Konfigurieren eines VAP auf dem WAP351, WAP131 und WAP371

Ziel

Virtual Access Points (VAPs) segmentieren das WLAN in mehrere Broadcast-Domänen, die das WLAN-Äquivalent zu Ethernet-VLANs darstellen. VAPs simulieren mehrere Access Points in einem physischen WAP-Gerät. Der Cisco WAP131 unterstützt bis zu vier VAPs, der Cisco WAP351 und der WAP371 bis zu acht VAPs.

In diesem Dokument wird die Konfiguration eines VAP für die WAP351-, WAP131- und WAP371-Access Points erläutert.

Anwendbare Geräte

WAP351

WAP131

WAP371

Softwareversion

·V1.0.0.39 (WAP351)

·V1.0.0.39 (WAP131)

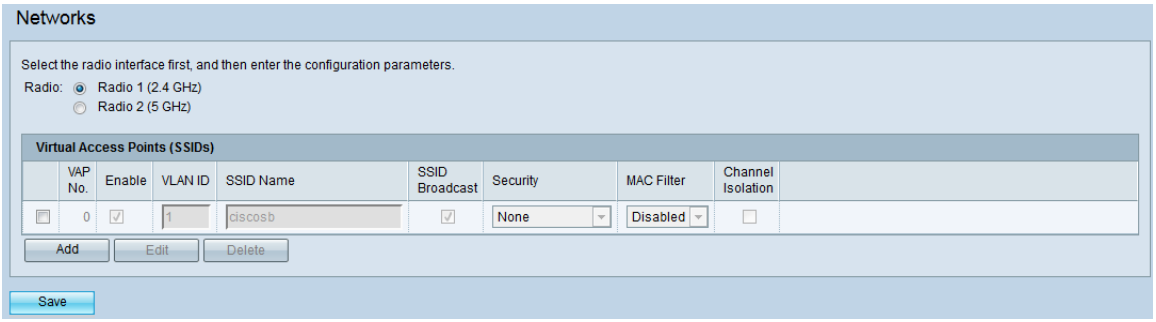
·V1.2.0.2 (WAP371)

Hinzufügen und Konfigurieren eines VAP

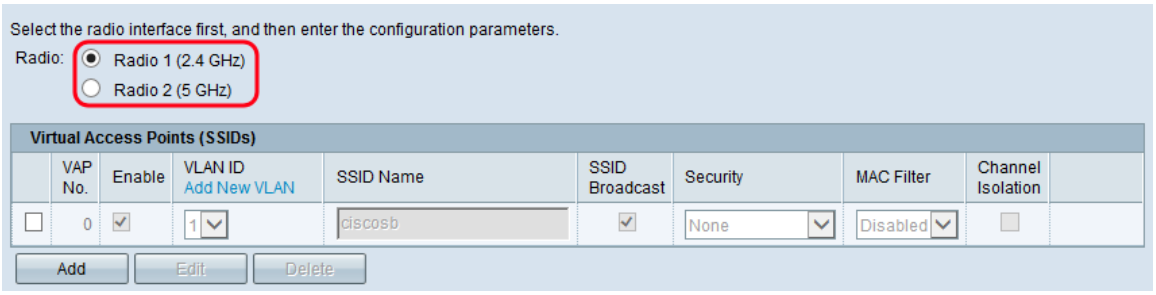
Hinweis: Jeder VAP wird durch einen benutzerdefinierten Service Set Identifier (SSID) identifiziert. Mehrere VAPs können nicht denselben SSID-Namen haben.

Hinweis: Damit Ihr Wireless-Netzwerk funktioniert, muss die Funkverbindung, der Ihr konfigurierter VAP zugeordnet ist, aktiviert und ordnungsgemäß konfiguriert sein. Weitere Informationen finden Sie unter *Konfigurieren der grundlegenden Funkeinstellungen auf dem WAP131 und WAP351* oder *Konfigurieren der grundlegenden Funkeinstellungen auf dem WAP371*.

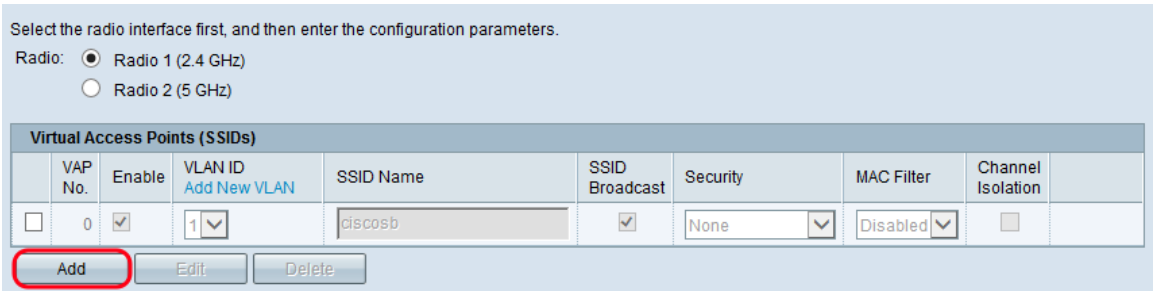
Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und navigieren Sie zu **Wireless > Networks**. Die Seite *Netzwerke* wird angezeigt:



Schritt 2: Wählen Sie im Feld *Radio (Funkübertragung)* das Optionsfeld für das Wireless-Funkmodul aus, für das Sie VAPs konfigurieren möchten.

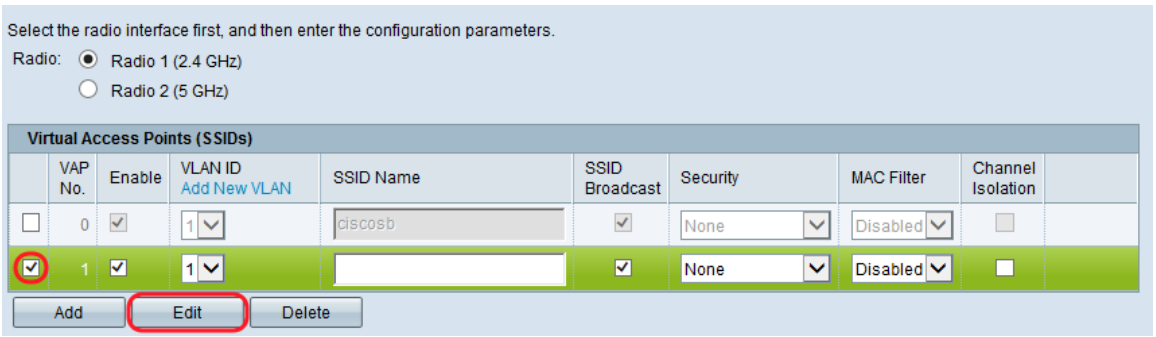


Schritt 3: Um einen neuen VAP hinzuzufügen, klicken Sie auf **Hinzufügen**. In der Tabelle wird ein neuer VAP angezeigt.

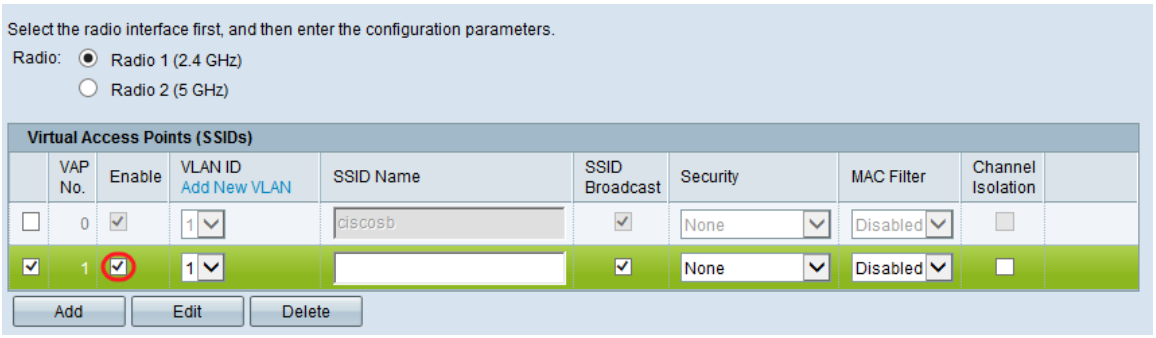


Hinweis: Der WAP131 unterstützt bis zu 4 VAPs, während der WAP371 und der WAP351 bis zu 8 VAPs unterstützen.

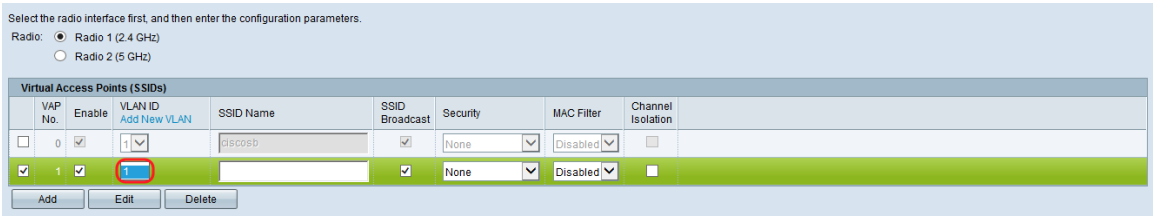
Schritt 4: Um mit der Bearbeitung eines VAP zu beginnen, klicken Sie auf das Kontrollkästchen ganz links neben dem Tabelleneintrag und dann auf **Bearbeiten**. Dadurch können Sie die ausgegrauten Felder des ausgewählten VAP ändern.



Schritt 5: Um die Verwendung des VAP zu aktivieren, stellen Sie sicher, dass das Kontrollkästchen *Aktivieren* aktiviert ist.

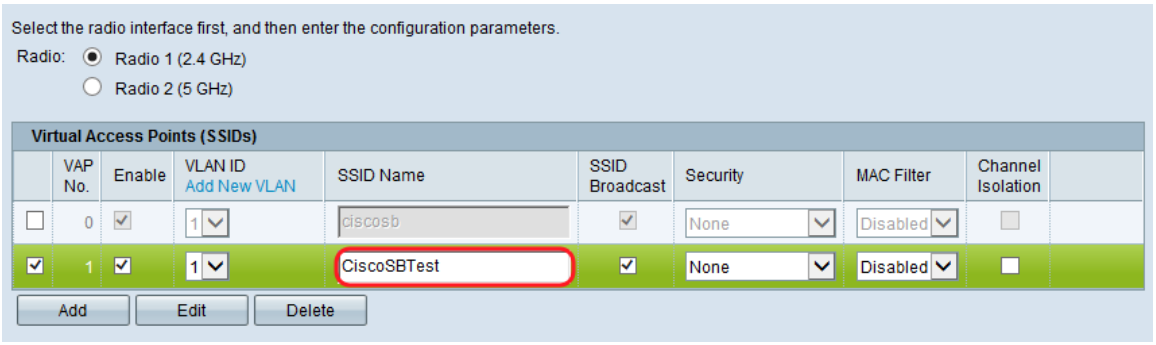


Schritt 6: Geben Sie im Feld "*VLAN ID*" die VLAN-ID an, die Sie dem VAP zuordnen möchten. Wenn Sie WAP131 oder WAP371 verwenden, geben Sie die VLAN-ID ein. Der maximal einzugebende Wert ist 4094.

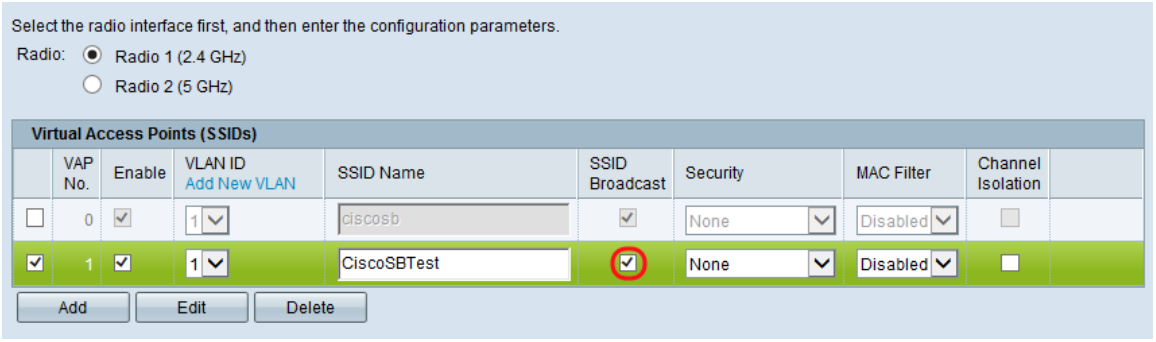


Hinweis: Die eingegebene VLAN-ID muss in Ihrem Netzwerk vorhanden und korrekt konfiguriert sein. Weitere Informationen finden Sie unter *VLAN-Konfiguration auf dem WAP351 Access Point*, *Verwalten getaggter und nicht getaggter VLAN-IDs auf dem WAP131* oder *Verwalten getaggter und nicht getaggter VLAN-IDs auf dem WAP371*.

Schritt 7: Geben Sie im Feld SSID Name (SSID-Name) den Namen des Wireless-Netzwerks ein. Jeder VAP muss einen eindeutigen SSID-Namen haben.

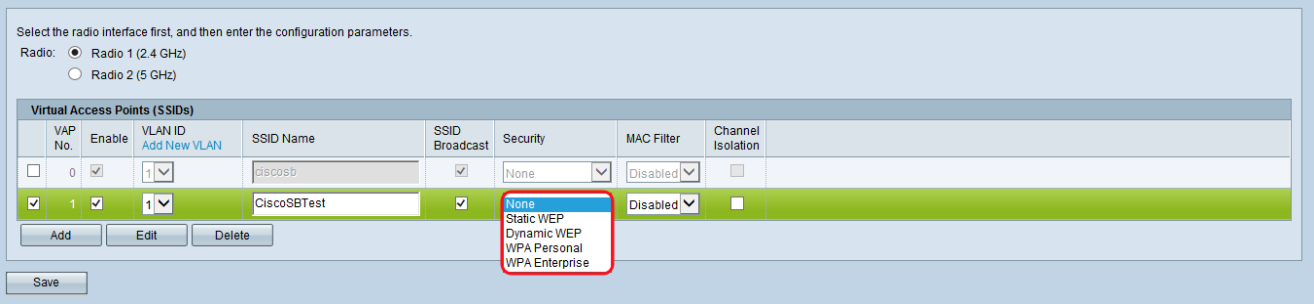


Schritt 8: Wenn der SSID-Name an die Clients gesendet werden soll, aktivieren Sie das Kontrollkästchen *SSID-Broadcast*. Dadurch wird den Clients in der Liste der verfügbaren Netzwerke der SSID-Name angezeigt.



Konfigurieren von Sicherheitseinstellungen

Schritt 1: Wählen Sie aus der Dropdown-Liste *Security* (Sicherheit) die Authentifizierungsmethode aus, die für die Verbindung mit dem VAP erforderlich ist. Wenn eine andere Option als **Keine** aktiviert ist, werden zusätzliche Felder angezeigt.



