

Grundlegende Konfiguration der Wireless-Einstellungen auf dem RV215W

Ziel

Wireless-Netzwerke sind Computernetzwerke, die nicht über Kabel verbunden sind. Ein Wireless Local Area Network (WLAN) ist ein Wireless-Netzwerk, das mehrere Geräte über eine kurze Distanz über eine Funkverbindung miteinander verbindet.

In diesem Artikel wird erläutert, wie Sie die grundlegenden Wireless-Einstellungen der RV215W konfigurieren, einschließlich der Konfiguration der Netzwerksicherheit.

Index

- [Allgemeine Einstellungen](#)
- [Drahtlostabelle bearbeiten](#)
- [Sicherheitseinstellungen deaktivieren](#)
- [WEP-Sicherheit konfigurieren](#)
- [WPA-Personal-Sicherheit konfigurieren](#)
- [WPA-Enterprise-Sicherheit konfigurieren](#)
- [Gemischte Sicherheit für WPA2-Personal/WPA2-Personal konfigurieren](#)
- [WPA2-Enterprise/WPA2-Enterprise-Gemischte Sicherheit konfigurieren](#)
- [MAC-Filterung bearbeiten](#)
- [Tageszeitabhängiger Zugriff](#)
- [Gastnetzwerk bearbeiten](#)
- [WPS-Methode 1 konfigurieren](#)
- [WPS-Methode 2 konfigurieren](#)
- [WPS-Methode 3 konfigurieren](#)

Unterstützte Geräte

- RV215W

Software-Version

- 1.1.0.5

Konfiguration der Grundeinstellungen

Allgemeine Einstellungen

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie Wireless > Basic Settings (Wireless > Grundeinstellungen). Die Seite Grundeinstellungen wird geöffnet:

Basic Settings

Radio: ☒ Enable

Wireless Network Mode: B/G/N-Mixed

Wireless Band Selection: ☒ 20MHz ☐ 20/40MHz

Wireless Channel: 6-2.437 GHz

AP Management VLAN: 1

U-APSD (WMM Power Save): ☒ Enable

	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	Guest Network	VLAN	Wireless Isolation with SSID	WMM	WPS
☐	☒ ON	ciscosb1	☒	WPA2-Personal Mixed	Disabled	☐	1	☐	☒	☒
☐	☐ OFF	ciscosb2	☐	Disabled	Disabled	☐	1	☐	☒	☐
☐	☐ OFF	ciscosb3	☐	Disabled	Disabled	☐	1	☐	☒	☐
☐	☐ OFF	ciscosb4	☐	Disabled	Disabled	☐	1	☐	☒	☐

Edit Edit Security Mode Edit MAC Filtering Time of Day Access Edit Guest Net Edit WPS

Save Cancel

Schritt 2: Aktivieren Sie im Feld "Radio" (Funkübertragung) die Option Enable (Aktivieren), um die Wireless-Funkübertragung zu aktivieren.

Schritt 3: Wählen Sie aus der Dropdown-Liste "Wireless Network Mode" (Wireless-Netzwerkmodus) den Wireless-Modus aus.

- B/G/N-Mixed (Gemischt B/G/N): Das Netzwerk enthält eine Kombination aus Wireless-B-, Wireless-G- und Wireless-N-Geräten.
- Nur B - Das Netzwerk enthält nur Wireless-B-Geräte.
- Nur G - Das Netzwerk enthält nur Wireless-G-Geräte.
- Nur N - Das Netzwerk enthält nur Wireless-N-Geräte.
- B/G-Mixed (Gemischt B/G): Das Netzwerk enthält eine Kombination aus Wireless-B-

und Wireless-G-Geräten.

- G/N Mixed (Gemischt G/N): Das Netzwerk enthält eine Kombination aus Wireless-G- und Wireless-N-Geräten.

Schritt 4: Wenn der Netzwerkmodus Wireless-N-Geräte enthält, klicken Sie auf das Optionsfeld, das der gewünschten Bandbreite des Wireless-Signals im Feld für die Wireless-Bandauswahl entspricht. Je höher die Bandbreite, desto mehr Daten kann das Signal übertragen.

- 20 MHz - Die Standardfrequenz für ein drahtloses Signal.
- 20/40 MHz - Verwendet automatisch ein 20-MHz- und ein 40-MHz-Signal. Ein 40-MHz-Signal bietet mehr Bandbreite, ist aber anfällig für mehr Interferenzen. Diese Option wird nur verwendet, wenn die angeschlossenen Wireless-Geräte mit einer Frequenz von 40 MHz kompatibel sind.

Schritt 5: Wählen Sie aus der Dropdown-Liste "Wireless Channel" (Wireless-Kanal) einen Wireless-Kanal für das Funkmodul aus. Wählen Sie einen Kanal aus, der derzeit nicht von Nachbarnetzwerken verwendet wird.

Schritt 6: Wählen Sie in der Dropdown-Liste "AP Management VLAN" ein VLAN aus, das als Management-VLAN verwendet werden soll.

