Konfigurieren von MAC-Filtern mit Wireless LAN Controllern (WLCs)

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie MAC-Filter mit Wireless LAN-Controllern (WLCs) konfiguriert werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Konfiguration von LAPs und Cisco WLCs
- Cisco Unified Wireless Security-Lösungen

Verwendete Komponenten

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

- Cisco 4400 WLC mit Softwareversion 5.2.178.0

- Cisco Serie 1230AG - LAPs
- 802.11 a/b/g Wireless Client-Adapter mit Firmware 4.4
- Aironet Desktop Utility (ADU) Version 4.4

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 Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Konventionen

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

Hintergrundinformationen

In diesem Dokument wird anhand eines Konfigurationsbeispiels beschrieben, wie MAC-Filter mit Wireless LAN-Controllern (WLCs) konfiguriert werden. Außerdem wird in diesem Dokument das Autorisieren von Lightweight Access Points (LAPs) gegenüber einem AAA-Server beschrieben.

MAC-Adressfilter (MAC-Authentifizierung) auf WLCs

Wenn Sie einen MAC-Adressfilter auf WLCs erstellen, wird Benutzern der Zugriff auf das WLAN-Netzwerk basierend auf der MAC-Adresse des verwendeten Clients gewährt oder verweigert.

Es gibt zwei Arten der MAC-Authentifizierung, die von WLCs unterstützt werden:

- Lokale MAC-Authentifizierung
- Verwendung der MAC-Authentifizierung mit einem RADIUS-Server

Bei der lokalen MAC-Authentifizierung werden die MAC-Benutzeradressen in einer Datenbank auf dem WLC gespeichert. Wenn ein Benutzer versucht, auf das für die MAC-Filterung konfigurierte WLAN zuzugreifen, wird die MAC-Adresse des Clients anhand der lokalen Datenbank auf dem WLC überprüft, und der Client erhält bei erfolgreicher Authentifizierung Zugriff auf das WLAN.

Standardmäßig unterstützt die lokale WLC-Datenbank bis zu 512 Benutzereinträge.

Die lokale Benutzerdatenbank ist auf maximal 2048 Einträge beschränkt. Die lokale Datenbank speichert Einträge für die folgenden Elemente:

- Lokale Managementbenutzer, darunter Lobby-Botschafter
- Lokale Netzwerkbenutzer, einschließlich Gastbenutzer
- MAC-Filtereinträge
- Ausschlusslisteneinträge
- Einträge in der Zugriffspunkt-Autorisierungsliste

Alle diese Benutzertypen dürfen die konfigurierte Datenbankgröße nicht überschreiten.

Verwenden Sie den folgenden CLI-Befehl, um die lokale Datenbank zu erweitern:

```
<Cisco Controller>config database size ?
```

```
<count>        Enter the maximum number of entries (512-2048)
```

Alternativ kann die MAC-Adressauthentifizierung auch mit einem RADIUS-Server durchgeführt werden. Der einzige Unterschied besteht darin, dass die MAC-Adressdatenbank des Benutzers auf dem RADIUS-Server und nicht auf dem WLC gespeichert wird. Wenn eine Benutzerdatenbank auf einem RADIUS-Server gespeichert wird, leitet der WLC die MAC-Adresse des Clients zur Client-Validierung an den RADIUS-Server weiter. Anschließend überprüft der RADIUS-Server die MAC-Adresse anhand der vorhandenen Datenbank. Bei erfolgreicher Client-Authentifizierung erhält der Client Zugriff auf das WLAN. Jeder RADIUS-Server, der die MAC-Adressauthentifizierung unterstützt, kann verwendet werden.

Konfigurieren der lokalen MAC-Authentifizierung auf WLCs

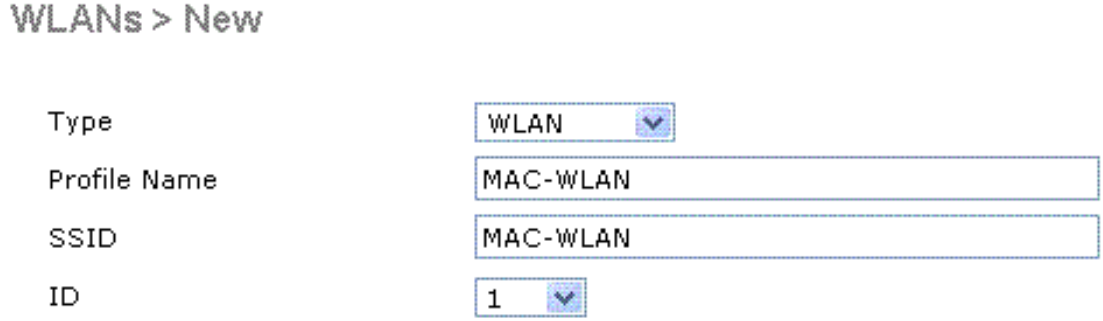
Lokale MAC-Authentifizierung auf den WLCs konfigurieren:

1. WLAN konfigurieren und MAC-Filterung aktivieren.
2. Konfigurieren Sie die lokale Datenbank auf dem WLC mit Client-MAC-Adressen.**Hinweis:** Vor der Konfiguration der MAC-Authentifizierung müssen Sie den WLC für den Basisbetrieb konfigurieren und die LAPs beim WLC registrieren. In diesem Dokument wird davon ausgegangen, dass der WLC bereits für den Basisbetrieb konfiguriert ist und dass die LAPs beim WLC registriert sind. Wenn Sie ein neuer Benutzer sind und versuchen möchten, den WLC für den Basisbetrieb mit LAPs einzurichten, finden Sie weitere Informationen unter Problembehandlung bei einem Lightweight AP, der einem WLC nicht beitritt.**Hinweis**: Es ist keine spezielle Konfiguration auf dem Wireless-Client erforderlich, um die MAC-Authentifizierung zu unterstützen.

WLAN konfigurieren und MAC-Filterung aktivieren

So konfigurieren Sie ein WLAN mit MAC-Filterung:

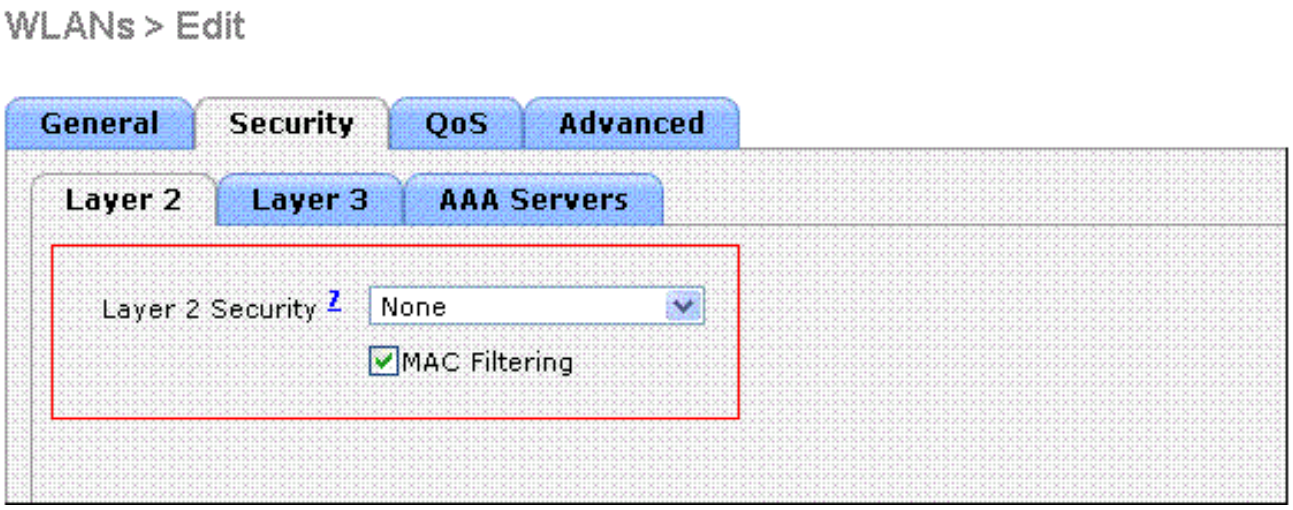
1. Klicken Sie in der Controller-GUI auf **WLANs**, um ein WLAN zu erstellen.Das Fenster WLANs wird angezeigt. In diesem Fenster werden die auf dem Controller konfigurierten WLANs aufgeführt.
2. Klicken Sie auf **Neu**, um ein neues WLAN zu konfigurieren.In diesem Beispiel heißt das WLAN *MAC-WLAN*, und die WLAN-ID ist
   1.