Folgende Optionen sind verfügbar:

·Keine

·Statisches WEP

·Dynamisches WEP

WPA Personal

WPA Enterprise

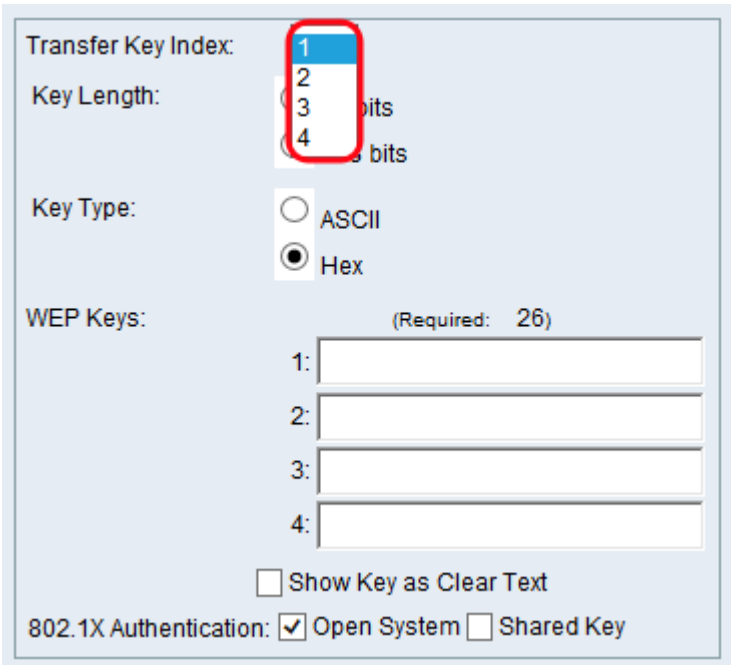
Hinweis: WPA Personal und WPA Enterprise sind die bevorzugten Authentifizierungstypen für maximale Sicherheit. Static WEP und Dynamic WEP sollten nur mit Legacy-Geräten verwendet werden und erfordern, dass die Funkübertragung auf den 802.11a- oder den 802.11b/g-Modus eingestellt wird. Weitere Informationen finden Sie unter *Konfigurieren der grundlegenden Funkeinstellungen auf dem WAP131 und WAP351* oder *Konfigurieren der grundlegenden Funkeinstellungen auf dem WAP371*.

Statisches WEP

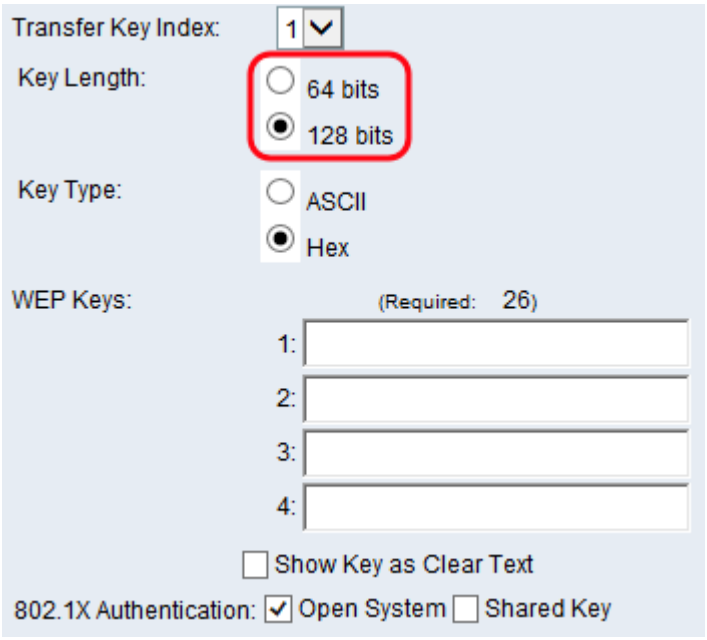
Static WEP ist die am wenigsten sichere Authentifizierungsmethode. Sie verschlüsselt Daten im Wireless-Netzwerk anhand eines statischen Schlüssels. Da dieser statische Schlüssel unrechtmäßig erworben werden kann, sollte die WEP-Authentifizierung nur bei Bedarf mit älteren Geräten verwendet werden.

Hinweis: Wenn Sie *Static WEP* als Sicherheitsmethode auswählen, wird eine Eingabeaufforderung angezeigt, die Ihnen mitteilt, dass die Wahl der Sicherheitsmethode sehr unsicher ist.

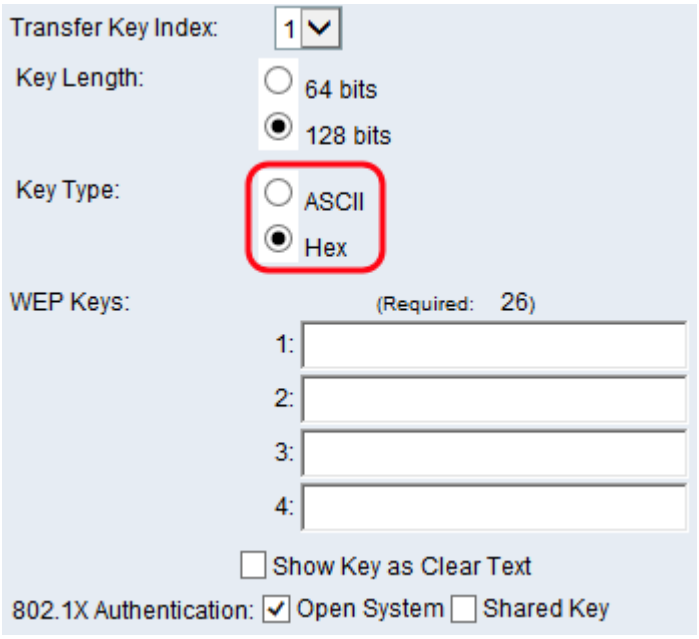
Schritt 1: Wählen Sie in der Dropdown-Liste *Transfer Key Index* den Index des WEP-Schlüssels aus der Liste der Schlüssel aus, die das Gerät zur Verschlüsselung von Daten verwenden wird.



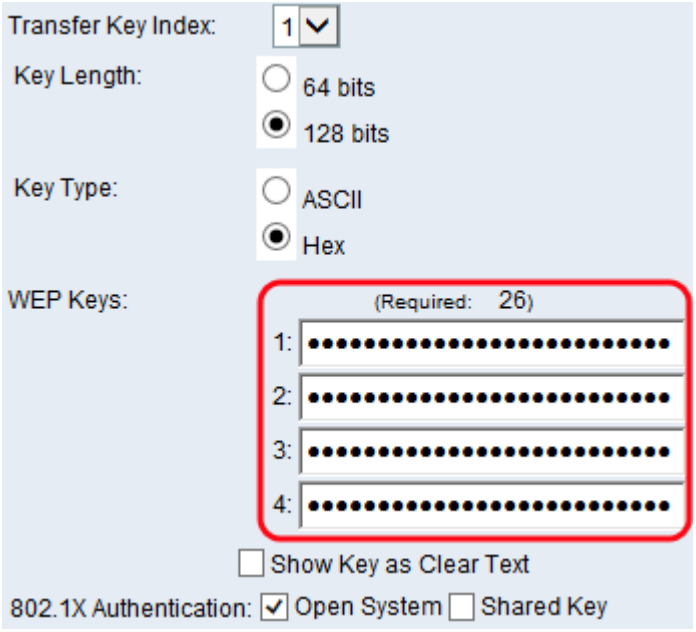
Schritt 2: Wählen Sie eine Optionsschaltfläche im Feld *Schlüssellänge*, um anzugeben, ob der Schlüssel 64 Bit oder 128 Bit lang ist.



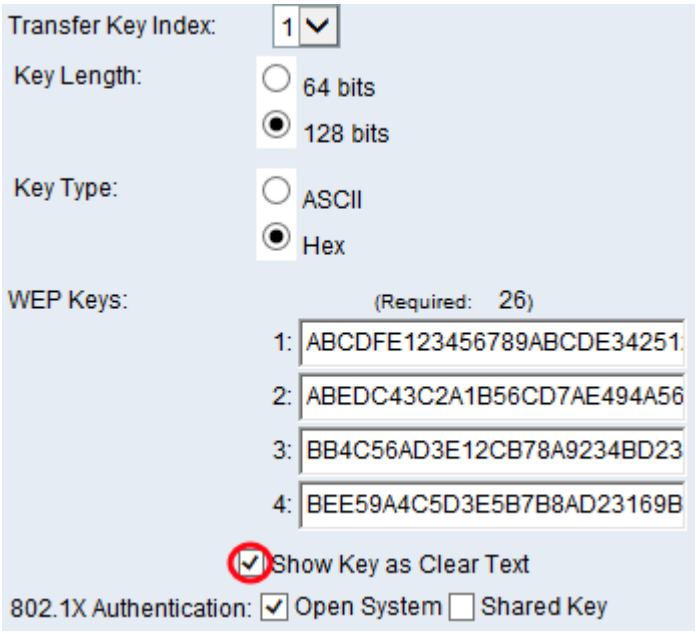
Schritt 3: Wählen Sie im Feld *Key Type* (*Schlüsseltyp*) aus, ob Sie die Schlüssel im ASCII- oder Hexadezimalformat eingeben möchten. ASCII enthält alle Buchstaben, Zahlen und Symbole, die auf der Tastatur vorhanden sind, während Hexadezimalzeichen nur Zahlen oder Buchstaben A bis F enthalten dürfen.



Schritt 4: Geben Sie im Feld *WEP-Schlüssel* bis zu 4 verschiedene WEP-Schlüssel für Ihr Gerät ein. Jeder Client, der mit diesem Netzwerk verbunden werden soll, muss über einen der gleichen WEP-Schlüssel im gleichen Steckplatz verfügen, der vom Gerät angegeben wird.

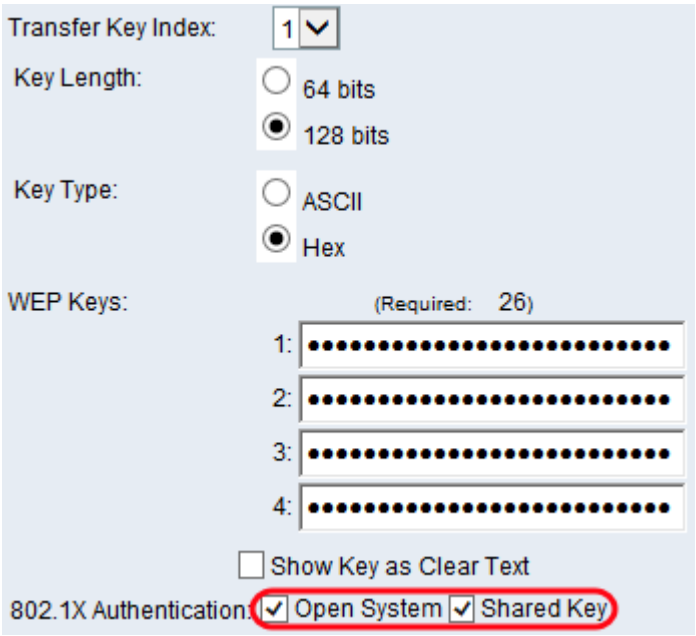


Schritt 5: (Optional) Klicken Sie im Feld *Schlüssel als Klartext anzeigen* auf das Kontrollkästchen, wenn Sie die Zeichenfolgen der Schlüssel angeben.



Hinweis: Bei Verwendung einer anderen Firmware auf dem WAP351, WAP131 oder WAP371 fehlt möglicherweise das Feld *Schlüssel als Klartext anzeigen*.

Schritt 6: Geben Sie im Feld *802.1X Authentication* (*802.1X-Authentifizierung*) den Authentifizierungsalgorithmus an, den Sie verwenden möchten, indem Sie die Optionen *Open System* und/oder *Shared Key* auswählen. Der Authentifizierungsalgorithmus definiert die Methode, mit der bestimmt wird, ob eine Client-Station dem WAP-Gerät zugeordnet werden darf, wenn statisches WEP der Sicherheitsmodus ist.



Die verfügbaren Optionen sind wie folgt definiert:

·Open System (Offenes System): Die Authentifizierung ermöglicht es jeder Client-Station, dem WAP-Gerät zuzuordnen, ob diese Client-Station über den richtigen WEP-Schlüssel verfügt oder nicht. Dieser Algorithmus wird im Nur-Text-, IEEE 802.1X- und WPA-Modus verwendet. Wenn der Authentifizierungsalgorithmus auf *Open System* festgelegt ist, kann jeder Client dem WAP-Gerät eine Verbindung herstellen.

·Shared Key (Gemeinsam genutzter Schlüssel): Für die Authentifizierung muss die Client-Station über den richtigen WEP-Schlüssel verfügen, um eine Verbindung zum WAP-Gerät

herzustellen. Wenn der Authentifizierungsalgorithmus auf *Shared Key* festgelegt ist, kann eine Station mit einem falschen WEP-Schlüssel keine Verbindung zum WAP-Gerät herstellen.

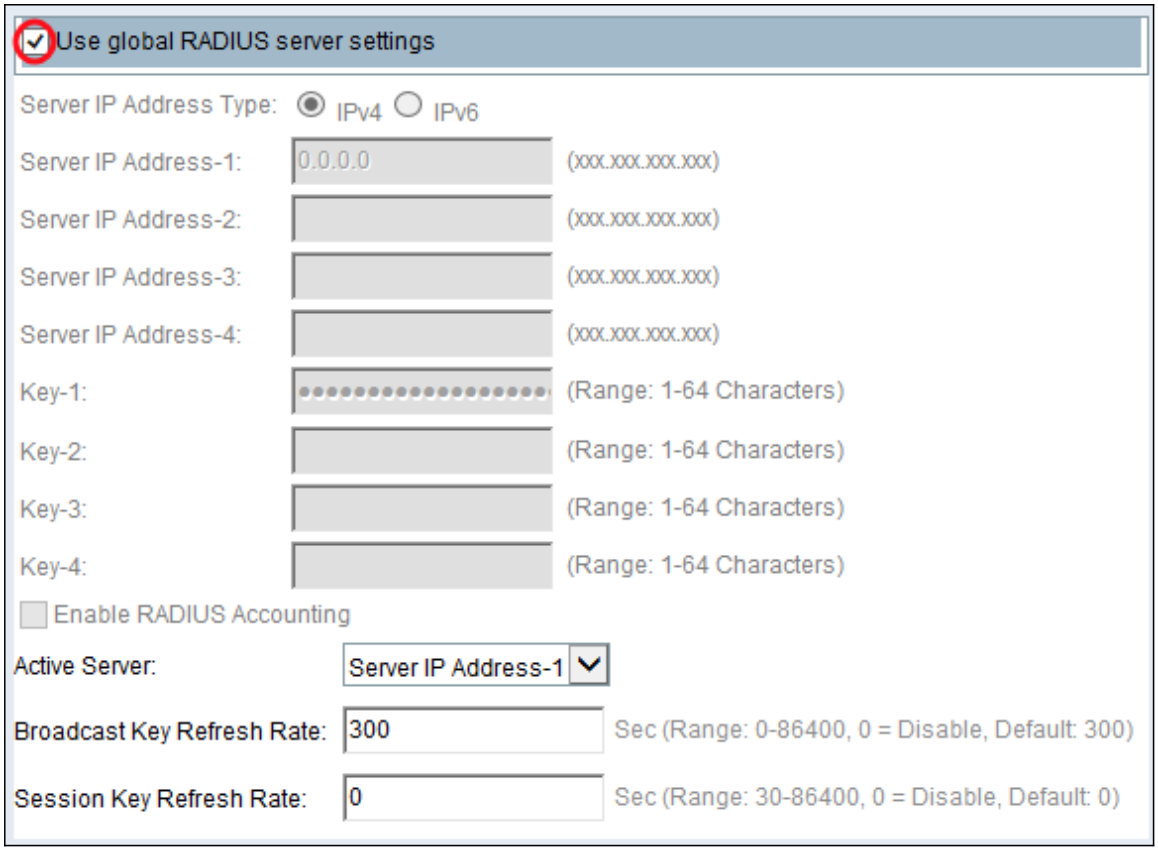
·Open System and Shared Key (System und gemeinsamer Schlüssel öffnen): Wenn Sie beide Authentifizierungsalgorithmen ausgewählt haben, müssen die für die Verwendung von WEP im Modus "shared key" konfigurierten Client-Stationen über einen gültigen WEP-Schlüssel verfügen, um eine Verbindung mit dem WAP-Gerät herzustellen. Außerdem können die Client-Stationen, die für die Verwendung von WEP als offenes System konfiguriert sind (Modus für gemeinsam genutzte Schlüssel nicht aktiviert), dem WAP-Gerät eine Verbindung herstellen, selbst wenn sie nicht über den richtigen WEP-Schlüssel verfügen.