Schritt 7: Aktivieren Sie Aktivieren im Feld U-APSD, um Unscheduled Automatic Power Save Delivery (U-APSD) zu aktivieren. U-APSD ist eine Funktion, mit der das Funkgerät Strom sparen kann. U-APSD kann jedoch die Durchsatzleistung des Funkmoduls reduzieren.

Schritt 8: Klicken Sie auf Save (Speichern).

Drahtlostabelle bearbeiten

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie Wireless > Basic Settings (Wireless > Grundeinstellungen). Die Seite Grundeinstellungen wird geöffnet:

Basic Settings

Radio: ☒ Enable

Wireless Network Mode: B/G/N-Mixed

Wireless Band Selection: ☒ 20MHz ☐ 20/40MHz

Wireless Channel: 6-2.437 GHZ

AP Management VLAN: 1

U-APSD (WMM Power Save): ☒ Enable

☐	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	Guest Network	VLAN	Wireless Isolation with SSID	WMM	WPS
☒	☒ ON	ciscosb1	☒	WPA2-Personal	Enabled	☒	1	☒	☒	☒
☐	☐ OFF	ciscosb2	☐	Disabled	Disabled	☐	1	☐	☒	☐
☐	☐ OFF	ciscosb3	☐	Disabled	Disabled	☐	1	☐	☒	☐
☐	☐ OFF	ciscosb4	☐	Disabled	Disabled	☐	1	☐	☒	☐

Schritt 2: Aktivieren Sie das Kontrollkästchen des Netzwerks, das Sie in der Wireless-Tabelle bearbeiten möchten.

Schritt 3: Klicken Sie auf Bearbeiten, um das angegebene Netzwerk zu bearbeiten.

Schritt 4: Klicken Sie auf die Schaltfläche Enable SSID (SSID aktivieren), um das Netzwerk zu aktivieren. Service Set Identifier (SSID) ist der Name des Wireless-Netzwerks.

Schritt 5: Geben Sie den Namen des Netzwerks in das Feld "SSID-Name" ein. Alle Geräte im Netzwerk müssen diese SSID für die Kommunikation untereinander verwenden.

Schritt 6: Aktivieren Sie SSID-Broadcast, um Wireless-Broadcast zu aktivieren. Der RV215W meldet seine Verfügbarkeit für Wireless-Geräte in der Nähe, wenn SSID-Broadcast aktiviert ist.

Schritt 7: Aktivieren Sie Gastnetzwerk, um das konfigurierte Netzwerk als Gastnetzwerk zu konfigurieren. Ein Gastnetzwerk ist ein kleiner Teil eines Netzwerks, der für temporäre Benutzer konzipiert wurde. Damit können Gäste das Netzwerk nutzen, ohne private Wi-Fi-Schlüssel bereitstellen zu müssen.

Anmerkung: Das Gastnetzwerk kann nicht im AP-Verwaltungs-VLAN konfiguriert werden.

Schritt 8: Wählen Sie aus der Dropdown-Liste VLAN (VLAN) das VLAN aus, das mit dem Netzwerk verbunden ist.

Schritt 9: Überprüfen Sie die Wireless-Isolierung mit der SSID, um zu verhindern, dass Geräte im

angegebenen Netzwerk miteinander kommunizieren.

Schritt 10: Aktivieren Sie WMM, um Wi-Fi Multimedia (WMM) im Netzwerk zu aktivieren. WMM wird verwendet, um das Streaming von Multimedia-Inhalten über Wireless-Geräte zu verbessern. WMM weist dem Multimedieverkehr, der über eine Wireless-Verbindung gesendet wird, eine höhere Priorität zu.

Schritt 11: (Optional) Aktivieren Sie WPS, um das angegebene Netzwerk als Wi-Fi Protected Setup (WPS)-Netzwerk zuzuweisen. WPS ist eine Funktion, die eine einfache und sichere Netzwerkkonfiguration ermöglicht. Mit dieser Funktion können Geräte auf einfache Weise eine Verbindung mit dem Netzwerk herstellen.

Schritt 12: Klicken Sie auf Save (Speichern).

Sicherheit deaktivieren

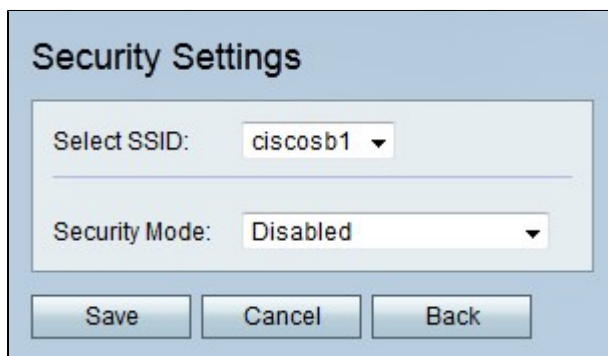
Die Wireless-Sicherheit kann auf dem RV215W deaktiviert werden, um die Einrichtung von Testnetzwerken zu erleichtern. Es wird jedoch nicht empfohlen, die Sicherheit zu deaktivieren.

