Konfigurieren der Arbeitsgruppen-Bridge auf WAP121- und WAP321-Zugangspunkten

Ziel

Die Funktion Arbeitsgruppen-Bridge ermöglicht dem Wireless Access Point (WAP) die Überbrückung des Datenverkehrs zwischen einem Remote-Client und dem Wireless LAN, das mit dem Arbeitsgruppen-Bridge-Modus verbunden ist. Das der Remote-Schnittstelle zugeordnete WAP-Gerät wird als Access Point-Schnittstelle bezeichnet, und das dem WLAN zugeordnete Gerät wird als Infrastruktur-Schnittstelle bezeichnet. Diese Funktion wird empfohlen, wenn die WDS-Funktion nicht verwendet werden kann, da die WDS-Funktion eine bevorzugte Bridge-Lösung für WAP121 und WAP321 ist. Wenn die Arbeitsgruppen-Bridge-Funktion aktiviert ist, funktioniert die WDS-Bridge-Funktion nicht. Weitere Informationen zur Konfiguration der WDS Bridge finden Sie im Artikel *Wireless Distribution System (WDS) Bridge Configuration on WAP121 and WAP321 Access Points*.

In diesem Artikel wird erläutert, wie die Arbeitsgruppen-Bridge auf WAP121- und WAP321-Access Points konfiguriert wird.

