

Konfigurationsbeispiel für H-REAP-Betriebsmodi

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Hintergrundinformationen](#)

[H-REAP über REAP](#)

[Konfiguration](#)

[Netzwerkdiagramm](#)

[Konfiguration](#)

[Primieren des Access Points mit einem Controller und Konfigurieren von H-REAP](#)

[H-REAP-Betriebstheorie](#)

[H-REAP-Switching-Status](#)

[Zentrale Authentifizierung, Central Switching](#)

[Zentrale Authentifizierung, Central Switching überprüfen](#)

[Abschaltung der Authentifizierung, Abschalten](#)

[Zentrale Authentifizierung, lokales Switching](#)

[Zentrale Authentifizierung, lokales Switching überprüfen](#)

[Deaktivierung der Authentifizierung, lokales Switching](#)

[Lokale Authentifizierung, lokales Switching](#)

[Lokale Authentifizierung, lokales Switching überprüfen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird das Konzept des Hybrid Remote Edge Access Point (H-REAP) vorgestellt und die verschiedenen Betriebsmodi mit einer Beispielkonfiguration erläutert.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Kenntnisse der Wireless LAN Controller (WLCs) und Konfiguration der WLC-Basisparameter

- Kenntnisse von REAP

Verwendete Komponenten

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

- Cisco WLC der Serie 4400 mit Firmware-Version 7.0.116.0
- Cisco 1131AG Lightweight Access Point (LAP)
- Cisco Router der Serie 2800 mit Version 12.4(11)T.
- Cisco Aironet 802.11a/b/g Client-Adapter mit Firmware-Version 4.0
- Cisco Aironet Desktop Utility Version 4.0
- Cisco Secure ACS mit Version 4.0

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

H-REAP ist eine Wireless-Lösung für Bereitstellungen in Zweigstellen und Zweigstellen. Mit H-REAP können Kunden Access Points (APs) in einer Zweigstelle oder in einer Außenstelle über eine WAN-Verbindung konfigurieren und steuern, ohne in jedem Büro einen Controller bereitzustellen zu müssen.

H-REAPs können den Client-Datenverkehr lokal umschalten und die Client-Authentifizierung lokal ausführen, wenn die Verbindung zum Controller unterbrochen wird. Wenn H-REAPs mit dem Controller verbunden sind, können sie auch den Datenverkehr zurück zum Controller leiten. Im Connected Mode kann der hybride REAP auch eine lokale Authentifizierung durchführen.

H-REAP wird nur auf folgenden Geräten unterstützt:

- APs 1130AG, 1140, 1240, 1250, 1260, AP801, AP 802, 1040 und AP3550
- Cisco Controller der Serien 5500, 4400, 2100, 2500 und Flex 7500
- Catalyst 3750G Integrated Controller Switch
- Catalyst Wireless Services Module (WiSM) der Serie 6500
- Wireless LAN Controller Module (WLCM) für Integrated Services Router (ISRs)

Client-Datenverkehr auf H-REAPs kann entweder lokal am AP umgeschaltet oder zurück an einen Controller getunnelt werden. Dies hängt von der Konfiguration pro WLAN ab. Außerdem kann der lokal geschaltete Client-Datenverkehr auf dem H-REAP mit 802.1Q-Tags versehen werden, um eine kabelgebundene Trennung zu ermöglichen. Während eines WAN-Ausfalls besteht der Service aller lokal geschalteten, lokal authentifizierten WLANs weiter.

Hinweis: Wenn sich die Access Points im H-REAP-Modus befinden und lokal am Remote-Standort

geswitcht werden, wird die dynamische Zuweisung von Benutzern zu einem spezifischen VLAN, das auf der RADIUS-Serverkonfiguration basiert, nicht unterstützt. Sie sollten jedoch in der Lage sein, Benutzer bestimmten VLANs zuzuweisen, die auf der statischen VLAN-Zuordnung zu Service Set Identifier (SSID) basieren, die lokal am AP durchgeführt wird. Aus diesem Grund kann einem Benutzer, der zu einer bestimmten SSID gehört, ein bestimmtes VLAN zugewiesen werden, dem die SSID lokal am WAP zugeordnet ist.

Hinweis: Wenn Voice-over-WLAN wichtig ist, sollten die APs im lokalen Modus ausgeführt werden, damit sie Unterstützung für CCKM und Connection Admission Control (CAC) erhalten, die im H-REAP-Modus nicht unterstützt werden.

[H-REAP über REAP](#)

Weitere Informationen zum Verständnis von REAP finden Sie im [Konfigurationsbeispiel für Remote-Edge-APs \(REAP\) mit einfachen APs und Wireless LAN-Controllern \(WLCs\)](#).

Aufgrund dieser Mängel des REAP wurde H-REAP eingeführt:

- REAP verfügt über keine kabelgebundene Trennung. Dies liegt an der fehlenden 802.1Q-Unterstützung. Daten von den WLANs werden im selben kabelgebundenen Subnetz gespeichert.
- Bei einem WAN-Ausfall beendet ein REAP-AP den Dienst, der auf allen WLANs angeboten wird, mit Ausnahme des ersten, der im Controller angegeben ist.

So kann H-REAP diese beiden Mängel beheben:

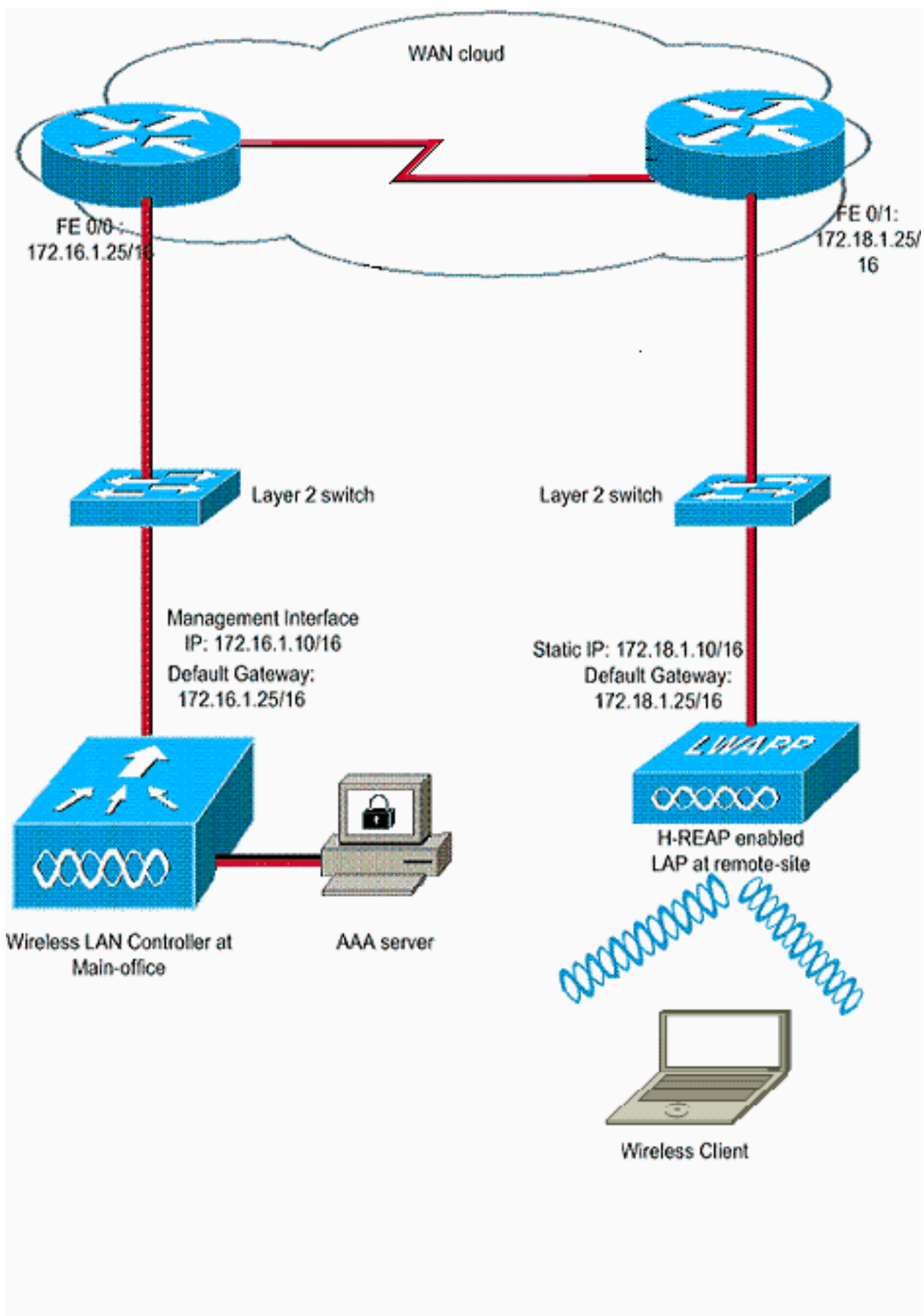
- Bietet dot1Q-Unterstützung und VLAN-zu-SSID-Zuordnung. Diese VLAN-SSID-Zuordnung muss mit H-REAP erfolgen. Stellen Sie dabei sicher, dass konfigurierte VLANs ordnungsgemäß über die Ports in zwischengeschalteten Switches und Routern zugelassen sind.
- Bietet kontinuierlichen Service für alle WLANs, die für lokales Switching konfiguriert sind.

