Integrationsleitfaden für WLC und NAC Guest Server (NGS)

Inhalt

Einleitung

Dieses Dokument enthält einen Leitfaden zur Integration von NAC Guest Server und Wireless LAN Controllern.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

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

- Cisco Wireless LAN Controller (WLC) 4.2.61.0
- Catalyst 3560 mit IOS® Version 12.2(25)SEE2
- Cisco ADU-Version 4.0.0.279
- NAC Guest Server Version 1.0

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).

Hintergrundinformationen

Cisco NAC Guest Server ist ein umfassendes Bereitstellungs- und Reporting-System, das Gästen, Besuchern, Auftragnehmern, Beratern und Kunden temporären Netzwerkzugriff ermöglicht. Der Guest Server arbeitet mit der Cisco NAC Appliance oder dem Cisco Wireless LAN Controller zusammen, die/der das Captive Portal und den Durchsetzungspunkt für den Gastzugriff bereitstellt.

Mit Cisco NAC Guest Server können beliebige Benutzer mit Berechtigungen auf einfache Weise temporäre Gastkonten erstellen und Gäste sponsern. Cisco NAC Guest Server führt die vollständige Authentifizierung von Sponsoren durch, d. h. der Benutzer, die Gastkonten erstellen. Sponsoren können dem Gast Kontoinformationen per Ausdruck, E-Mail oder SMS zukommen lassen. Die gesamte Umgebung, von der Erstellung des Benutzerkontos bis hin zum Gastzugriff auf das Netzwerk, wird für die Überwachung und Berichterstellung gespeichert.

Beim Erstellen von Gastkonten werden diese entweder im Cisco NAC Appliance Manager (Clean Access Manager) bereitgestellt oder in der integrierten Datenbank auf dem Cisco NAC Guest Server gespeichert. Wenn Sie die integrierte Datenbank des Gastservers verwenden, können externe Netzwerkzugriffsgeräte wie der Cisco Wireless LAN Controller Benutzer mithilfe des RADIUS-Protokolls (Remote Authentication Dial In User Service) gegenüber dem Gastserver authentifizieren.

Der Cisco NAC Guest Server stellt das Gastkonto für den Zeitraum bereit, der bei der Erstellung des Kontos festgelegt wurde. Nach Ablauf des Kontos löscht der Guest Server das Konto entweder direkt vom Cisco NAC Appliance Manager oder sendet eine RADIUS-Nachricht, die das Netzwerkzugriffsgerät (NAD) über die verbleibende gültige Zeit für das Konto informiert, bevor der Benutzer vom NAD entfernt werden muss.

Der Cisco NAC Guest Server ermöglicht die Abrechnung des Gastzugriffs auf das Netzwerk durch Konsolidierung des gesamten Prüfpfads von der Erstellung des Gastkontos bis hin zur Gastnutzung des Kontos. So können Berichte über eine zentrale Verwaltungsoberfläche erstellt werden.

Konzepte für den Gastzugriff

Cisco NAC Guest Server verwendet eine Reihe von Begriffen, um die für den Gastzugriff erforderlichen Komponenten zu erläutern.

Gastbenutzer

Der Gastbenutzer ist die Person, die ein Benutzerkonto für den Zugriff auf das Netzwerk benötigt.

Sponsor

Der Sponsor ist die Person, die das Gastbenutzerkonto erstellt. Diese Person ist häufig ein Mitarbeiter des Unternehmens, das den Netzwerkzugriff bereitstellt. Bei den Sponsoren kann es sich um bestimmte Personen mit bestimmten Tätigkeitsbereichen oder um Mitarbeiter handeln, die sich bei einem Unternehmensverzeichnis wie Microsoft Active Directory (AD) anmelden können.

Netzwerkdurchsetzungsgerät

Diese Geräte sind die Komponenten der Netzwerkinfrastruktur, die den Netzwerkzugriff ermöglichen. Darüber hinaus leiten Netzwerkdurchsetzungsgeräte Gastbenutzer an ein Captive Portal weiter, wo sie die Details zu ihren Gastkonten eingeben können. Wenn ein Gast seinen temporären Benutzernamen und sein Kennwort eingibt, vergleicht das Netzwerkdurchsetzungsgerät diese Anmeldeinformationen mit den vom Guest Server erstellten Gastkonten.