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie Wireless > Basic Settings (Wireless > Grundeinstellungen). Die Seite Grundeinstellungen wird geöffnet.

Schritt 2. Aktivieren Sie das Kontrollkästchen des Netzwerks, das Sie bearbeiten möchten.

Schritt 3: Klicken Sie auf Sicherheitsmodus bearbeiten, um die Sicherheit des angegebenen Netzwerks zu bearbeiten. Die Seite Sicherheitseinstellungen wird geöffnet:

Schritt 4: Wählen Sie optional aus der Dropdown-Liste Select SSID (SSID auswählen) die SSID aus, für die Sie die Sicherheit konfigurieren möchten.



The image shows a 'Security Settings' window. It has a light blue header with the title 'Security Settings'. Below the header is a white area containing two dropdown menus. The first dropdown is labeled 'Select SSID:' and has 'ciscosb1' selected. The second dropdown is labeled 'Security Mode:' and has 'Disabled' selected. At the bottom of the window are three buttons: 'Save', 'Cancel', and 'Back'.

Schritt 5: Wählen Sie aus der Dropdown-Liste "Sicherheitsmodus" die Option Deaktiviert. Die Sicherheitsfunktion ist für das Wireless-Netzwerk deaktiviert.

Schritt 6: Klicken Sie auf Save (Speichern).

Konfigurieren der WEP-Sicherheit

Wired Equivalent Privacy (WEP) ist ein Algorithmus, der ein Wireless-Netzwerk sichert. WEP stellt eine grundlegende Verschlüsselungsmethode bereit, die weniger sicher ist als WPA. WEP wird verwendet, wenn angeschlossene Netzwerkgeräte WPA nicht unterstützen.

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie Wireless > Basic Settings (Wireless > Grundeinstellungen). Die Seite Grundeinstellungen wird geöffnet.

Schritt 2. Aktivieren Sie das Kontrollkästchen des Netzwerks, das Sie bearbeiten möchten.

Schritt 3: Klicken Sie auf Sicherheitsmodus bearbeiten, um die Sicherheit des angegebenen Netzwerks zu bearbeiten. Die Seite Sicherheitseinstellungen wird geöffnet:



The screenshot shows a web interface titled "Security Settings". It contains several configuration options:

- Select SSID:** A dropdown menu with "ciscosb1" selected.
- Security Mode:** A dropdown menu with "WEP" selected.
- Authentication Type:** A dropdown menu with "Open System" selected, with "(Default: Open System)" in parentheses.
- Encryption:** A dropdown menu with "26/128-bit(26 hex digits)" selected.
- Passphrase:** A text input field containing "passphrase1" and a "Generate" button.
- Key 1:** A text input field filled with dots.
- Key 2:** A text input field filled with dots.
- Key 3:** A text input field filled with dots.
- Key 4:** A text input field filled with dots.
- TX Key:** A dropdown menu with "1" selected.
- Unmask Password:** An unchecked checkbox.

At the bottom of the form are three buttons: "Save", "Cancel", and "Back".

Schritt 4: Wählen Sie optional aus der Dropdown-Liste Select SSID (SSID auswählen) die SSID aus, für die Sie die Sicherheit konfigurieren möchten.

Schritt 5: Wählen Sie in der Dropdown-Liste "Sicherheitsmodus" die Option WEP aus.

Schritt 6: Wählen Sie in der Dropdown-Liste "Authentifizierungstyp" einen Authentifizierungstyp für das Wireless-Netzwerk aus.

- Offenes System - Jeder kann eine Verbindung mit dem Access Point herstellen, aber der WEP-Schlüssel wird benötigt, um den Datenverkehr durch den Access Point des Netzwerks zu leiten.
- Gemeinsamer Schlüssel - Ein WEP-Schlüssel ist erforderlich, um eine Verbindung zum Access Point herzustellen und Datenverkehr durch den Access Point des Netzwerks weiterzuleiten.

Schritt 7: Wählen Sie in der Dropdown-Liste Verschlüsselung eine Verschlüsselungsmethode für den WEP-Schlüssel aus.

- 10/64-Bit (10 Hexadezimalziffern) - Stellt einen 40-Bit-Schlüssel bereit.
- 26/128-Bit (26 Hexadezimalziffern) - Stellt einen 104-Bit-Schlüssel bereit. Dies ist die sicherere Verschlüsselung.

Schritt 8: Geben Sie im Feld Passphrase eine Passphrase ein, die mehr als acht Zeichen enthält.

Schritt 9: Klicken Sie auf Generate (Generieren), um Schlüssel in den Feldern Schlüssel 1, Schlüssel 2, Schlüssel 3 und Schlüssel 4 zu erstellen.

Anmerkung: Sie können Schlüssel auch manuell in die Felder Schlüssel 1, Schlüssel 2, Schlüssel 3 und Schlüssel 4 eingeben.

Schritt 10: Wählen Sie in der Dropdown-Liste "TX Key" (TX-Schlüssel) den Schlüssel aus, den Benutzer eingeben müssen, um auf das Wireless-Netzwerk zuzugreifen.