[Konfiguration](#)

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

[Netzwerkdiagramm](#)

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfiguration

In diesem Beispiel wird davon ausgegangen, dass der Controller bereits mit Basiskonfigurationen konfiguriert ist. Der Controller verwendet folgende Konfigurationen:

- IP-Adresse der Verwaltungsschnittstelle - 172.16.1.10/16
- IP-Adresse der AP-Manager-Schnittstelle: 172.16.1.11/16
- IP-Adresse des Standard-Gateway-Routers: 172.16.1.25/16
- IP-Adresse des virtuellen Gateways - 1.1.1.1

Hinweis: Dieses Dokument enthält keine WAN-Konfigurationen und -Konfigurationen für Router und Switches, die zwischen dem H-REAP und dem Controller verfügbar sind. Dabei wird davon ausgegangen, dass Sie die verwendete WAN-Kapselung und die verwendeten Routing-Protokolle kennen. Darüber hinaus wird in diesem Dokument davon ausgegangen, dass Sie wissen, wie diese konfiguriert werden, um die Verbindung zwischen dem H-REAP und dem Controller über die WAN-Verbindung aufrechtzuerhalten. In diesem Beispiel wird die HDLC-Kapselung auf der WAN-Verbindung verwendet.

[Primieren des Access Points mit einem Controller und Konfigurieren von H-REAP](#)

Wenn der Access Point einen Controller in einem Remote-Netzwerk erkennen soll, in dem keine CAPWAP-Erkennungsmechanismen verfügbar sind, können Sie eine Primierung verwenden. Mit dieser Methode können Sie den Controller festlegen, mit dem der Access Point verbunden werden soll.

Um einen H-REAP-fähigen Access Point zu bedienen, verbinden Sie den Access Point mit dem kabelgebundenen Netzwerk in der Hauptniederlassung. Beim Hochfahren sucht der H-REAP-fähige Access Point zunächst selbst nach einer IP-Adresse. Sobald eine IP-Adresse über einen DHCP-Server abgerufen wird, startet er und sucht nach einem Controller, der den Registrierungsprozess durchführt.

Ein H-REAP AP kann die IP-Adresse des Controllers auf eine der in [Lightweight AP \(LAP\) Registration to a Wireless LAN Controller \(WLC\)](#) beschriebenen Weisen erfassen.

Hinweis: Sie können die LAP auch so konfigurieren, dass der Controller über CLI-Befehle am Access Point erkannt wird. Weitere Informationen finden Sie unter [H-REAP Controller Discovery mit CLI-Befehlen](#).

Im Beispiel in diesem Dokument wird die DHCP-Option 43-Prozedur verwendet, mit der der H-REAP die IP-Adresse des Controllers ermitteln kann. Anschließend wird eine Verbindung zum Controller hergestellt, das aktuelle Software-Image und die aktuelle Software-Konfiguration vom Controller heruntergeladen und der Funklink initialisiert. Es speichert die heruntergeladene Konfiguration im nichtflüchtigen Speicher, der im Standalone-Modus verwendet werden kann.

Wenn die LAP beim Controller registriert ist, führen Sie die folgenden Schritte aus:

1. Wählen Sie in der Controller-GUI **Wireless > Access Points aus**. Es wird die bei diesem Controller registrierte LAP angezeigt.
2. Klicken Sie auf den AP, den Sie konfigurieren möchten.

Wireless

All APs

Current Filter: None [Change Filter] [Clear Filter]

Number of APs: 1

AP Name	AP Model	AP MAC	AP Up Time	Admin Status	Operational Status
AP001a.a219.ad44	AIR-LAP1131AG-A-K9	00:1e:a2:19:ad:44	0 d, 00 h 06 m 12 s	Enabled	REG

3. Klicken Sie im Fenster APs>Details auf die Registerkarte High Availability (Hohe Verfügbarkeit), und legen Sie die Controller-Namen fest, die die APs für die Registrierung verwenden werden. Klicken Sie anschließend auf **Apply (Übernehmen)**.

Wireless

All APs > Details for AP001a.a219.ad44

General Credentials Interfaces High Availability Inventory Advanced

	Name	Management IP Address
Primary Controller	WLC-4400	172.16.1.10
Secondary Controller		
Tertiary Controller		

AP Failover Priority: Low

Sie können bis zu drei Controller-Namen definieren (primär, sekundär und tertiär). Die APs suchen den Controller in der gleichen Reihenfolge wie in diesem Fenster. Da in diesem Beispiel nur ein Controller verwendet wird, wird im Beispiel der Controller als primärer Controller definiert.

4. Konfigurieren der LAP für H-REAPUm die LAP so zu konfigurieren, dass sie im H-REAP-Modus betrieben wird, wählen Sie im Fenster APs>Details auf der Registerkarte Allgemein den **AP-Modus** als H-REAP aus dem entsprechenden Dropdown-Menü aus.Dadurch wird die LAP für den Betrieb im H-REAP-Modus konfiguriert.

Hinweis: In diesem Beispiel sehen Sie, dass die IP-Adresse des Access Points in den statischen Modus geändert und die statische IP-Adresse 172.18.1.10 zugewiesen wurde. Diese Zuweisung erfolgt, da es sich um das Subnetz handelt, das in der Außenstelle verwendet wird. Aus diesem Grund verwenden Sie die IP-Adresse des DHCP-Servers, jedoch nur während der ersten Registrierungsphase. Nachdem der Access Point am Controller registriert wurde, ändern Sie die Adresse in eine statische IP-Adresse.

Nachdem Ihre LAP mit dem Controller ausgestattet und für den H-REAP-Modus konfiguriert ist, besteht der nächste Schritt darin, H-REAP auf Controllerseite zu konfigurieren und die H-REAP-Switching-Zustände zu besprechen.

H-REAP-Betriebstheorie

Die H-REAP-fähige LAP wird in den folgenden beiden Modi betrieben:

- **Angeschlossener Modus:** Ein H-REAP befindet sich im Anschlussmodus, wenn die Verbindung der CAPWAP-Kontrollebene zum WLC aktiv und betriebsbereit ist. Das bedeutet, dass die WAN-Verbindung zwischen der LAP und dem WLC nicht unterbrochen ist.
- **Eigenständiger Modus:** Ein H-REAP befindet sich im Standalone-Modus, wenn die WAN-Verbindung zum WLC ausfällt. Wenn dieser H-REAP beispielsweise nicht mehr über eine Verbindung zum WLC verfügt, der über die WAN-Verbindung verbunden ist.

Der Authentifizierungsmechanismus für die Authentifizierung eines Clients kann als **Central** oder **Local** definiert werden.

- **Central Authentication (Zentrale Authentifizierung):** Bezieht sich auf den Authentifizierungstyp, der den Prozess des WLC vom Remote-Standort aus umfasst.
- **Local Authentication (Lokale Authentifizierung):** Bezieht sich auf die Authentifizierungstypen, für die keine Verarbeitung vom WLC zur Authentifizierung erforderlich ist.

Hinweis: Alle 802.11-Authentifizierungs- und Zuordnungsvorgänge finden am H-REAP statt, unabhängig davon, in welchem Modus sich die LAP befindet. Im Connected-Modus leitet H-REAP diese Zuordnungen und Authentifizierungen dann an den WLC weiter. Im Standalone-Modus kann die LAP den WLC nicht über derartige Ereignisse informieren.

Wenn ein Client eine Verbindung zu einem H-REAP-AP herstellt, leitet der Access Point alle Authentifizierungsmeldungen an den Controller weiter. Nach erfolgreicher Authentifizierung werden die Datenpakete entweder lokal geschickt oder zurück zum Controller getunnelt. Dies entspricht der Konfiguration des WLAN, mit dem es verbunden ist.

Mit H-REAP können die auf einem Controller konfigurierten WLANs in zwei verschiedenen Modi betrieben werden:

- **Zentrales Switching:** Ein WLAN auf H-REAP wird im zentralen Switching-Modus betrieben, wenn der Datenverkehr dieses WLAN so konfiguriert ist, dass er an den WLC getunnelt wird.
- **Lokales Switching:** Ein WLAN auf H-REAP wird im lokalen Switching-Modus betrieben, wenn der Datenverkehr dieses WLAN lokal an der kabelgebundenen Schnittstelle der LAP selbst terminiert wird, ohne dass ein Tunnel zum WLC erfolgt. **Hinweis:** Nur WLANs 1 bis 8 können für H-REAP Local Switching konfiguriert werden, da nur diese WLANs auf die APs der Serien 1130, 1240 und 1250 angewendet werden können, die H-REAP-Funktionen unterstützen.