WLAN konfigurieren und MAC-Filterung aktivieren

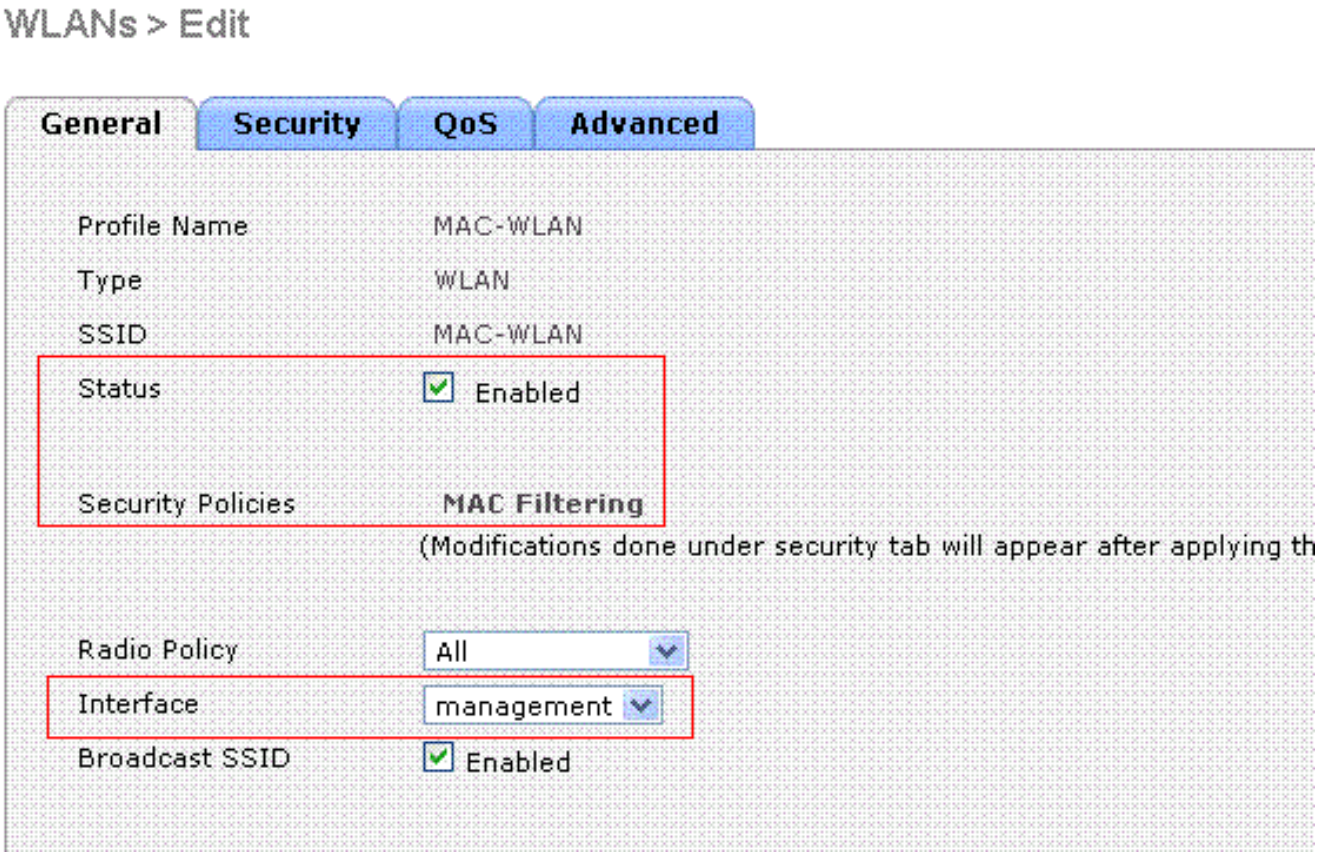
3. Klicken Sie auf Apply (Anwenden).
4. Definieren Sie im Fenster **WLANs > Edit** (WLANs > Bearbeiten) die WLAN-spezifischen

Parameter.



Parameter definieren

Aktivieren Sie unter **Security > Layer 2 > Layer 2 Security** Policies (Sicherheit > Layer 2-Sicherheitsrichtlinien) das Kontrollkästchen **MAC Filtering** (**MAC-Filterung**).Dadurch wird die MAC-Authentifizierung für das WLAN aktiviert.Wählen Sie unter **General (Allgemein)** > Interface name (Schnittstellenname) die Schnittstelle aus, der das WLAN zugeordnet ist.In diesem Beispiel ist das WLAN der Verwaltungsschnittstelle zugeordnet.Wählen Sie die anderen Parameter aus, die von den Designanforderungen des WLAN abhängen.Klicken Sie auf Apply
(Anwenden).



Schnittstelle zugeordnetes WLAN

Im nächsten Schritt wird die lokale Datenbank auf dem WLC mit den Client-MAC-Adressen konfiguriert.

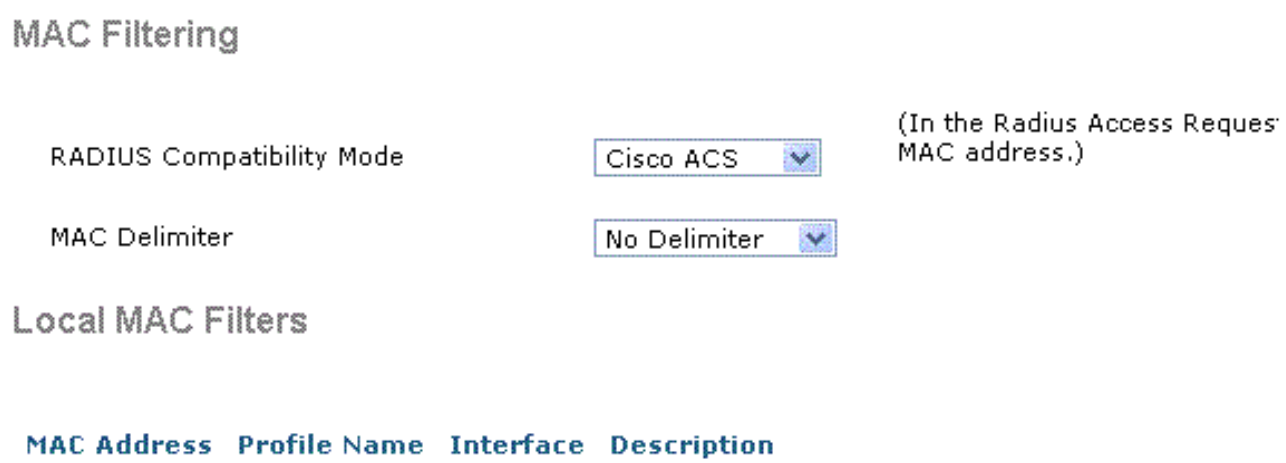
Weitere Informationen zur Konfiguration dynamischer Schnittstellen (VLANs) auf WLCs finden Sie

unter Konfigurationsbeispiel für VLANs auf Wireless LAN-Controllern.