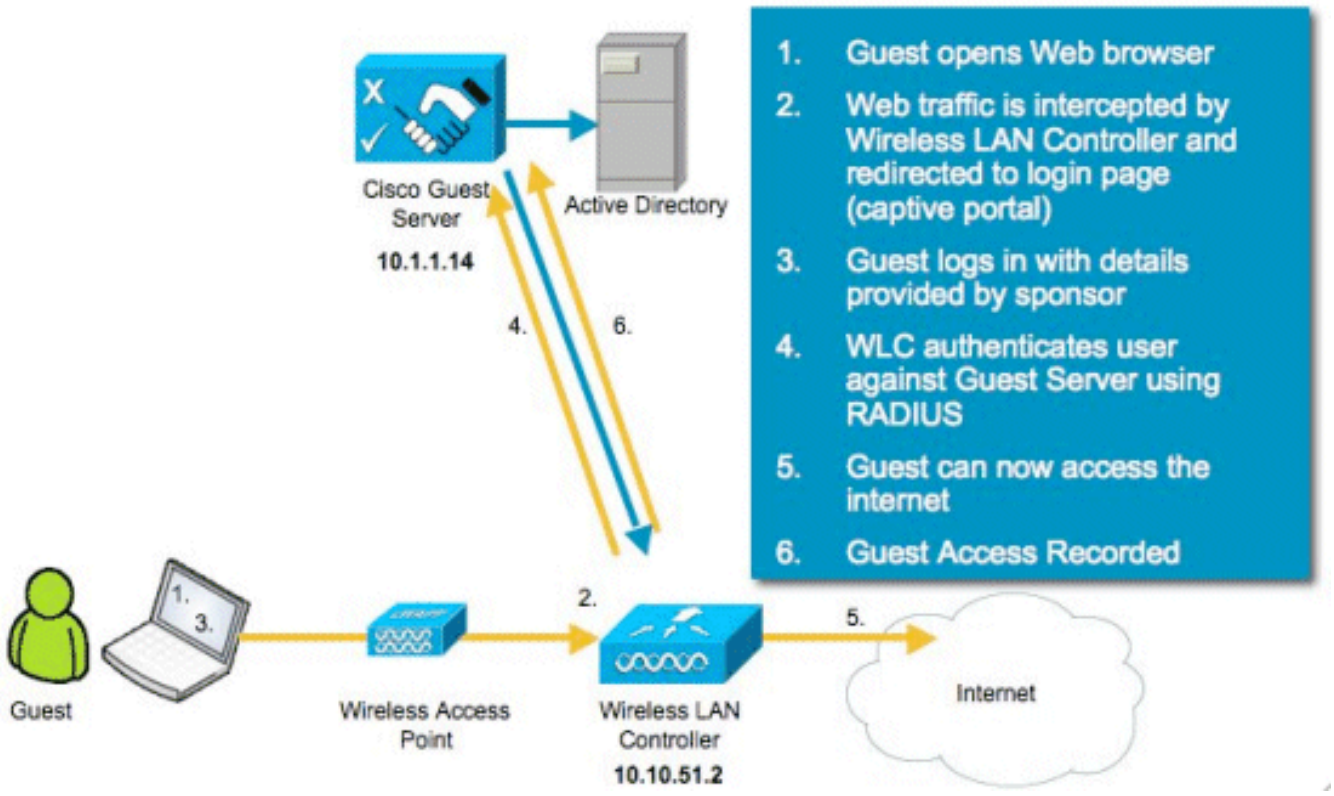
Gastserver

Hierbei handelt es sich um den Cisco NAC Guest Server, der alle Komponenten des Gastzugriffs zusammenfasst. Der Guest Server verbindet diese Elemente miteinander: den Sponsor, der das Guest-Konto erstellt, die an den Gast weitergeleiteten Kontodetails, die Gastauthentifizierung mit dem Netzwerkdurchsetzungsgerät und die Verifizierung des Netzwerkdurchsetzungsgeräts des Gasts mit dem Guest Server. Darüber hinaus konsolidiert Cisco NAC Guest Server die Abrechnungsinformationen von Geräten zur Netzwerkdurchsetzung, um einen zentralen Punkt für den Gastzugriff zu schaffen.

Detaillierte Dokumentation zu NGS finden Sie in CCO.

http://www.cisco.com/en/US/docs/security/nac/guestserver/configuration_guide/10/nacguestserver.html

Überblick über die Labortopologie



Konfigurieren des Wireless LAN-Controllers (WLC)

Führen Sie die folgenden Schritte aus, um den WLC zu konfigurieren:

1. Initialisieren Sie den Controller und den Access Point.
2. Konfigurieren der Controller-Schnittstellen
3. Konfigurieren Sie RADIUS.
4. Konfigurieren der WLAN-Einstellungen

Initialisierung

Verwenden Sie für die Erstkonfiguration eine Konsolenverbindung wie HyperTerminal, und befolgen Sie die Setup-Anweisungen, um die Anmelde- und Schnittstelleninformationen einzugeben. Der Befehl **reset system** initiiert diese Aufforderungen ebenfalls.