H-REAP-Switching-Status

Zusammen mit den im vorherigen Abschnitt erwähnten Authentifizierungs- und Switching-Modi kann ein H-REAP in einem der folgenden Zustände betrieben werden:

- [Zentrale Authentifizierung, Central Switching](#)
- [Abschaltung der Authentifizierung, Abschalten](#)
- [Zentrale Authentifizierung, lokales Switching](#)
- [Deaktivierung der Authentifizierung, lokales Switching](#)
- [Lokale Authentifizierung, lokales Switching](#)

Zentrale Authentifizierung, Central Switching

In diesem Zustand leitet der WLAN für das angegebene WLAN alle Client-Authentifizierungsanforderungen an den Controller weiter und leitet alle Client-Daten an den WLC weiter. Dieser Status ist nur gültig, wenn sich der H-REAP im Modus "Connected" befindet. WLANs, die für diesen Modus konfiguriert sind, gehen bei WAN-Ausfällen verloren, unabhängig von der Authentifizierungsmethode.

In diesem Beispiel werden folgende Konfigurationseinstellungen verwendet:

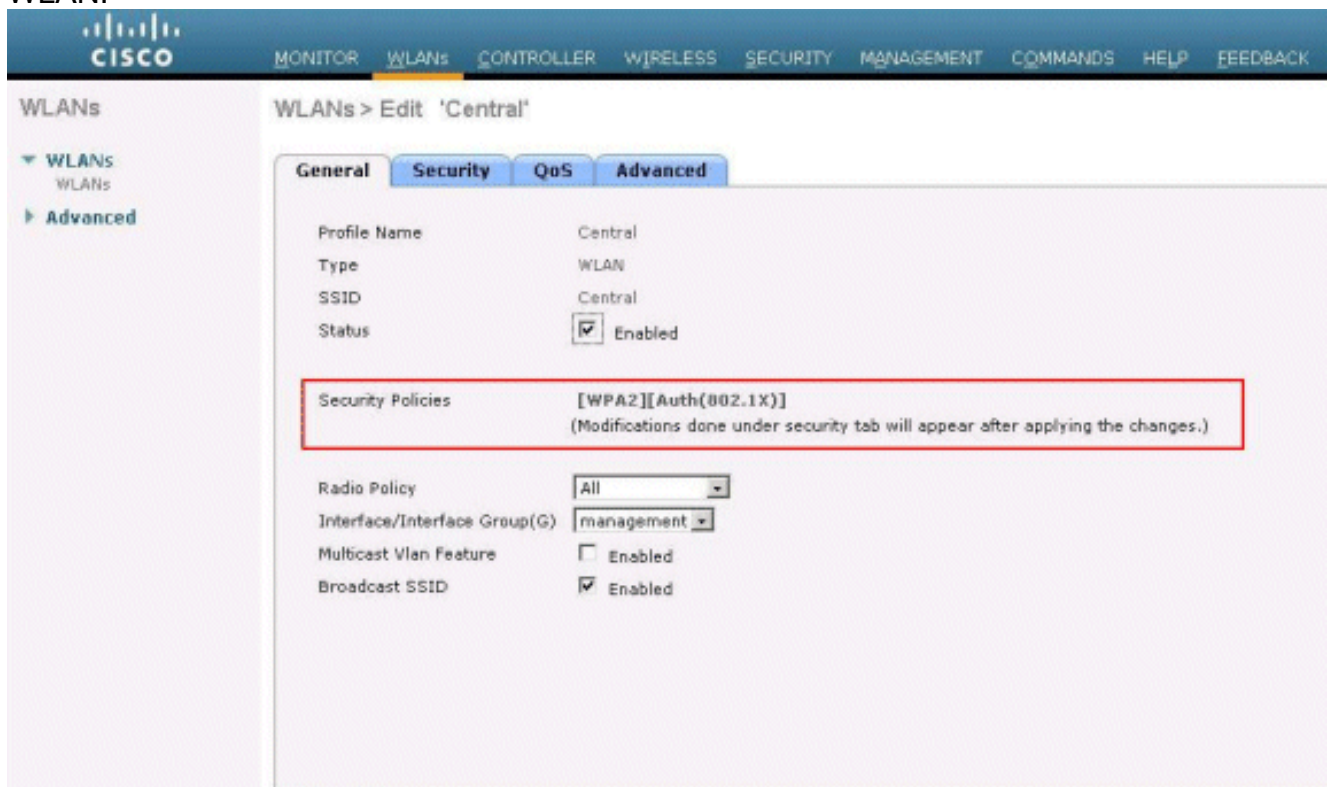
- WLAN/SSID-Name: **Zentral**
- Layer-2-Sicherheit: **WPA2**
- Lokales H-REAP-Switching: **deaktiviert**

Gehen Sie wie folgt vor, um den WLC für die zentrale Authentifizierung, das zentrale Switching über die GUI zu konfigurieren:

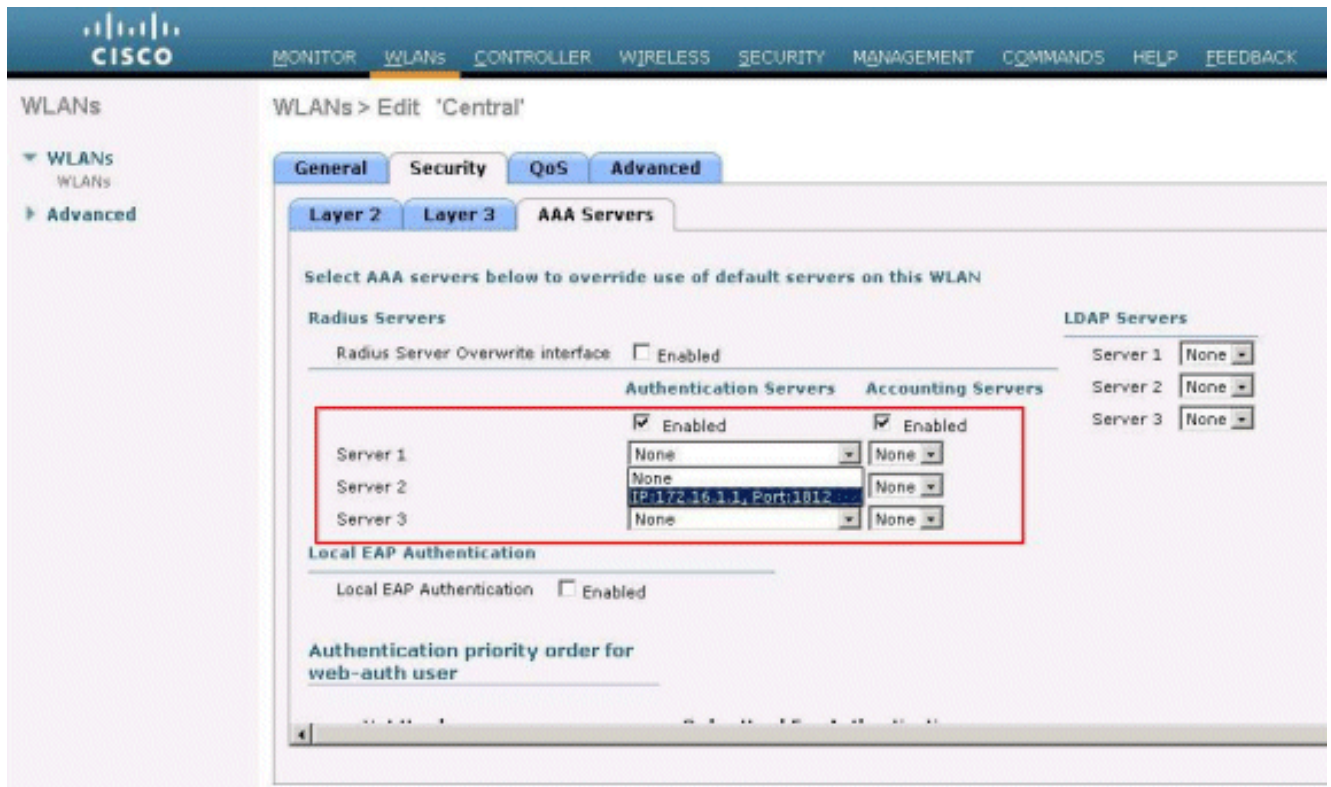
1. Klicken Sie auf **WLANs**, um ein neues WLAN mit dem Namen **Central** zu erstellen, und klicken Sie dann auf **Apply**.