Konfigurieren der lokalen Datenbank auf dem WLC mithilfe von Client-MAC-Adressen

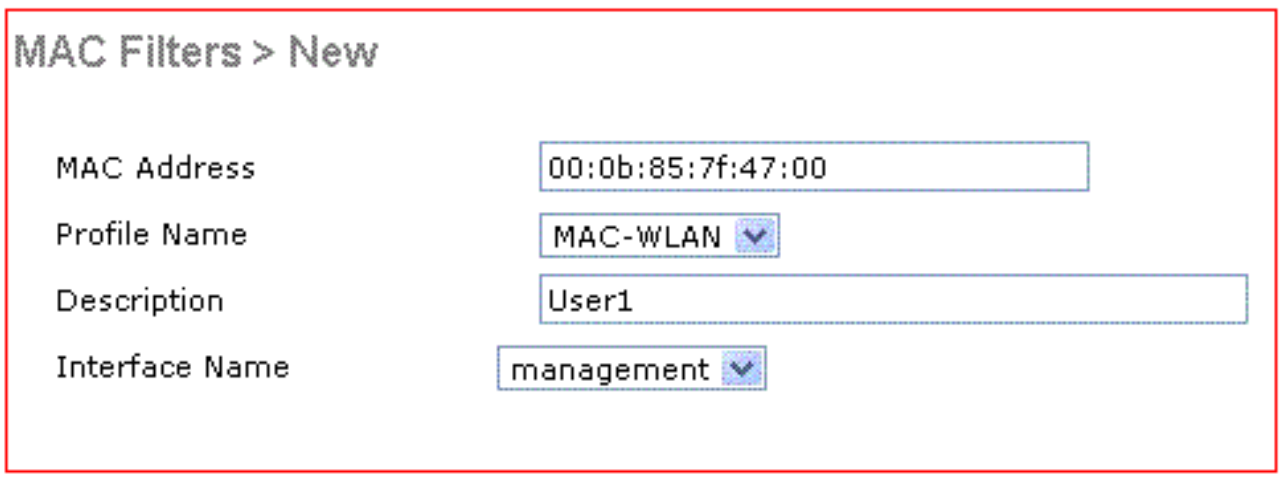
So konfigurieren Sie die lokale Datenbank mit einer Client-MAC-Adresse auf dem WLC:

1. Klicken Sie in der Controller-GUI auf **Sicherheit** und dann im Menü links auf **MAC Filtering** (**MAC-Filterung**).Das Fenster MAC Filtering (MAC-Filterung) wird angezeigt.



Fenster "MAC Filtering"

2. Klicken Sie auf **Neu**, um einen Eintrag für die lokale Datenbank-MAC-Adresse auf dem WLC zu erstellen.
3. Geben Sie im Fenster **MAC Filters > New (MAC-Filter > Neu)** die MAC-Adresse, den Profilnamen, die Beschreibung und den Schnittstellennamen für den Client ein.Hier ein Beispiel:



Erstellen einer lokalen Datenbank für eine MAC-Adresse

4. Klicken Sie auf Apply (Anwenden).
5. Wiederholen Sie die Schritte 2-4, um der lokalen Datenbank weitere Clients hinzuzufügen.Wenn Clients jetzt eine Verbindung mit diesem WLAN herstellen, überprüft der WLC die MAC-Adresse des Clients anhand der lokalen Datenbank. Wenn die Überprüfung erfolgreich ist, erhält der Client Zugriff auf das Netzwerk.**Hinweis**: In diesem Beispiel wurde nur ein MAC-Adressfilter ohne weiteren Layer-2-Sicherheitsmechanismus verwendet. Cisco empfiehlt, die Authentifizierung von MAC-Adressen zusammen mit anderen

Sicherheitsmethoden auf Layer 2 oder Layer 3 zu verwenden. Es ist nicht ratsam, zur Sicherung Ihres WLAN-Netzwerks nur die MAC-Adressauthentifizierung zu verwenden, da diese keinen leistungsstarken Sicherheitsmechanismus bietet.

Konfigurieren der MAC-Authentifizierung mit einem RADIUS-Server

Verwenden Sie diese Links, um die MAC-Authentifizierung mit einem RADIUS-Server zu konfigurieren. In diesem Beispiel wird der Cisco Secure ACS-Server als RADIUS-Server verwendet.

1. WLAN konfigurieren und MAC-Filterung aktivieren
2. Konfigurieren der Client-MAC-Adressen für den RADIUS-Server

WLAN konfigurieren und MAC-Filterung aktivieren

So konfigurieren Sie ein WLAN mit MAC-Filterung:

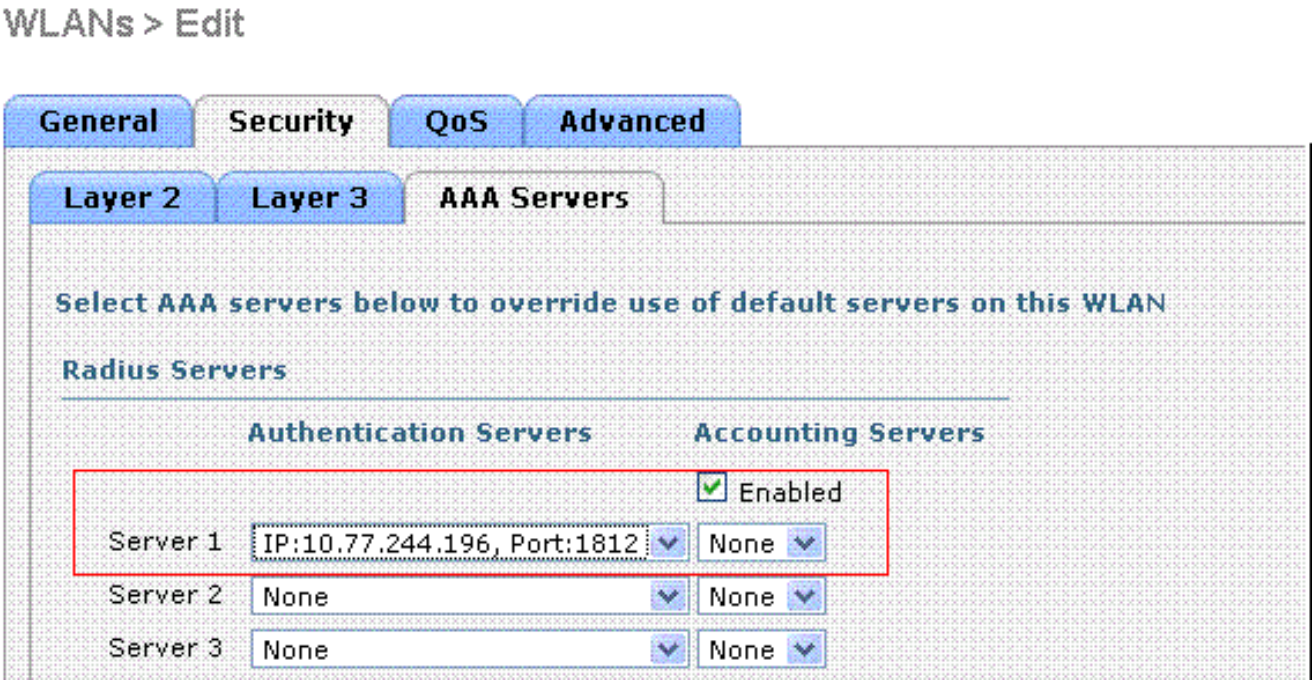
1. Klicken Sie in der Controller-GUI auf **WLANs**, um ein WLAN zu erstellen.Das Fenster WLANs wird angezeigt. In diesem Fenster werden die auf dem Controller konfigurierten WLANs aufgeführt.
2. Klicken Sie auf **Neu**, um ein neues WLAN zu konfigurieren.In diesem Beispiel hat das WLAN den Namen *MAC-ACS-WLAN*, und die WLAN-ID lautet