Anwendbare Geräte

WAP121
WAP321

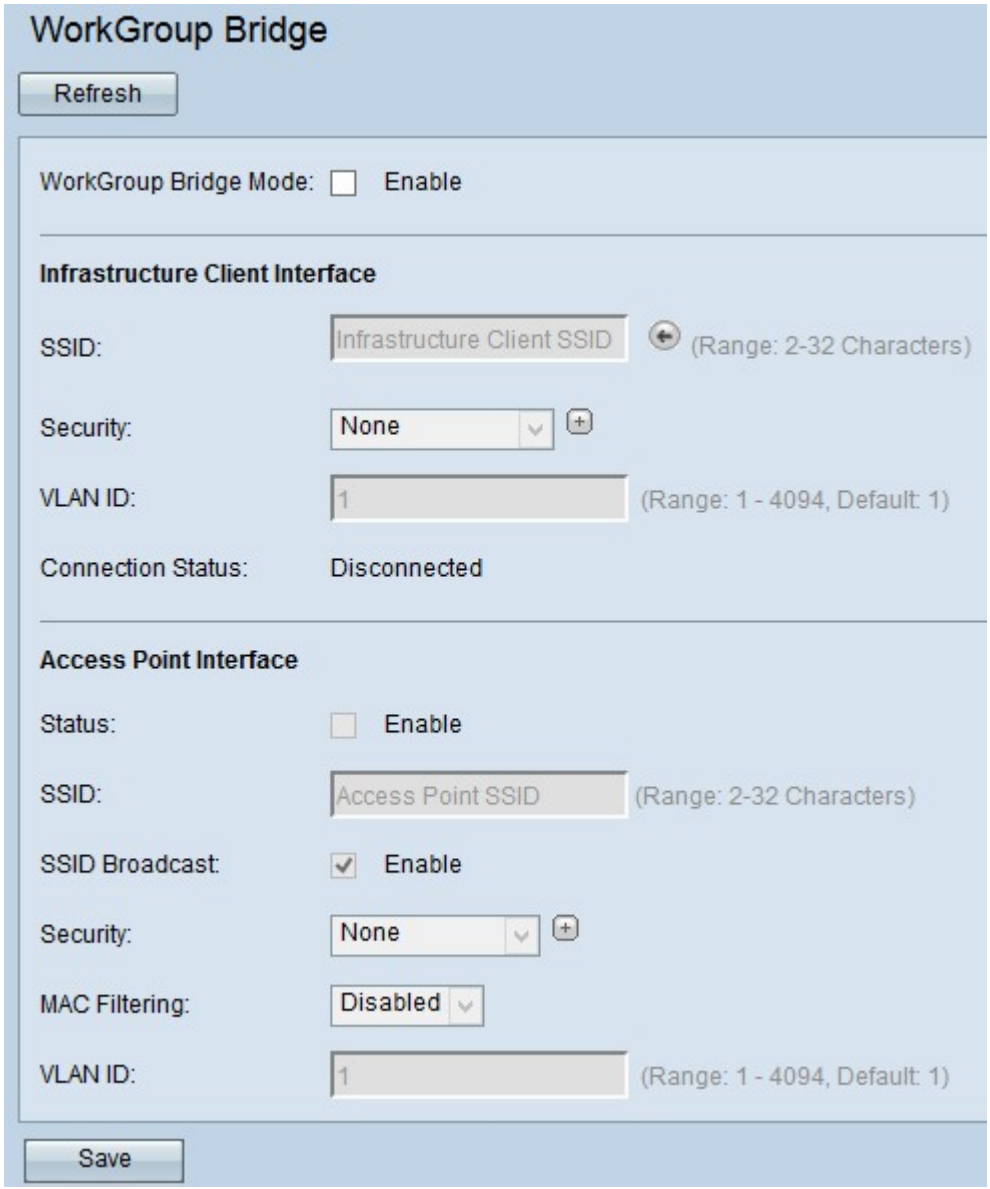
Softwareversion

·1,0/3,4

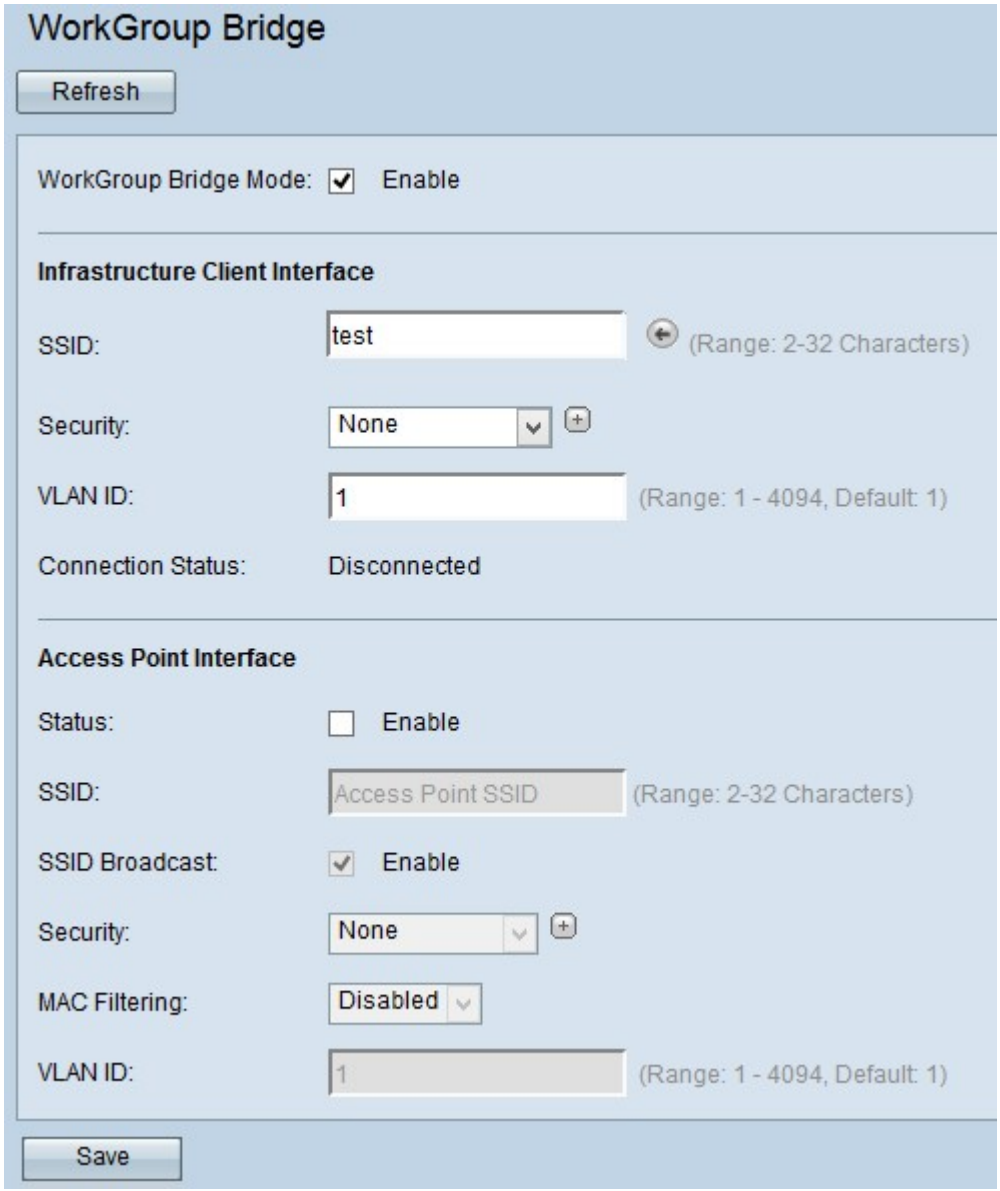
Arbeitsgruppen-Bridge konfigurieren

Hinweis: Damit die Arbeitsgruppen-Bridge aktiviert werden kann, muss das Clustering im WAP aktiviert sein. Wenn sie deaktiviert ist, müssen Sie die Single-Point-Einrichtung deaktivieren, die wiederum Clustering aktiviert. Alle WAP-Geräte, die an der Workgroup Bridge teilnehmen, müssen über gemeinsame Einstellungen für das Funkmodul, den IEEE 802.11-Modus, die Kanalbandbreite und den Kanal verfügen (Audio wird nicht empfohlen). Um sicherzustellen, dass diese Einstellungen auf allen Geräten gleich sind, überprüfen Sie die Funkeinstellungen. Informationen zum Konfigurieren dieser Einstellungen finden Sie im Artikel *Konfiguration der grundlegenden Wireless-Funkeinstellungen auf dem WAP121 und den WAP321 Access Points*.

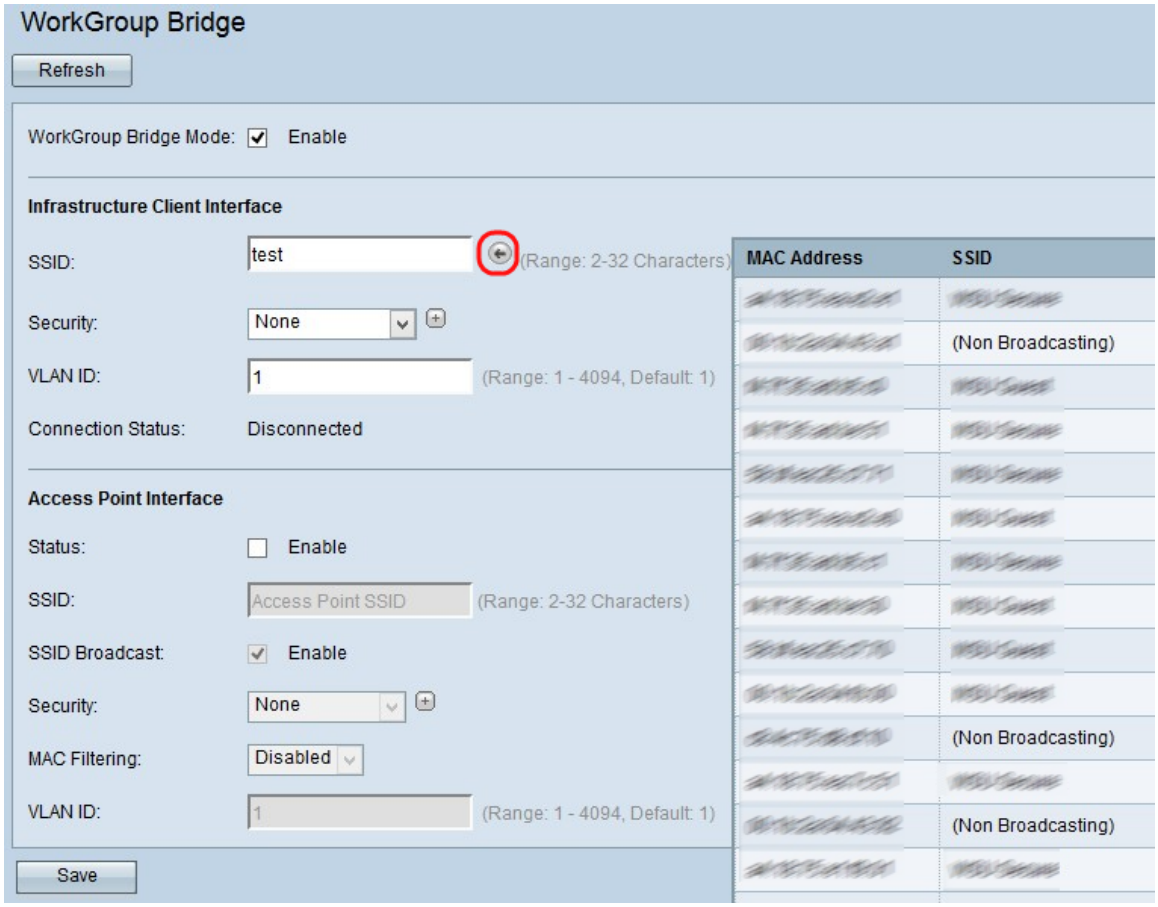
Schritt 1: Melden Sie sich beim Konfigurationsprogramm für Access Points an, und wählen Sie **Wireless > Work Group Bridge aus**. Die Seite *WorkGroup Bridge* wird geöffnet:



Schritt 2: Aktivieren Sie im Feld *WorkGroup Bridge Mode* **Enable (Aktivieren)**, um die Funktion Arbeitsgruppen-Bridge zu aktivieren.

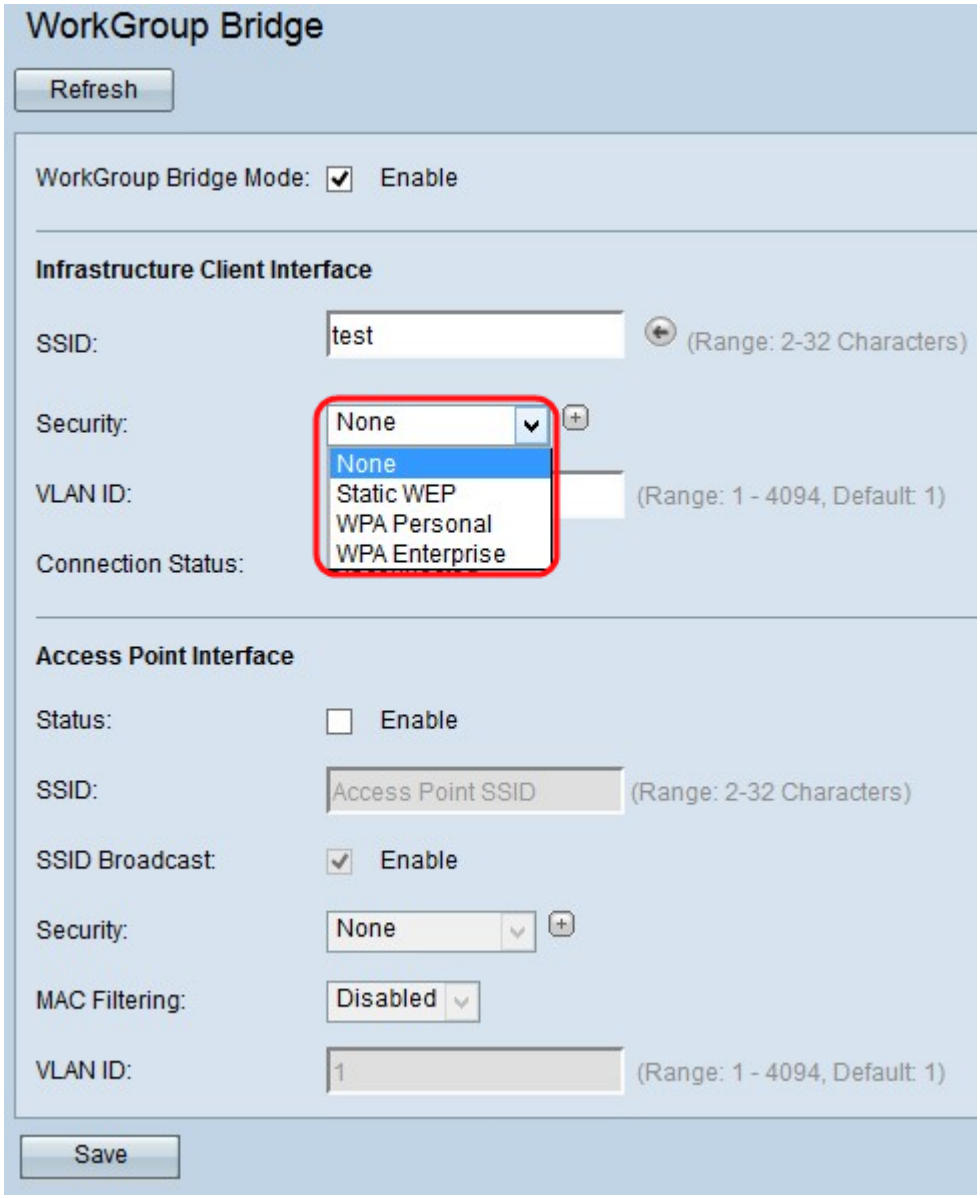


Schritt 3: Geben Sie den Namen Service Set Identifier (SSID) im *SSID*-Feld für die Infrastruktur-Client-Schnittstelle ein.