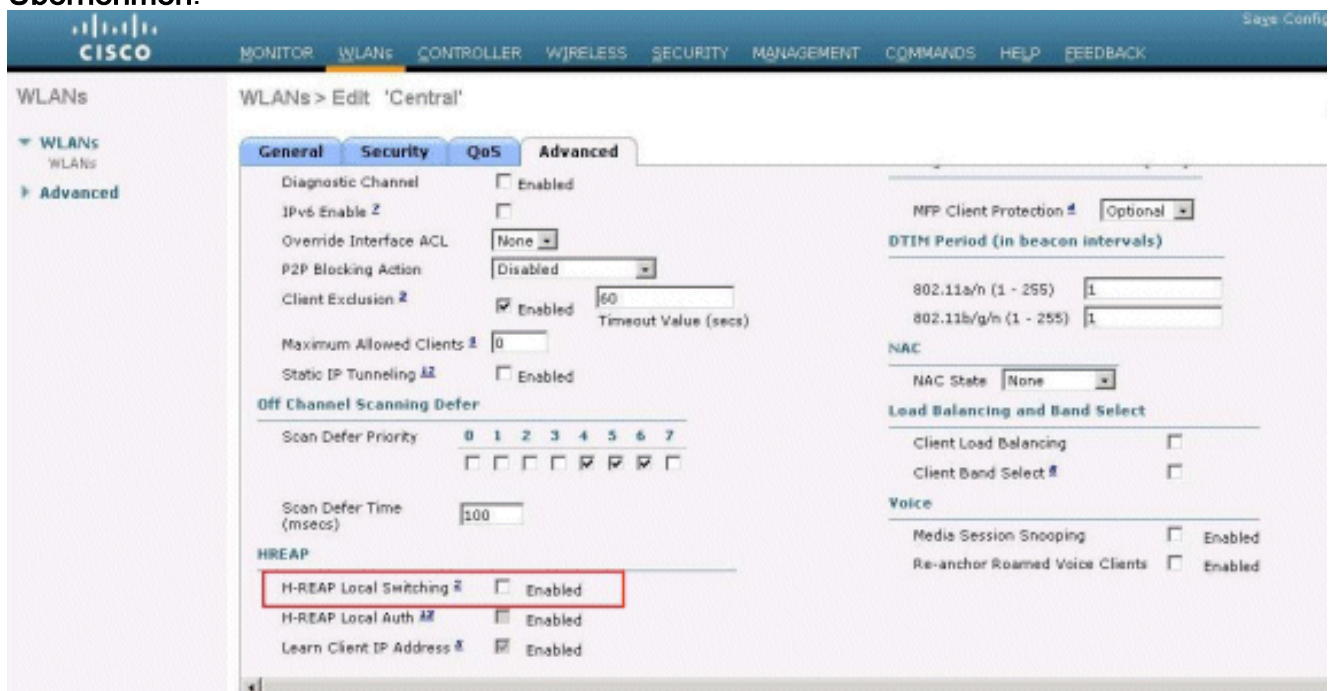
2. Da dieses WLAN eine zentrale Authentifizierung verwendet, wird die WPA2-Authentifizierung im Sicherheitsfeld für Layer 2 verwendet. WPA2 ist die standardmäßige Layer-2-Sicherheit für ein WLAN.



3. Wählen Sie die Registerkarte "AAA-Server" aus, und wählen Sie dann den für die Authentifizierung konfigurierten Server aus.



4. Da dieses WLAN zentrales Switching verwendet, müssen Sie sicherstellen, dass das Kontrollkästchen H-REAP Local Switching (Lokales Switching) deaktiviert ist (d. h., das Kontrollkästchen Local Switching (Lokales Switching) ist nicht aktiviert). Klicken Sie anschließend auf **Übernehmen**.



Zentrale Authentifizierung, Central Switching überprüfen

Führen Sie diese Schritte aus:

1. Konfigurieren Sie den Wireless-Client mit den gleichen SSID- und Sicherheitskonfigurationen. In diesem Beispiel ist die SSID *Central* und die Sicherheitsmethode *WPA2*.

2. Geben Sie den Benutzernamen und das Kennwort ein, wie im RADIUS-Server->Benutzer-Setup konfiguriert, um die zentrale SSID im Client zu aktivieren. In diesem Beispiel wird *User1* als Benutzername und Kennwort



Enter Wireless Network Password

Please enter your EAP-FAST username and password to log on to the wireless network.

User Name : User1

Password : ●●●●●●

Log on to :

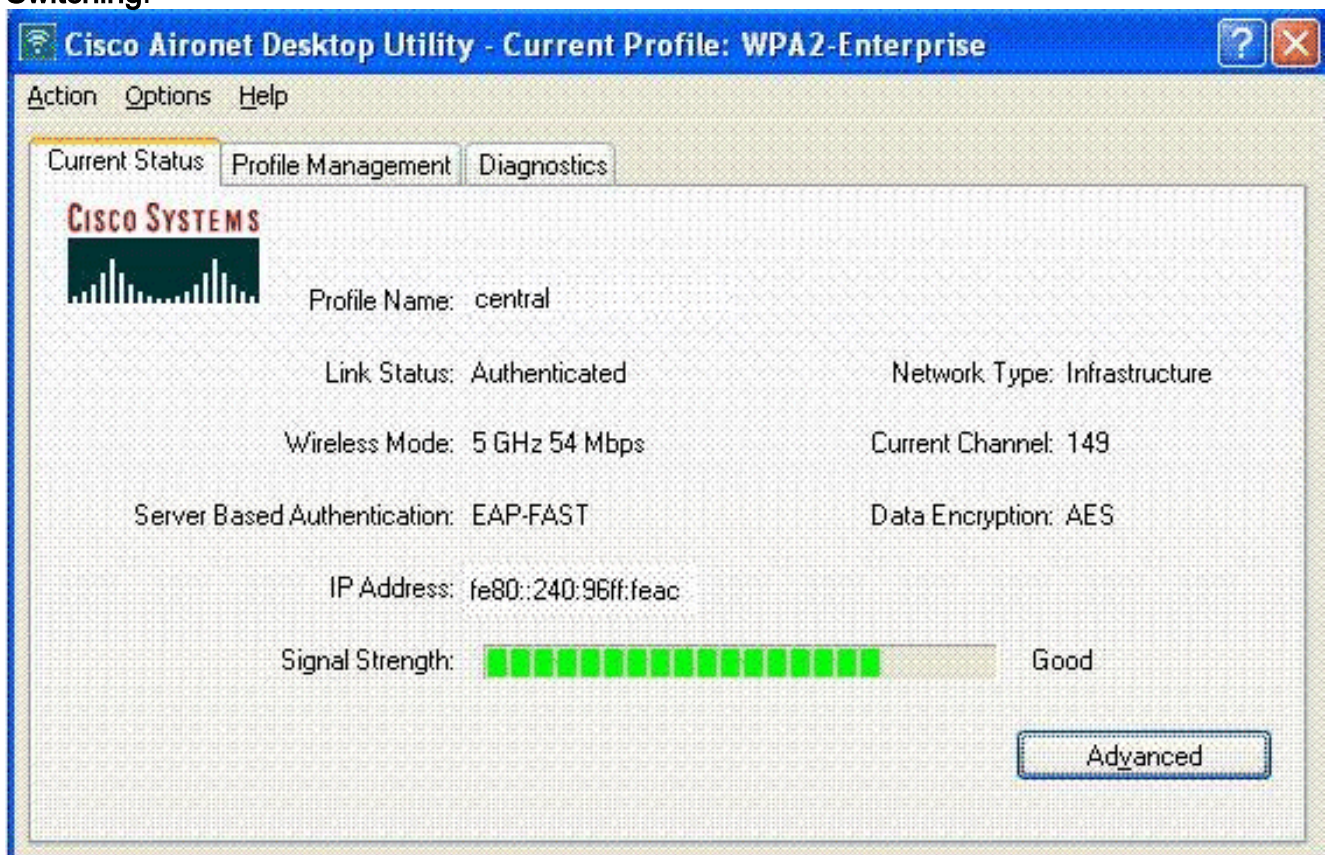
Card Name : Cisco Aironet 802.11 a/b/g Wireless Adapter

Profile Name : WPA-Enterprise

OK Cancel

verwendet.

Der Client wird vom RADIUS-Server zentral authentifiziert und dem H-REAP AP zugeordnet. Der H-REAP befindet sich jetzt in **zentraler Authentifizierung, zentralem Switching**.



Cisco Aironet Desktop Utility - Current Profile: WPA2-Enterprise

Action Options Help

Current Status Profile Management Diagnostics

CISCO SYSTEMS

Profile Name: central

Link Status: Authenticated Network Type: Infrastructure

Wireless Mode: 5 GHz 54 Mbps Current Channel: 149

Server Based Authentication: EAP-FAST Data Encryption: AES

IP Address: fe80::240:96ff:feac

Signal Strength: Good

Advanced

[Abschaltung der Authentifizierung, Abschalten](#)

Mit derselben Konfiguration, die im Abschnitt [Central Authentication, Central Switching](#) (Zentrale Authentifizierung, Zentrale Switching) erläutert wird, deaktivieren Sie die WAN-Verbindung, die den Controller verbindet. Jetzt wartet der Controller auf eine Heartbeat-Antwort vom Access Point. Eine Heartbeat-Antwort ähnelt Keepalive-Nachrichten. Der Controller versucht fünf aufeinander folgende Heartbeats, jeweils jede Sekunde.