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_44:36:c3]: WLC
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): admin
Service Interface IP Address Configuration [none][DHCP]: <ENTER>
Enable Link Aggregation (LAG) [yes][NO]:no
Management Interface IP Address: 10.10.51.2
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.10.51.1
Management Interface VLAN Identifier (0 = untagged): 0
Management Interface Port Num [1 to 2]: 1
Management Interface DHCP Server IP Address: 10.10.51.1
AP Transport Mode [layer2][LAYER3]: layer3
AP Manager Interface IP Address: 10.10.51.3
AP-Manager is on Management subnet, using same values
AP Manager Interface DHCP Server (10.10.5<X>.1):<ENTER>
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: mobile-1
Enable Symmetric Mobility Tunneling: No
Network Name (SSID): wireless-1
Allow Static IP Addresses [YES][no]:<ENTER>
Configure a RADIUS Server now? [YES][no]:<ENTER>
Enter the RADIUS Server's Address: 10.1.1.12
Enter the RADIUS Server's Port [1812]:<ENTER>
Enter the RADIUS Server's Secret: cisco
Enter Country Code (enter 'help' for a list of countries) [US]:<ENTER>
Enable 802.11b Network [YES][no]:<ENTER>
Enable 802.11a Network [YES][no]:<ENTER>
Enable 802.11g Network [YES][no]:<ENTER>
Enable Auto-RF [YES][no]:<ENTER>
Configure a NTP server now? [YES][no]: no
Configure the system time now? [YES][no]: yes
Enter the date in MM/DD/YY format: mm/dd/yy