Schritt 11. (Optional) Aktivieren Sie die Option zum Maskieren des Kennworts, um die Zeichenfolgen der Schlüssel anzuzeigen.

Schritt 12: Klicken Sie auf Save (Speichern).

Konfigurieren der WPA-Personal-Sicherheit

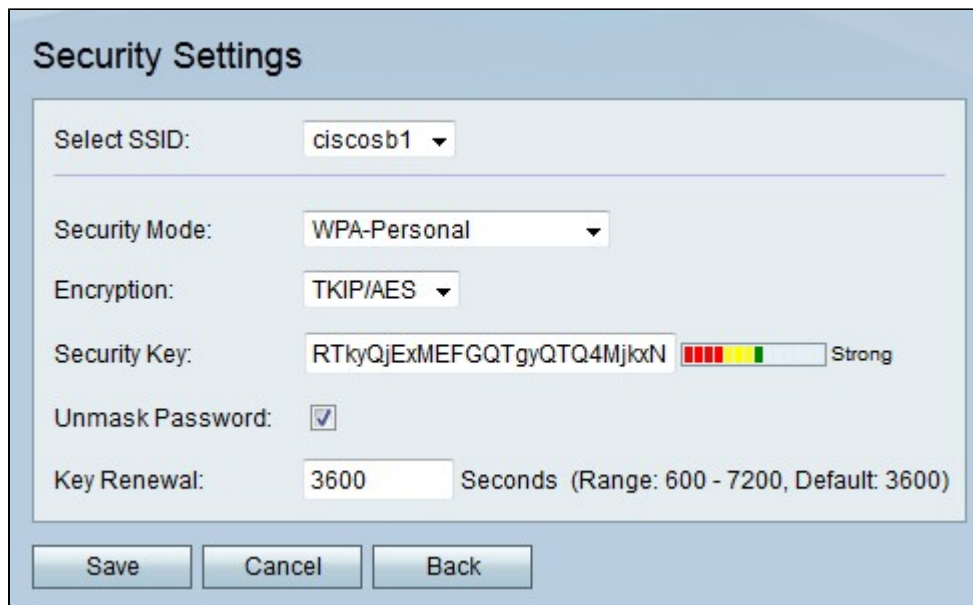
Wi-Fi Protected Access (WPA) ist ein Sicherheitsstandard für Wireless-Netzwerke. WPA wurde erstellt, um WEP aufgrund der Sicherheitsfehler in WEP zu ersetzen. WPA-Personal ist eine

Version von WPA, die für Netzwerke mit nur wenigen Benutzern verwendet wird. WPA-Personal stellt einen gemeinsamen Schlüssel bereit, den jeder Benutzer für den Zugriff auf das Wireless-Netzwerk verwendet. WPA wurde mit den Verschlüsselungsmethoden Temporal Key Integrity Protocol (TKIP) und Advanced Encryption Standard (AES) eingeführt. Mehr Netzwerkgeräte unterstützen TKIP, jedoch ist AES die stärkere Verschlüsselungsmethode.

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie Wireless > Basic Settings (Wireless > Grundeinstellungen). Die Seite Grundeinstellungen wird geöffnet.

Schritt 2. Aktivieren Sie das Kontrollkästchen des Netzwerks, das Sie bearbeiten möchten.

Schritt 3: Klicken Sie auf Sicherheitsmodus bearbeiten, um die Sicherheit des angegebenen Netzwerks zu bearbeiten. Die Seite Sicherheitseinstellungen wird geöffnet:



The screenshot shows a web interface titled "Security Settings". It contains several configuration fields:

- Select SSID:** A dropdown menu with "ciscosb1" selected.
- Security Mode:** A dropdown menu with "WPA-Personal" selected.
- Encryption:** A dropdown menu with "TKIP/AES" selected.
- Security Key:** A text input field containing "RTkyQjExMEFGQTgyQTQ4MjlkxN". To the right of the input is a strength indicator with four colored bars (red, yellow, green, blue) and the word "Strong".
- Unmask Password:** A checkbox that is checked.
- Key Renewal:** A text input field containing "3600", followed by the text "Seconds (Range: 600 - 7200, Default: 3600)".

At the bottom of the form are three buttons: "Save", "Cancel", and "Back".

Schritt 4: Wählen Sie optional aus der Dropdown-Liste Select SSID (SSID auswählen) die SSID aus, für die Sie die Sicherheit konfigurieren möchten.

Schritt 5: Wählen Sie in der Dropdown-Liste "Sicherheitsmodus" die Option WPA-Personal aus.

Schritt 6: Wählen Sie in der Dropdown-Liste Verschlüsselung eine Verschlüsselungsmethode für den WPA-Schlüssel aus.

- TKIP/AES - Diese Option wird gewählt, wenn nicht alle mit dem Wireless-Netzwerk verbundenen Geräte AES unterstützen.
- AES - Diese Option ist vorzuziehen, wenn alle mit den Wireless-Geräten verbundenen Geräte AES unterstützen.

Schritt 7: Geben Sie einen Sicherheitsschlüssel in das Feld Sicherheitsschlüssel ein.