Schritt 7: Klicken Sie auf **Speichern**.

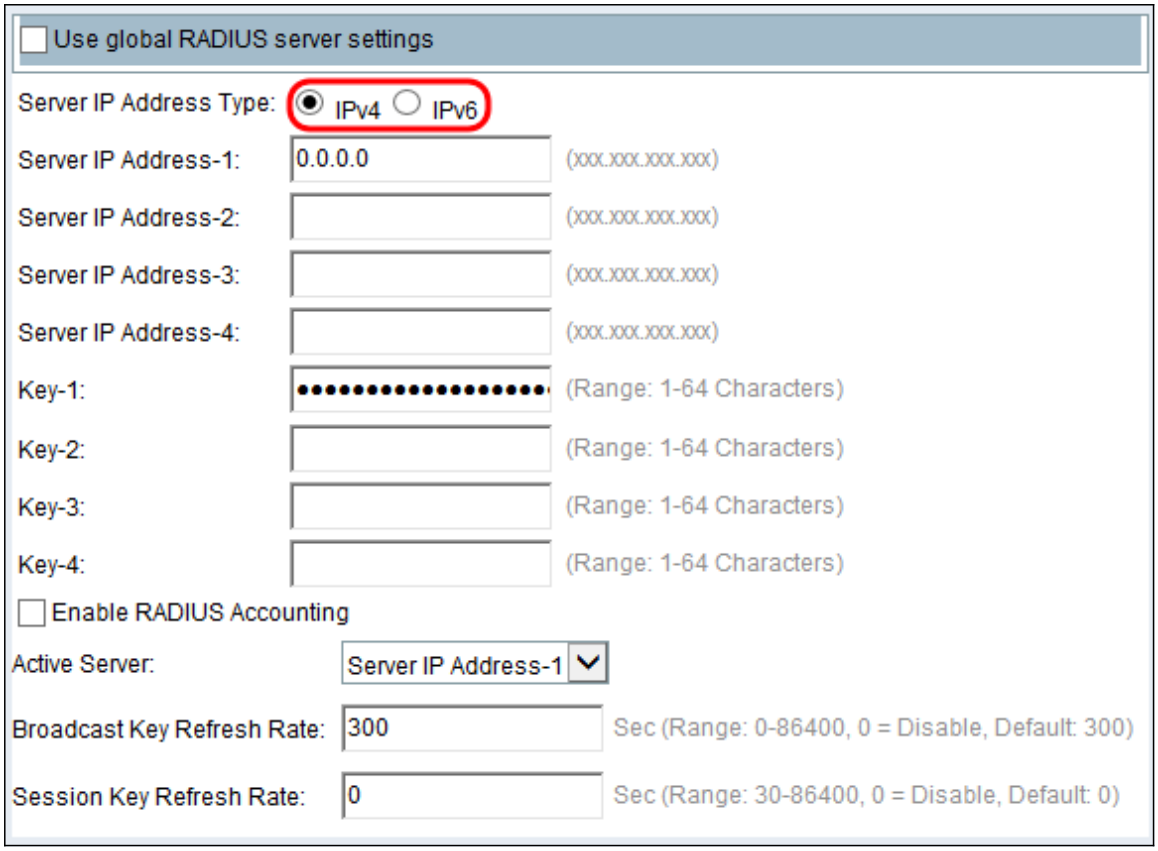
Dynamisches WEP

Dynamisches WEP bezieht sich auf die Kombination der 802.1x-Technologie mit dem Extensible Authentication Protocol (EAP). Dieser Modus erfordert die Verwendung eines externen RADIUS-Servers zur Authentifizierung von Benutzern. Das WAP-Gerät benötigt einen RADIUS-Server, der EAP unterstützt, z. B. den Microsoft Internet Authentication Server. Um mit Microsoft Windows-Clients arbeiten zu können, muss der Authentifizierungsserver PEAP (Protected EAP) und MSCHAP v2 unterstützen. Sie können eine Vielzahl von Authentifizierungsmethoden verwenden, die vom IEEE 802.1X-Modus unterstützt werden, einschließlich Zertifikate, Kerberos und Authentifizierung mit öffentlichen Schlüsseln. Sie müssen jedoch die Client-Stationen so konfigurieren, dass sie dieselbe Authentifizierungsmethode verwenden, die das WAP-Gerät verwendet.

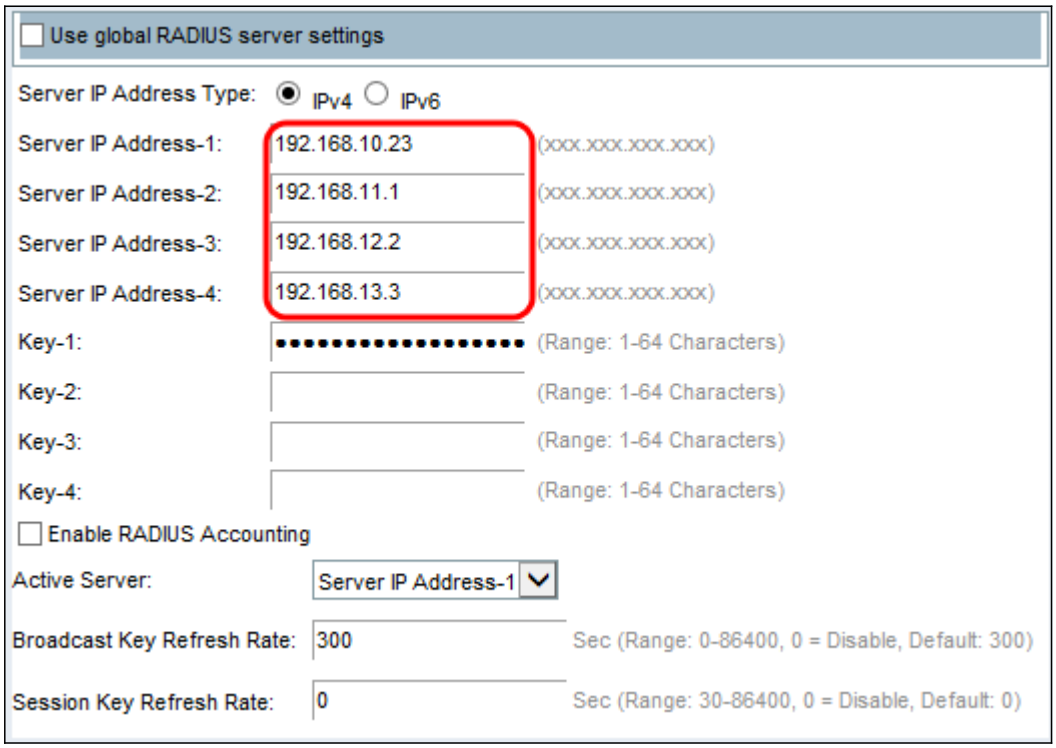
Schritt 1: Standardmäßig ist die Option *Globale RADIUS-Servereinstellungen verwenden* aktiviert. Deaktivieren Sie das Kontrollkästchen, wenn Sie den VAP für die Verwendung eines anderen RADIUS-Serversatzes konfigurieren möchten. Fahren Sie andernfalls mit Schritt 8 fort.



Schritt 2: Wählen Sie im Feld *Server IP Address Type* (IP-Adresstyp des Servers) den von Ihrem WAP-Gerät verwendeten IP-Adresstyp des Servers aus. Die Optionen sind *IPv4* oder *IPv6*. IPv4 verwendet 32-Bit-Binärzahlen, die in Dezimalpunktschreibweise dargestellt werden. IPv6 verwendet Hexadezimalzahlen und Doppelpunkte, um eine 128-Bit-Binärzahl darzustellen. Das WAP-Gerät kontaktiert nur den oder die RADIUS-Server für den Adresstyp, den Sie in diesem Feld ausgewählt haben. Wenn Sie IPv6 auswählen, fahren Sie mit Schritt 4 fort.

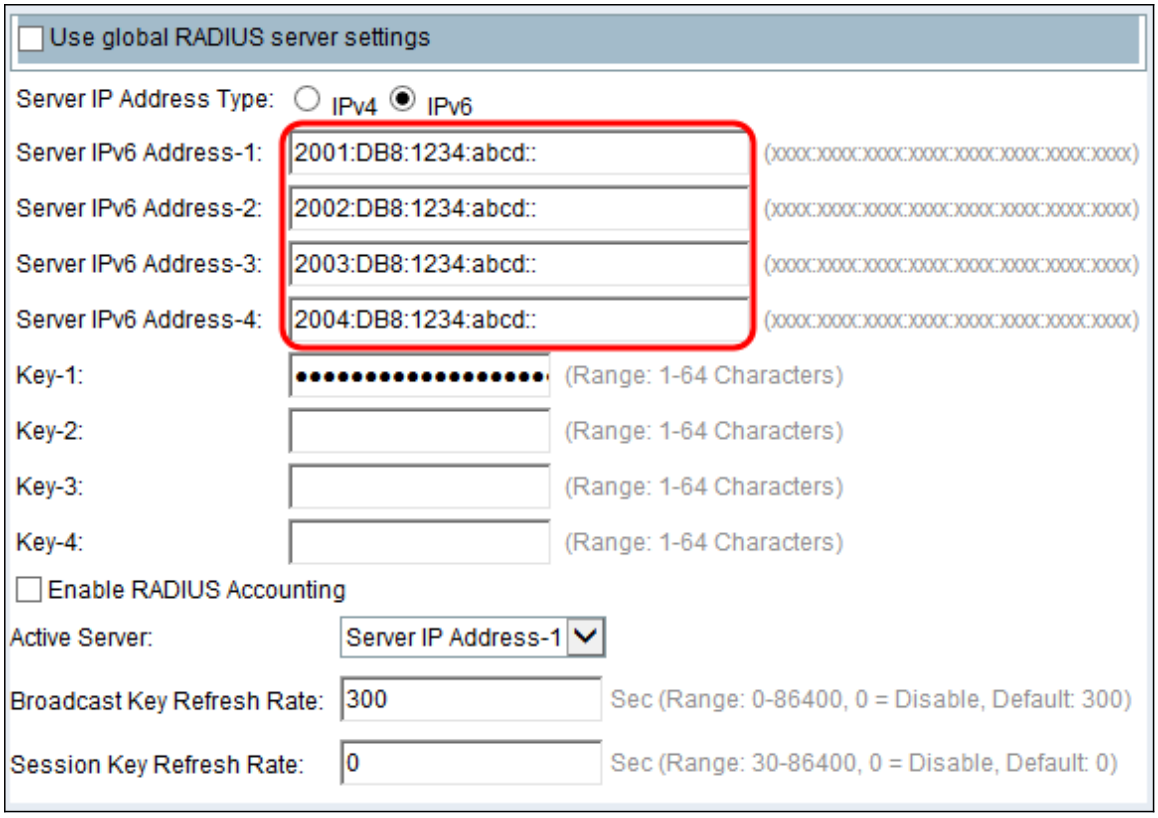


Schritt 3: Wenn Sie **IPv4** in Schritt 2 ausgewählt haben, geben Sie die IP-Adresse des RADIUS-Servers ein, den alle VAPs standardmäßig verwenden. Fahren Sie anschließend mit Schritt 5 fort.



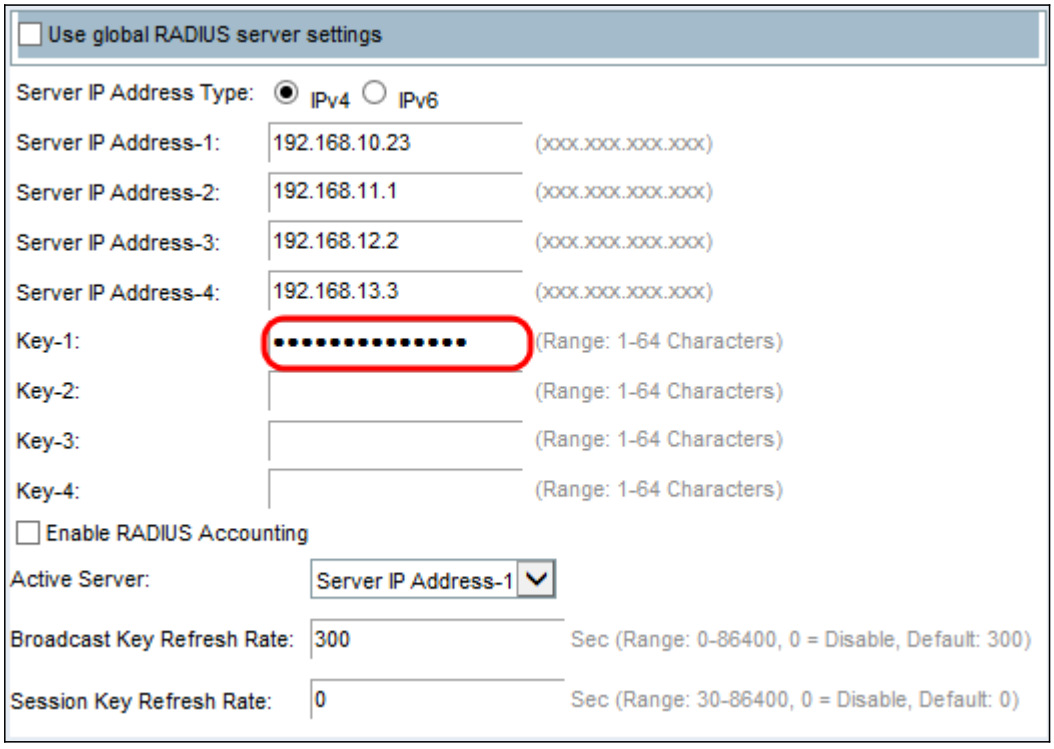
Hinweis: Sie können bis zu drei IPv4-Backup-RADIUS-Serveradressen einrichten. Wenn die Authentifizierung mit dem primären Server fehlschlägt, wird jeder konfigurierte Backup-Server nacheinander versucht.

Schritt 4: Wenn Sie **IPv6** in Schritt 2 ausgewählt haben, geben Sie die IPv6-Adresse des primären globalen RADIUS-Servers ein.