Enter the time in HH:MM:SS format: hh:mm:ss
```

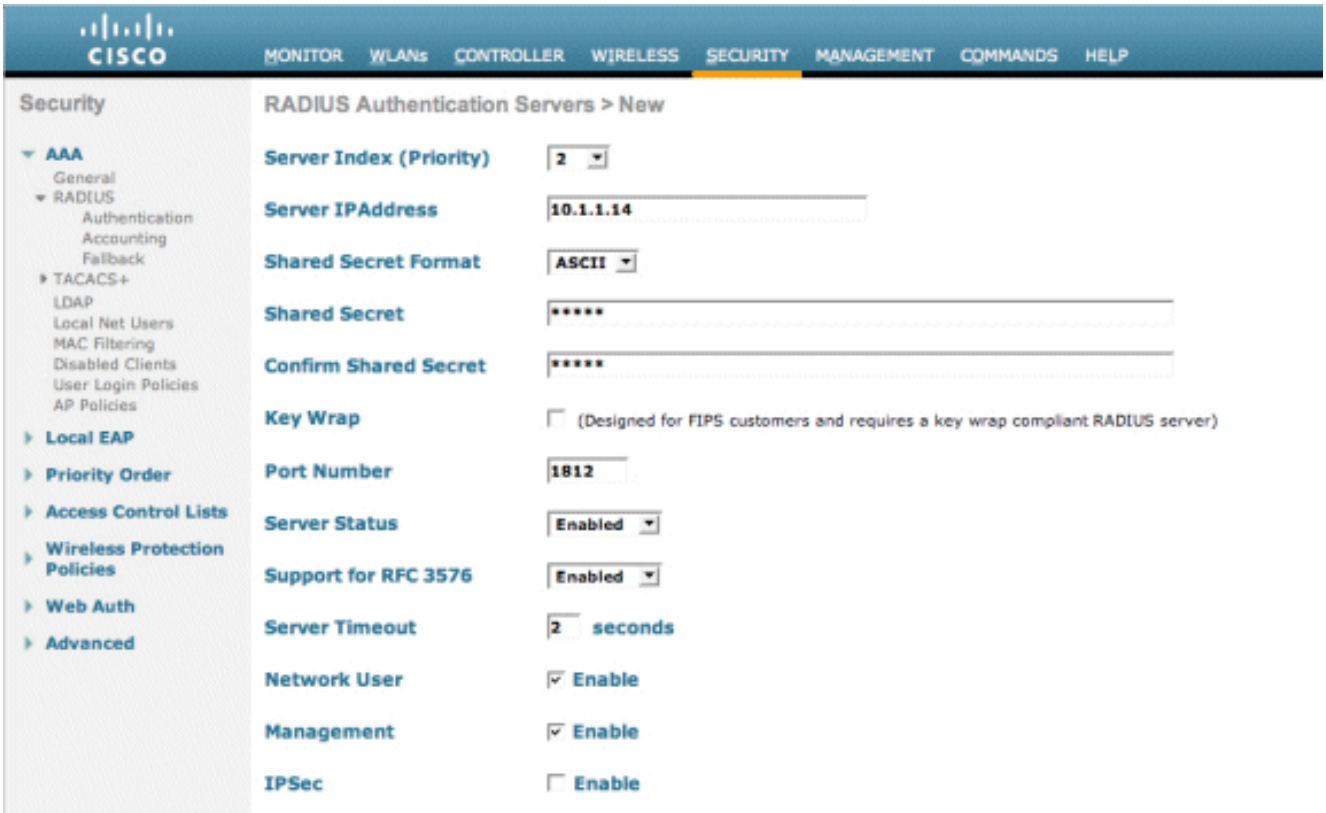
Cisco NAC Guest Server

Cisco NAC Guest Server ist eine Bereitstellungs- und Reporting-Lösung, die Clients wie Gästen, Auftragnehmern usw. einen temporären Netzwerkzugriff ermöglicht. Der Cisco NAC Guest Server kann mit Cisco Unified Wireless Network- oder Cisco NAC Appliance-Lösungen verwendet werden. In diesem Dokument werden Sie durch die Schritte zur Integration des Cisco NAC Guest Servers in einen Cisco WLC geführt, der ein Gastbenutzerkonto erstellt und den temporären Netzwerkzugriff des Gasts verifiziert.

Führen Sie die folgenden Schritte aus, um die Integration abzuschließen:

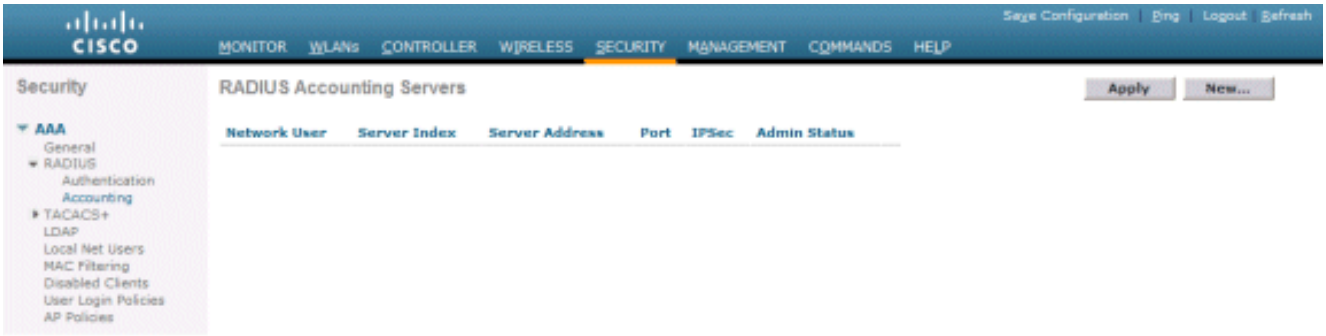
1. Fügen Sie den Cisco NAC Guest Server als Authentifizierungsserver im WLC hinzu.Navigieren Sie zu Ihrem WLC (https://10.10.51.2, admin/admin), um dies zu konfigurieren.Wählen Sie **Security > RADIUS > Authentication aus**.

Wählen Sie **Neu**.Fügen Sie die IP-Adresse (10.1.1.14) für den Cisco NAC Guest Server hinzu.Fügen Sie den freigegebenen Schlüssel hinzu.Bestätigen Sie den gemeinsamen geheimen
Schlüssel.

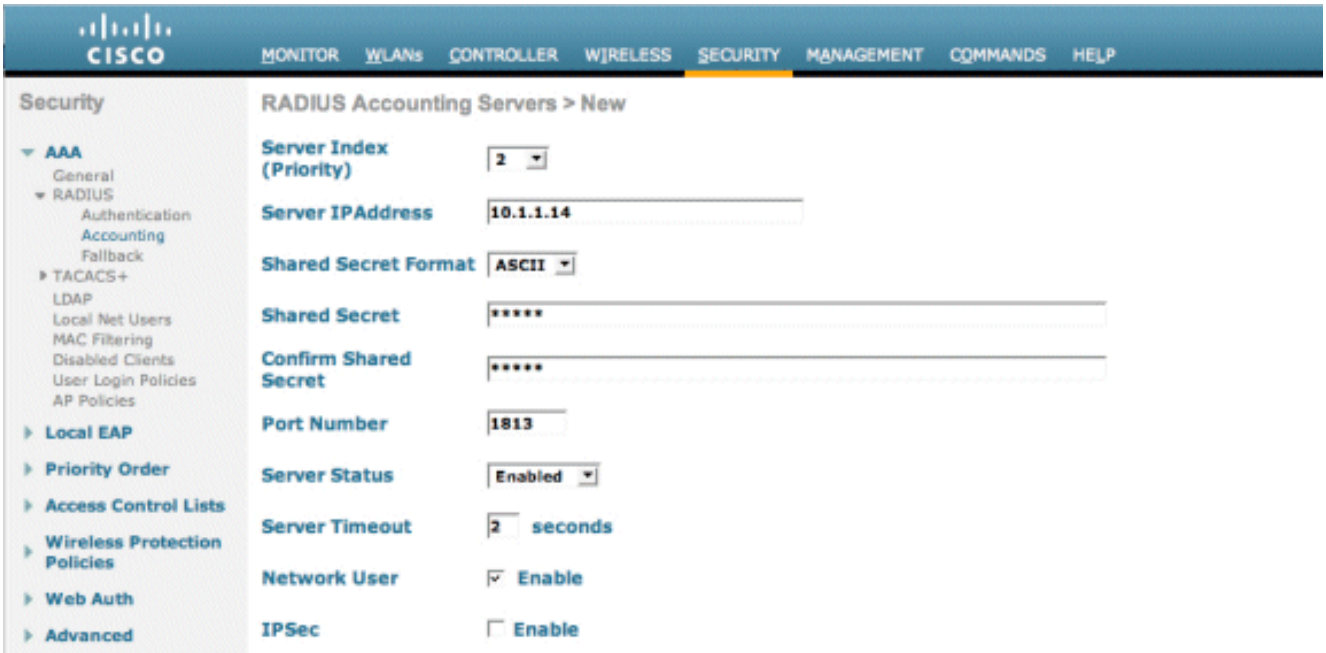


Wählen Sie **Anwenden aus**.

2. Fügen Sie den Cisco NAC Guest Server als Accounting-Server im WLC hinzu.Wählen Sie **Security > RADIUS > Accounting aus**.

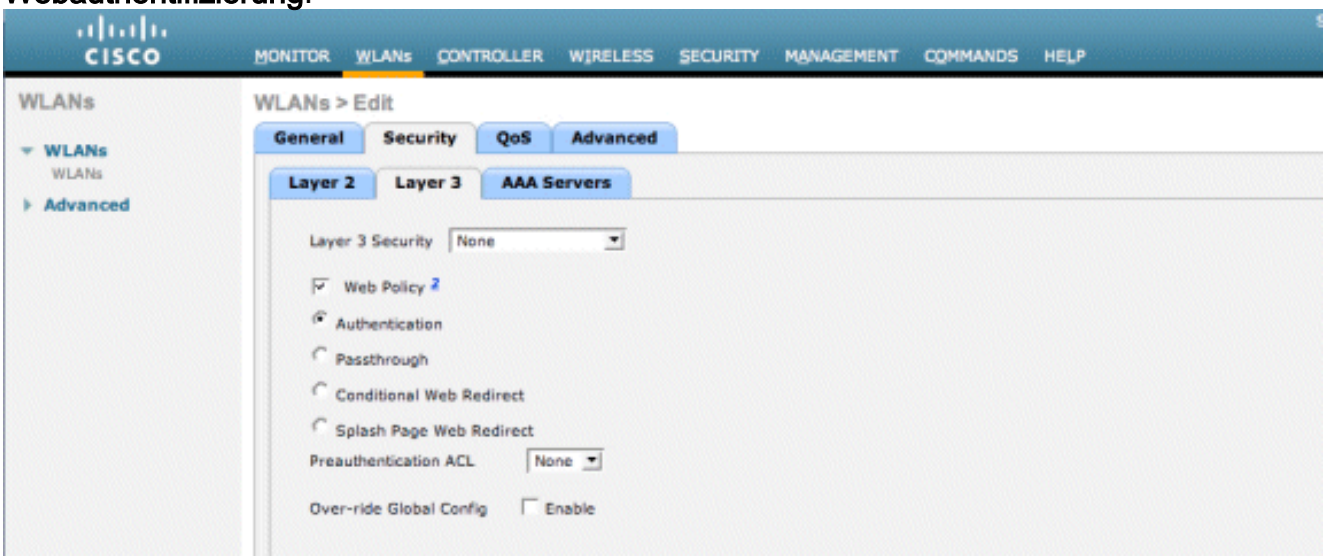


