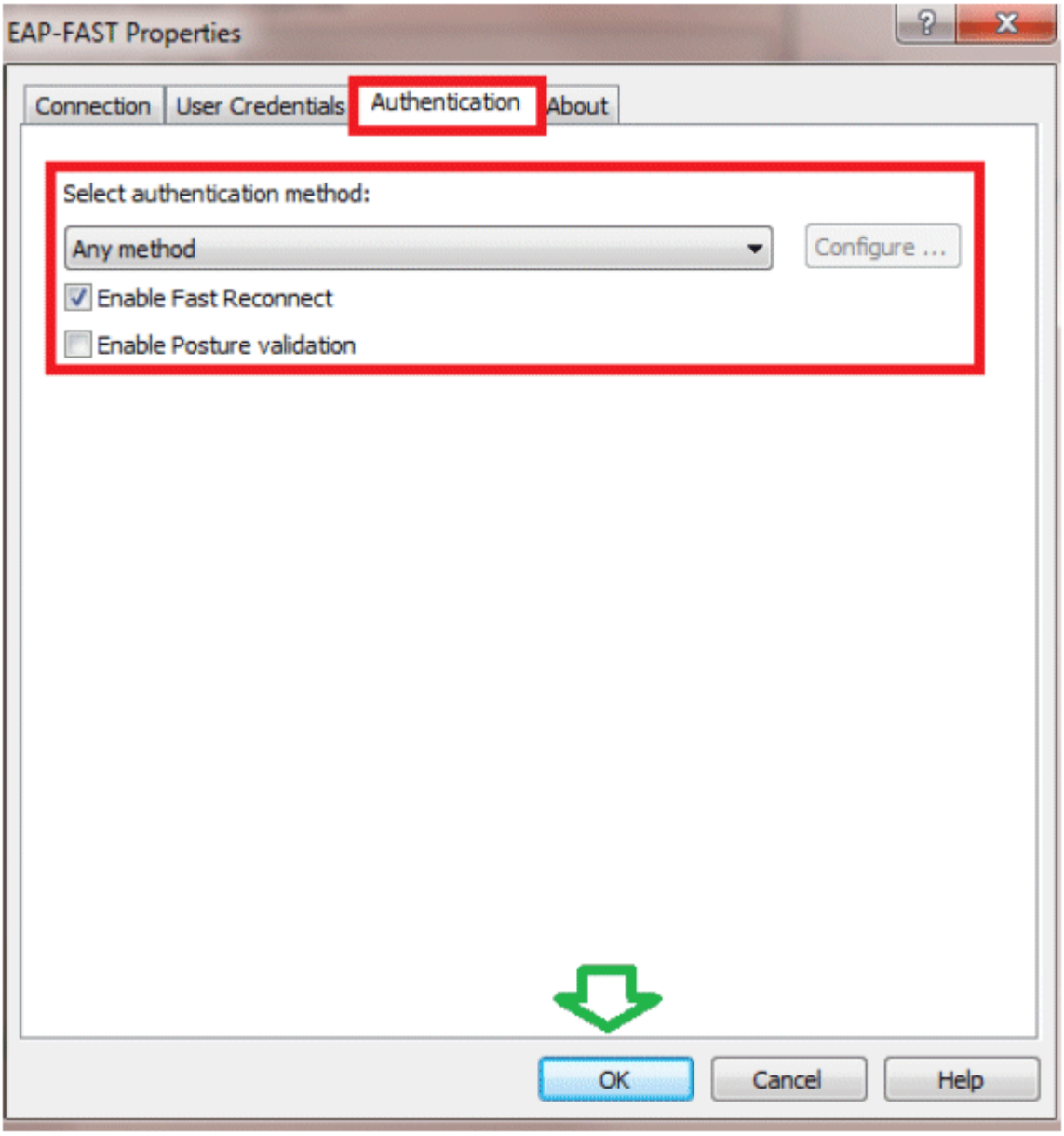
8. Aktivieren Sie die **automatische PAC-Bereitstellung zulassen**, und stellen Sie sicher, dass **Serverzertifikat validieren** deaktiviert ist.