Schritt 8. (Optional) Aktivieren Sie die Option zum Maskieren des Kennworts, um die Zeichenfolge des Schlüssels anzuzeigen.

Schritt 9: Geben Sie im Feld "Key Renewal" (Schlüsselverlängerung) einen Zeitpunkt ein. Dies ist die Zeit, die der RV215W den Schlüssel verwendet, bevor ein neuer generiert wird.

Schritt 10: Klicken Sie auf Save (Speichern).

WPA-Enterprise-Sicherheit konfigurieren

Wi-Fi Protected Access (WPA) ist ein Sicherheitsstandard für Wireless-Netzwerke. WPA wurde erstellt, um WEP aufgrund der Sicherheitsfehler in WEP zu ersetzen. WPA-Enterprise ist eine Version von WPA, die für Netzwerke mit vielen Benutzern (z. B. Unternehmen) empfohlen wird. Die für den Zugriff verwendete Authentifizierung wird von einem RADIUS-Server gesteuert. Das bedeutet, dass jedem verbundenen Benutzer ein eindeutiger Schlüssel für den Zugriff auf das Wireless-Netzwerk zugewiesen wird. WPA wurde mit den Verschlüsselungsmethoden Temporal Key Integrity Protocol (TKIP) und Advanced Encryption Standard (AES) eingeführt. Mehr Netzwerkgeräte unterstützen TKIP, jedoch ist AES die stärkere Verschlüsselungsmethode.

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie Wireless > Basic Settings (Wireless > Grundeinstellungen). Die Seite Grundeinstellungen wird geöffnet.

Schritt 2. Aktivieren Sie das Kontrollkästchen des Netzwerks, das Sie bearbeiten möchten.

Schritt 3: Klicken Sie auf Sicherheitsmodus bearbeiten, um die Sicherheit des angegebenen Netzwerks zu bearbeiten. Die Seite Sicherheitseinstellungen wird geöffnet:

Security Settings

Select SSID: ciscosb1

Security Mode: WPA-Enterprise

Encryption: AES

RADIUS Server: 192 . 168 . 1 . 250 (Hint: 192.168.1.200)

RADIUS Port: 1812 (Range: 1 - 65535, Default: 1812)

Shared Key: SharedKey1

Key Renewal: 3600 Seconds (Range: 600 - 7200, Default: 3600)

Save Cancel Back

Schritt 4: Wählen Sie optional aus der Dropdown-Liste Select SSID (SSID auswählen) die SSID aus, für die Sie die Sicherheit konfigurieren möchten.

Schritt 5: Wählen Sie in der Dropdown-Liste "Sicherheitsmodus" die Option WPA-Enterprise aus.

Schritt 6: Wählen Sie in der Dropdown-Liste Verschlüsselung eine Verschlüsselungsmethode für den WPA-Schlüssel aus.

- TKIP/AES - Diese Option wird gewählt, wenn nicht alle mit dem Wireless-Netzwerk verbundenen Geräte AES unterstützen.
- AES - Diese Option ist vorzuziehen, wenn alle mit den Wireless-Geräten verbundenen Geräte AES unterstützen.

Schritt 7: Geben Sie die IP-Adresse des RADIUS-Servers in das Feld "RADIUS Server" ein.

Schritt 8: Geben Sie die Portnummer für den Zugriff auf den RADIUS-Server im Feld "RADIUS Port" ein.

Schritt 9: Geben Sie den vorinstallierten Schlüssel für die Wireless-Benutzer in das Feld "Gemeinsamer Schlüssel" ein. Ein vorinstallierter Schlüssel ist ein Schlüssel, der für alle Benutzer verwendet wird. Die Funktion für vorinstallierte Schlüssel ist neben der RADIUS-Authentifizierung eine zusätzliche Sicherheitsfunktion.

Schritt 10: Geben Sie im Feld "Key Renewal" (Schlüsselverlängerung) einen Zeitpunkt ein. Dies ist die Zeit, die der RV215W den Schlüssel verwendet, bevor ein neuer generiert wird.

Schritt 11: Klicken Sie auf Save (Speichern).