Wählen Sie **Neu**.Fügen Sie die IP-Adresse (10.1.1.14) für den Cisco NAC Guest Server hinzu.Fügen Sie den freigegebenen Schlüssel hinzu.Bestätigen Sie den gemeinsamen geheimen
Schlüssel.

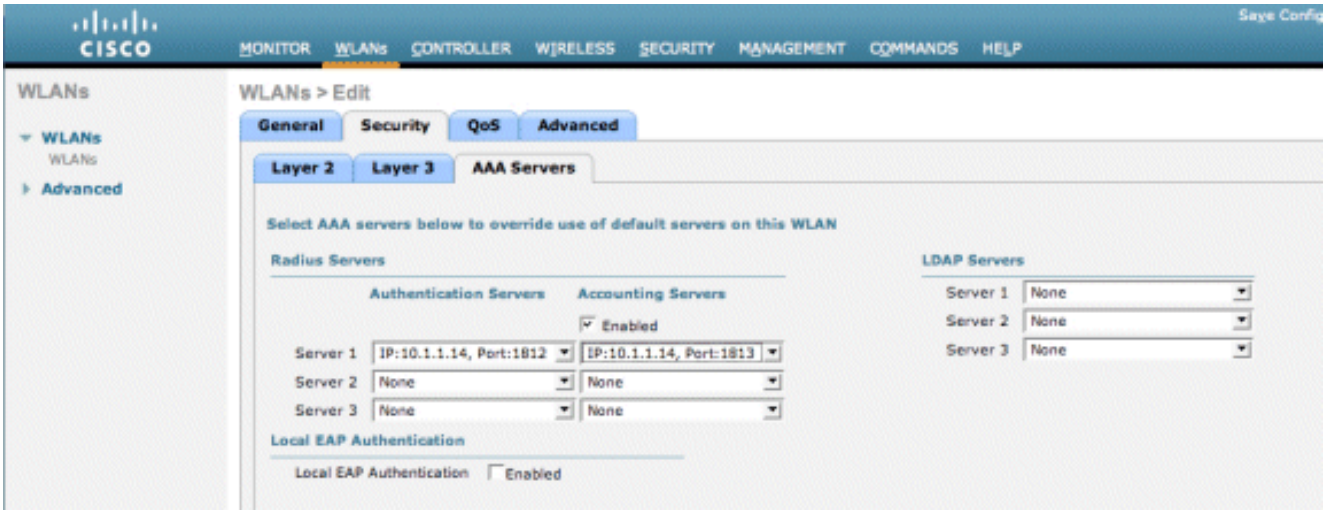


Wählen Sie **Anwenden aus**.

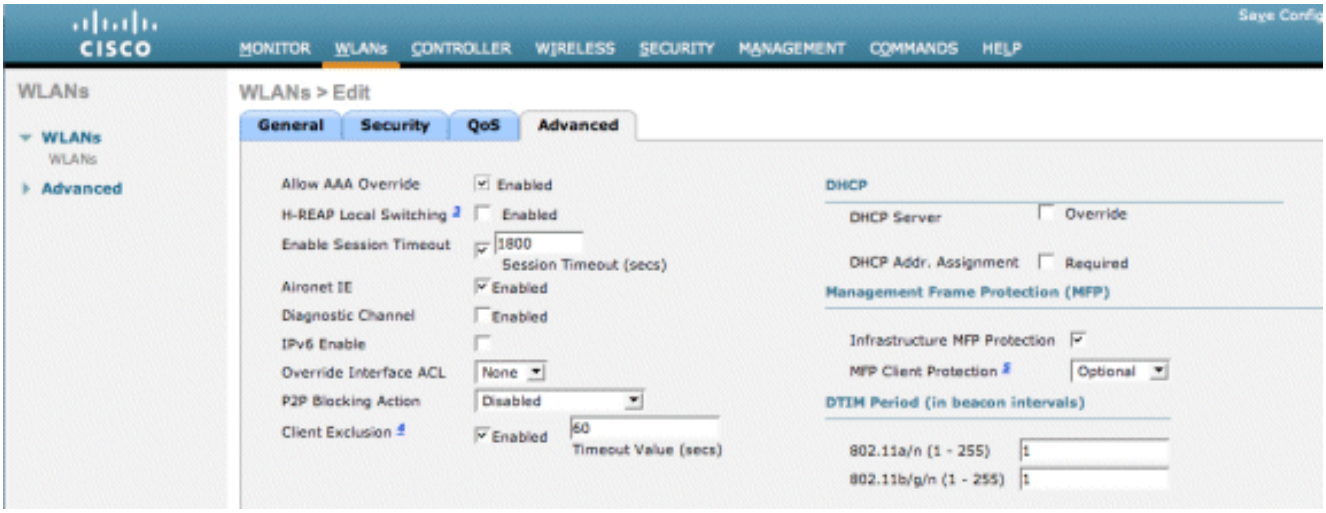
3. Ändern Sie das WLAN (Wireless-x), um den NAC Guest Server zu verwenden.Bearbeiten des WLAN (Wireless-x)Wählen Sie die Registerkarte **Sicherheit**.Ändern Sie die Layer-2-Sicherheit in **Keine** und die Layer-3-Sicherheit in die Verwendung der **Webauthentifizierung**.



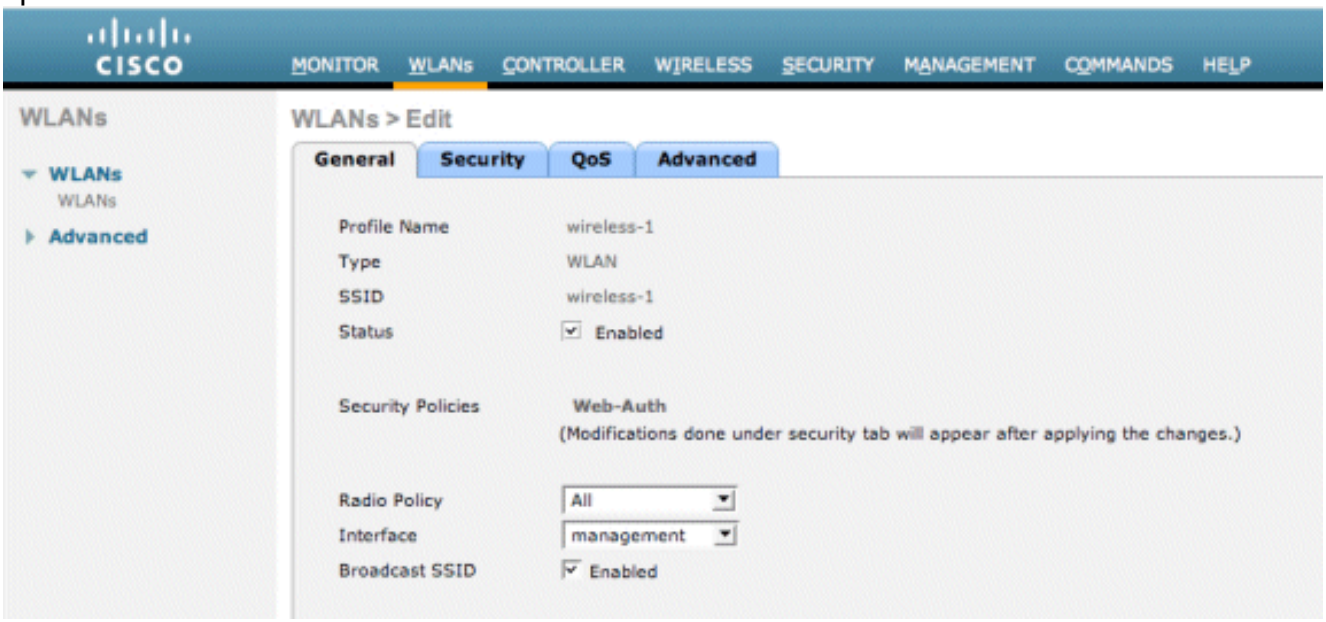
Wählen Sie die **AAA-Server** auf der Registerkarte Sicherheit aus.Wählen Sie im Feld Server 1 den **RADIUS-Server (10.1.1.14) aus**.Wählen Sie im Feld Server 1 den **Accounting-Server (10.1.1.14)**
aus.



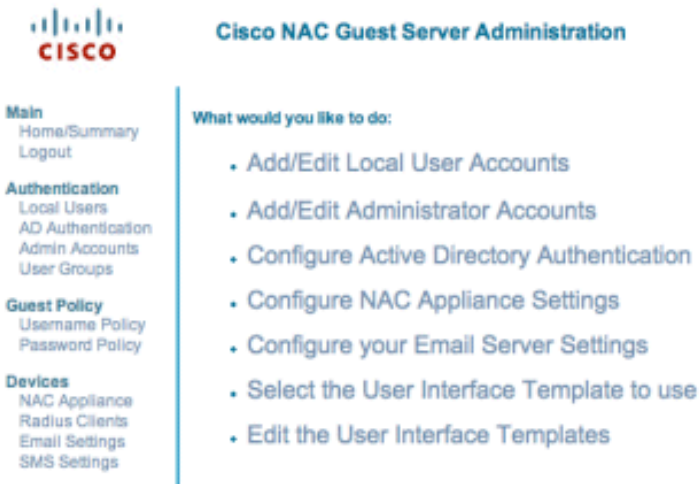
Wählen Sie die Registerkarte **Erweitert aus**.Aktivieren Sie **AAA-Außerkraftsetzung zulassen**. Auf diese Weise kann das Timeout für jede Clientsitzung über die NAC Guest Appliance festgelegt
werden.



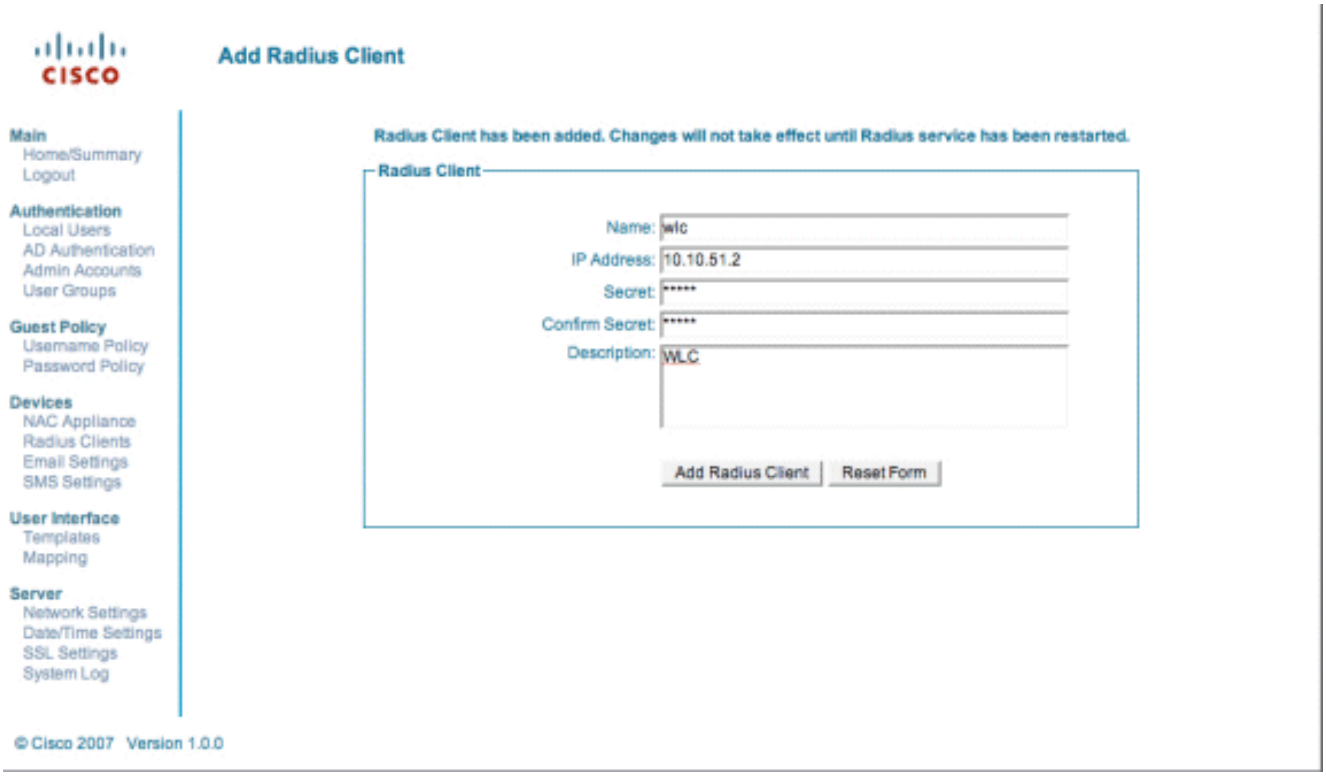
Hinweis: Wenn **AAA override** für die SSID aktiviert ist, wird die verbleibende Lebensdauer des Gastbenutzers auf dem NGS als Sitzungs-Timeout zum Zeitpunkt der Anmeldung des Gastbenutzers an den WLC übertragen.Wählen Sie **Apply** (Anwenden), um die WLAN-Konfiguration zu
speichern.



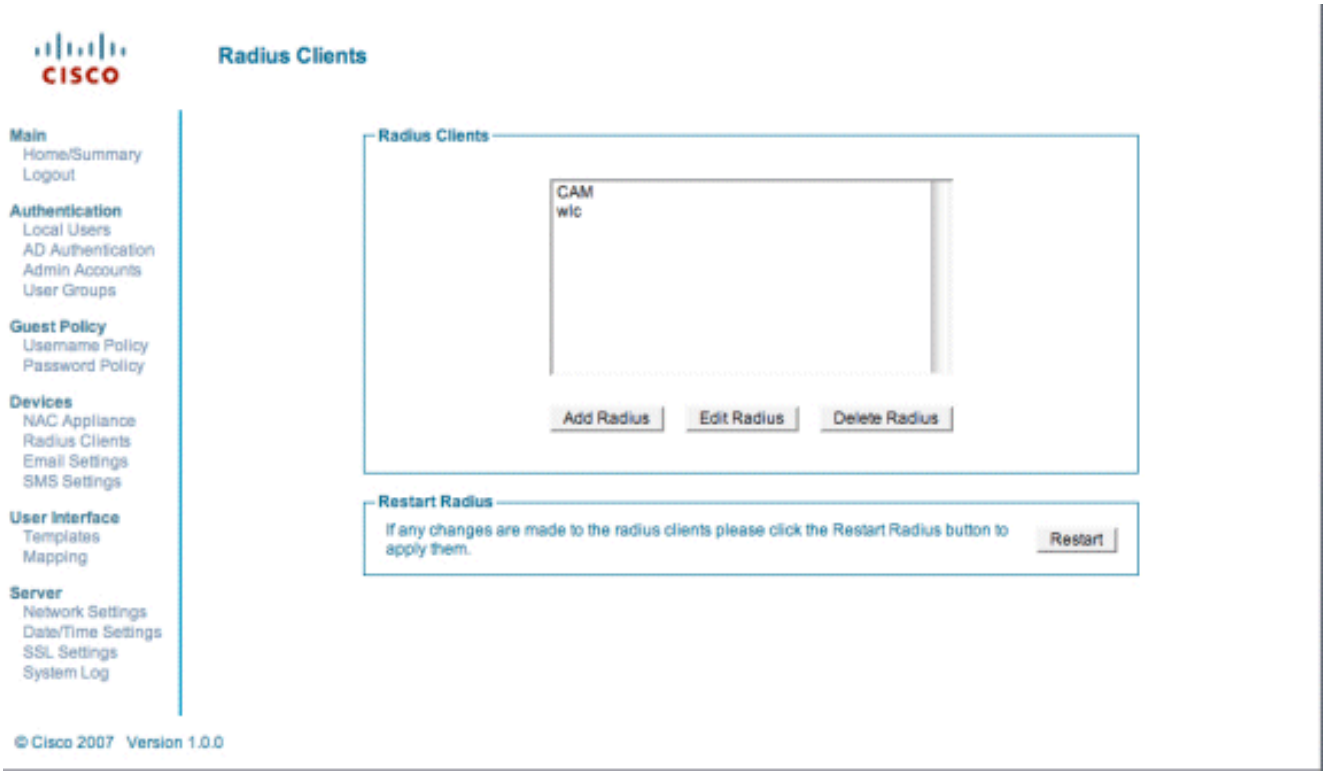