9. Klicken Sie auf die Registerkarte **User Credentials** (Benutzeranmeldeinformationen), und geben Sie die Anmeldeinformationen für user2 ein. Alternativ können Sie Ihre Windows-Anmeldeinformationen verwenden, um sich anzumelden. In diesem Beispiel werden wir das jedoch nicht verwenden.

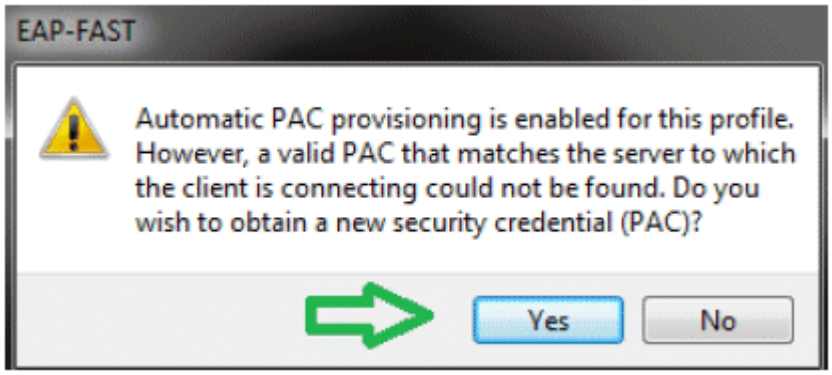


10. Klicken Sie auf **OK**.



Das Client-Dienstprogramm kann jetzt mit user2 verbunden werden.

Hinweis: Wenn user2 versucht, sich zu authentifizieren, sendet der RADIUS-Server eine PAC. Akzeptieren Sie die PAC, um die Authentifizierung abzuschließen.



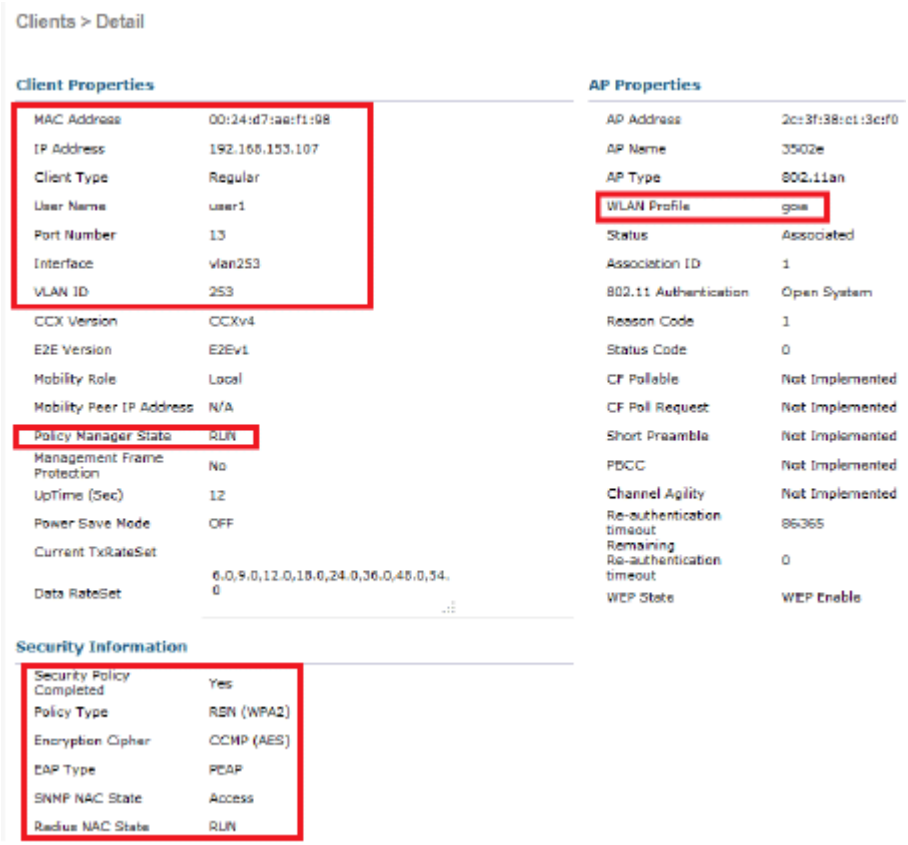
Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter-Tool (OIT) (nur registrierte Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **show**-Befehlsausgabe anzuzeigen.