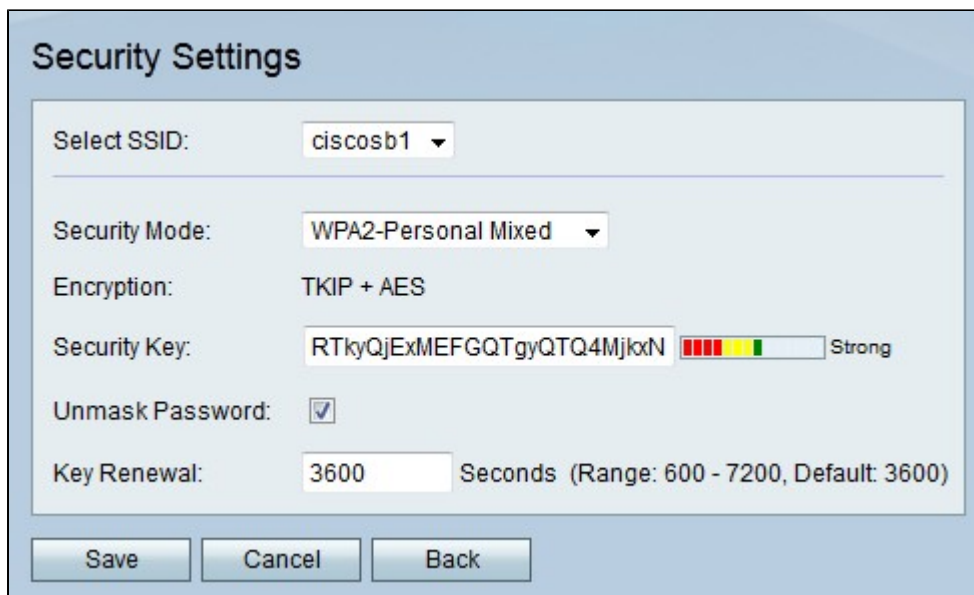
Gemischte Sicherheit für WPA2-Personal/WPA2-Personal konfigurieren

Wi-Fi Protected Access 2 (WPA2) ist ein Sicherheitsstandard für Wireless-Netzwerke. WPA2 ist eine Erweiterung von WPA. WPA2 bietet mehr Sicherheit als WPA, WPA2 erfordert jedoch mehr Verarbeitungsleistung. WPA2-Personal/WPA2-Personal Mixed sind Versionen von WPA2, die für Netzwerke mit wenigen Benutzern verwendet werden. WPA2-Personal Mixed wurde für Abwärtskompatibilität älterer Geräte entwickelt, die WPA2 nicht verwenden können. Verwenden Sie WPA2-Personal Mixed nach Möglichkeit nicht, da die Verbindung weniger sicher ist. WPA2-Personal stellt einen gemeinsamen Schlüssel bereit, den jeder Benutzer für den Zugriff auf das Wireless-Netzwerk verwendet. WPA2 verwendet die Verschlüsselungsmethoden TKIP (Temporal Key Integrity Protocol) und AES (Advanced Encryption Standard). Mehr Netzwerkgeräte unterstützen TKIP, jedoch ist AES die stärkere Verschlüsselungsmethode.

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie Wireless > Basic Settings (Wireless > Grundeinstellungen). Die Seite Grundeinstellungen wird geöffnet.

Schritt 2. Aktivieren Sie das Kontrollkästchen des Netzwerks, das Sie bearbeiten möchten.

Schritt 3: Klicken Sie auf Sicherheitsmodus bearbeiten, um die Sicherheit des angegebenen Netzwerks zu bearbeiten. Die Seite Sicherheitseinstellungen wird geöffnet:



The screenshot shows a web interface titled "Security Settings". It contains the following fields and controls:

- Select SSID:** A dropdown menu with "ciscosb1" selected.
- Security Mode:** A dropdown menu with "WPA2-Personal Mixed" selected.
- Encryption:** A text field displaying "TKIP + AES".
- Security Key:** A text field containing the key "RTkyQjExMEFGQTgyQTQ4MjIxN". To the right of the key is a strength indicator bar with four segments (red, yellow, green, blue) and the label "Strong".
- Unmask Password:** A checkbox that is checked.
- Key Renewal:** A text field with "3600" and the label "Seconds (Range: 600 - 7200, Default: 3600)".
- Buttons:** At the bottom are three buttons: "Save", "Cancel", and "Back".

Schritt 4: Wählen Sie optional aus der Dropdown-Liste Select SSID (SSID auswählen) die SSID aus, für die Sie die Sicherheit konfigurieren möchten.

Schritt 5: Wählen Sie in der Dropdown-Liste "Sicherheitsmodus" die Option WPA2-Personal oder WPA2-Personal Mixed (Gemischt) aus. WPA2-Personal wird verwendet, wenn alle Geräte im

Wireless-Netzwerk AES unterstützen. WPA2-Personal Mixed (Gemischt) wird verwendet, wenn nicht alle Geräte AES unterstützen.

Anmerkung: Der von der Sicherheitsmethode verwendete Verschlüsselungstyp wird im Feld Verschlüsselung angezeigt.

Schritt 6: Geben Sie einen Sicherheitsschlüssel in das Feld Sicherheitsschlüssel ein.

Schritt 7. (Optional) Aktivieren Sie die Option zum Maskieren des Kennworts, um die Zeichenfolgen des Schlüssels anzuzeigen.

Schritt 8: Geben Sie im Feld "Key Renewal" (Schlüsselverlängerung) einen Zeitpunkt ein. Dies ist die Zeit, die der RV215W den Schlüssel verwendet, bevor ein neuer generiert wird.

Schritt 9: Klicken Sie auf Save (Speichern).