4. Überprüfen Sie, ob der Controller als Radius-Client im Cisco NAC Guest Server hinzugefügt wurde.Navigieren Sie zum NAC Guest Server (https://10.1.1.14/admin), um dies zu konfigurieren.**Hinweis:** Sie erhalten die Seite Administration, wenn Sie /admin in der URL angeben.



Wählen Sie **Radius Clients**.Wählen Sie **Radius hinzufügen aus**.Geben Sie die Informationen zum Radius-Client ein:Geben Sie einen Namen ein: WLC-Systemname.Geben Sie die IP-Adresse ein: IP address of WLC **(10.10.51.2)**.Geben Sie den gleichen geheimen Schlüssel ein, den Sie in Schritt 1 eingegeben haben.Bestätige deinen gemeinsamen geheimen Schlüssel.Geben Sie eine Beschreibung ein.Wählen Sie **Radius-Client hinzufügen aus**.

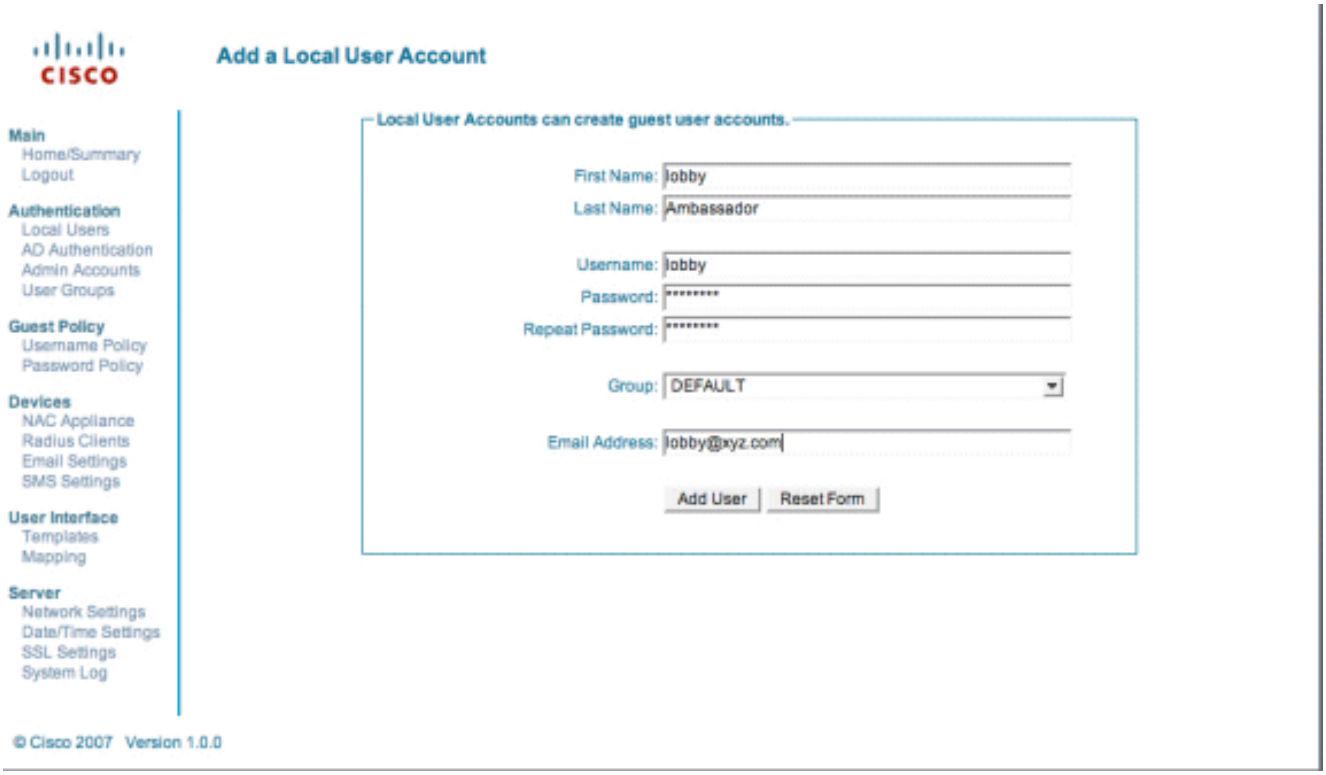


Starten Sie den Radius-Dienst neu, damit die Änderungen wirksam werden.Wählen Sie **Radius Clients**.Wählen Sie im Feld Neustart-Radius die Option **Neu starten**.



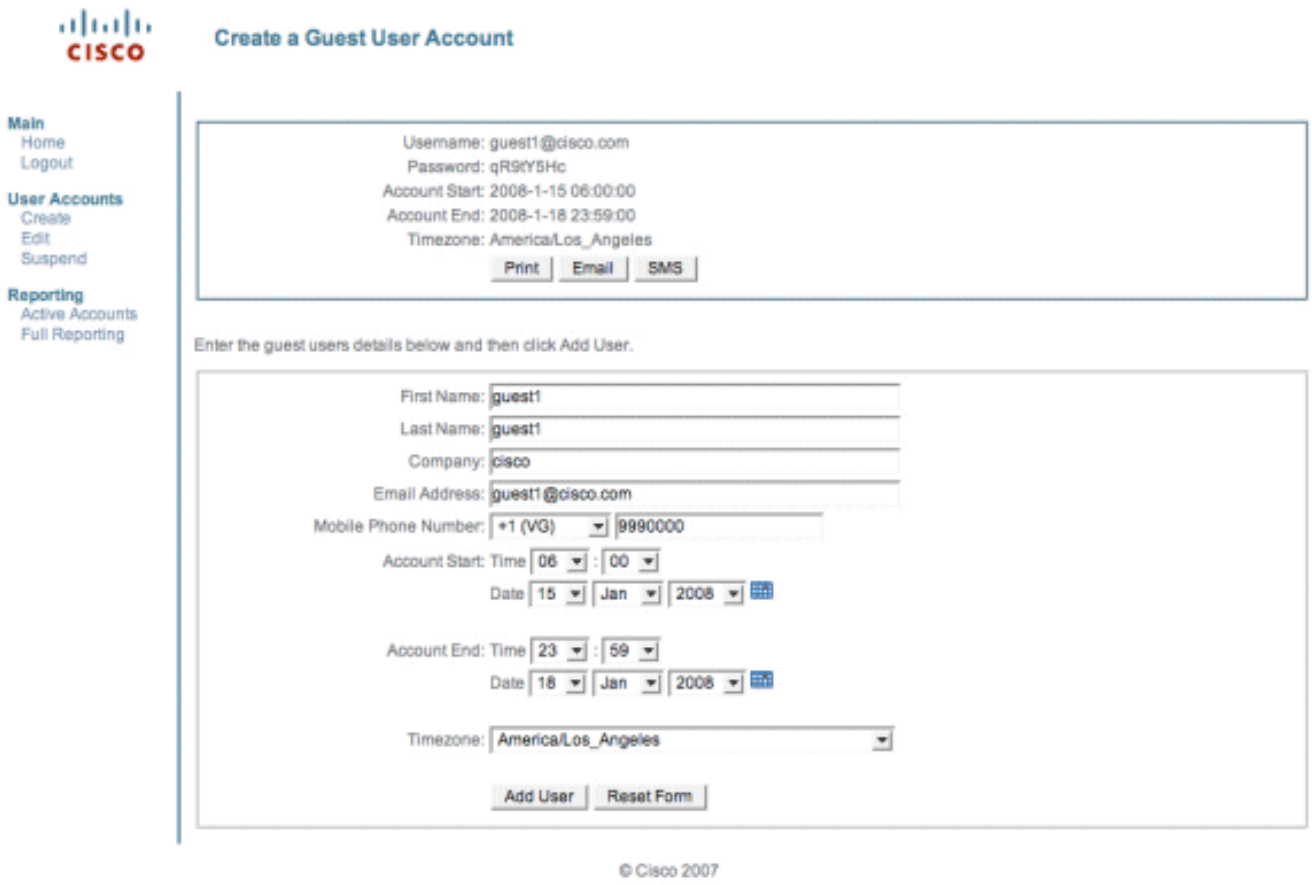
5. Erstellen Sie auf dem Cisco NAC Guest Server einen lokalen Benutzer, d. h. einen Lobby Ambassador.Wählen Sie **Lokale Benutzer aus**.Wählen Sie **Benutzer hinzufügen aus**.**Hinweis:**

Sie müssen alle Felder ausfüllen.Geben Sie einen Vornamen ein: **lobby**.Geben Sie einen Nachnamen ein: **Ambassador**.Benutzername: **Lobby** eingeben.Geben Sie ein Kennwort ein: **password**.Behalten Sie Gruppe als **Standard bei**.Geben Sie die E-Mail-Adresse **lobby@xyz.com ein**.Wählen Sie **Benutzer hinzufügen aus**.