Benutzer1 überprüfen (PEAP-MSCHAPv2)

Wählen Sie in der WLC-GUI **Monitor** > **Clients** aus, und wählen Sie die MAC-Adresse aus.



WLC RADIUS-Statistiken:

<#root>

```
(Cisco Controller) >
```

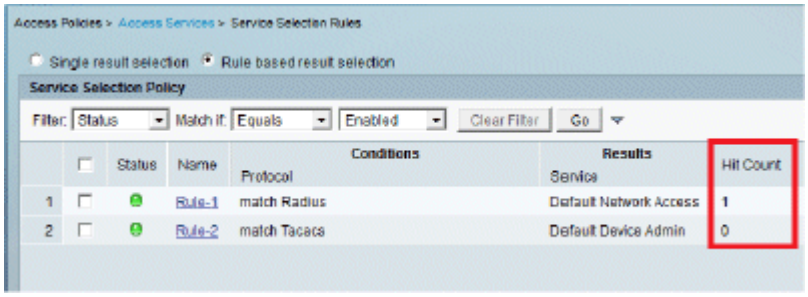
```
show radius auth statistics
```

```
Authentication Servers:
Server Index..................................... 1
Server Address................................... 192.168.150.24
Msg Round Trip Time.............................. 1 (msec)
First Requests................................... 8
Retry Requests................................... 0
Accept Responses................................. 1
Reject Responses................................. 0
Challenge Responses.............................. 7
Malformed Msgs................................... 0
Bad Authenticator Msgs........................... 0
Pending Requests................................. 0
Timeout Requests................................. 0
Unknowntype Msgs................................. 0
Other Drops...................................... 0
```

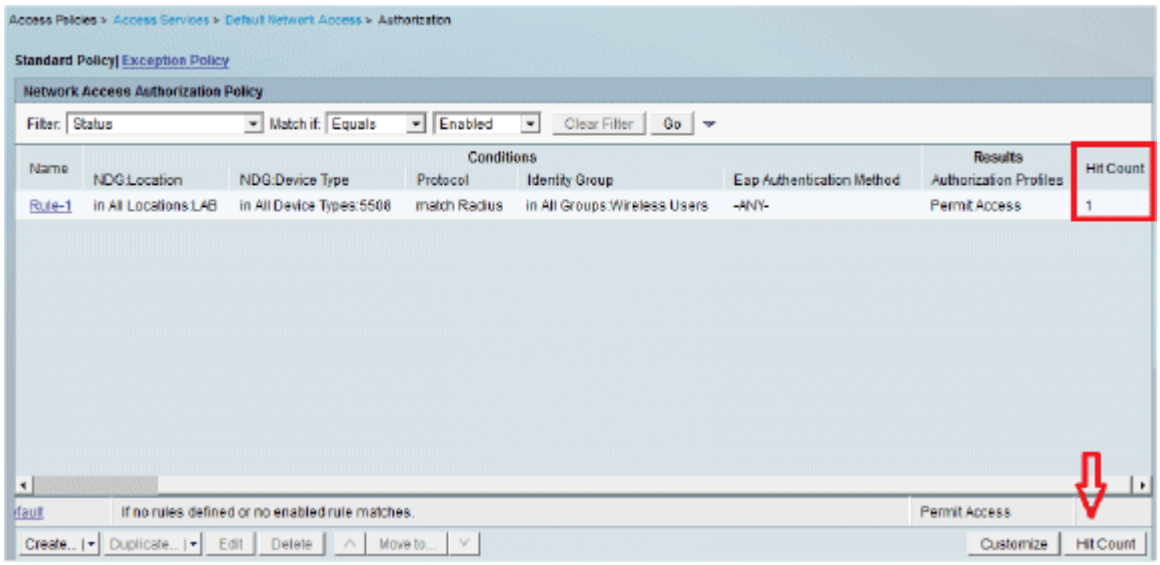
ACS-Protokolle:

1. Führen Sie die folgenden Schritte aus, um die Trefferzahlen anzuzeigen:

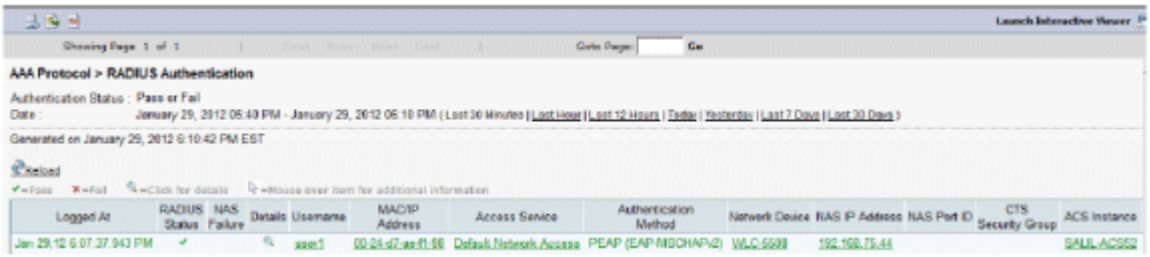
   a. Wenn Sie die Protokolle innerhalb von 15 Minuten nach der Authentifizierung überprüfen, stellen Sie sicher, dass Sie die Trefferanzahl aktualisieren.



   b. Sie haben unten auf derselben Seite eine Registerkarte für **Trefferanzahl**.



2. Klicken Sie auf **Überwachung und Berichte**, um das Popup-Fenster Neu zu öffnen. Gehen Sie zu **Authentifizierungen -Radius -Today**. Sie können auch auf **Details** klicken, um zu überprüfen, welche Serviceauswahlregel angewendet wurde.



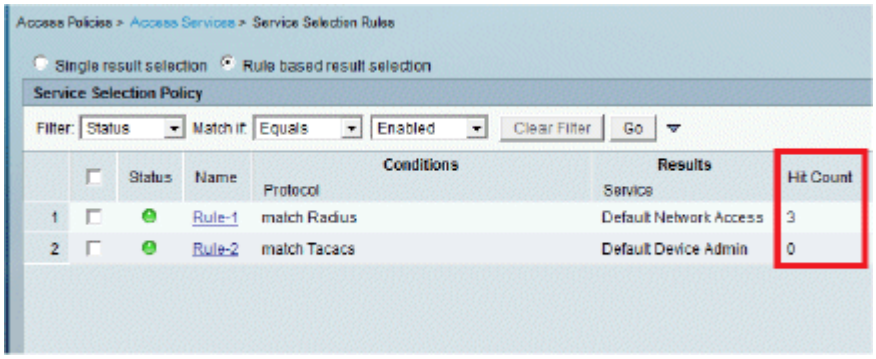
Überprüfung von Benutzer 2 (EAP-FAST)

Wählen Sie in der WLC-GUI **Monitor** > **Clients** aus, und wählen Sie die MAC-Adresse aus.