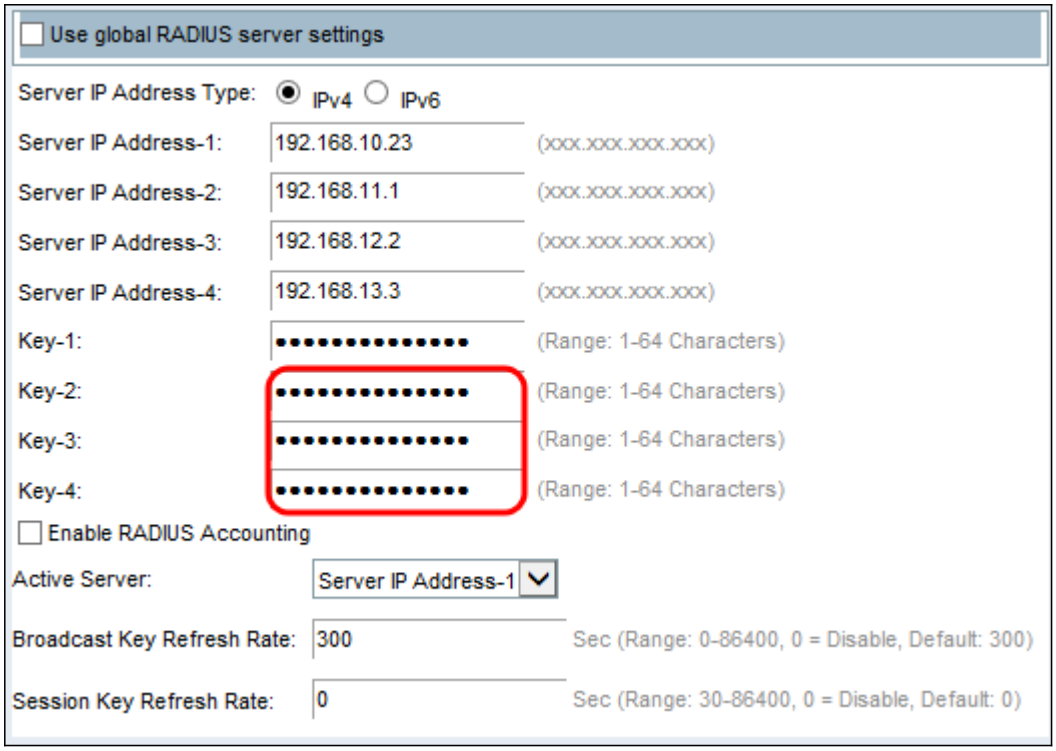


Hinweis: Sie können bis zu drei IPv6-Backup-RADIUS-Serveradressen einrichten. Wenn die Authentifizierung mit dem primären Server fehlschlägt, wird jeder konfigurierte Backup-Server nacheinander versucht.

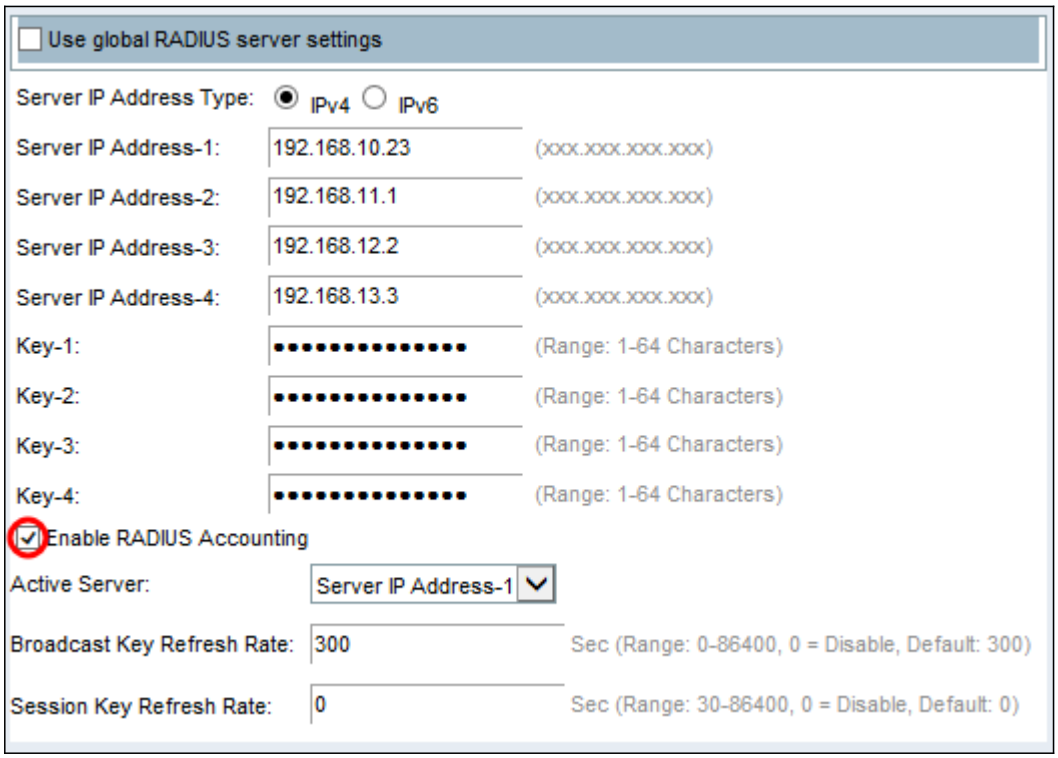
Schritt 5: Geben Sie im Feld *Key-1* den gemeinsamen geheimen Schlüssel ein, den das WAP-Gerät zur Authentifizierung des primären RADIUS-Servers verwendet.



Schritt 6: Geben Sie in den Feldern *Key-2* to *Key-4* den RADIUS-Schlüssel ein, der den konfigurierten Backup-RADIUS-Servern zugeordnet ist. Die Server-IP-Adresse 2 verwendet *Key-2*, die Server-IP-Adresse 3 verwendet *Key-3* und die Server-IP-Adresse 4 verwendet *Key-4*.



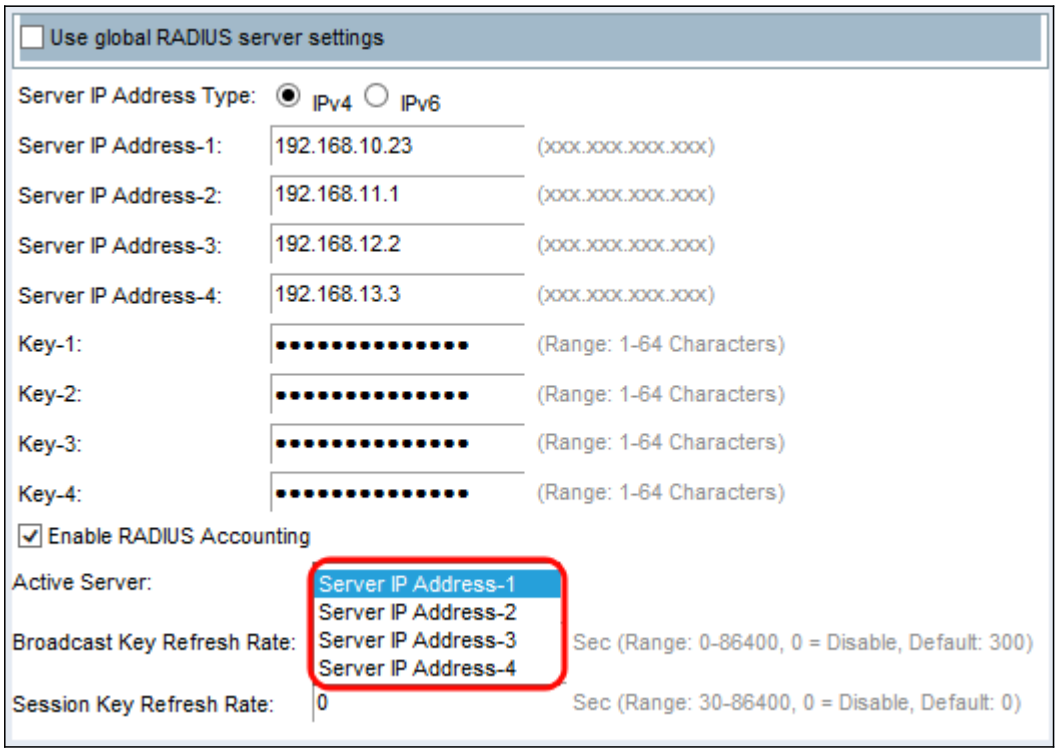
Schritt 7: (Optional) Aktivieren Sie im Feld *Enable RADIUS Accounting (RADIUS-Accounting aktivieren*) das Kontrollkästchen, wenn Sie die Nachverfolgung und Messung der Ressourcen aktivieren möchten, die ein bestimmter Benutzer verbraucht hat. Bei Aktivierung von RADIUS Accounting werden die Systemzeit und die Menge der übertragenen und empfangenen Daten nachverfolgt. Die Informationen werden im Radius-Server gespeichert. Dies wird für den primären RADIUS-Server und alle Backup-Server aktiviert.



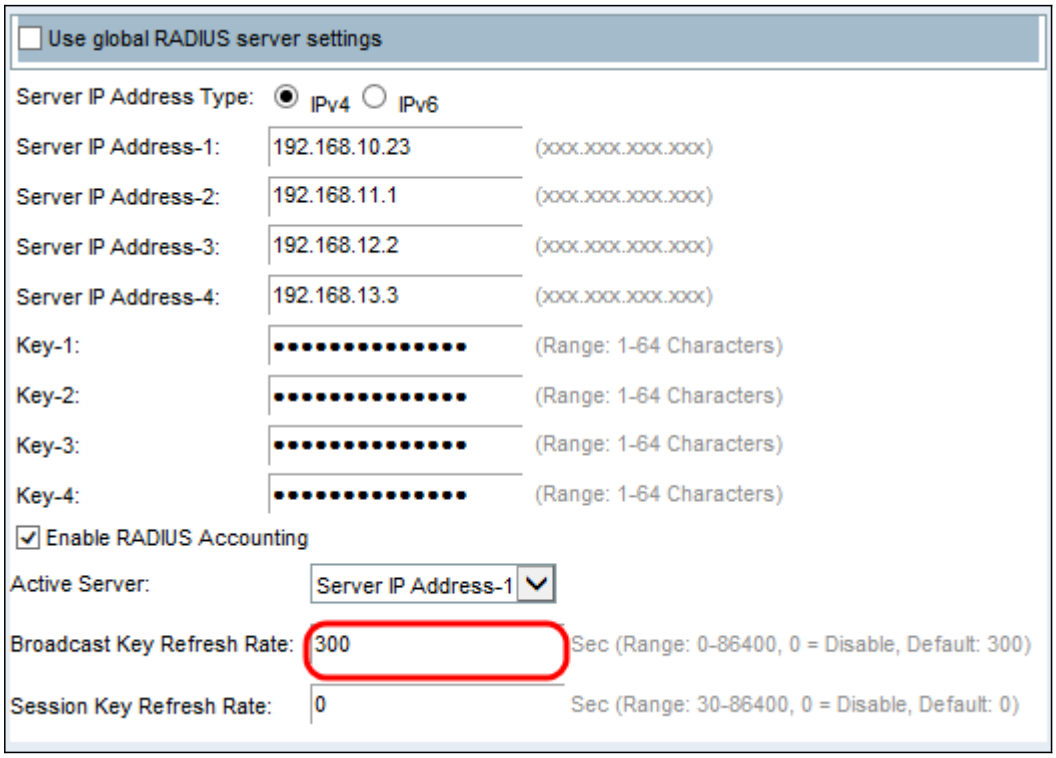
Hinweis: Wenn Sie RADIUS Accounting aktiviert haben, ist dieser für den primären RADIUS-Server und alle Backup-Server aktiviert.

Schritt 8: Wählen Sie den ersten Server aus, der im Feld *Active Server* aktiv ist. Dadurch kann der aktive RADIUS-Server manuell ausgewählt werden, anstatt dass das WAP-Gerät versucht, jeden konfigurierten Server nacheinander zu kontaktieren und den ersten aktiven

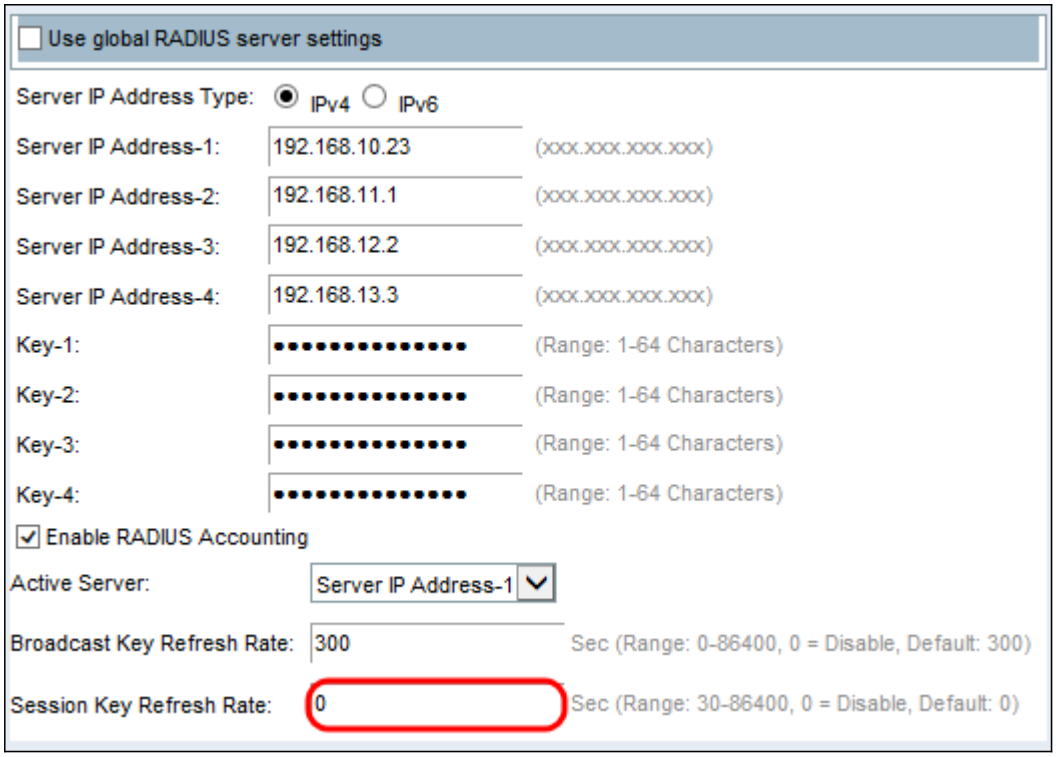
Server auszuwählen.



Schritt 9: Geben Sie im Feld *Broadcast Key Refresh Rate (Aktualisierungsrate für Sendeschlüssel*) das Intervall ein, in dem der Schlüssel Broadcast (Gruppe) für Clients aktualisiert wird, die diesem VAP zugeordnet sind. Der Standardwert ist 300 Sekunden.