Da der WLC nicht mit einer Heartbeat-Antwort vom H-REAP empfangen wird, wird die LAP vom WLC nicht registriert.

Geben Sie den Befehl **debug capwap events enable** aus der CLI des WLC ein, um den Deregistrierungsprozess zu überprüfen. Dies ist die Beispielausgabe dieses **Debug**-Befehls:

```
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Did not receive heartbeat reply from AP 00:15:c7:ab:55:90
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamContext: Down capwap event for AP 00:15:c7:ab:55:90 slot 0
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamContext: Deregister capwap event for AP 00:15:c7:ab:55:90 slot 0
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamContext: Down capwap event for AP 00:15:c7:ab:55:90 slot 1
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamContext: Deregister capwap event for AP 00:15:c7:ab:55:90 slot 1
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Received capwap Down event for AP 00:15:c7:ab:55:90 slot 0!
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Deregister capwap event for AP 00:15:c7:ab:55:90 slot 0
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Received capwap Down event for AP 00:15:c7:ab:55:90 slot 1!
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Deregister capwap event for AP 00:15:c7:ab:55:90 slot 1
```

Der H-REAP wechselt in den Standalone-Modus.

Da dieses WLAN zuvor zentral authentifiziert und zentral geschaltet wurde, wurden Steuerungs- und Datenverkehr zurück an den Controller geleitet. Daher kann der Client ohne den Controller die Verbindung zum H-REAP nicht aufrechterhalten, und die Verbindung wird getrennt. Dieser Zustand von H-REAP, bei dem sowohl die Clientzuordnung als auch die Authentifizierung deaktiviert ist, wird als "Authentication Down" (Authentifizierungsabschaltung) bezeichnet.

[Zentrale Authentifizierung, lokales Switching](#)

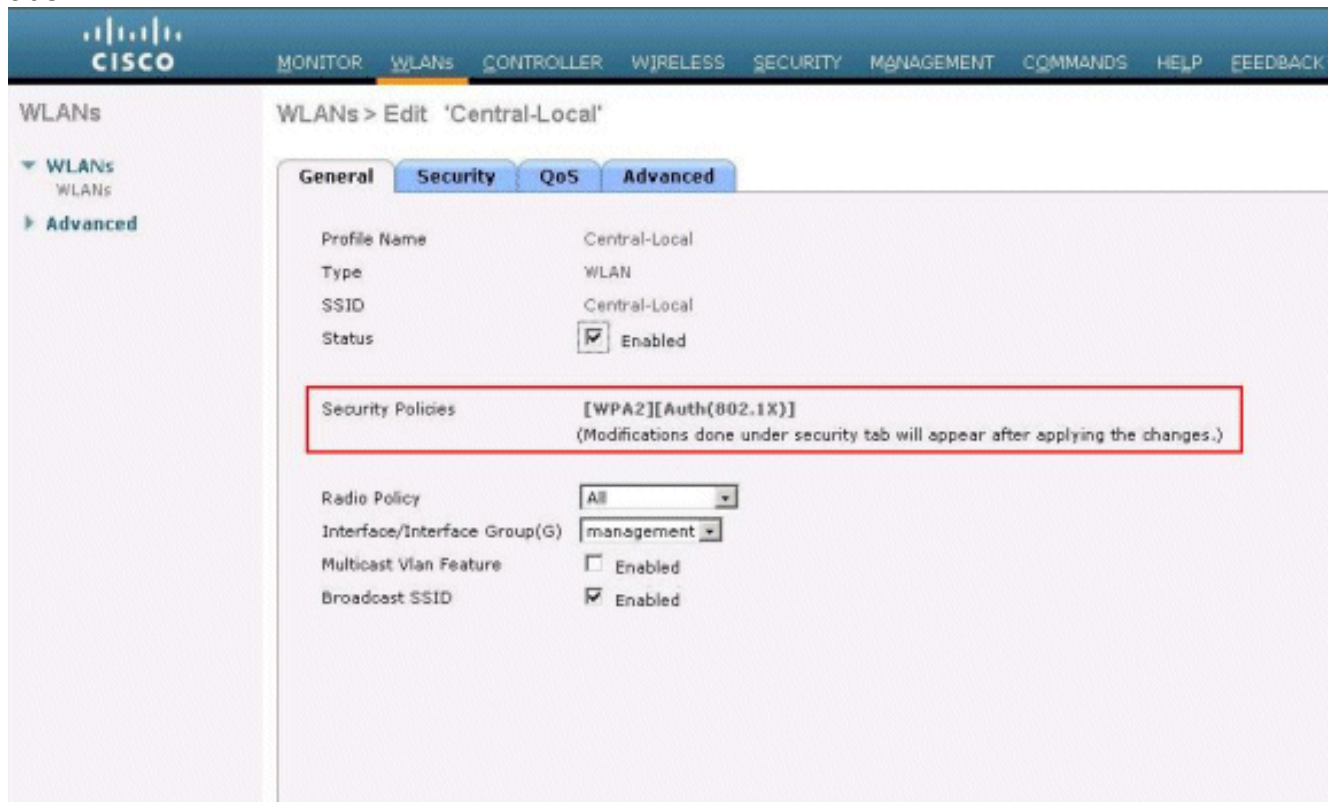
In diesem Zustand verarbeitet der WLC für das angegebene WLAN die gesamte Client-Authentifizierung, und die H-REAP LAP schaltet Datenpakete lokal. Nachdem sich der Client erfolgreich authentifiziert hat, sendet der Controller CAPWAP-Kontrollbefehle an den H-REAP und weist die LAP an, die Datenpakete des Clients lokal zu verändern. Diese Nachricht wird nach erfolgreicher Authentifizierung pro Client gesendet. Dieser Status ist nur im Modus "Verbunden" anwendbar.

In diesem Beispiel werden folgende Konfigurationseinstellungen verwendet:

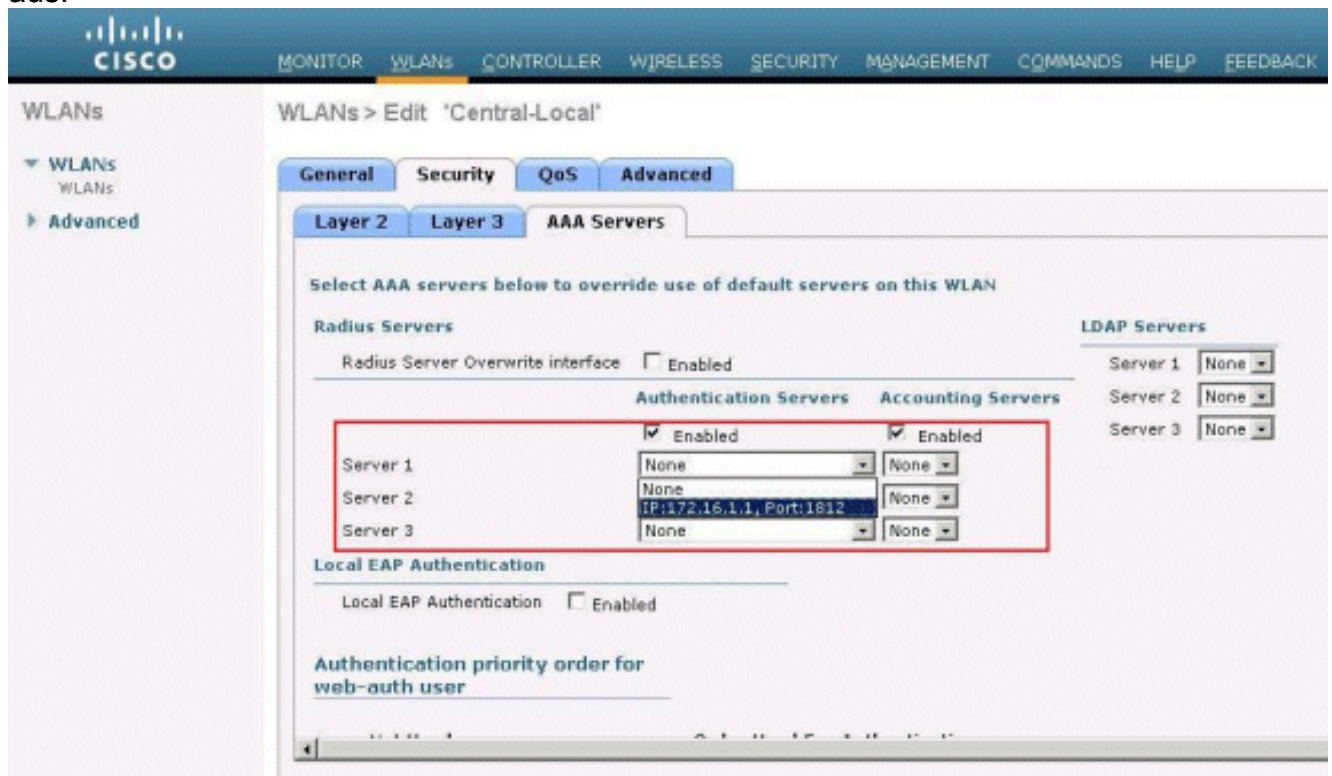
- WLAN/SSID-Name: **Zentral-Lokal**
- Layer-2-Sicherheit: **WPA2**.
- Lokales H-REAP-Switching: **Aktiviert**

Gehen Sie in der Controller-GUI wie folgt vor:

1. Klicken Sie auf **WLANs**, um ein neues WLAN mit dem Namen Central-Local zu erstellen, und klicken Sie dann auf **Apply**.
2. Da dieses WLAN eine zentrale Authentifizierung verwendet, wählen Sie im Feld "Layer 2 Security" **WPA2 Authentication** aus.