Tipp: Sie können auch auf das **Pfeilsymbol** neben dem *SSID*-Feld klicken, um nach ähnlichen benachbarten SSIDs zu suchen. Diese Funktion ist nur aktiviert, wenn die AP-Erkennung in der standardmäßig deaktivierten Erkennung nicht autorisierter APs aktiviert ist. Lesen Sie den Artikel *Rogue AP Detection auf dem WAP121 und WAP321 Access Points*, um die Erkennung nicht autorisierter APs zu aktivieren.

Schritt 4: Wählen Sie in der Dropdown-Liste *Security* (Sicherheit) den Sicherheitstyp aus, um eine Client-Station auf dem Upstream-WAP-Gerät (Infrastruktur-Client-Schnittstelle) zu authentifizieren. Mögliche Werte sind:



·Keine - Offen oder keine Sicherheit. Dies ist der Standardwert. Wenn Sie diese Option auswählen, fahren Sie mit Schritt 5 fort.

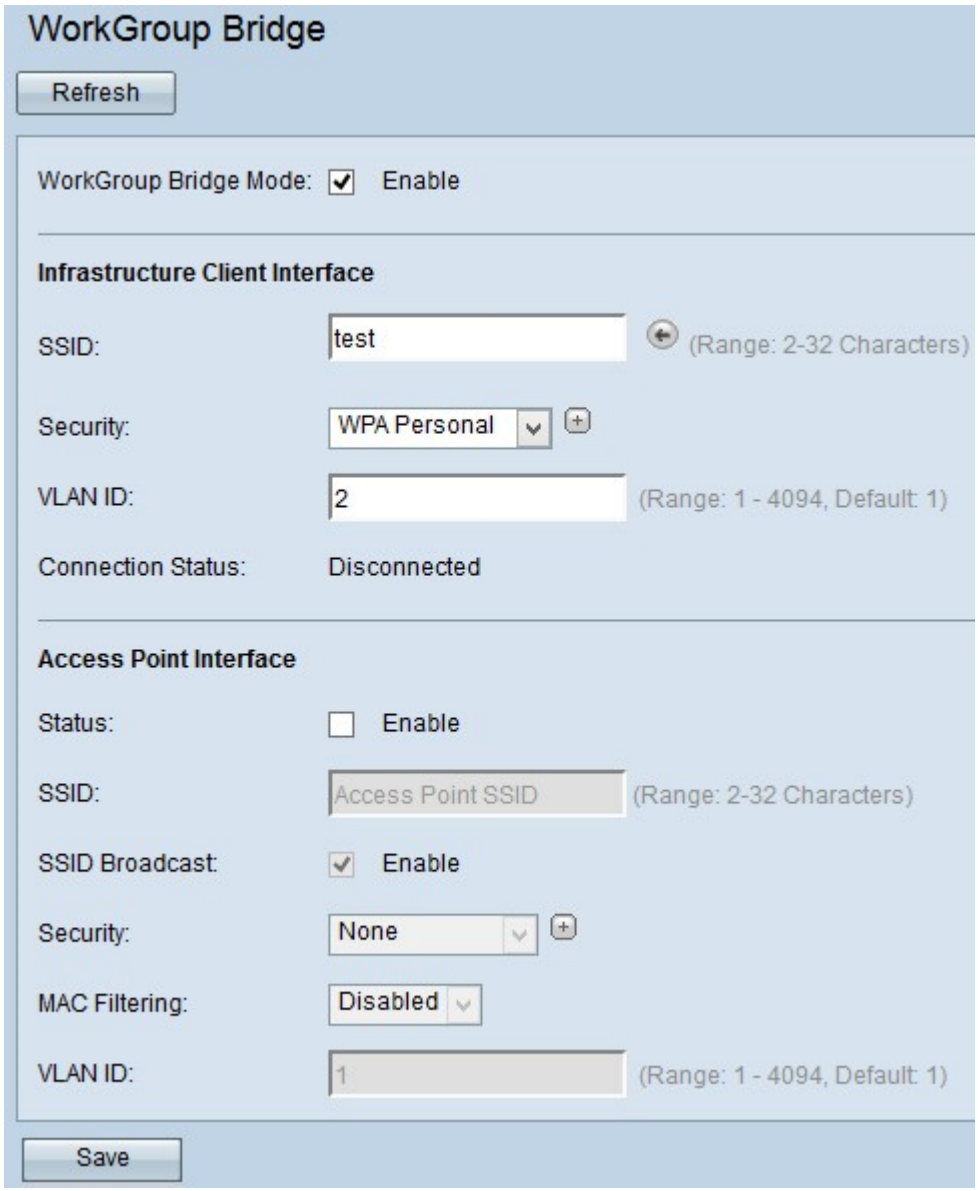
·Static WEP - Static WEP ist die minimale Sicherheit und kann bis zu 4 Schlüssel mit einer Länge von 64 bis 128 Bit unterstützen. In allen Knoten muss derselbe Schlüssel verwendet werden. Die Konfiguration für statische WEP finden Sie unter Static WEP.

·WPA Personal - WPA Personal ist im Vergleich zu WEP fortgeschrittener und unterstützt Schlüssel mit einer Länge von 8-63 Zeichen. Die Verschlüsselungsmethode ist RC4 für WPA und Advanced Encryption Standard (AES) für WPA2. WPA2 wird empfohlen, da es über einen leistungsfähigeren Verschlüsselungsstandard verfügt. Die Konfiguration von WPA Personal finden Sie unter WPA Personal for Client Interface.

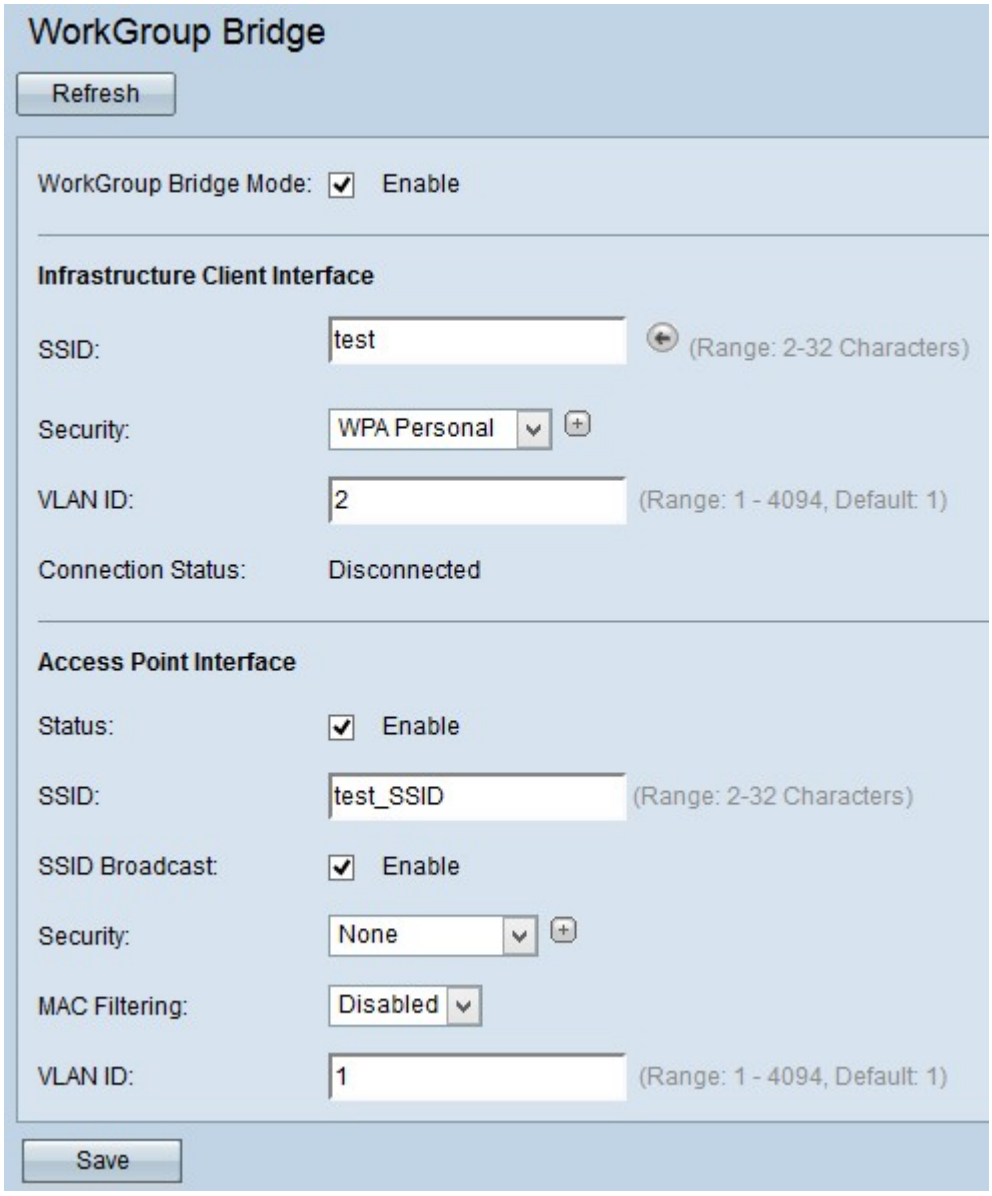
·WPA Enterprise: WPA Enterprise ist die fortschrittlichste und empfohlene Sicherheitslösung. Es verwendet Protected Extensible Authentication Protocol (PEAP), in dem jeder Wireless-Benutzer unter WAP mit individuellen Benutzernamen und Kennwörtern autorisiert ist, die sogar AES-Verschlüsselungsstandards unterstützen können. Zusätzlich zu PEAP wird auch Transport Layer Security (TLS) verwendet, bei dem jeder Benutzer ein zusätzliches Zertifikat bereitstellen muss, um Zugriff zu erhalten. Die Verschlüsselungsmethode ist RC4 für WPA und Advanced Encryption Standard (AES) für WPA2. Für die Konfiguration des WPA-Unternehmens gehen Sie zu WPA Enterprise.