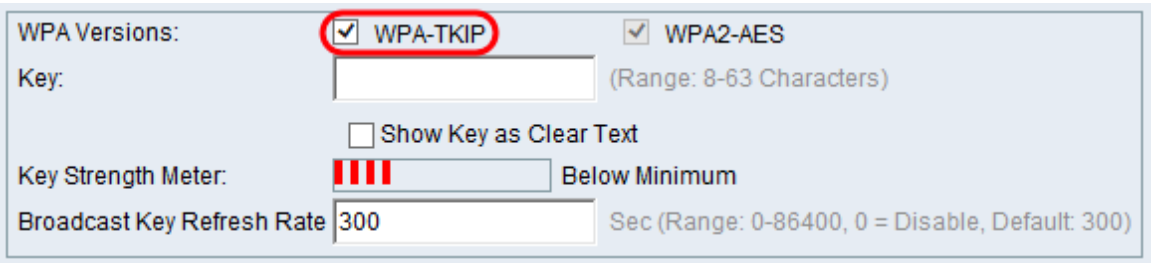
Schritt 10: Geben Sie im Feld *Session Key Refresh Rate (Aktualisierungsrate für Sitzungsschlüssel*) das Intervall ein, in dem das WAP-Gerät den Sitzungsschlüssel (Unicast) für jeden dem VAP zugeordneten Client aktualisiert. Der Standardwert ist 0.



WPA Personal

WPA Personal ist ein IEEE 802.11i-Standard der Wi-Fi Alliance, der AES-CCMP- und TKIP-Verschlüsselung umfasst. WPA verwendet einen Pre-Shared Key (PSK), anstatt IEEE 802.1X und EAP zu verwenden, wie dies im Enterprise WPA-Sicherheitsmodus der Fall ist. Der PSK wird nur für eine Erstprüfung auf Anmeldeinformationen verwendet. WPA wird auch als WPA-PSK bezeichnet. Dieser Sicherheitsmodus ist abwärtskompatibel für die Wireless-Clients, die das ursprüngliche WPA unterstützen.

Schritt 1: Aktivieren Sie im Feld *WPA-Versionen* das Kontrollkästchen *WPA-TKIP*, wenn Sie WPA-TKIP aktivieren möchten. Sie können WPA-TKIP und WPA2-AES gleichzeitig aktivieren. Der WAP unterstützt immer WPA2-AES, sodass Sie ihn nicht konfigurieren können.



Die verfügbaren Optionen sind wie folgt definiert:

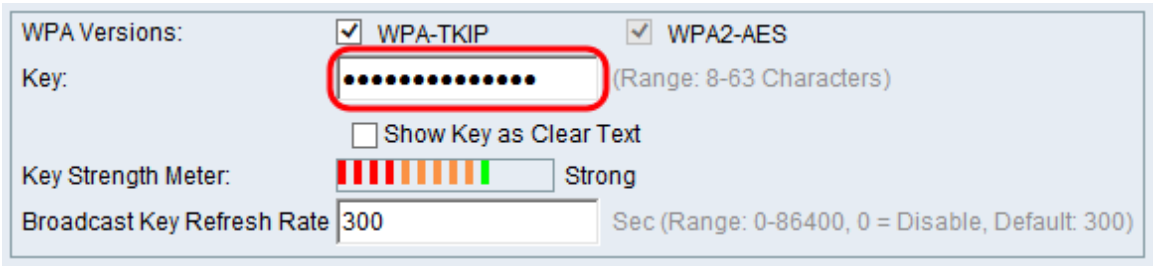
·WPA-TKIP - Das Netzwerk verfügt über einige Client-Stationen, die nur das ursprüngliche WPA- und TKIP-Sicherheitsprotokoll unterstützen. Gemäß den neuesten Anforderungen der WiFi Alliance wird die Entscheidung nur für WPA-TKIP nicht empfohlen.

·WPA2-AES - Alle Client-Stationen im Netzwerk unterstützen das WPA2- und das AES-CCMP-Verschlüsselungs-/Sicherheitsprotokoll. Diese WPA-Version bietet die beste Sicherheit gemäß IEEE 802.11i-Standard. Gemäß den neuesten Anforderungen der WiFi Alliance muss der Access Point diesen Modus ständig unterstützen.

·WPA-TKIP und WPA2-AES: Wenn das Netzwerk über eine Mischung von Clients verfügt, von denen einige WPA2 und andere nur das ursprüngliche WPA unterstützen, aktivieren Sie beide Kontrollkästchen. Bei dieser Einstellung können sowohl WPA- als auch WPA2-Client-Stationen eine Verbindung herstellen und authentifizieren. Für Clients, die diese Einstellung unterstützen, wird jedoch das robustere WPA2 verwendet. Diese WPA-Konfiguration ermöglicht mehr Interoperabilität anstelle einiger Sicherheitsfunktionen.

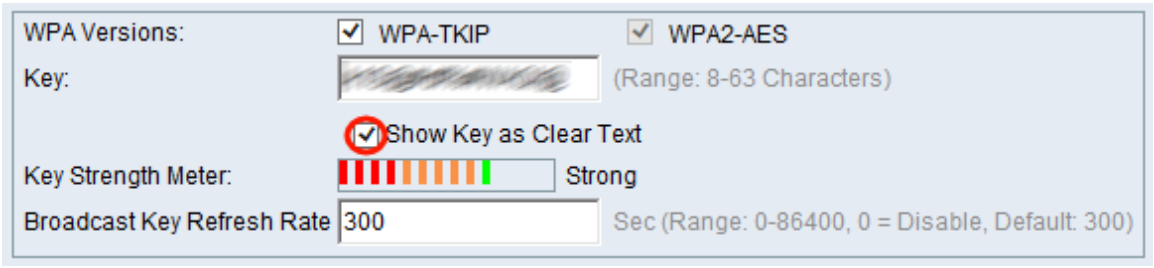
Hinweis: WPA-Clients müssen über einen dieser Schlüssel (einen gültigen TKIP-Schlüssel oder einen gültigen AES-CCMP-Schlüssel) verfügen, um eine Verbindung zum WAP-Gerät herstellen zu können.

Schritt 2: Geben Sie im *Feld Key* den gemeinsamen geheimen Schlüssel für die WPA Personal Security ein. Geben Sie mindestens 8 und maximal 63 Zeichen ein.



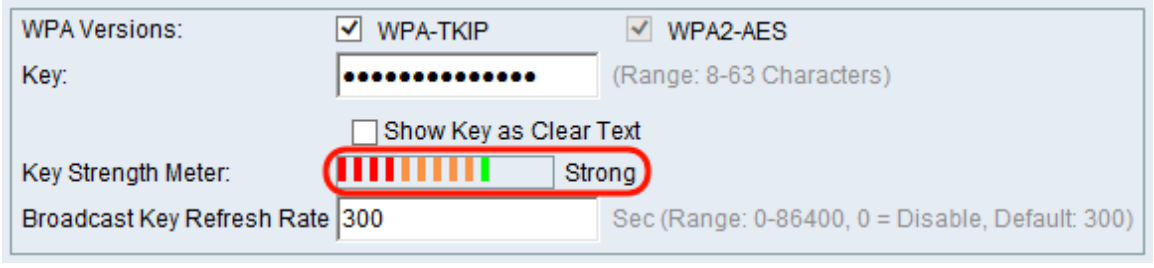
Hinweis: Zu den zulässigen Zeichen gehören Groß- und Kleinbuchstaben, numerische Ziffern und Sonderzeichen (?!/\@#$%^&*).

Schritt 3: (Optional) Aktivieren Sie das Kontrollkästchen *Schlüssel als Klartext anzeigen*, wenn der von Ihnen eingegebene Text sichtbar sein soll. Das Kontrollkästchen ist standardmäßig deaktiviert.

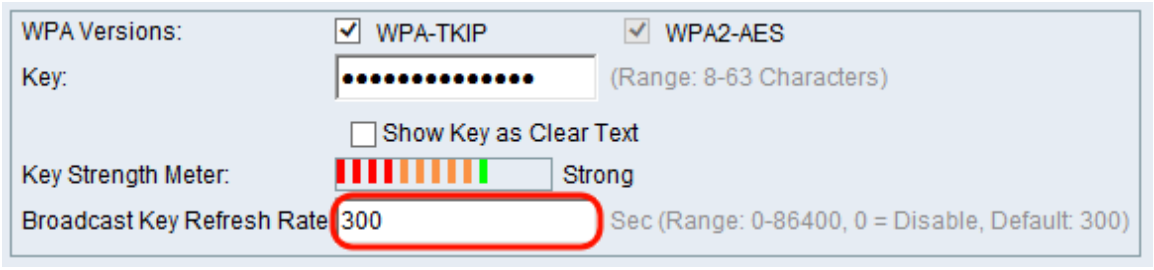


Hinweis: Bei Verwendung einer anderen Firmware auf dem WAP351, WAP131 oder WAP371 fehlt möglicherweise das Feld *Schlüssel als Klartext anzeigen*.

Hinweis: Im Feld *Schlüsselstärkemessgerät* wird der Schlüssel anhand von Komplexitätskriterien geprüft, z. B. wie viele verschiedene Zeichen verwendet werden und wie lange der Schlüssel ist. Wenn die Funktion zur Überprüfung der WPA-PSK-Komplexität aktiviert ist, wird der Schlüssel nur akzeptiert, wenn er die Mindestkriterien erfüllt. Weitere Informationen zur Komplexität von WPA-PSK *finden Sie unter* Konfigurieren der Kennwortkomplexität für WAP131, WAP351 und WAP371.



Schritt 4: Geben Sie im Feld *Broadcast Key Refresh Rate (Aktualisierungsrate für Sendeschlüssel*) das Intervall ein, in dem der Schlüssel Broadcast (Gruppe) für Clients aktualisiert wird, die diesem VAP zugeordnet sind. Der Standardwert ist 300 Sekunden.

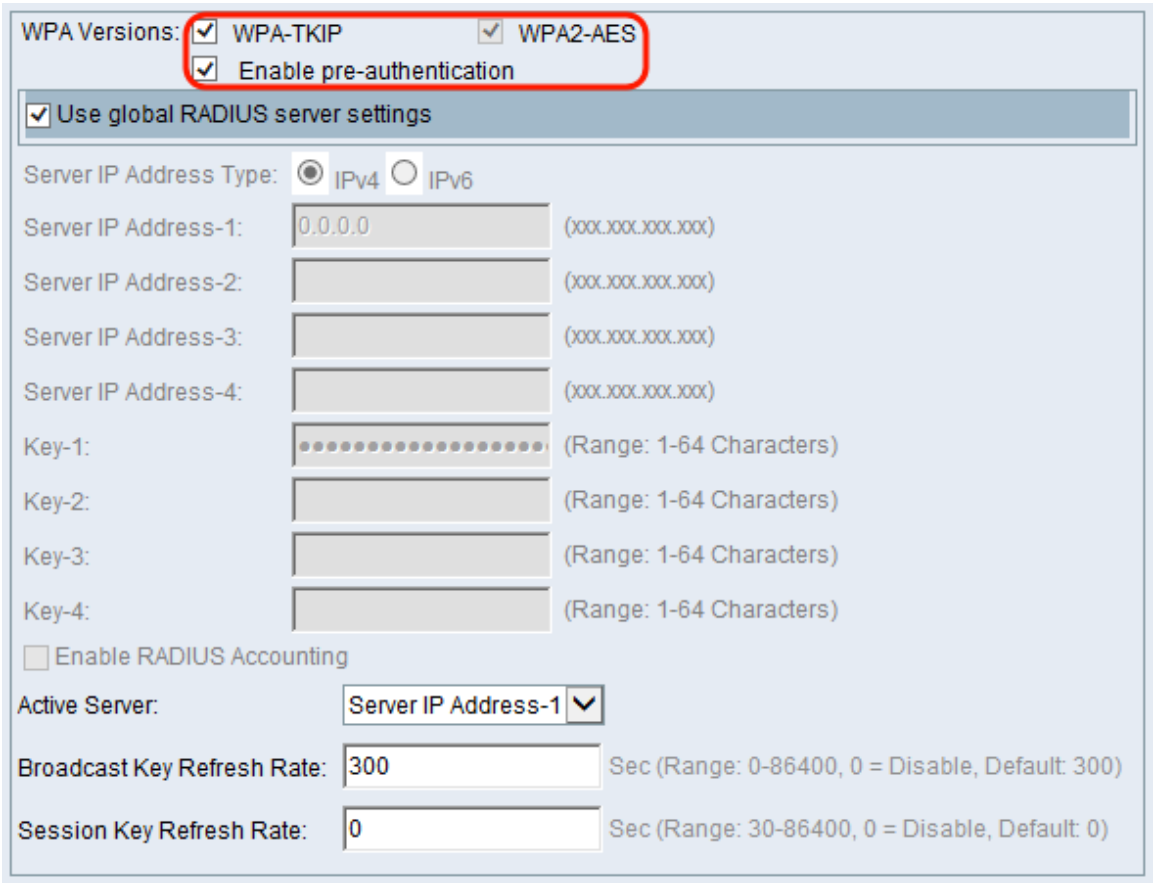


WPA-Enterprise

WPA Enterprise mit RADIUS ist eine Implementierung des Standards IEEE 802.11i der Wi-Fi Alliance, der CCMP (AES) und TKIP-Verschlüsselung umfasst. Für den Enterprise-Modus muss ein RADIUS-Server zur Authentifizierung der Benutzer verwendet werden. Der Sicherheitsmodus ist abwärtskompatibel mit den Wireless-Clients, die das ursprüngliche WPA unterstützen.

Hinweis: Der dynamische VLAN-Modus ist standardmäßig aktiviert, sodass der RADIUS-Authentifizierungsserver entscheiden kann, welches VLAN für die Stationen verwendet wird.

Schritt 1: Aktivieren Sie im Feld *WPA-Versionen* das Kontrollkästchen der zu unterstützenden Client-Stationen. Alle sind standardmäßig aktiviert. Der Access Point muss WPA2-AES ständig unterstützen, damit Sie ihn nicht konfigurieren können.