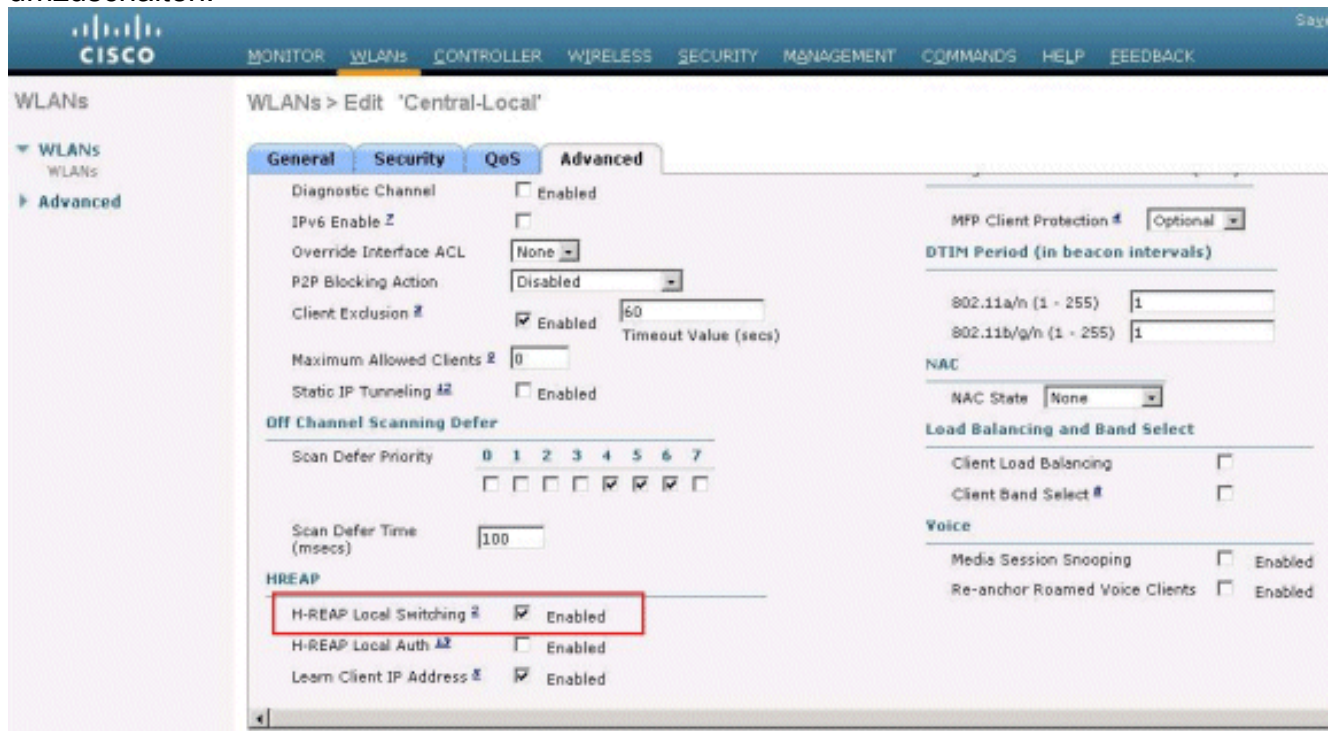


3. Wählen Sie im Abschnitt Radius Servers (Radius-Server) den für die Authentifizierung konfigurierten Server aus.



4. Aktivieren Sie das Kontrollkästchen **H-REAP Local Switching** (Lokales H-REAP-Switching), um den Client-Datenverkehr, der zu diesem WLAN lokal am H-REAP gehört,

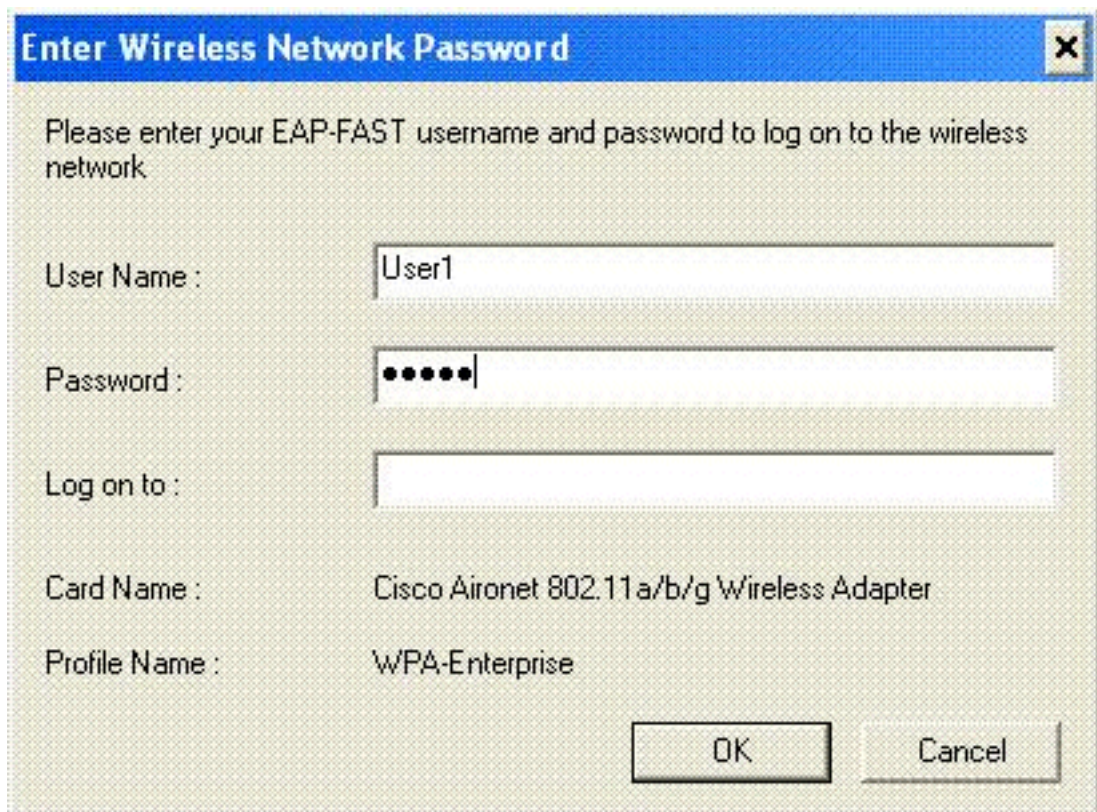
umzuschalten.