6. Melden Sie sich als lokaler Benutzer an, und erstellen Sie ein Gastkonto.Navigieren Sie zum NAC Guest Server (https://10.1.1.14), melden Sie sich mit dem in Schritt 5 erstellten Benutzernamen/Kennwort an, und konfigurieren Sie Folgendes:

Wählen Sie **Erstellen** als Gastbenutzerkonto aus.**Hinweis:** Sie müssen alle Felder ausfüllen.Geben Sie einen Vornamen ein.Geben Sie einen Nachnamen ein.Geben Sie das Unternehmen ein.Geben Sie die Email-Adresse ein.**Hinweis:** Die E-Mail-Adresse ist der Benutzername.Geben Sie das Kontenende ein: **Zeit**.Wählen Sie **Benutzer hinzufügen aus**.



7. Stellen Sie eine Verbindung zum Gast-WLAN her, und melden Sie sich als Gast-Benutzer an.Verbinden Sie den Wireless-Client mit dem Gast-WLAN (Wireless-x).Öffnen Sie den Webbrowser, um zur Seite Web-Auth Login (Web-Auth-Anmeldung) umgeleitet zu werden.**Hinweis:** Alternativ können Sie auch **https://1.1.1.1/login.html** eingeben, um zur Anmeldeseite weitergeleitet zu werden.Geben Sie den in Schritt 6 erstellten Gastbenutzernamen ein.Geben Sie das Kennwort ein, das in Schritt 6 automatisch generiert wurde.Senden Sie eine Telnet-Verbindung zum WLC, und überprüfen Sie, ob das Sitzungstimeout mit dem Befehl **show client detail** festgelegt wurde.Wenn das Sitzungstimeout abläuft, wird die Verbindung zum Gastclient getrennt, und der Ping wird beendet.