Hinweis: Je nach Wahl des IEEE 802.11-Modus kann die Verfügbarkeit der oben genannten Optionen variieren.

Schritt 5: Geben Sie die VLAN-ID im Feld *VLAN-ID* für die Infrastruktur-Client-Schnittstelle ein.



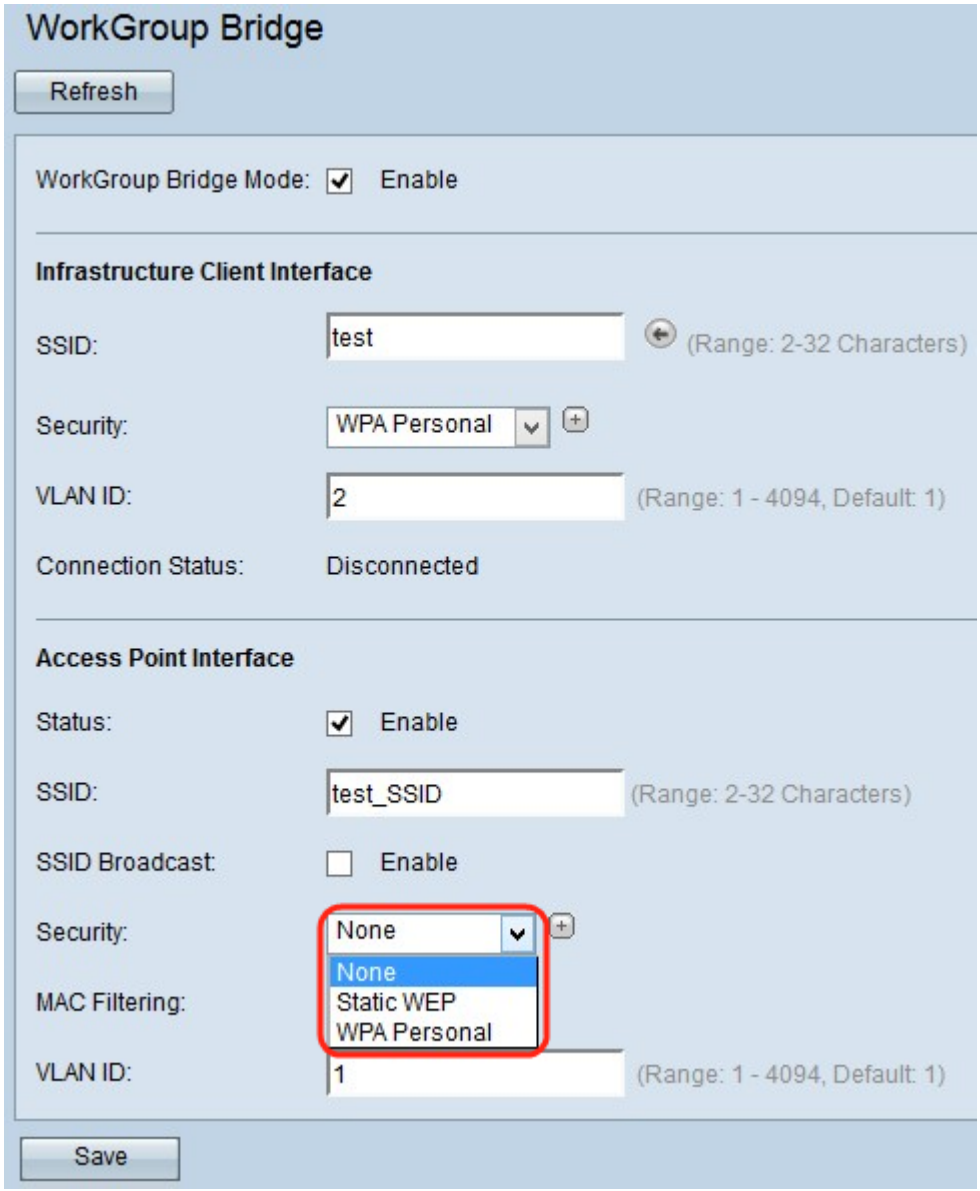
Schritt 6: Aktivieren Sie **Aktivieren** im Feld *Status*, um Bridging auf der Access Point-Schnittstelle zu aktivieren.



Schritt 7: Geben Sie den Service Set Identifier (SSID) im *SSID*-Feldnamen für die Schnittstelle des Access Points ein.

Schritt 8: (Optional) Wenn Sie die Downstream-SSID übertragen möchten, aktivieren Sie im *SSID-Broadcast*-Feld **Aktivieren**, um die Übertragung durchzuführen. Es ist standardmäßig aktiviert.

Schritt 9: Wählen Sie in der Dropdown-Liste Security (Sicherheit) den Sicherheitstyp aus, um nachgeschaltete Client-Stationen am WAP-Gerät (Access Point Interface) zu authentifizieren. Mögliche Werte sind:

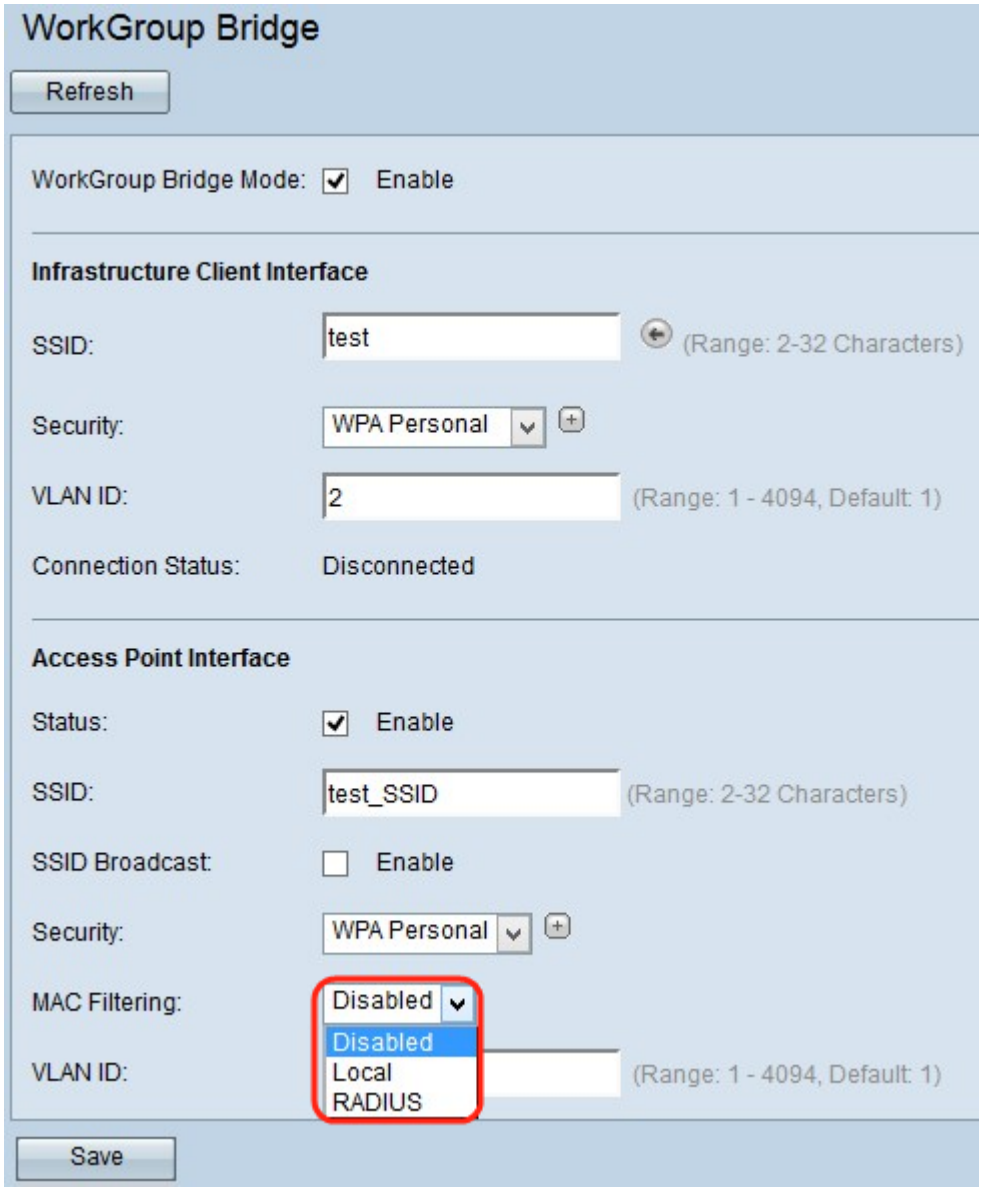


·Keine - Offen oder keine Sicherheit. Dies ist der Standardwert. Wenn Sie diese Option wählen, überspringen Sie Schritt 10.

·Static WEP - Static WEP ist die minimale Sicherheit und kann bis zu 4 Schlüssel mit einer Länge von 64 bis 128 Bit unterstützen. Die Konfiguration für statische WEP finden Sie unter Static WEP.

·WPA Personal - WPA Personal ist im Vergleich zu WEP fortgeschrittener und unterstützt Schlüssel mit einer Länge von 8 bis 63 Zeichen. Die Verschlüsselungsmethode ist entweder Temporal Key Integrity Protocol (TKIP) oder Counter Cipher Mode mit Block Chaining Message Authentication Code Protocol (CCMP). WPA2 mit CCMP wird empfohlen, da es über einen leistungsfähigeren Verschlüsselungsstandard, Advanced Encryption Standard (AES), verfügt, als das TKIP, das nur einen 64-Bit-RC4-Standard verwendet. Die Konfiguration von WPA Personal finden Sie unter WPA Personal for Access Point Interface.

Schritt 10: Wählen Sie aus der Dropdown-Liste *MAC Filtering (MAC-Filterung)* den Typ aus, den Sie für die Access Point-Schnittstelle konfigurieren möchten. Wenn diese Funktion aktiviert ist, wird Benutzern basierend auf der MAC-Adresse des Clients, den sie verwenden, der Zugriff auf den WAP gewährt oder verweigert. Mögliche Werte sind:

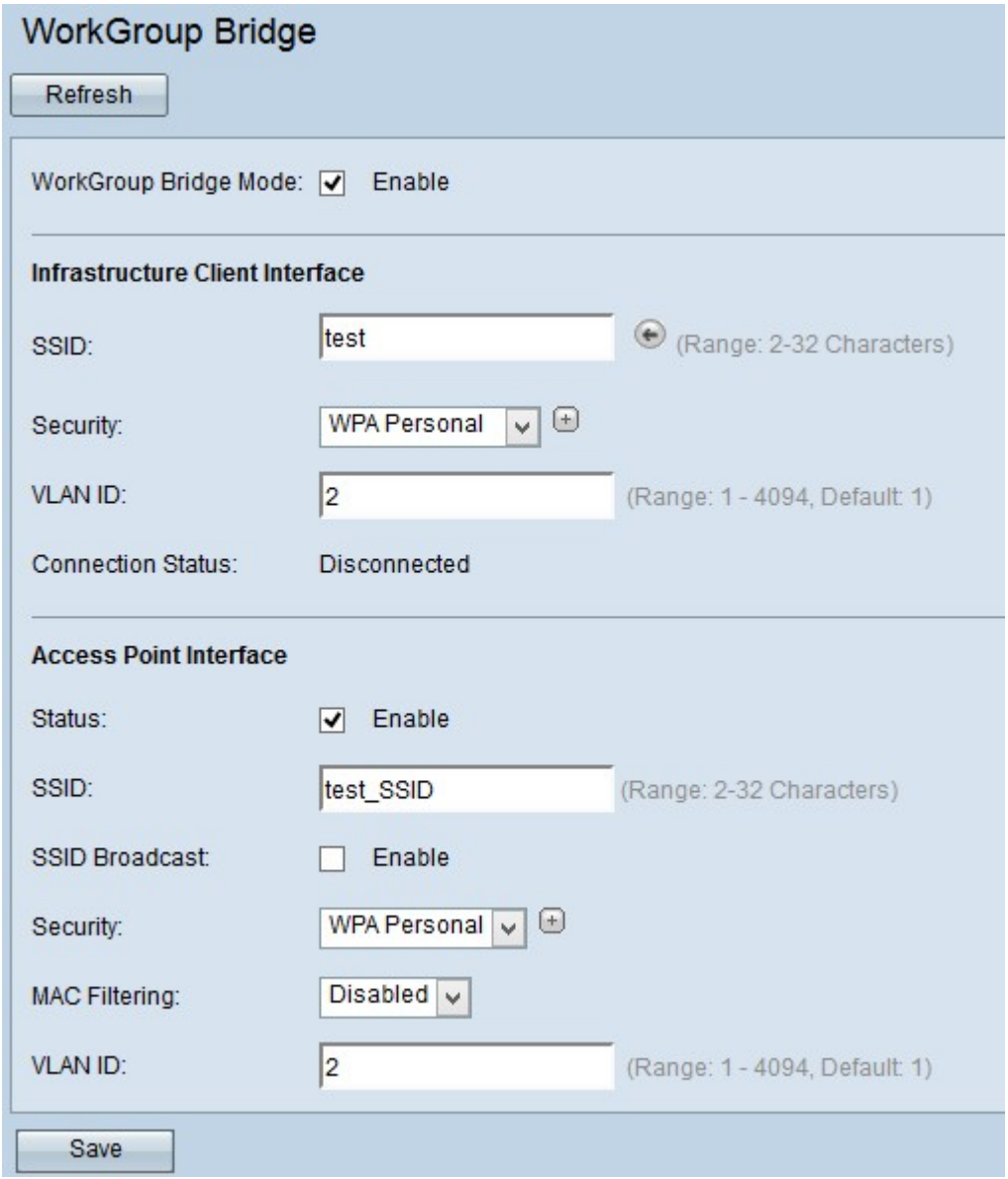


·Disabled (Deaktiviert): Alle Clients können auf das Upstream-Netzwerk zugreifen. Dies ist der Standardwert.

·Local (Lokal): Die Clients, die auf das Upstream-Netzwerk zugreifen können, sind auf die Clients beschränkt, die in einer lokal definierten MAC-Adressliste angegeben sind.

·Radius - Der Client-Satz, der auf das Upstream-Netzwerk zugreifen kann, ist auf die in einer MAC-Adressliste auf einem RADIUS-Server angegebenen Clients beschränkt.