Zentrale Authentifizierung, lokales Switching überprüfen

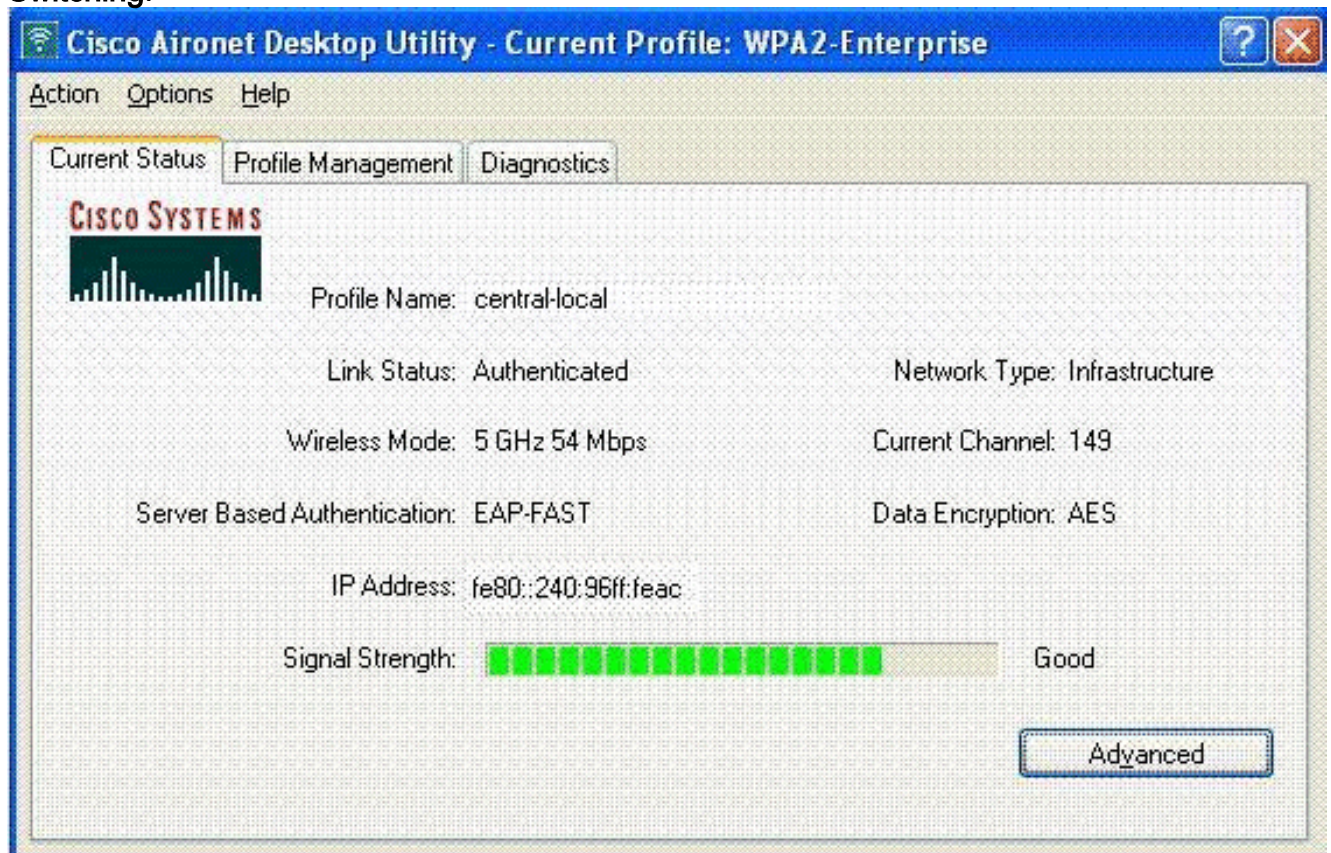
Führen Sie diese Schritte aus:

1. Konfigurieren Sie den Wireless-Client mit den gleichen SSID- und Sicherheitskonfigurationen. In diesem Beispiel ist die SSID *Central-Local* und die Sicherheitsmethode *WPA2*.
2. Geben Sie den Benutzernamen und das Kennwort wie im RADIUS-Server->Benutzer-Setup konfiguriert ein, um die zentrale lokale SSID im Client zu aktivieren. In diesem Beispiel wird *User1* als Benutzername und Kennwort



verwendet.

3. Klicken Sie auf **OK**. Der Client wird vom RADIUS-Server zentral authentifiziert und dem H-REAP AP zugeordnet. Der H-REAP befindet sich jetzt in **zentraler Authentifizierung, lokalem Switching**.



[Deaktivierung der Authentifizierung, lokales Switching](#)

Wenn ein lokal geschaltetes WLAN für einen Authentifizierungstyp konfiguriert ist, der auf dem WLC verarbeitet werden muss (z. B. EAP-Authentifizierung [dynamisches WEP/WPA/WPA2/802.11i], WebAuth oder NAC), wird bei WAN-Ausfall der **Authentifizierungs-**

Lokal-Switching-Zustand aktiviert. In diesem Zustand lehnt der H-REAP für das angegebene WLAN alle neuen Clients ab, die eine Authentifizierung versuchen. Es werden jedoch weiterhin Beacons gesendet und Antworten überprüft, um die ordnungsgemäße Verbindung der vorhandenen Clients sicherzustellen. Dieser Status ist nur im Standalone-Modus gültig.

Verwenden Sie zum Überprüfen dieses Zustands die gleiche Konfiguration, die im Abschnitt [Zentrale Authentifizierung, Lokales Switching](#) beschrieben wird.

Wenn die WAN-Verbindung, die den WLC verbindet, ausfällt, leitet der WLC die Registrierung des H-REAP weiter.

Nach der Registrierung wechselt H-REAP in den Standalone-Modus.

Der über dieses WLAN verbundene Client behält seine Verbindung bei. Da der Controller jedoch nicht für den Authentifizierer verfügbar ist, lassen H-REAP keine neuen Verbindungen von diesem WLAN zu.

Dies kann durch die Aktivierung eines anderen Wireless-Clients im selben WLAN überprüft werden. Sie können feststellen, dass die Authentifizierung für diesen Client fehlschlägt und dass der Client nicht zugeordnet werden darf.

Hinweis: Wenn die Anzahl der WLAN-Clients gleich null ist, beendet H-REAP alle zugeordneten 802.11-Funktionen und keine Beacons mehr für die angegebene SSID. Dadurch wird das WLAN in den nächsten H-REAP-Zustand versetzt, die **Authentifizierung wird deaktiviert, und es wird ein Switching durchgeführt.**

Lokale Authentifizierung, lokales Switching

In diesem Zustand verarbeitet die H-REAP LAP Client-Authentifizierungen und schaltet Client-Datenpakete lokal. Dieser Status ist nur im Standalone-Modus und nur für Authentifizierungstypen gültig, die lokal am Access Point behandelt werden können und keine Verarbeitung des Controllers erfordern.

Der H-REAP, der sich zuvor im **zentralen Authentifizierungs-, lokalen Switching-Zustand** befand, wechselt in diesen Zustand, vorausgesetzt, der konfigurierte Authentifizierungstyp kann lokal am Access Point behandelt werden. Wenn die konfigurierte Authentifizierung nicht lokal verwaltet werden kann, z. B. die 802.1x-Authentifizierung, wird im Standalone-Modus der H-REAP zum **Authentifizierungs-Dead**, zum **lokalen Switching-Modus**, wechselt.

Dies sind einige der gängigen Authentifizierungsmechanismen, die lokal am Access Point im Standalone-Modus behandelt werden können:

- Offen
- Gemeinsam
- WPA-PSK
- WPA2-PSK

Hinweis: Alle Authentifizierungsprozesse werden vom WLC behandelt, wenn sich der Access Point im Modus "Connected" befindet. Während sich der H-REAP im Standalone-Modus befindet, werden offene, gemeinsam genutzte und WPA/WPA2-PSK-Authentifizierungen auf die LAPs übertragen, in denen die gesamte Client-Authentifizierung erfolgt.

Hinweis: Bei Verwendung von Hybrid-REAP mit aktiviertem lokalem Switching im WLAN wird die

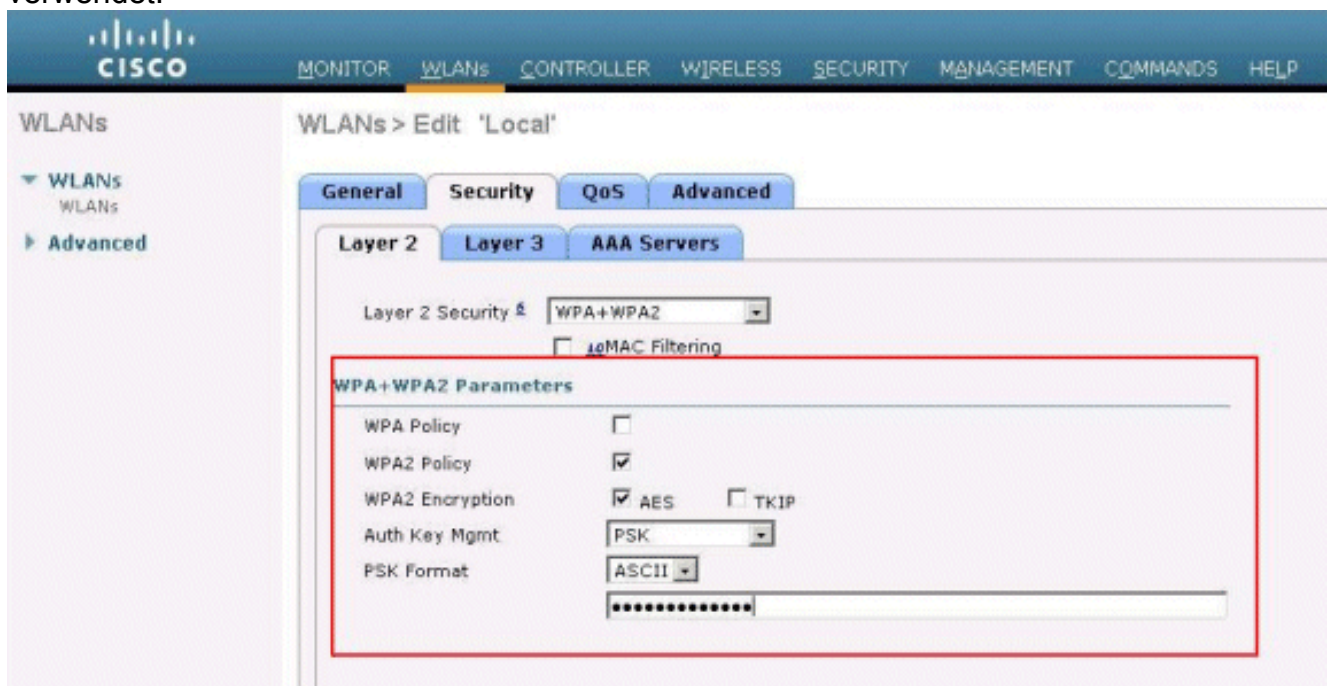
externe Webauthentifizierung nicht unterstützt.