Konfigurieren der gemischten Sicherheit von WPA2-Enterprise/WPA2-Enterprise

Wi-Fi Protected Access 2 (WPA2) ist ein Sicherheitsstandard für Wireless-Netzwerke. WPA2 ist eine Erweiterung von WPA. WPA2 bietet mehr Sicherheit als WPA, WPA2 erfordert jedoch mehr Verarbeitungsleistung. WPA2-Enterprise/WPA2-Enterprise-Mixed sind Versionen von WPA2, die für Netzwerke mit vielen Benutzern, z. B. einem Unternehmen, verwendet werden. WPA2-Enterprise-Mixed wurde für Abwärtskompatibilität älterer Geräte entwickelt, die WPA2 nicht verwenden können. Verwenden Sie möglichst WPA2-Enterprise-Mixed nicht, da es eine weniger sichere Verbindung bietet. Die Authentifizierung, um zu bestimmen, ob ein Benutzer Zugriff erhält, wird von einem RADIUS-Server gesteuert. Das bedeutet, dass jedem verbundenen Benutzer ein eindeutiger Schlüssel für den Zugriff auf das Wireless-Netzwerk zugewiesen wird. WPA2 verwendet die Verschlüsselungsmethoden TKIP (Temporal Key Integrity Protocol) und AES (Advanced Encryption Standard). Mehr Netzwerkgeräte unterstützen TKIP, jedoch ist AES die stärkere Verschlüsselungsmethode.

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie Wireless > Basic Settings (Wireless > Grundeinstellungen). Die Seite Grundeinstellungen wird geöffnet.

Schritt 2. Aktivieren Sie das Kontrollkästchen des Netzwerks, das Sie bearbeiten möchten.

Schritt 3: Klicken Sie auf Sicherheitsmodus bearbeiten, um die Sicherheit des angegebenen Netzwerks zu bearbeiten. Die Seite Sicherheitseinstellungen wird geöffnet:

Security Settings

Select SSID:

Security Mode:

Encryption: AES

RADIUS Server: (Hint: 192.168.1.200)

RADIUS Port: (Range: 1 - 65535, Default: 1812)

Shared Key:

Key Renewal: Seconds (Range: 600 - 7200, Default: 3600)

Schritt 4: Wählen Sie optional aus der Dropdown-Liste Select SSID (SSID auswählen) die SSID aus, für die Sie die Sicherheit konfigurieren möchten.

Schritt 5: Wählen Sie aus der Dropdown-Liste "Sicherheitsmodus" die Option WPA2-Enterprise oder WPA2-Enterprise Mixed (WPA2-Enterprise gemischt). WPA2-Enterprise wird verwendet, wenn alle Geräte im Wireless-Netzwerk AES unterstützen. WPA2-Enterprise Mixed (WPA2-Enterprise Gemischt) wird verwendet, wenn nicht alle Geräte AES unterstützen.

Anmerkung: Der von der Sicherheitsmethode verwendete Verschlüsselungstyp wird im Feld Verschlüsselung angezeigt.

Schritt 6: Geben Sie die IP-Adresse des RADIUS-Servers in das Feld "RADIUS Server" ein.

Schritt 7: Geben Sie den Port für den Zugriff auf den RADIUS-Server in das Feld "RADIUS Port" ein.

Schritt 8: Geben Sie den vorinstallierten Schlüssel für die Wireless-Benutzer in das Feld "Gemeinsamer Schlüssel" ein. Ein vorinstallierter Schlüssel ist ein Schlüssel, der für alle Benutzer verwendet wird. Die Funktion für vorinstallierte Schlüssel ist neben der RADIUS-Authentifizierung eine zusätzliche Sicherheitsfunktion.

Schritt 9: Geben Sie im Feld "Key Renewal" (Schlüsselverlängerung) einen Zeitpunkt ein. Dies ist die Zeit, die der RV215W den Schlüssel verwendet, bevor ein neuer generiert wird.

Schritt 10: Klicken Sie auf Save (Speichern).

MAC-Filterung bearbeiten

Die MAC-Filterung wird verwendet, um den Zugriff auf das Wireless-Netzwerk basierend auf der MAC-Adresse des angeschlossenen Geräts zu erlauben oder zu verweigern.

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie Wireless > Basic Settings (Wireless > Grundeinstellungen). Die Seite Grundeinstellungen wird geöffnet:

Basic Settings

Radio: ☒ Enable

Wireless Network Mode: B/G/N-Mixed

Wireless Band Selection: ☒ 20MHz ☐ 20/40MHz

Wireless Channel: 6-2.437 GHZ

AP Management VLAN: 1

U-APSD (WMM Power Save): ☒ Enable

	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	Guest Network	VLAN	Wireless Isolation with SSID	WMM	WPS
☒	☒ ON	ciscosb1	☒	WPA2-Personal Mixed	Disabled	☐	1	☒	☒	☒
☐	☐ OFF	ciscosb2	☐	Disabled	Disabled	☐	1	☐	☒	☐
☐	☐ OFF	ciscosb3	☐	Disabled	Disabled	☐	1	☐	☒	☐
☐	☐ OFF	ciscosb4	☐	Disabled	Disabled	☐	1	☐	☒	☐

Edit Edit Security Mode **Edit MAC Filtering** Time of Day Access Edit Guest Net Edit WPS

Save Cancel

Schritt 2. Aktivieren Sie das Kontrollkästchen des Netzwerks, das Sie bearbeiten möchten.