   WLANs > New

Type	WLAN
Profile Name	MAC-ACS-WLAN
SSID	MAC-ACS-WLAN
ID	2

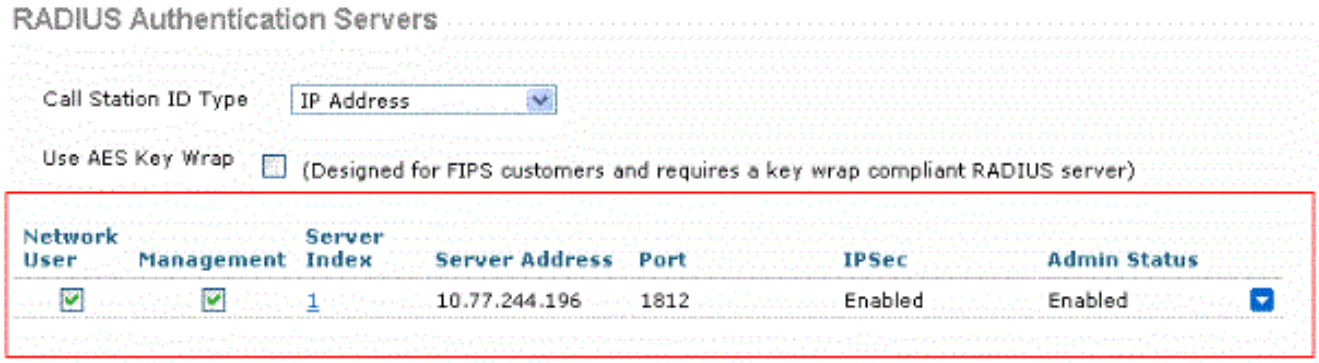
   2.

   Neues WLAN konfigurieren MAC-Filterung aktivieren
3. Klicken Sie auf **Apply (Anwenden).**
4. Definieren Sie im Fenster **WLANs > Edit** (WLANs > Bearbeiten) die WLAN-spezifischen Parameter.Aktivieren Sie unter **Security > Layer 2 > Layer 2 Security** Policies (Sicherheit > Layer **2**-Sicherheitsrichtlinien) das Kontrollkästchen **MAC Filtering** (**MAC-Filterung**).Dadurch wird die MAC-Authentifizierung für das WLAN aktiviert.Wählen Sie unter **General (Allgemein)** > Interface name (Schnittstellenname) die Schnittstelle aus, der das WLAN zugeordnet ist.Wählen Sie unter **Security > AAA Servers > RADIUS servers** (Sicherheit > AAA-Server > RADIUS-Server) den RADIUS-Server aus, der für die MAC-Authentifizierung verwendet werden
   kann.

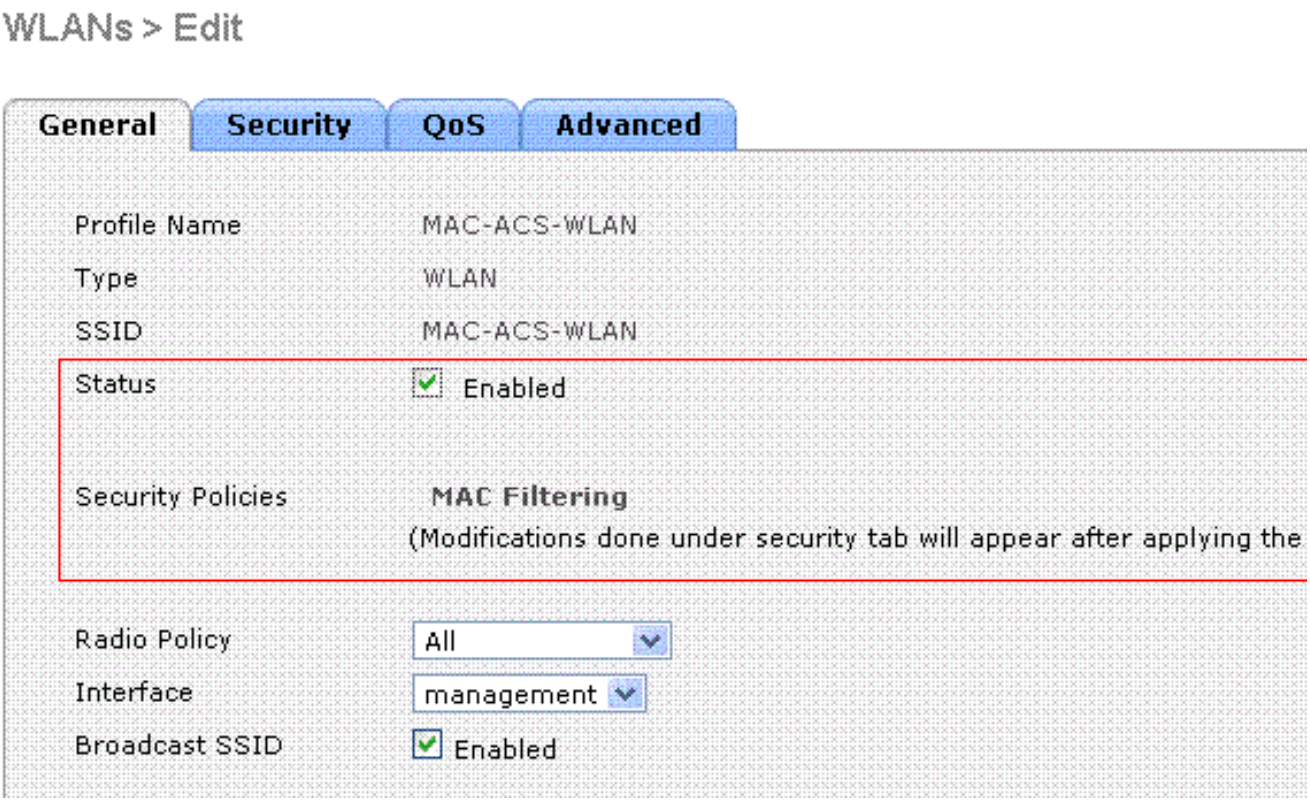


Wählen Sie den RADIUS-Server für die MAC-Authentifizierung aus.