In diesem Beispiel werden folgende Konfigurationseinstellungen verwendet:

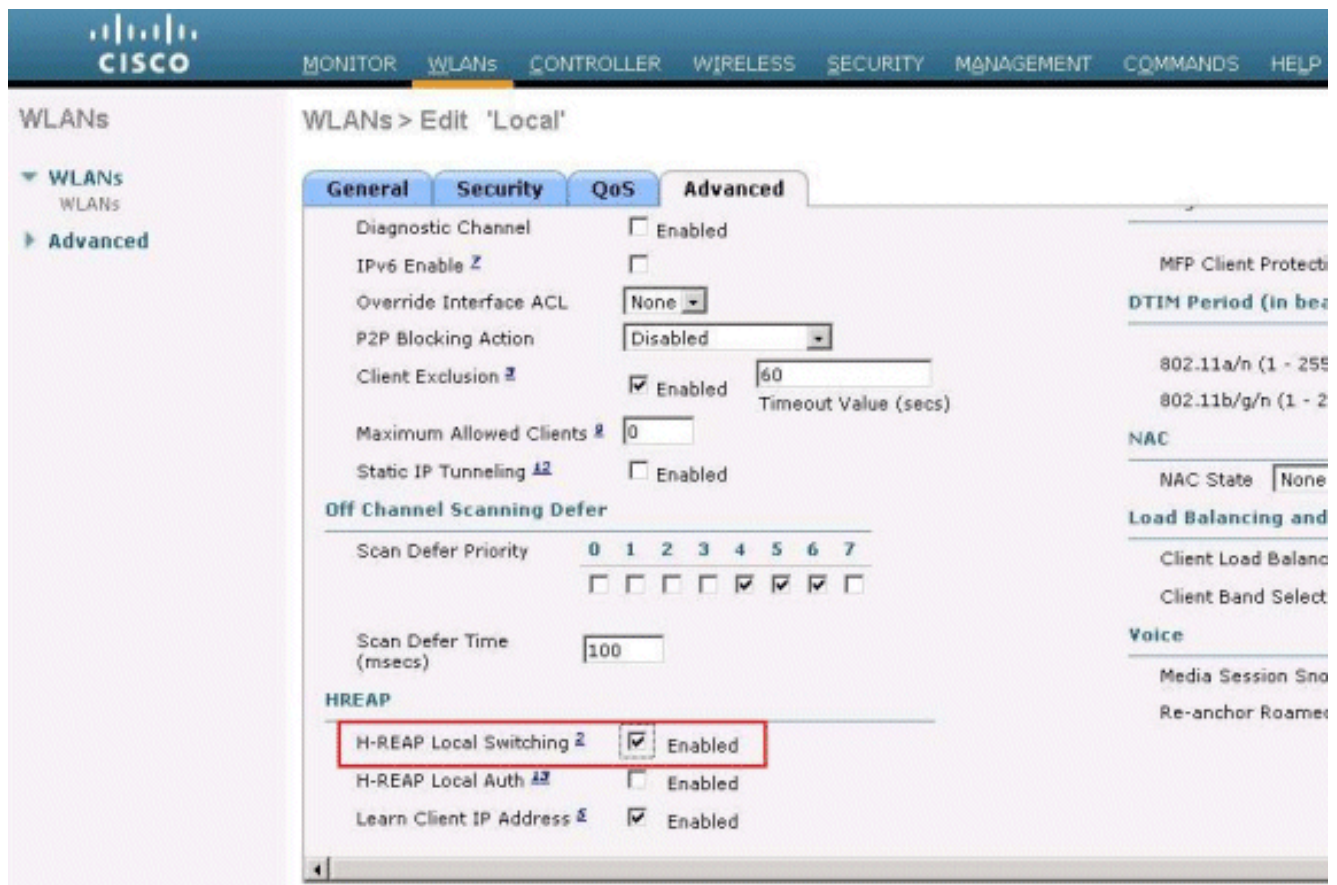
- WLAN/SSID-Name: **Lokal**
- Layer-2-Sicherheit: **WPA-PSK**
- Lokales H-REAP-Switching: **aktiviert**

Gehen Sie in der Controller-GUI wie folgt vor:

1. Klicken Sie auf **WLANS**, um ein neues WLAN mit dem Namen Lokal (Lokal) zu erstellen, und klicken Sie dann auf **Apply (Übernehmen)**.
2. Da dieses WLAN eine lokale Authentifizierung verwendet, wählen Sie **WPA-PSK** oder einen der oben genannten Sicherheitsmechanismen aus, die lokal im Sicherheitsfeld für Layer 2 behandelt werden können. In diesem Beispiel wird **WPA-PSK** verwendet.



3. Nach der Auswahl müssen Sie die zu verwendende Pre-Shared Key/Pass-Kennzeichenfolge konfigurieren. Dies muss auf Clientseite identisch sein, damit die Authentifizierung erfolgreich ist.
4. Aktivieren Sie das Kontrollkästchen **H-REAP Local Switching** (Lokales H-REAP-Switching), um den Client-Datenverkehr, der zu diesem WLAN lokal am H-REAP gehört, umzuschalten.



Lokale Authentifizierung, lokales Switching überprüfen

Führen Sie diese Schritte aus:

1. Konfigurieren Sie den Client mit den gleichen SSID- und Sicherheitskonfigurationen. Hier ist die SSID *lokal* und die Sicherheitsmethode *WPA-PSK*.
2. Aktivieren Sie die lokale SSID im Client. Der Client wird beim Controller zentral authentifiziert und dem H-REAP zugeordnet. Der Client-Datenverkehr wird für den lokalen Switch konfiguriert. Nun befindet sich der H-REAP im Status Zentrale Authentifizierung, Lokales Switching.
3. Deaktivieren Sie die WAN-Verbindung, die mit dem Controller verbunden ist. Der Controller durchläuft wie gewohnt den Deregistrierungsprozess. H-REAP wird vom Controller registriert. Nach der Registrierung wechselt H-REAP in den Standalone-Modus. Der Client, der zu diesem WLAN gehört, ist jedoch weiterhin mit H-REAP verknüpft. Da der Authentifizierungstyp hier lokal am Access Point ohne Controller behandelt werden kann, erlaubt H-REAP auch Verbindungen von einem beliebigen neuen Wireless-Client über dieses WLAN.
4. Aktivieren Sie zur Verifizierung dieses Vorgangs alle anderen Wireless-Clients im selben WLAN. Wie Sie sehen, wird der Client erfolgreich authentifiziert und zugeordnet.

Fehlerbehebung

- Um weitere Probleme bei der Client-Konnektivität am Konsolenport von H-REAP zu beheben, geben Sie den folgenden Befehl ein:

```
AP_CLI#show capwap reap association
```

- Verwenden Sie folgenden Befehl, um weitere Probleme bei der Client-Konnektivität am Controller zu beheben und die Ausgabe von weiteren Debugging-Vorgängen zu beschränken:

```
AP_CLI#debug mac addr
```

- Verwenden Sie folgenden Befehl, um die 802.11-Verbindungsprobleme eines Clients zu debuggen:

```
AP_CLI#debug dot11 state enable
```

- Debuggen Sie den 802.1X-Authentifizierungsprozess eines Clients und Fehler mit diesem Befehl:

```
AP_CLI#debug dot1x events enable
```

- Backend-Controller-/RADIUS-Meldungen können mit dem folgenden Befehl gedebuggt werden:

```
AP_CLI#debug aaa events enable
```

- Alternativ können Sie den folgenden Befehl verwenden, um eine vollständige Anpassung der Befehle für das Client-Debuggen zu aktivieren:

```
AP_CLI#debug client
```

Zugehörige Informationen

- [Grundlegende Konfigurationsbeispiel für Wireless LAN Controller und Lightweight Access Point](#)
- [Konfigurationsbeispiel für VLANs auf Wireless LAN-Controllern](#)
- [Cisco Wireless LAN Controller Configuration Guide, Release 7.0](#)
- [Hybrid-REAP - Design- und Bereitstellungsleitfaden](#)
- [Grundlegende Fehlerbehebung für den Hybrid Remote Edge Access Point \(H-REAP\)](#)
- [Konfigurationsbeispiel für WLAN-Controller-Failover für Lightweight Access Points](#)
- [Wireless-Produktunterstützung](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)