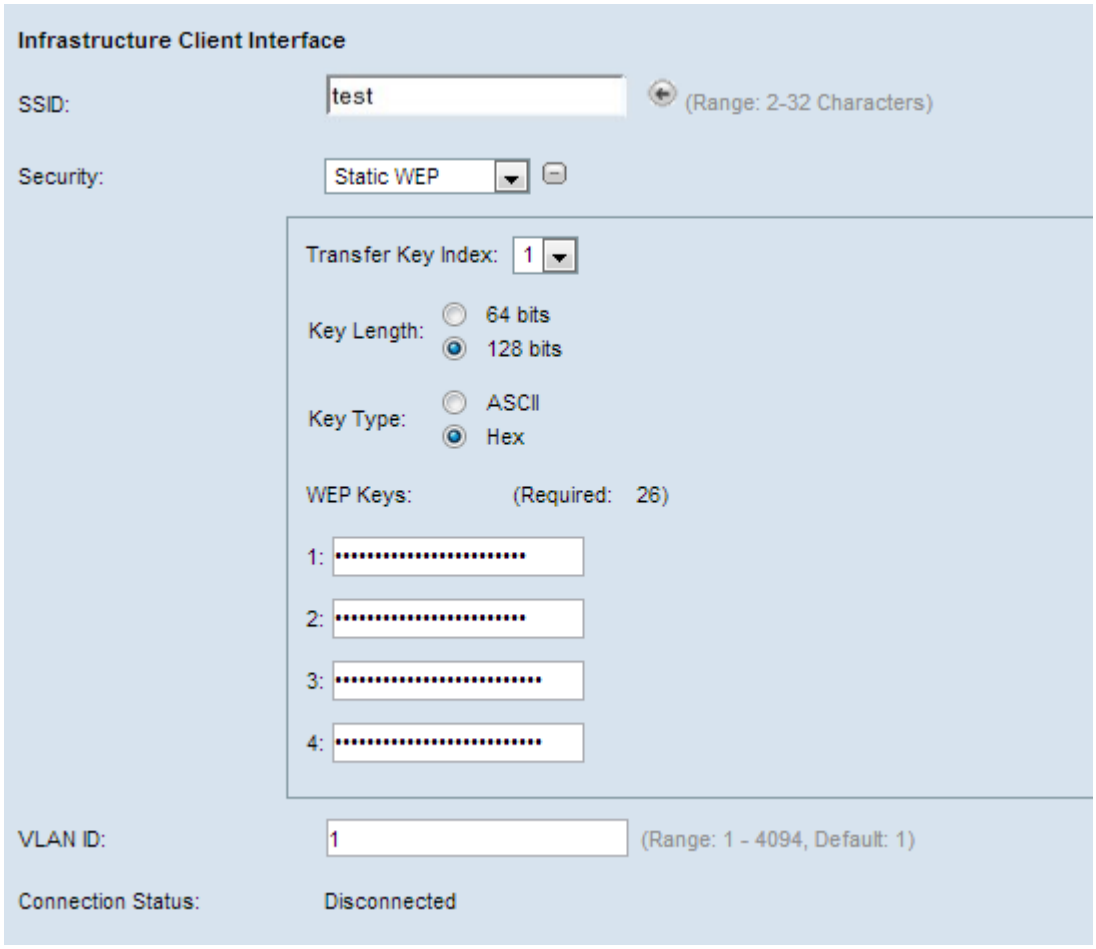
Schritt 11: Geben Sie die VLAN-ID in das VLAN-ID-Feld für die Client-Schnittstelle des Access Points ein.



Hinweis: Um das Bridging von Paketen zu ermöglichen, sollte die VLAN-Konfiguration für die Access Point-Schnittstelle und die kabelgebundene Schnittstelle mit der der Infrastruktur-Client-Schnittstelle übereinstimmen.

Schritt 12: Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

Statisches WEP



Schritt 1: Wenn Sie Static WEP (Statischer WEP) auswählen, werden einige zusätzliche Felder angezeigt. Wählen Sie aus der Dropdown-Liste im Feld *Transfer Key Index* (*Transfer Key-Index*) einen Schlüsselindex aus. Die verfügbaren Werte sind 1, 2, 3 und 4. Der Standardwert ist 2. Der Schlüsselindex ist für verschiedene WLANs unterschiedlich. Die mit einem bestimmten WLAN verbundenen Geräte müssen über denselben Schlüsselindex verfügen. Dieser Schlüssel wird zur Verschlüsselung von Daten für die Kommunikation verwendet.

Schritt 2: Wählen Sie im Feld *Schlüssellänge* entweder das Optionsfeld **64 Bit** oder das Optionsfeld **128 Bit** aus. Gibt die Länge des verwendeten Schlüssels an.

Schritt 3: Klicken Sie im Feld *Schlüsseltyp* auf das gewünschte Optionsfeld. WEP-Schlüssel sind normalerweise in Hexadezimalform.

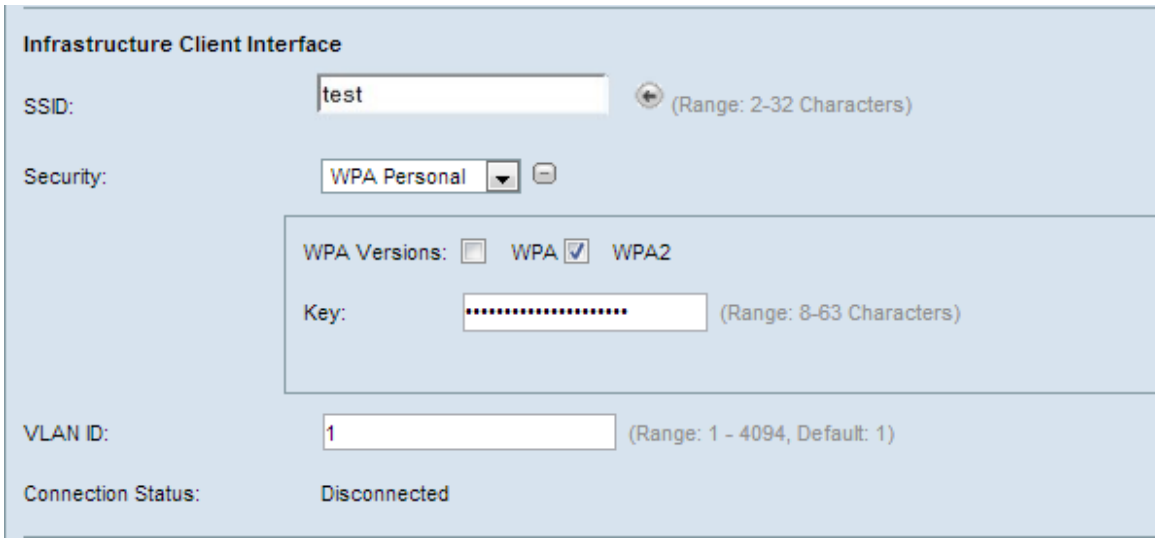
·ASCII — ASCII (American Standard Code for Information Interchange) ist ein Zeichenkodierungsschema, das auf dem englischen Alphabet basiert, das in 128 Zeichen kodiert ist.

·HEX — HEX (Hexadezimal) ist ein numerisches Positionssystem mit Base 16. Sie verwendet 16 verschiedene Symbole 0-9 für 0 bis 9 Zahlen und A,B,C,D,E,F für die Darstellung von Werten zwischen zehn und fünfzehn. Jedes Hexadezimal stellt vier Binärziffern dar.

Schritt 4: Geben Sie in den nächsten vier Feldern im Feld *WEP-Schlüssel* bis zu vier WEP-Schlüssel ein, die als 1,2,3 und 4 gekennzeichnet sind. Dies ist eine Zeichenfolge, die als Schlüssel eingegeben wird. Die Länge des Schlüssels variiert je nach Länge und Typ des Schlüssels. Die erforderliche Länge wird neben dem Feld "WEP Key" (WEP-Schlüssel) angegeben. Die WEP-Schlüsselzeichenfolgen müssen in allen WAP-Knoten (AP und Clients) übereinstimmen und an denselben Stellen im gleichen Feld angeordnet sein. Das

bedeutet, wenn Zeichenfolge 1 in einem Gerät Schlüssel 1 ist, muss Zeichenfolge 1 auch auf den anderen Geräten in der Arbeitsgruppen-Bridge der Schlüssel 1 sein.