Hinweis: Bevor Sie den RADIUS-Server im Fenster **WLAN > Edit (WLAN > Bearbeiten)** auswählen können, müssen Sie den RADIUS-Server im Fenster **Security > Radius Authentication (Sicherheit > RADIUS-Authentifizierung)** definieren und den RADIUS-Server aktivieren.

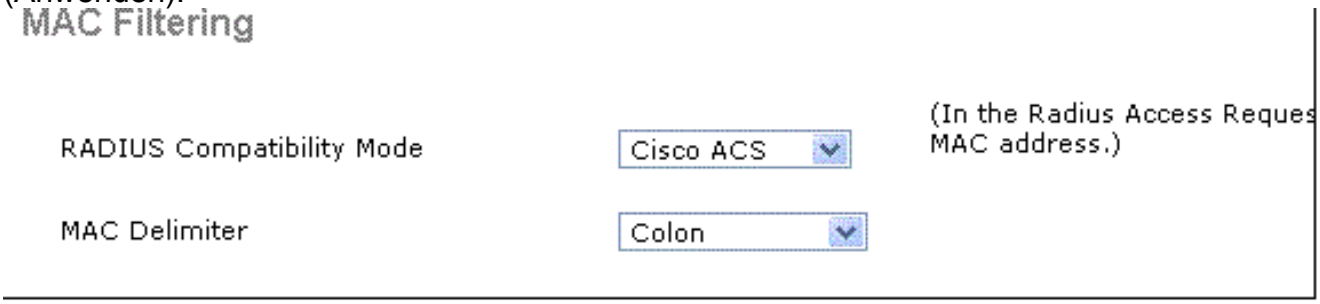


*Radius-Authentifizierungsserver*Wählen Sie die anderen Parameter aus, die von den Designanforderungen des WLAN abhängen.Klicken Sie auf **Apply (Anwenden).**



Design-Anforderungsparameter

5. Klicken Sie auf **Sicherheit > MAC-Filterung**.
6. Wählen Sie im Fenster MAC Filtering (MAC-Filterung) unter RADIUS Compatibility Mode (RADIUS-Kompatibilitätsmodus) den Typ des RADIUS-Servers aus.In diesem Beispiel wird **Cisco ACS** verwendet.
7. Wählen Sie im Pulldown-Menü "MAC Delimiter" das MAC Delimiter aus.In diesem Beispiel wird **Doppelpunkt** verwendet.
8. Klicken Sie auf Apply (Anwenden).



RADIUS-Servertyp auswählen

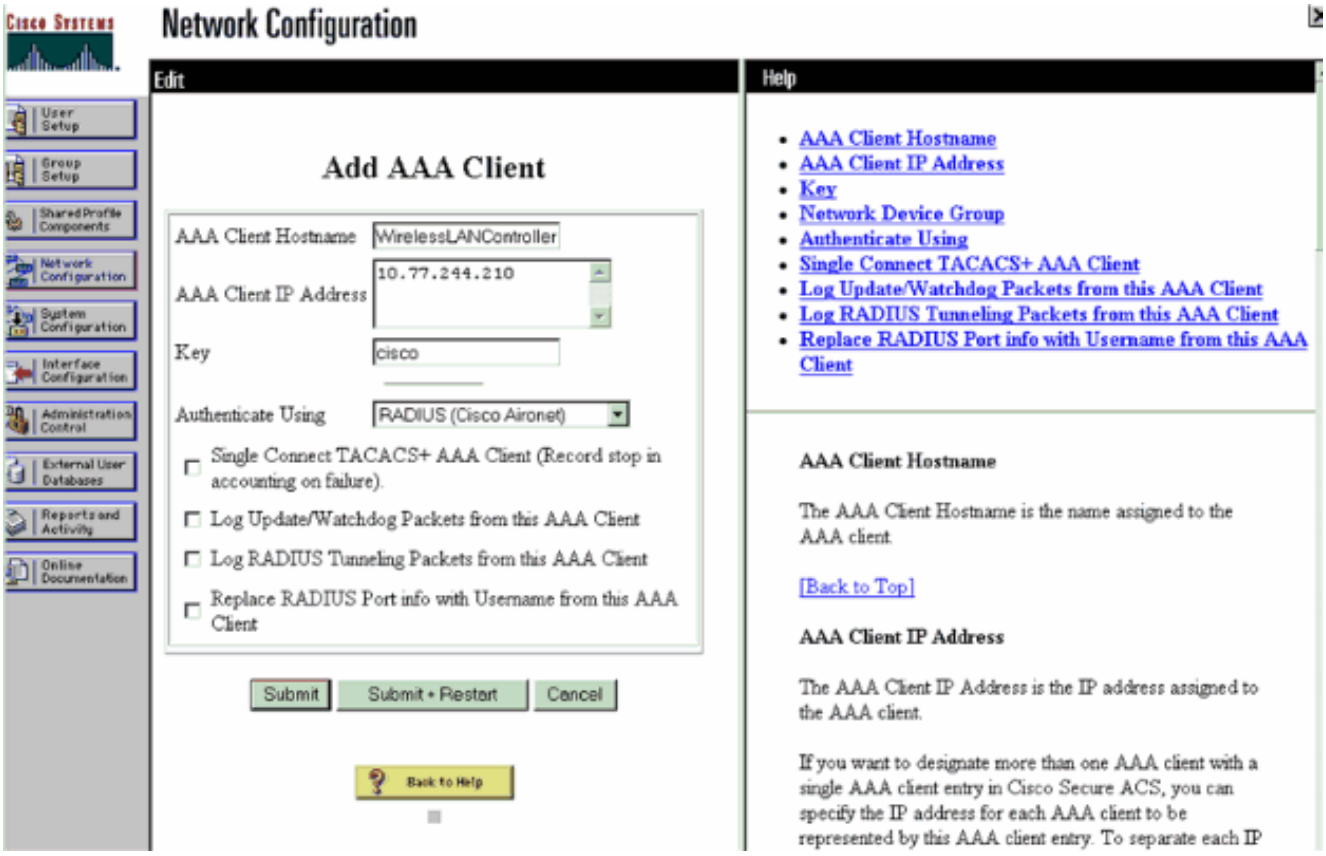
Im nächsten Schritt wird der ACS-Server mit den Client-MAC-Adressen konfiguriert.