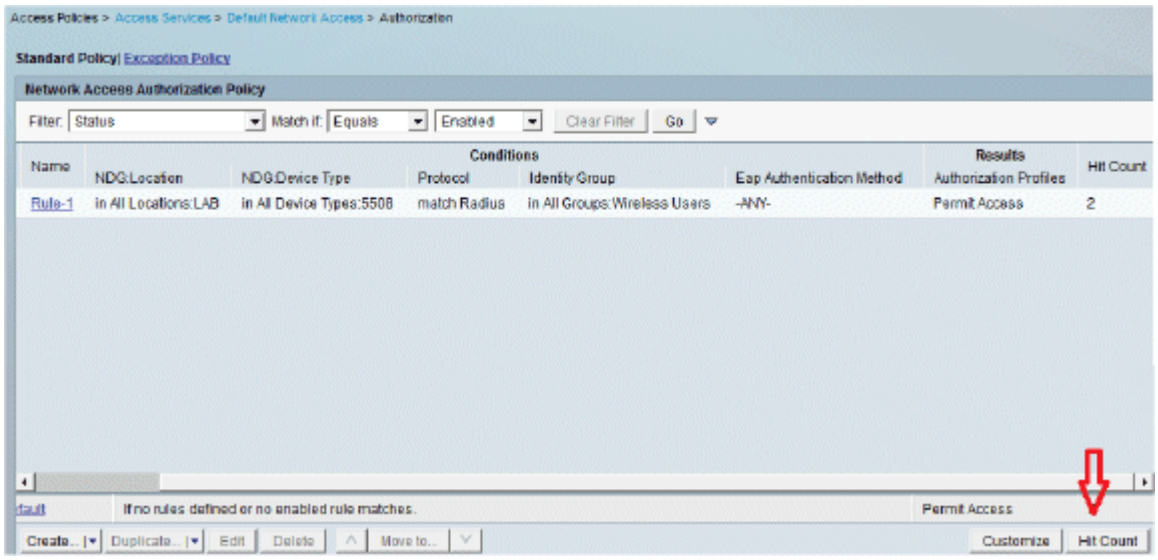
ACS-Protokolle:

1. Führen Sie die folgenden Schritte aus, um die Trefferzahlen anzuzeigen:

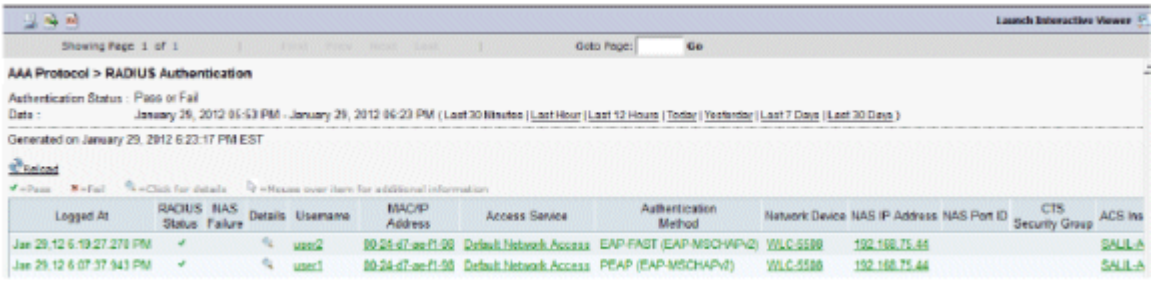
   a. Wenn Sie die Protokolle innerhalb von 15 Minuten nach der Authentifizierung überprüfen, stellen Sie sicher, dass Sie die HIT-Anzahl aktualisieren.



   b. Sie haben unten auf derselben Seite eine Registerkarte für **Trefferanzahl**.



2. Klicken Sie auf **Überwachung und Berichte**, um das Popup-Fenster Neu zu öffnen. Gehen Sie zu **Authentifizierungen -Radius -Today**. Sie können auch auf **Details** klicken, um zu überprüfen, welche Serviceauswahlregel angewendet wurde.



Fehlerbehebung

In diesem Abschnitt finden Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

Befehle für die Fehlerbehebung

Das Output Interpreter-Tool (OIT) (nur registrierte Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **show**-Befehlsausgabe anzuzeigen.

Hinweis: Lesen Sie Wichtige Informationen zu Debug-Befehlen, bevor Sie **Debug-**Befehle verwenden.

1. Wenn Probleme auftreten, geben Sie am WLC die folgenden Befehle ein:

   - **debug client** *<mac add of the client>*
   - **debug aaa all enable**
   - **show client detail** *<mac addr>* - Überprüfen Sie den Status des Richtlinien-Managers.
   - **show radius auth statistics**: Überprüfen Sie den Fehlergrund.
   - **debug disable-all** - Debug-Befehle deaktivieren.
   - **clear stats radius auth all** - Clear radius statistics on the WLC.

2. Überprüfen Sie die Protokolle im ACS, und notieren Sie den Fehlergrund.

Zugehörige Informationen

- **Technischer Support und Dokumentation für Cisco Systeme**

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.