Die verfügbaren Optionen sind wie folgt definiert:

·WPA-TKIP - Das Netzwerk verfügt über einige Client-Stationen, die nur das ursprüngliche

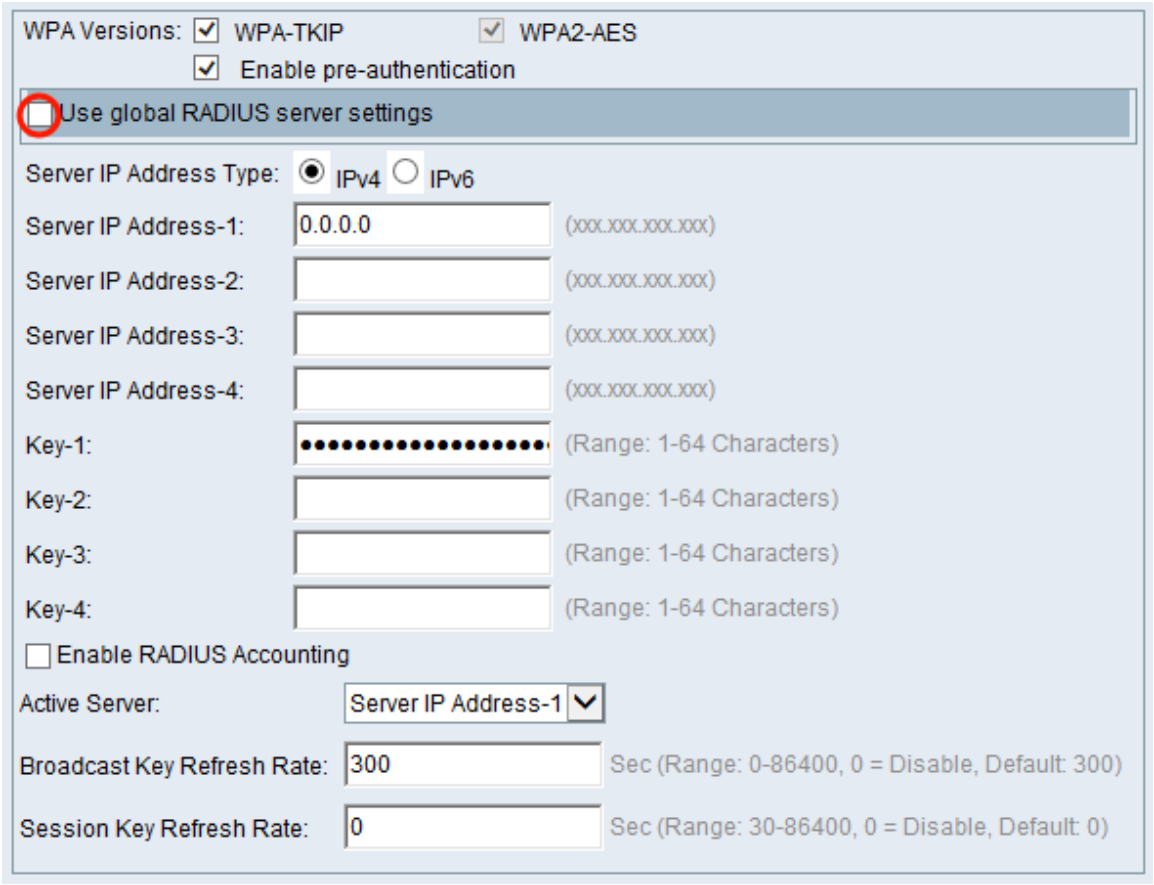
WPA- und TKIP-Sicherheitsprotokoll unterstützen. Beachten Sie, dass die Auswahl von nur WPA-TKIP für den Access Point gemäß den neuesten Anforderungen der WiFi Alliance nicht zulässig ist.

·WPA2-AES - Alle Client-Stationen im Netzwerk unterstützen die WPA2-Version und das AES-CCMP-Verschlüsselungs-/Sicherheitsprotokoll. Diese WPA-Version bietet die beste Sicherheit gemäß IEEE 802.11i-Standard. Gemäß den neuesten Anforderungen der Wi-Fi Alliance muss der WAP diesen Modus ständig unterstützen.

·Vorauthentifizierung aktivieren: Wenn Sie nur WPA2 oder WPA2 und WPA2 als WPA-Version auswählen, können Sie die Vorauthentifizierung für die WPA2-Clients aktivieren. Aktivieren Sie diese Option, wenn die WPA2-Wireless-Clients die Pre-Authentication-Pakete senden sollen. Die Vorabauthentifizierungsinformationen werden vom WAP-Gerät, das der Client derzeit verwendet, an das Ziel-WAP-Gerät weitergeleitet. Durch die Aktivierung dieser Funktion kann die Authentifizierung für Roaming-Clients beschleunigt werden, die mit mehreren WAPs verbunden sind. Diese Optionen gelten nicht, wenn Sie WPA für WPA-Versionen ausgewählt haben, da die ursprüngliche WPA diese Funktion nicht unterstützt.

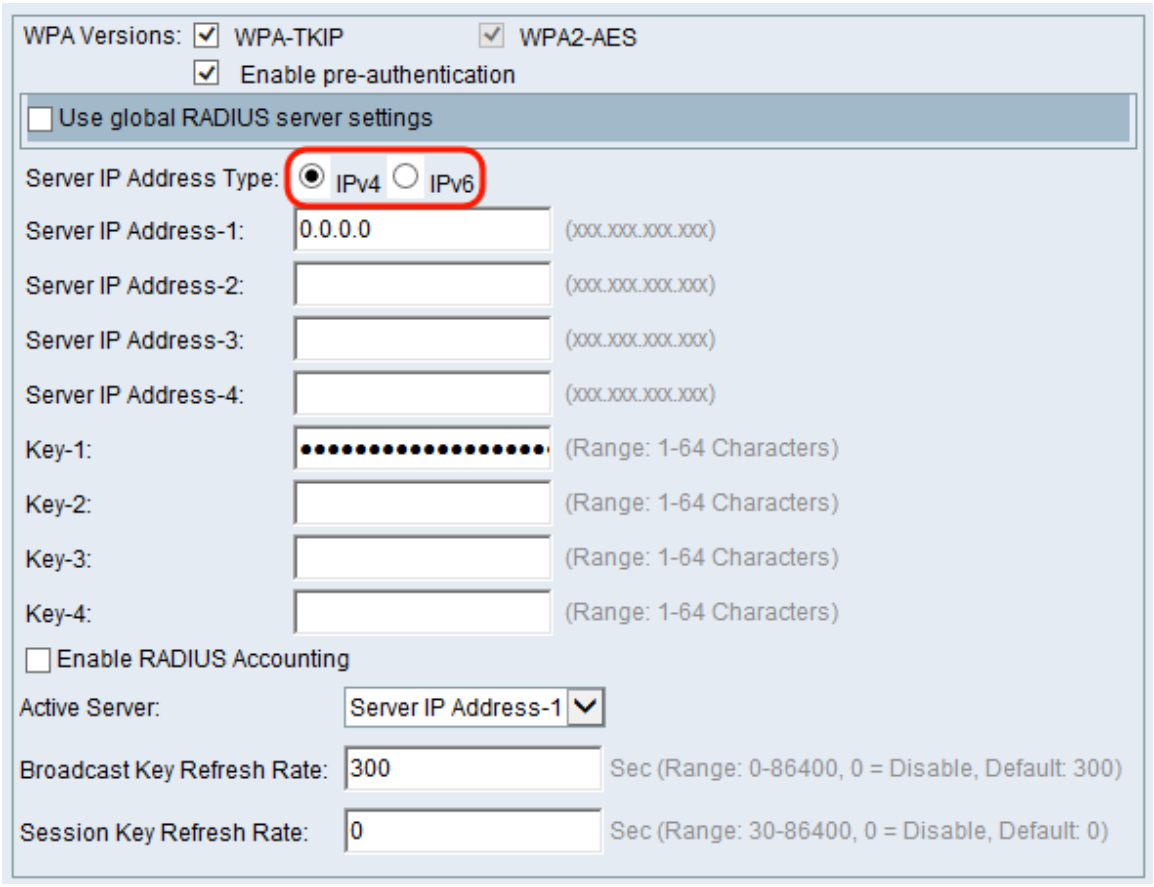
Hinweis: Client-Stationen, die für die Verwendung von WPA mit RADIUS konfiguriert sind, müssen über eine der folgenden Adressen und Schlüssel verfügen: Eine gültige TKIP-RADIUS- oder gültige CCMP (AES)-IP-Adresse und ein RADIUS-Schlüssel.

Schritt 2: Standardmäßig ist die Option *Globale RADIUS-Servereinstellungen verwenden* aktiviert. Deaktivieren Sie das Kontrollkästchen, wenn Sie den VAP für die Verwendung eines anderen RADIUS-Serversatzes konfigurieren möchten. Fahren Sie andernfalls mit Schritt 9 fort.

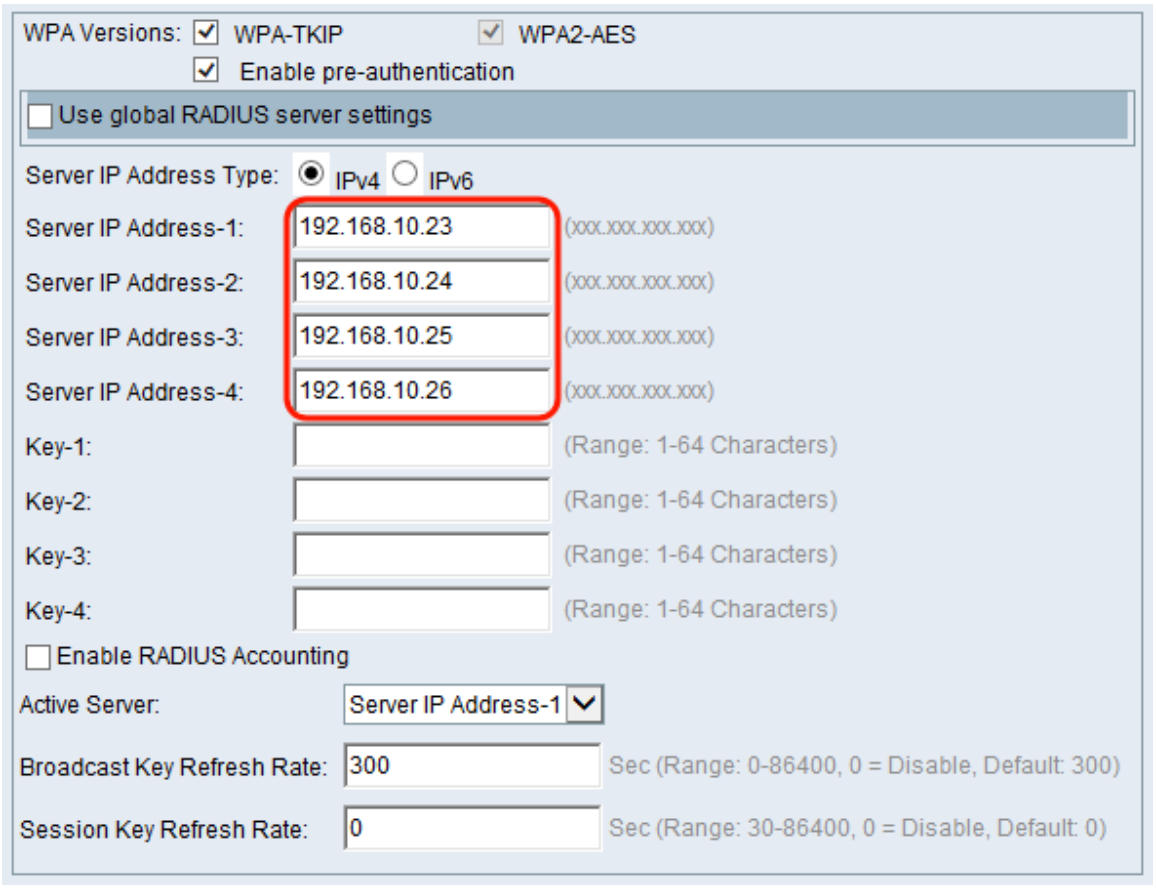


Schritt 3: Wählen Sie im Feld *Server IP Address Type* (IP-Adresstyp des Servers) den von Ihrem WAP-Gerät verwendeten IP-Adresstyp des Servers aus. Die Optionen sind *IPv4* oder

IPv6. IPv4 verwendet 32-Bit-Binärzahlen, die in Dezimalpunktschreibweise dargestellt werden. IPv6 verwendet Hexadezimalzahlen und Doppelpunkte, um eine 128-Bit-Binärzahl darzustellen. Das WAP-Gerät kontaktiert nur den oder die RADIUS-Server für den Adresstyp, den Sie in diesem Feld ausgewählt haben.

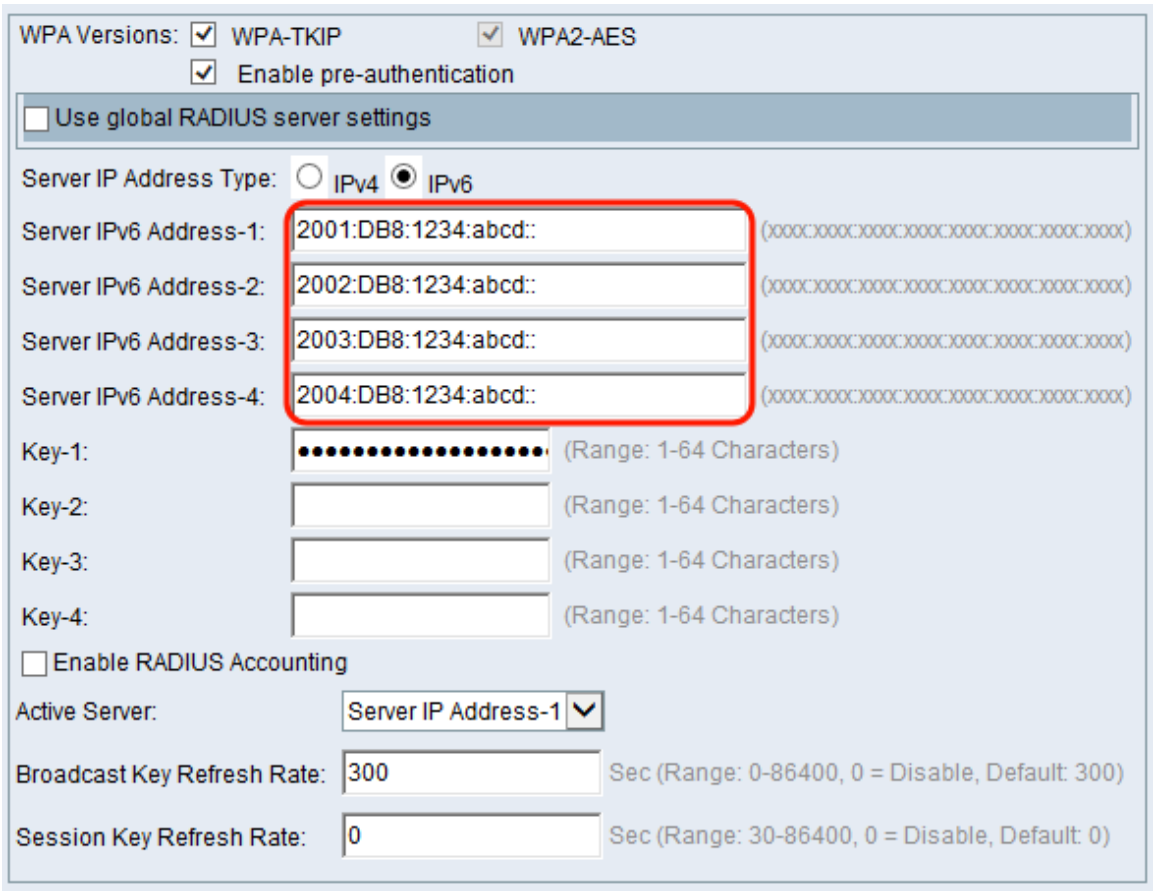


Schritt 4: Wenn Sie in Schritt 2 **IPv4** ausgewählt haben, geben Sie die IP-Adresse des RADIUS-Servers ein, den alle VAPs standardmäßig verwenden. Fahren Sie anschließend mit Schritt 6 fort.