Konfigurieren der Client-MAC-Adressen für den RADIUS-Server

So fügen Sie dem ACS eine MAC-Adresse hinzu:

1. Definieren des WLC als AAA-Client auf dem ACS-Server Klicken Sie in der ACS-GUI auf **Network Configuration**.
2. Wenn das Fenster Network Configuration (Netzwerkkonfiguration) angezeigt wird, definieren Sie den Namen des WLC, die IP-Adresse, den gemeinsamen geheimen Schlüssel und die Authentifizierungsmethode (RADIUS Cisco Aironet oder RADIUS Airrespace).Weitere Authentifizierungsserver, die nicht dem ACS angehören, finden Sie in der Dokumentation

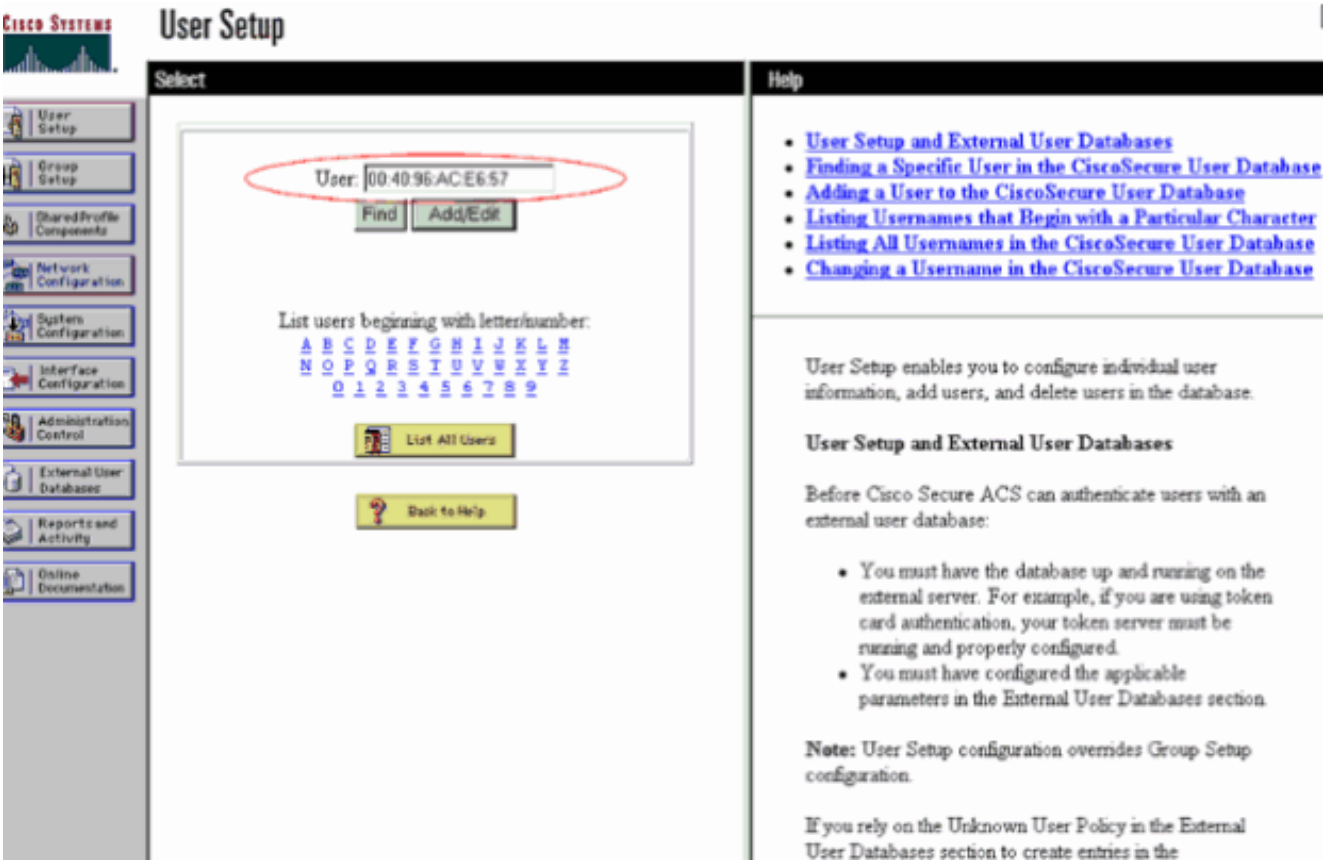
des
Herstellers.



AAA-Client hinzufügen

Hinweis: Der gemeinsam genutzte geheime Schlüssel, den Sie auf dem WLC konfigurieren, und der ACS-Server müssen übereinstimmen. Beim gemeinsamen geheimen Schlüssel wird zwischen Groß- und Kleinschreibung unterschieden.

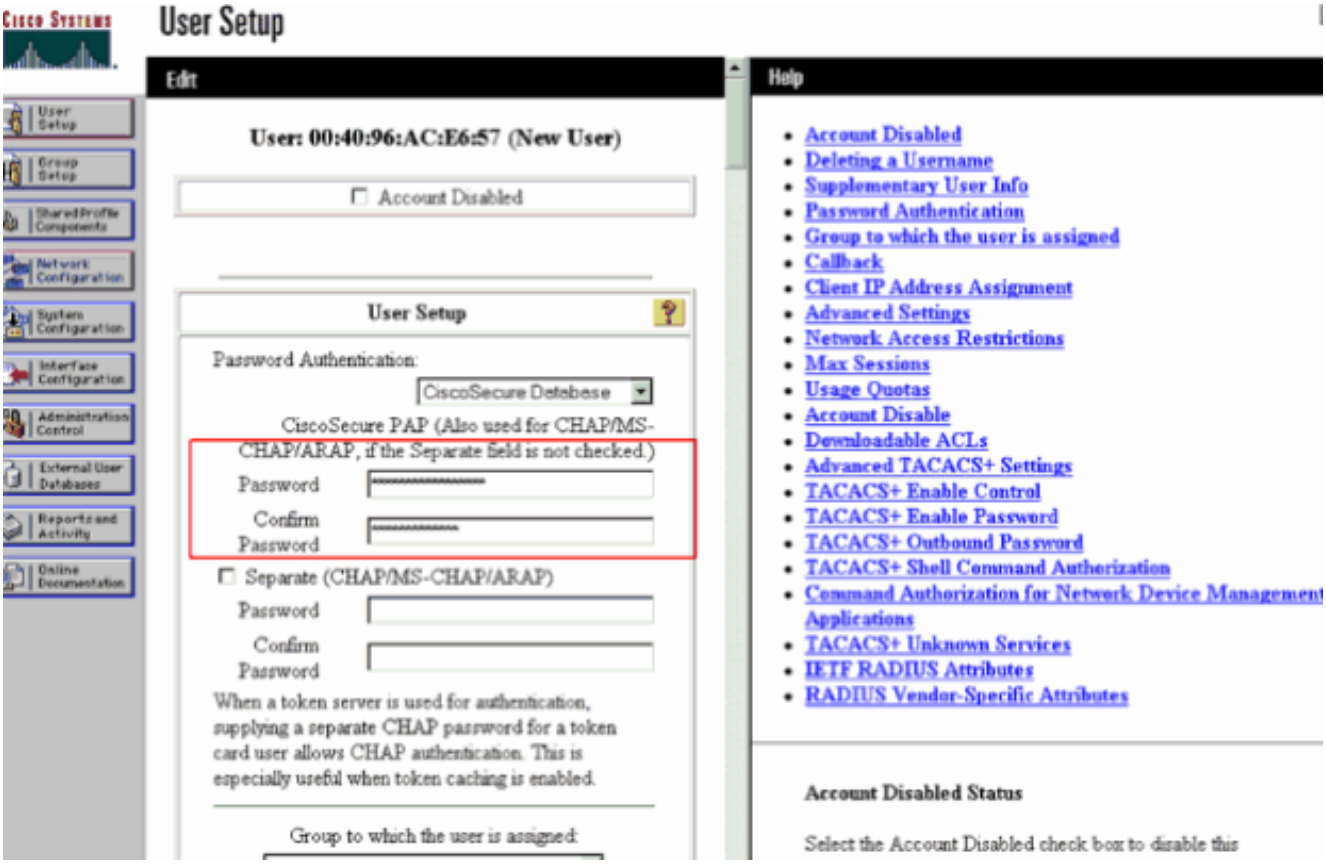
3. Klicken Sie im ACS-Hauptmenü auf **User Setup (Benutzereinrichtung)**.
4. Geben Sie im Textfeld User (Benutzer) die MAC-Adresse ein, um sie zur Benutzerdatenbank hinzuzufügen.