WPA Personal für Client-Schnittstelle



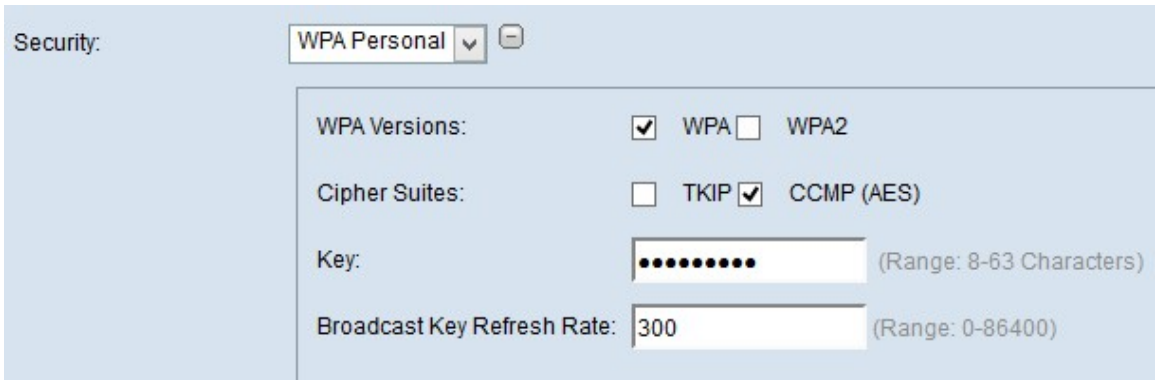
Schritt 1: Überprüfen Sie die gewünschten WPA-Versionen im Feld *WPA-Versionen*. In der Regel wird WPA nur dann ausgewählt, wenn einige WAPs im Bridge-System WPA2 nicht unterstützen. WPA2 ist die erweiterte und empfohlene Version.

·WPA - Wenn das Netzwerk über Client-Stationen verfügt, die die ursprüngliche Version von WPA unterstützen.

·WPA2 - Wenn alle Client-Stationen im Netzwerk WPA2 unterstützen. Diese Protokollversion bietet die beste Sicherheit gemäß IEEE 802.11i-Standard.

Schritt 2: Geben Sie den gemeinsam genutzten WPA-Schlüssel in das *Feld Schlüssel* ein. Der Schlüssel kann alphanumerische Zeichen, Groß- und Kleinbuchstaben und Sonderzeichen enthalten.

WPA Personal für Access Point-Schnittstelle



Schritt 1: Überprüfen Sie die gewünschten WPA-Versionen im Feld *WPA-Versionen*. In der Regel wird WPA nur dann ausgewählt, wenn einige der beteiligten WAPs WPA2 nicht unterstützen. Andernfalls wird WPA2 empfohlen.

·WPA - Wenn das Netzwerk über Client-Stationen verfügt, die die ursprüngliche Version WPA unterstützen.

·WPA2 - Wenn alle Client-Stationen im Netzwerk WPA2 unterstützen. Diese Protokollversion bietet die beste Sicherheit gemäß IEEE 802.11i-Standard.

Hinweis: Wenn das Netzwerk aus einer Kombination von Clients von WPA und WPA2 besteht, aktivieren Sie beide Kontrollkästchen. Dadurch können sowohl WPA- als auch WPA2-Client-Stationen eine Verbindung herstellen und authentifizieren. Für Clients, die diese Funktion unterstützen, wird jedoch das robustere WPA2 verwendet.

Schritt 2: Wählen Sie im Feld *Cipher Suites* die gewünschten Chiffre-Suiten aus.

·TKIP - Temporal Key Integrity Protocol (TKIP) verwendet nur einen 64-Bit-RC4-Standard.

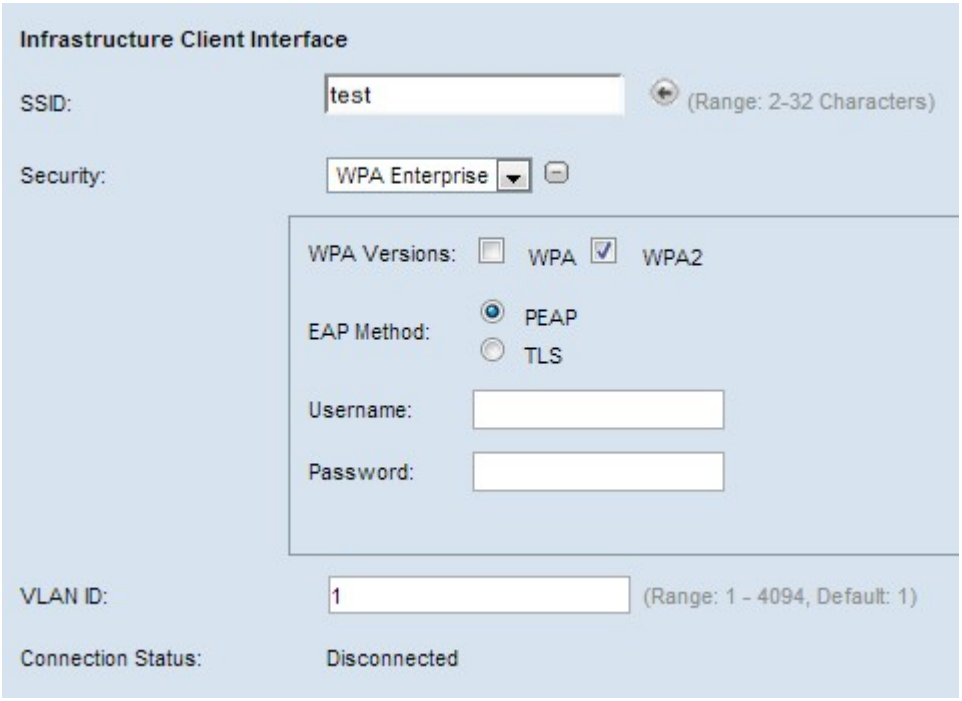
·CCMP (AES) - Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP) ist das von AES (Advanced Encryption Standard) verwendete Sicherheitsprotokoll. WPA2 mit CCMP wird empfohlen, da es über einen leistungsfähigeren Verschlüsselungsstandard verfügt.

Hinweis: Sie können entweder eine oder beide auswählen. Sowohl TKIP- als auch AES-Clients können mit dem WAP-Gerät verbunden werden.

Schritt 3: Geben Sie den gemeinsam genutzten WPA-Schlüssel in das *Feld Schlüssel* ein. Der Schlüssel kann alphanumerische Zeichen, Groß- und Kleinbuchstaben und Sonderzeichen enthalten.

Schritt 4: Geben Sie die Rate im Feld *Aktualisierungsrate* für den *Sendeschlüssel ein*.

WPA-Enterprise



Schritt 1.Überprüfen Sie die gewünschten WPA-Versionen im Feld *WPA-Versionen*. In der Regel wird WPA nur dann ausgewählt, wenn einige WAPs im Bridge-System WPA2 nicht unterstützen. WPA2 ist die erweiterte und empfohlene Version.

·WPA - Wenn das Netzwerk über Client-Stationen verfügt, die die ursprüngliche Version WPA unterstützen.

·WPA2 - Wenn alle Client-Stationen im Netzwerk WPA2 unterstützen. Diese

Protokollversion bietet die beste Sicherheit gemäß IEEE 802.11i-Standard.

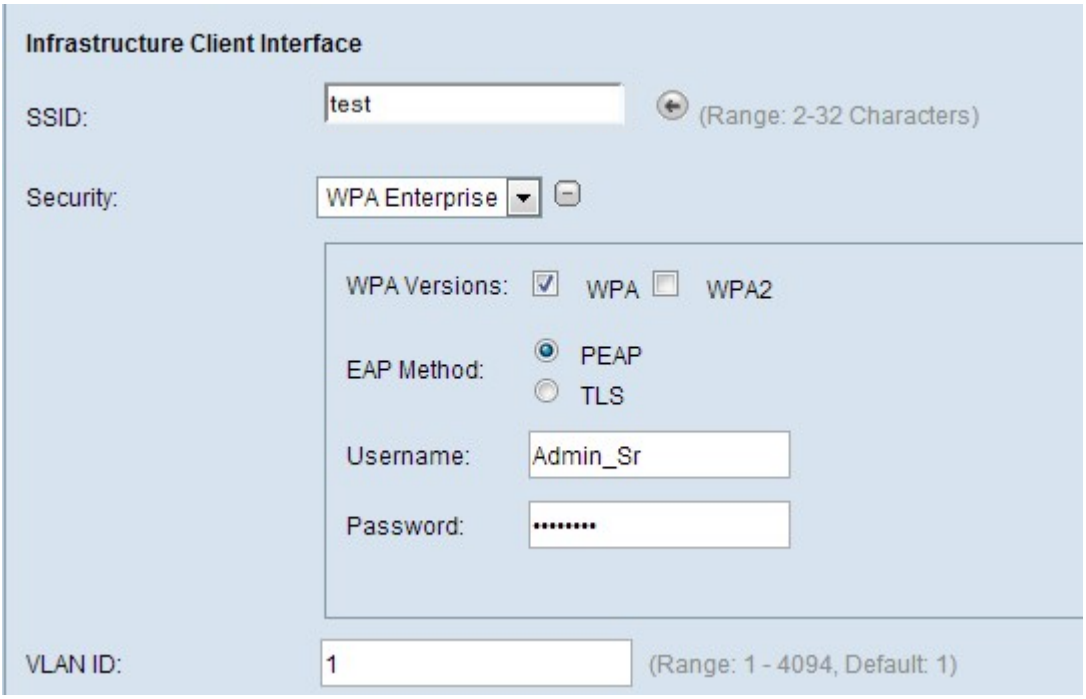
Hinweis: Wenn das Netzwerk eine Mischung aus WPA- und WPA2-Clients ist, aktivieren Sie die beiden Kontrollkästchen. Dadurch können sowohl WPA- als auch WPA2-Client-Stationen eine Verbindung herstellen und authentifizieren. Für Clients, die diese Funktion unterstützen, wird jedoch das robustere WPA2 verwendet.