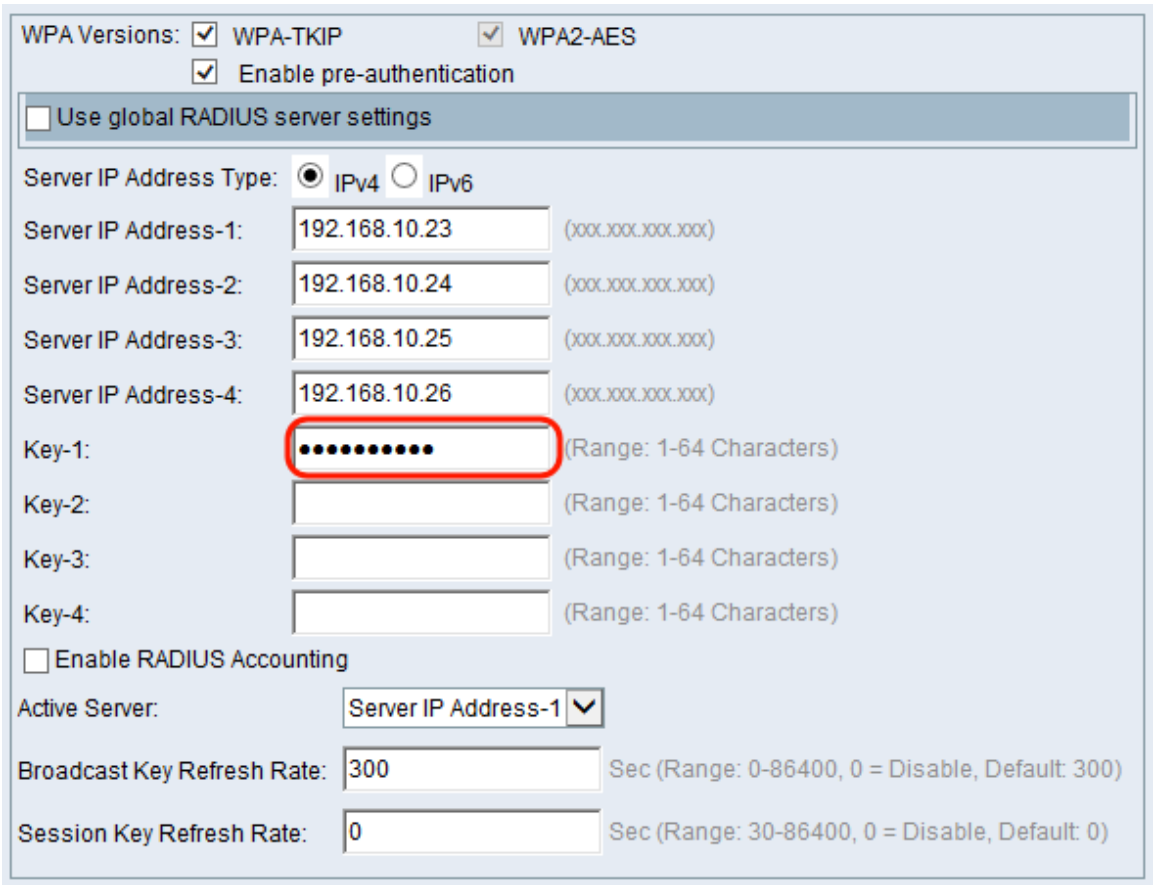
Hinweis: Sie können bis zu drei IPv4-Backup-RADIUS-Serveradressen einrichten. Wenn die Authentifizierung mit dem primären Server fehlschlägt, wird jeder konfigurierte Backup-Server nacheinander versucht.

Schritt 5: Wenn Sie **IPv6** in Schritt 2 ausgewählt haben, geben Sie die IPv6-Adresse des primären globalen RADIUS-Servers ein.

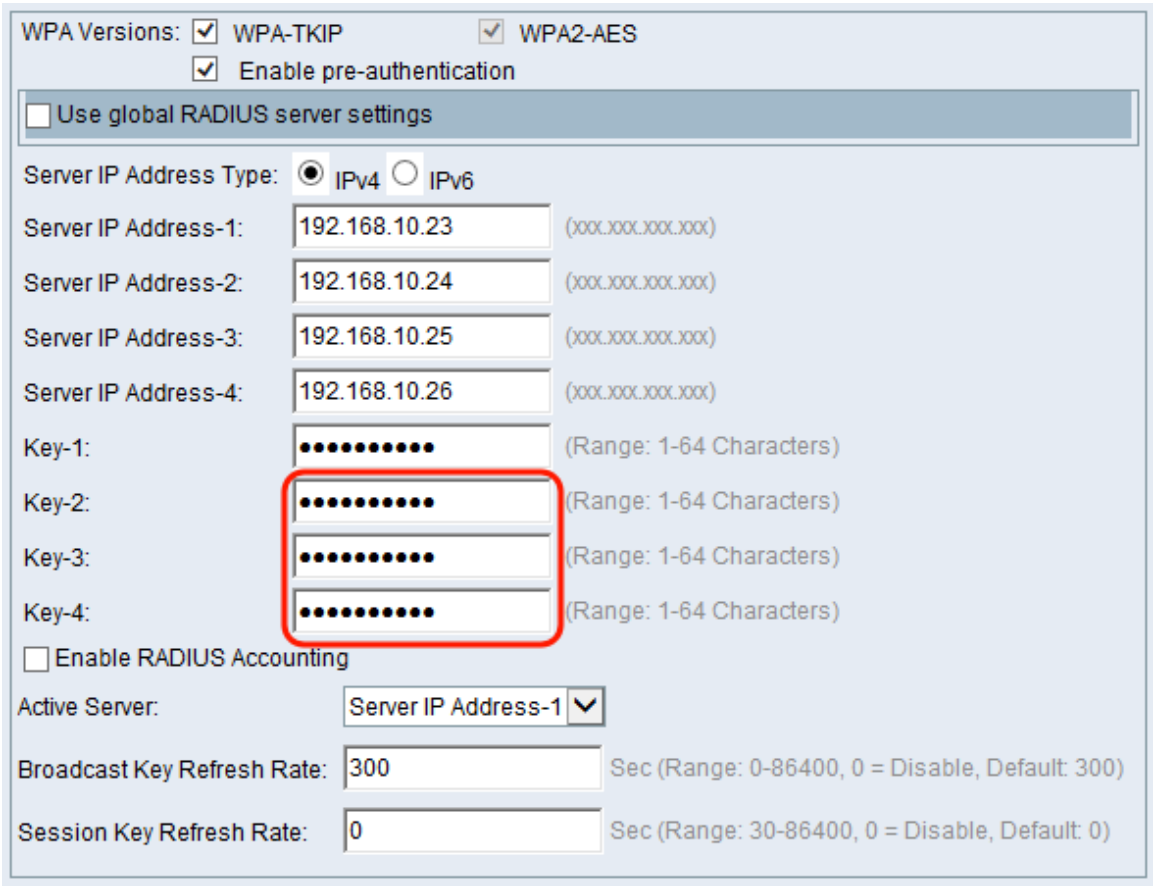


Hinweis: Sie können bis zu drei IPv6-Backup-RADIUS-Serveradressen einrichten. Wenn die Authentifizierung mit dem primären Server fehlschlägt, wird jeder konfigurierte Backup-Server nacheinander versucht.

Schritt 6: Geben Sie im Feld *Key-1* den gemeinsamen geheimen Schlüssel ein, den das WAP-Gerät zur Authentifizierung des primären RADIUS-Servers verwendet.

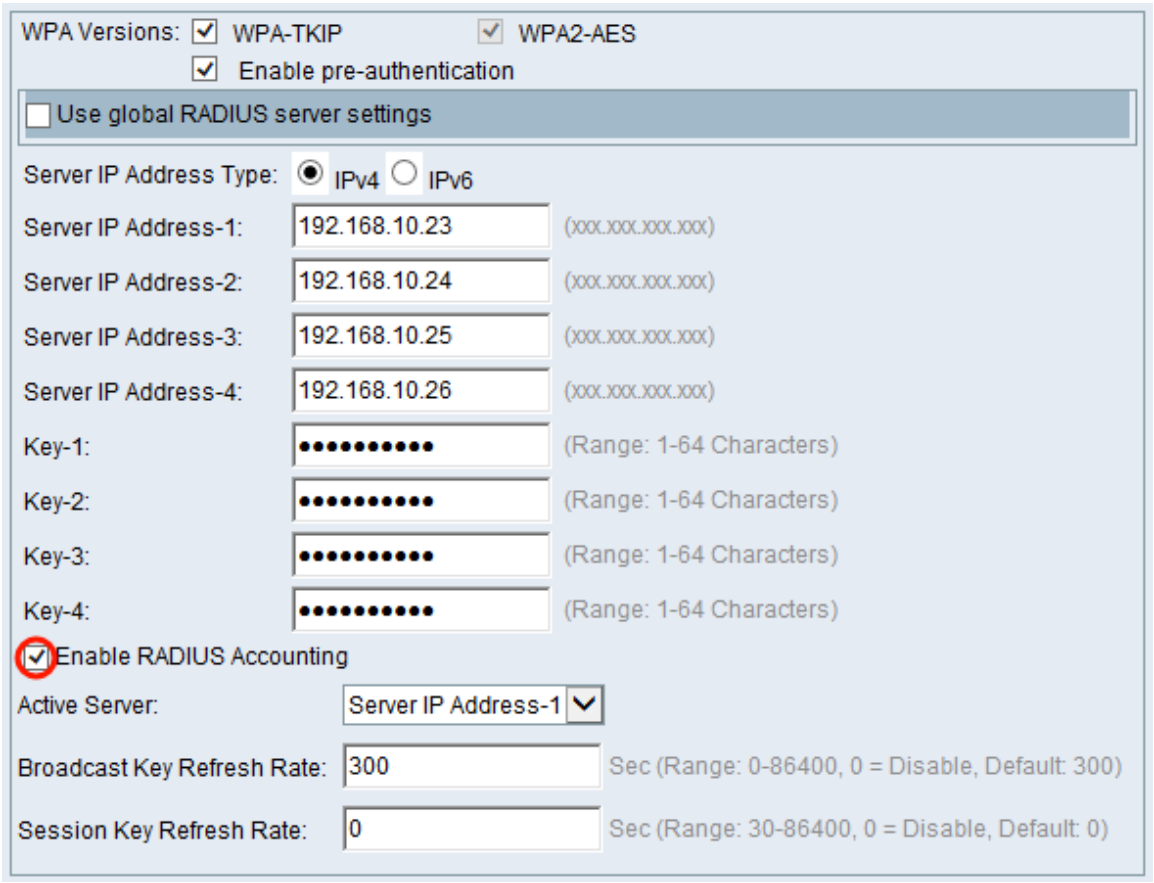


Schritt 7: Geben Sie in den Feldern *Key-2* to *Key-4* den RADIUS-Schlüssel ein, der den konfigurierten Backup-RADIUS-Servern zugeordnet ist. Die Server-IP-Adresse 2 verwendet *Key-2*, die Server-IP-Adresse 3 verwendet *Key-3* und die Server-IP-Adresse 4 verwendet *Key-4*.



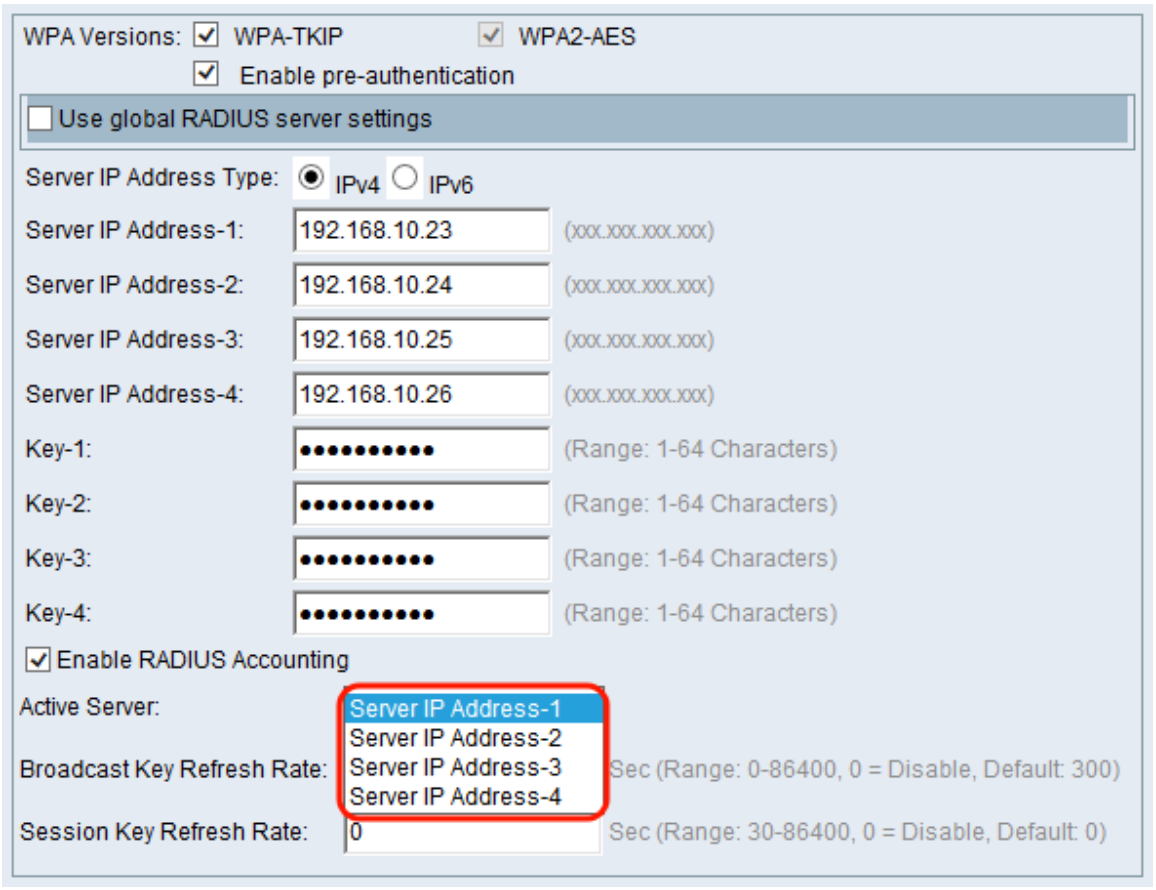
Schritt 8: (Optional) Aktivieren Sie im Feld *Enable RADIUS Accounting (RADIUS-Accounting*

aktivieren) das Kontrollkästchen, wenn Sie die Nachverfolgung und Messung der Ressourcen aktivieren möchten, die ein bestimmter Benutzer verbraucht hat. Durch Aktivieren der RADIUS-Accounting können Sie die Systemzeit eines bestimmten Benutzers und die Menge der übertragenen und empfangenen Daten verfolgen.