MAC-Adresse eingeben

Hinweis: Die MAC-Adresse muss mit der identisch sein, die der WLC für den Benutzernamen und das Kennwort sendet. Wenn die Authentifizierung fehlschlägt, überprüfen Sie das Protokoll der fehlgeschlagenen Versuche, um festzustellen, wie die MAC-Adresse vom WLC gemeldet wird. Schneiden Sie die MAC-Adresse nicht aus, und fügen Sie sie nicht ein, da dadurch Phantom-Zeichen eingefügt werden können.

5. Geben Sie im Fenster User Setup (Benutzereinrichtung) die MAC-Adresse in das Textfeld Secure-PAP Password (Sicheres PAP-Kennwort)
   ein.



Geben Sie die MAC-Adresse in das Feld für das sichere PAP-Kennwort ein.

Hinweis: Die MAC-Adresse muss mit der identisch sein, die der WLC für den Benutzernamen und das Kennwort sendet. Wenn die Authentifizierung fehlschlägt, überprüfen Sie das Protokoll der fehlgeschlagenen Versuche, um festzustellen, wie die MAC-Adresse vom Access Point gemeldet wird. Schneiden Sie die MAC-Adresse nicht aus, und fügen Sie sie nicht ein, da dadurch Phantom-Zeichen eingefügt werden können.

6. Klicken Sie auf **Senden**.
7. Wiederholen Sie die Schritte 2-5, um der ACS-Datenbank weitere Benutzer hinzuzufügen.Wenn Clients jetzt eine Verbindung mit diesem WLAN herstellen, übergibt der WLC die Anmeldeinformationen an den ACS-Server. Der ACS-Server überprüft die Anmeldeinformationen anhand der ACS-Datenbank. Wenn die Client-MAC-Adresse in der Datenbank vorhanden ist, gibt der ACS RADIUS-Server eine erfolgreiche Authentifizierung des WLC zurück, und der Client kann Zugriff auf das WLAN erhalten.

MAC-Filter für WLC über die CLI konfigurieren

In diesem Dokument wurde bereits die Verwendung der WLC-Benutzeroberfläche zum Konfigurieren von MAC-Filtern erläutert. Sie können die CLI auch verwenden, um MAC-Filter auf dem WLC zu konfigurieren. MAC-Filter auf dem WLC konfigurieren:

- Führen Sie den Befehl **config wlan mac-filters enable wlan_id** aus, um die MAC-Filterung zu aktivieren. Geben Sie den Befehl **show wlan** ein, um zu überprüfen, ob die MAC-Filterung für das WLAN aktiviert ist.
- **config macfilter add**-Befehl:Mit dem Befehl **config macfilter add** können Sie einen macfilter, eine Schnittstelle, eine Beschreibung usw. hinzufügen.Verwenden Sie den Befehl **config macfilter add**, um einen Eintrag für den MAC-Filter auf dem Cisco Wireless LAN-Controller zu erstellen. Mit diesem Befehl können Sie einem Wireless LAN auf dem Cisco Wireless LAN Controller lokal einen Client hinzufügen. Dieser Filter umgeht den RADIUS-

Authentifizierungsprozess.

```
config macfilter add  <MAC_address> <WLAN_id> <Interface_name> <description> <IP_address>
```

BeispielGeben Sie eine statische MAC-IP-Adresszuordnung ein. Auf diese Weise kann ein *passiver Client* unterstützt werden, der kein DHCP verwendet und keine unerwünschten IP-Pakete überträgt.

```
(Cisco Controller) >config macfilter add 00:E0:77:31:A3:55 1 lab02 "labconnect" 10.92.125.51
```

- **config macfilter ip-address-**BefehlMit dem Befehl **config macfilter ip-address** können Sie einen MAC-Filter einer IP-Adresse zuordnen. Verwenden Sie diesen Befehl, um eine IP-Adresse in der lokalen MAC-Filter-Datenbank zu konfigurieren:

  ```
  config macfilter ip-address <MAC_address> <IP_address>
  ```

  Beispiel

  ```
  (Cisco Controller) >config macfilter ip-address 00:E0:77:31:A3:55 10.92.125.51
  ```

Konfigurieren eines Timeouts für deaktivierte Clients

Sie können eine Zeitüberschreitung für deaktivierte Clients konfigurieren. Clients, die sich bei Zuordnungsversuchen dreimal nicht authentifizieren können, werden automatisch von weiteren Zuordnungsversuchen abgeschnitten. Nach Ablauf der Zeitüberschreitung kann der Client die Authentifizierung erneut versuchen, bis er eine Verbindung herstellt oder die Authentifizierung versagt, und er wird wieder ausgeschlossen. Geben Sie den Befehl **config wlan exclusionlist wlan_id timeout** ein, um die Zeitüberschreitung für deaktivierte Clients zu konfigurieren. Der Timeoutwert kann zwischen 1 und 65535 Sekunden liegen, oder Sie können 0 eingeben, um den Client dauerhaft zu deaktivieren.

Überprüfung

So überprüfen Sie, ob der MAC-Filter richtig konfiguriert ist:

- **show macfilter summary**: Zeigt eine Zusammenfassung aller MAC-Filtereinträge an.
- **show macfilter detail <MAC-Adresse des Clients>** - Detaillierte Anzeige eines MAC-Filtereintrags

Hier ist ein Beispiel für den Befehl **show macfilter summary**:

```
(Cisco Controller) >show macfilter summary

MAC Filter RADIUS Compatibility mode..... Cisco ACS
MAC Filter Delimiter..................... None

Local Mac Filter Table

MAC Address               WLAN Id          Description
-----------------------   --------------   --------------------------------
00:40:96:ac:e6:57           1              Guest


(Cisco Controller) >
```

Hier ist ein Beispiel für die **show macfilter** detailcommand:

```
(Cisco Controller) >show macfilter detail 00:40:96:ac:e6:57

MAC Address..................................... 00:40:96:ac:e6:57
WLAN Identifier................................. 1
```

```
Interface Name................................ mac-client
Description................................... Guest
```

Fehlerbehebung

Sie können die folgenden Befehle verwenden, um Probleme mit Ihrer Konfiguration zu beheben:

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

- **debug aaa all enable**: Ermöglicht das Debuggen aller AAA-Meldungen.
- **debug mac addr <Client-MAC-Adresse xx:xx:xx:xx:xx:xx>** - Verwenden Sie **den Befehl** debug mcommand, um das MAC-Debugging zu konfigurieren.