```
(Cisco Controller) >show client detail 00:13:e8:b7:5e:dd
Client MAC Address.............................. 00:13:e8:b7:5e:dd
Client Username ................................ podx@cisco.com
AP MAC Address.................................. 00:17:df:a6:e5:f0
Client State.................................... Associated
Wireless LAN Id................................. 1
BSSID........................................... 00:17:df:a6:e5:ff
Channel......................................... 60
IP Address...................................... 10.1.1.22
Association Id.................................. 1
Authentication Algorithm........................ Open System
Reason Code..................................... 0
Status Code..................................... 0
Session Timeout................................. 59
Client CCX version.............................. 4
Client E2E version.............................. 1
Mirroring....................................... Disabled
QoS Level....................................... Silver
Diff Serv Code Point (DSCP)..................... disabled
802.1P Priority Tag............................. disabled
WMM Support..................................... Enabled
U-APSD Support.................................. Disabled
Mobility State.................................. Local
--More-- or (q)uit
(Cisco Controller) >
```

Hinweis: Um die Webauthentifizierung vom Wireleass LAN Controller, WLC zum NAC Guest Server (NGS) einzurichten, müssen Sie die PAP-Modus-Authentifizierung in den

Webauthentifizierungseigenschaften verwenden. Wenn die Web-Authentifizierungsrichtlinie auf CHAP festgelegt ist, schlägt die Authentifizierung fehl, da CHAP von NGS nicht unterstützt wird.

Zugehörige Informationen

- Cisco NAC Appliance - Installations- und Konfigurationsleitfaden für Clean Access Manager, Version 4.1(3)
- Cisco NAC Appliance-Switch und Unterstützung für Wireless LAN-Controller
- Konfigurationsleitfaden für Cisco Wireless LAN Controller, Version 7.0.116.0
- (Video) Integration von Cisco Identity Services Engine (ISE) und Wireless LAN Controller (WLC)
- NAC (Clean Access): Konfigurieren des Gastzugriffs
- Bereitstellungsleitfaden: Cisco Guest Access Using Cisco Wireless LAN Controller, Version 4.1
- 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.