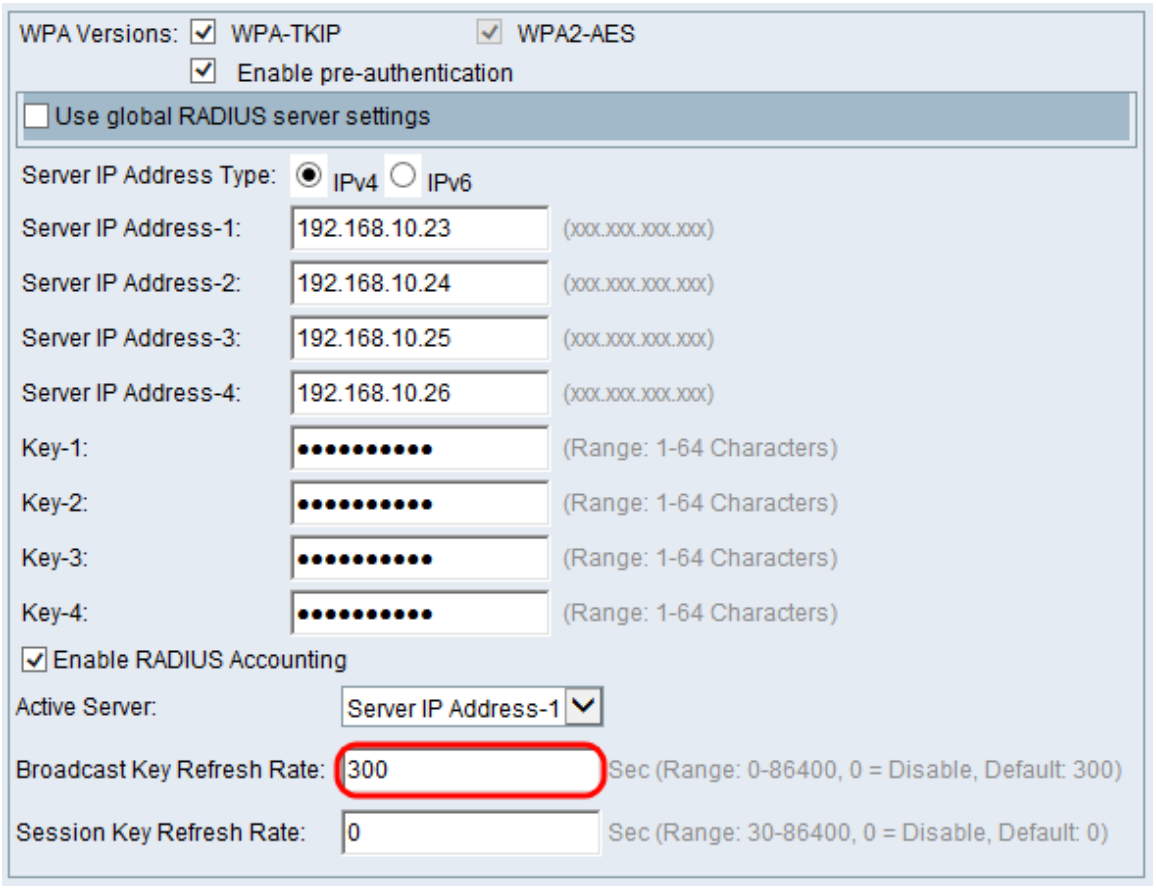


Hinweis: Wenn Sie RADIUS Accounting aktiviert haben, ist dieser für den primären RADIUS-Server und alle Backup-Server aktiviert.

Schritt 9: Wählen Sie den ersten Server aus, der im Feld *Active Server* aktiv ist. Dadurch kann der aktive RADIUS-Server manuell ausgewählt werden, anstatt dass das WAP-Gerät versucht, jeden konfigurierten Server nacheinander zu kontaktieren.

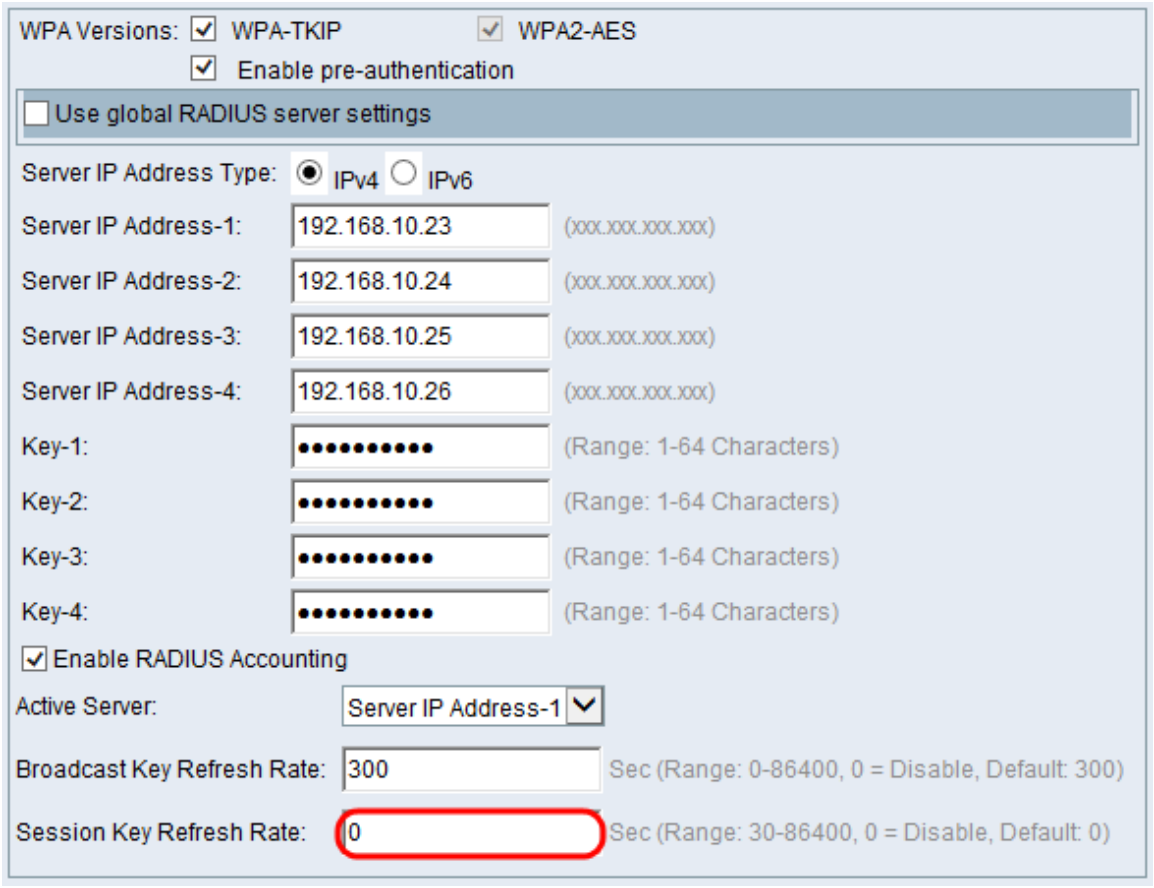


Schritt 10: Geben Sie im Feld *Broadcast Key Refresh Rate (Aktualisierungsrate für Sendeschlüssel*) das Intervall ein, in dem der Schlüssel Broadcast (Gruppe) für Clients aktualisiert wird, die diesem VAP zugeordnet sind. Der Standardwert ist 300 Sekunden.



Schritt 11: Geben Sie im Feld *Session Key Refresh Rate (Aktualisierungsrate für Sitzungsschlüssel*) das Intervall ein, in dem das WAP-Gerät die Sitzungsschlüssel (Unicast-

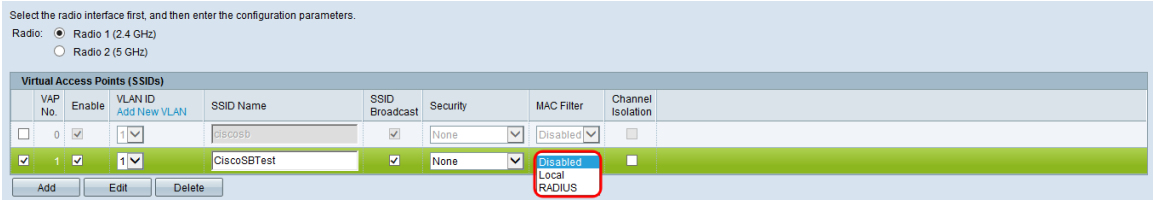
Schlüssel) für jeden dem VAP zugeordneten Client aktualisiert. Der Standardwert ist 0.



MAC-Filter

Der MAC-Filter gibt an, ob die Stationen, die auf diesen VAP zugreifen können, auf eine konfigurierte globale Liste von MAC-Adressen beschränkt sind.

Schritt 1: Wählen Sie in der Dropdown-Liste *MAC Filter (MAC-Filter)* den gewünschten Typ der MAC-Filterung aus.



Die verfügbaren Optionen sind wie folgt definiert:

·Disabled (Deaktiviert): MAC-Filterung wird nicht verwendet.

·Local (Lokal): Verwendet die MAC-Authentifizierungsliste, die Sie im Abschnitt MAC-Filterung konfigurieren, um weitere Informationen zur MAC-Filterung zu erhalten, finden Sie unter *Konfigurieren der MAC-Filterung auf dem WAP351 und WAP131*.

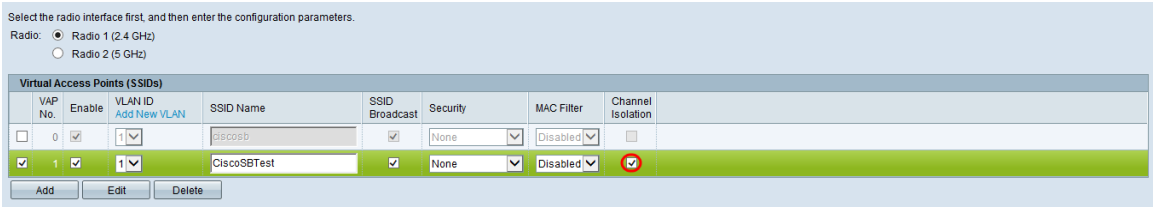
·RADIUS - Verwendet die MAC-Authentifizierungsliste auf einem externen RADIUS-Server.

Kanalisolierung

Wenn die Kanalisolierung deaktiviert ist, können die Wireless-Clients normalerweise

miteinander kommunizieren, indem sie Datenverkehr über das WAP-Gerät senden. Wenn diese Funktion aktiviert ist, blockiert das WAP-Gerät die Kommunikation zwischen den Wireless-Clients auf demselben VAP. Das WAP-Gerät lässt weiterhin Datenverkehr zwischen seinen Wireless-Clients und den kabelgebundenen Geräten im Netzwerk über eine WDS-Verbindung und mit anderen Wireless-Clients zu, die einem anderen VAP zugeordnet sind, jedoch nicht zwischen den Wireless-Clients.

Schritt 1: Aktivieren Sie im Feld *Kanalisolierung* das Kontrollkästchen, wenn Sie die Kanalisolierung aktivieren möchten.



Schritt 2: Klicken Sie auf **Speichern**.

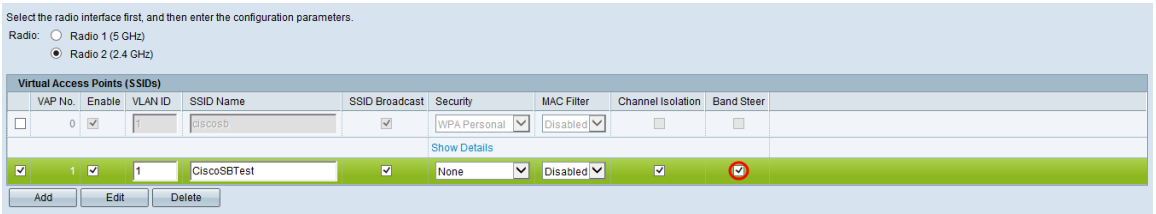
Hinweis: Nach dem Speichern neuer Einstellungen können die entsprechenden Prozesse beendet und neu gestartet werden. In diesem Fall kann die Verbindung zum WAP-Gerät unterbrochen werden. Wir empfehlen Ihnen, die Einstellungen für WAP-Geräte zu ändern, wenn ein Verbindungsverlust Ihre Wireless-Clients am wenigsten beeinträchtigt.

Bandlenker

Band Steer ist nur auf dem WAP371 verfügbar. Band Steer nutzt effektiv das 5-GHz-Band, indem Dual-Band-unterstützte Clients vom 2,4-GHz-Band bis zum 5-GHz-Band gesteuert werden. Dadurch wird das 2,4-GHz-Band für die Verwendung durch ältere Geräte ohne Dual-Radio-Unterstützung freigegeben.

Hinweis: Sowohl die 5-GHz- als auch die 2,4-GHz-Funkmodule müssen aktiviert sein, um die Band Steer zu verwenden. Weitere Informationen zum Aktivieren der Funkmodule finden Sie unter *Konfigurieren der grundlegenden Funkeinstellungen auf dem WAP371*.

Schritt 1: Band Steer wird auf VAP-Basis konfiguriert und muss auf beiden Funkmodulen aktiviert werden. Wenn Sie Band Steer aktivieren möchten, aktivieren Sie das Kontrollkästchen im Feld Bandsteuerung.

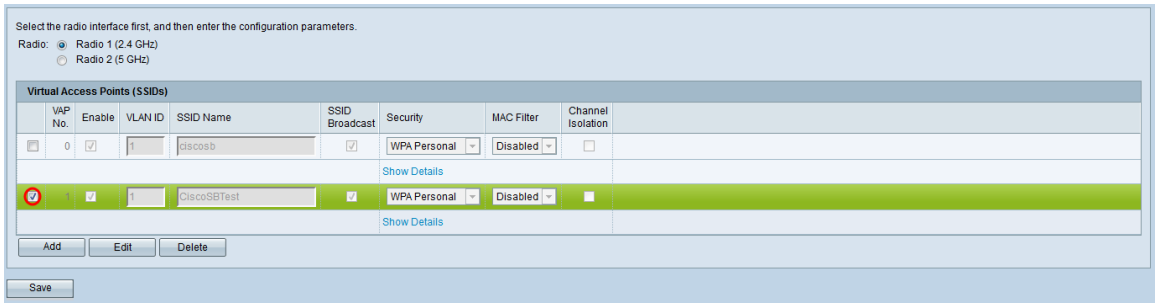


Hinweis: Bei VAPs mit zeitabhängigem Sprach- oder Videodatenverkehr wird keine Bandsteuerung empfohlen. Auch wenn das 5-GHz-Funkmodul zufällig weniger Bandbreite verbraucht, versucht es, die Clients auf dieses Funkmodul zu lenken.

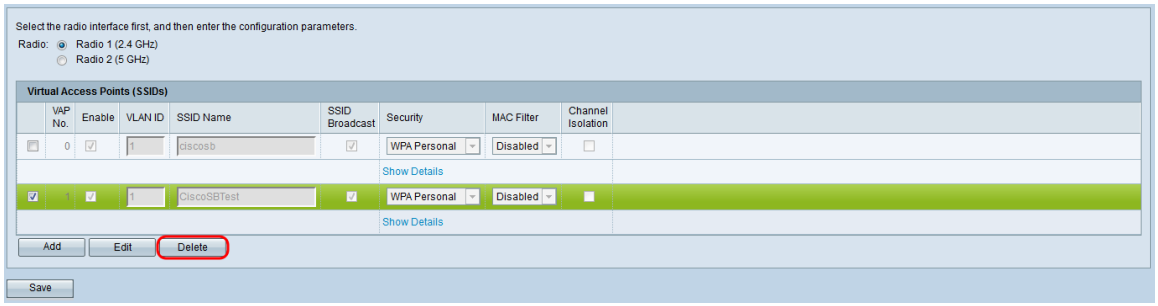
Schritt 2: Klicken Sie auf **Speichern**.

Löschen eines VAP

Schritt 1: Aktivieren Sie das Kontrollkästchen des VAP, den Sie löschen möchten.



Schritt 2: Klicken Sie auf **Löschen**, um den VAP zu löschen.



Schritt 3: Klicken Sie auf **Speichern**, um den Löschvorgang dauerhaft zu speichern.