Hier ist ein Beispiel für den Befehl **debug aaa all enable**:

```
Wed May 23 11:13:55 2007: Looking up local blacklist 004096ace657
Wed May 23 11:13:55 2007: Looking up local blacklist 004096ace657
Wed May 23 11:13:55 2007: User 004096ace657 authenticated
Wed May 23 11:13:55 2007: 00:40:96:ac:e6:57 Returning AAA Error 'Success' (0)
                          for mobile 00:40:96:ac:e6:57
Wed May 23 11:13:55 2007: AuthorizationResponse: 0xbadff97c
Wed May 23 11:13:55 2007: structureSize.............................76
Wed May 23 11:13:55 2007: resultCode...............................0
Wed May 23 11:13:55 2007: protocolUsed.............................0x00000008
Wed May 23 11:13:55 2007: proxyState................................
                               00:40:96:AC:E6:57-00:00
Wed May 23 11:13:55 2007: Packet contains 2 AVPs:
Wed May 23 11:13:55 2007:     AVP[01] Service-Type..........................
                                    0x0000000a (10) (4 bytes)
Wed May 23 11:13:55 2007:     AVP[02] Airespace / Interface-Name.............
                                    staff-vlan (10 bytes)
Wed May 23 11:13:55 2007: 00:40:96:ac:e6:57 processing avps[0]: attribute 6
Wed May 23 11:13:55 2007: 00:40:96:ac:e6:57 processing avps[1]: attribute 5
Wed May 23 11:13:55 2007: 00:40:96:ac:e6:57 Applying new AAA override for
                          station 00:40:96:ac:e6:57
Wed May 23 11:13:55 2007: 00:40:96:ac:e6:57 Override values for station 00:40:96:ac:e6:57
source: 2, valid bits: 0x200 qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff,
sessionTimeout: -1dataAvgC: -1, rTAvgC: -1, dataBurstC:

-1, rTimeBurstC: -1vlanIfName: 'mac-client'
```

Wenn ein Wireless-Client nicht in der MAC-Adressdatenbank auf dem WLC (lokale Datenbank) vorhanden ist oder der RADIUS-Server versucht, eine Verbindung mit dem WLAN herzustellen, kann dieser Client ausgeschlossen werden. Das folgende Beispiel zeigt den Befehl **debug aaa all enable** für eine fehlgeschlagene MAC-Authentifizierung:

```
Wed May 23 11:05:06 2007: Unable to find requested user entry for 004096ace657
Wed May 23 11:05:06 2007: AuthenticationRequest: 0xa620e50
Wed May 23 11:05:06 2007: Callback.....................................0x807e724
Wed May 23 11:05:06 2007: protocolType.................................0x00000001
Wed May 23 11:05:06 2007: proxyState................................
                               00:40:96:AC:E6:57-00:00
Wed May 23 11:05:06 2007: Packet contains 14 AVPs (not shown)
Wed May 23 11:05:06 2007: 00:40:96:ac:e6:57 Returning AAA Error 'No Server' (-7)
                          for mobile 00:40:96:ac:e6:57
Wed May 23 11:05:06 2007: AuthorizationResponse: 0xbadff7e4
Wed May 23 11:05:06 2007: structureSize.............................28
Wed May 23 11:05:06 2007: resultCode...............................-7
```

```
Wed May 23 11:05:06 2007: protocolUsed.............................0xffffffff
Wed May 23 11:05:06 2007: proxyState...............................
                                  00:40:96:AC:E6:57-00:00
Wed May 23 11:05:06 2007: Packet contains 0 AVPs:
```

Fehler: Wireless-Clients, die versuchen, sich über die MAC-Adresse zu authentifizieren, werden abgelehnt. Der Bericht über die fehlgeschlagene Authentifizierung zeigt interne Fehler an.

Wenn Sie ACS 4.1 auf einem Microsoft Windows 2003 Enterprise-Server verwenden, werden Clients, die versuchen, sich anhand der MAC-Adresse zu authentifizieren, abgelehnt. Dies geschieht, wenn ein AAA-Client den Attributwert Service-Type=10 an den AAA-Server sendet. Der Grund dafür ist die Cisco Bug-ID CSCsh62641. AAA-Clients, die von diesem Fehler betroffen sind, umfassen WLCs und Switches, die MAC Authentication Bypass verwenden.

Die Problemumgehungen:

- Downgrade auf ACS 4.0Oder
- Fügen Sie die zu authentifizierenden MAC-Adressen einem Netzwerkzugriffsschutz (Network Access Protection, NAP) unter der internen ACS DB-MAC-Adresstabelle hinzu.

Fehler: Es konnte kein MAC-Filter über die WLC-GUI hinzugefügt werden.

Dies kann aufgrund der Cisco Bug-ID CSCsj98722 der Fall sein. Der Fehler wurde in Version 4.2 behoben. Wenn Sie Versionen vor 4.2 ausführen, können Sie die Firmware auf Version 4.2 aktualisieren oder diese beiden Problemumgehungen verwenden.

- Verwenden Sie die CLI, um den MAC-Filter mit dem folgenden Befehl zu konfigurieren: **`config macfilter add`** `<MAC_address> <WLAN_id> <Interface_name>`
- Wählen Sie in der Web-GUI des Controllers auf der Registerkarte Security (Sicherheit) die Option **Any WLAN aus,** und geben Sie die zu filternde MAC-Adresse ein.

Fehler: Der unbeaufsichtigte Client wurde nicht in den Ausführungszustand versetzt.

Wenn auf dem Controller kein erforderliches DHCP konfiguriert ist, ermitteln die WAPs die IP-Adresse der Wireless-Clients, wenn die Wireless-Clients das erste IP-Paket oder ARP senden. Handelt es sich bei den WLAN-Clients um passive Geräte, z. B. Geräte, die keine Kommunikation initiieren, können die WAPs die IP-Adresse der WLAN-Geräte nicht ermitteln. Daher wartet der Controller zehn Sekunden, bis der Client ein IP-Paket sendet. Wenn das Paket vom Client nicht antwortet, verwirft der Controller alle Pakete an die passiven Wireless-Clients. Dieses Problem ist in der Cisco Bug-ID CSCsq46427 dokumentiert.

> **Hinweis**: Nur registrierte Cisco Benutzer können auf interne Tools und Informationen zugreifen.

Als empfohlene Problemumgehung für passive Geräte wie Drucker, drahtlose SPS-Pumpen usw. müssen Sie das WLAN für die MAC-Filterung einrichten und die AAA-Übersteuerung aktivieren, damit diese Geräte angeschlossen werden können.

Auf dem Controller kann ein MAC-Adressfilter erstellt werden, der die MAC-Adresse des Wireless-Geräts einer IP-Adresse zuordnet.

> **Hinweis**: Hierfür muss die MAC-Adressfilterung in der WLAN-Konfiguration für die Layer-2-Sicherheit aktiviert sein. Außerdem muss in den erweiterten Einstellungen der WLAN-Konfiguration `Allow AAA Override` aktiviert sein.

Geben Sie in der CLI den folgenden Befehl ein, um den MAC-Adressfilter zu erstellen:

```
config macfilter add <STA MAC addr> <WLAN_id> <Interface_name> <description> <STA IP address>
```

Hier ein Beispiel:

```
(Cisco Controller) > config macfilter add 00:01:02:03:04:05 1 my_interface "Zebra Printer"
192.168.1.1
```

Zugehörige Informationen

- Konfigurationsbeispiel für ACLs auf Wireless LAN-Controllern
- Konfigurationsbeispiele für die Authentifizierung auf Wireless LAN-Controllern
- Konfigurationsbeispiel für VLANs auf einem Wireless LAN Controller
- Konfigurationsanleitung für den Cisco Wireless LAN Controller, Version 4.1 - Einstellungsmitteilung
- Support-Seite für Wireless-Technologie
- Technischer Support und Downloads - Cisco Systems

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.