Schritt 2: Klicken Sie auf das entsprechende Optionsfeld, um zwischen den beiden EAP-Methoden zu wählen.

·PEAP - Protected EAP. Sie stützt sich auf TLS, vermeidet jedoch die Installation digitaler Zertifikate auf jedem Client. Stattdessen wird die Authentifizierung über einen Benutzernamen und ein Kennwort bereitgestellt. Wenn Sie diese Option auswählen, gehen Sie zu PEAP (Protected Extensible Authentication Protocol).

·TLS - Authentifizierung durch Austausch digitaler Zertifikate. Wenn Sie diese Option auswählen, gehen Sie zu TLS (Transport Layer Security).

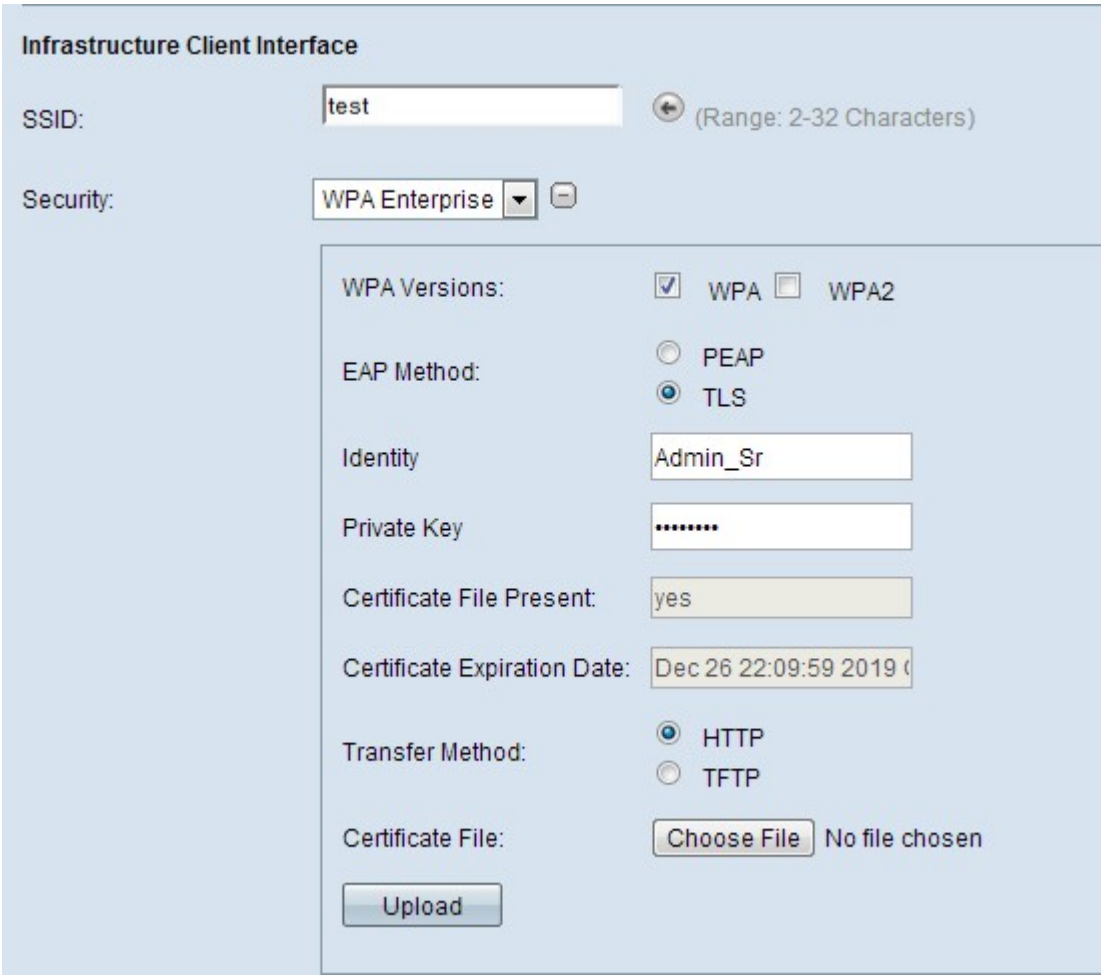
PEAP (Protected Extensible Authentication Protocol)



Schritt 1: Geben Sie im Feld *Benutzername* einen Benutzernamen ein.

Schritt 2: Geben Sie ein Kennwort in das Feld *Kennwort ein*.

TLS (Transport Layer Security)

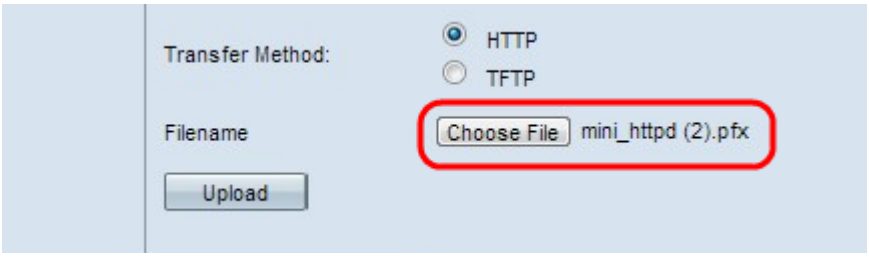


Schritt 1: Wählen Sie den Übertragungsmodus aus, um eine Zertifikatsdatei für die TLS-Authentifizierung herunterzuladen.

·HTTP - Wenn Sie das Zertifikat von einem Webserver des PC herunterladen möchten. Wenn Sie diese Option auswählen, gehen Sie zu HTTP.

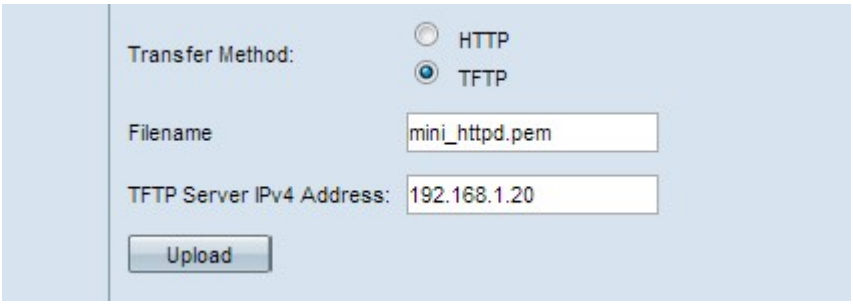
·TFTP — Wenn Sie das Zertifikat von einem Dateiserver herunterladen möchten. Wenn Sie diese Option auswählen, gehen Sie zu TFTP.

HTTP



Schritt 1: Klicken Sie auf **Datei auswählen**, um eine Zertifikatsdatei auszuwählen. Es muss sich um eine Zertifikatstypdatei mit den Erweiterungen .pem, .pfx usw. handeln. Andernfalls ist der Datei-Upload nicht erfolgreich.

TFTP



Schritt 1: Geben Sie den Namen der Zertifikatsdatei im Feld *Dateiname ein*.

Schritt 2: Geben Sie die IP-Adresse des TFTP-Servers ein.

Hinweis: Das Feld Transfer von Zertifikatsdateien zeigt an, ob ein Zertifikat im WAP vorhanden ist, und das Feld Ablaufdatum des Zertifikats zeigt das Ablaufdatum dieses Zertifikats an.

Schritt 3: Klicken Sie auf **Upload**, um die Datei auf das Gerät hochzuladen.