Schritt 3: Klicken Sie auf MAC-Filterung bearbeiten, um eine MAC-Zugriffskontrollliste für das angegebene Netzwerk zu erstellen. Die Seite Wireless MAC Filter wird geöffnet:

Wireless MAC Filter

SSID: ciscosb1

Wireless MAC Filter: ☒ Enable

Connection Control

- ☒ **Prevent** PCs listed below from accessing the wireless network.
☐ **Permit** PCs listed below to access the wireless network.



Hide Client List

Client List Table

Client Name	IP Address	MAC Address	Status	Save to MAC Address Filter List
9C:B7:0D:73:43:29 Disconnected				☒
Add to MAC				

MAC Address Table

01	9C:B7:0D:73:43:29	12		23	
02		13		24	
03		14		25	
04		15		26	
05		16		27	
06		17		28	
07		18		29	
08		19		30	
09		20		31	
10		21		32	
11		22			

Schritt 4: Aktivieren Sie Aktivieren, um die MAC-Filterung im Netzwerk zu aktivieren.

Schritt 5: Klicken Sie im Feld Verbindungssteuerung auf das Optionsfeld für den gewünschten Listentyp.

- PCs verhindern — Verhindert, dass PCs mit den aufgelisteten MAC-Adressen in das Netzwerk gelangen.
- Zulassen von PCs - Ermöglicht PCs mit den aufgelisteten MAC-Adressen den Zugriff auf das Netzwerk.

Schritt 6: Geben Sie die gewünschten MAC-Adressen in die MAC-Adresstabelle ein.

Schritt 7: Klicken Sie auf Save (Speichern).

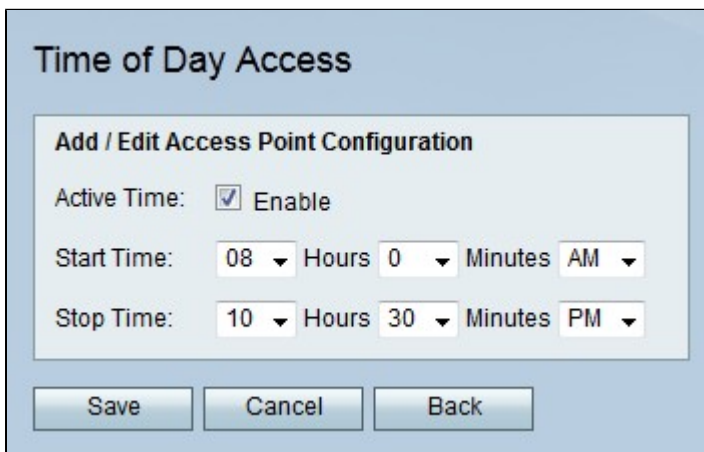
Tageszeitabhängiger Zugriff

Die Funktion "Time of Day Access" (Tageszeit-Zugriff) wird verwendet, um Benutzern den Zugriff nur auf Basis eines konfigurierten Zeitplans zu ermöglichen.

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie Wireless > Basic Settings (Wireless > Grundeinstellungen). Die Seite Grundeinstellungen wird geöffnet:

Schritt 2. Aktivieren Sie das Kontrollkästchen des Netzwerks, das Sie bearbeiten möchten.

Schritt 3: Klicken Sie auf Time of Day Access, um zu konfigurieren, wann Benutzer auf das angegebene Netzwerk zugreifen können. Die Seite Time of Day Access (Tageszeitzugriff) wird geöffnet:



Time of Day Access

Add / Edit Access Point Configuration

Active Time: ☒ Enable

Start Time: 08 Hours 0 Minutes AM

Stop Time: 10 Hours 30 Minutes PM

Save Cancel Back

Schritt 4: Aktivieren Sie im Feld "Active Time" (Aktive Zeit) die Option Enable (Aktivieren), um den Tageszeitzugriff für das Netzwerk zu aktivieren.

Schritt 5: Geben Sie im Feld Startzeit die Uhrzeit ein, zu der der Zugriff auf das Netzwerk beginnt.

Schritt 6: Geben Sie im Feld "Stopp Time" (Stopp-Zeit) den Zeitpunkt ein, zu dem der Zugriff auf das Netzwerk endet.

Schritt 7: Klicken Sie auf Save (Speichern).

Gastnetzwerk bearbeiten

Ein Gastnetzwerk ist ein kleiner Teil eines Netzwerks, der für temporäre Benutzer konzipiert wurde. Diese ermöglicht Gästen die Nutzung des Netzwerks, ohne dass private Wi-Fi-Schlüssel verfügbar gemacht werden müssen. Ein Gastnetzwerk kann so konfiguriert werden, dass die Zugriffszeit und die Bandbreitennutzung eines Benutzers eingeschränkt werden.

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie Wireless > Basic Settings (Wireless > Grundeinstellungen). Die Seite Grundeinstellungen wird geöffnet:

Basic Settings

Radio: ☒ Enable

Wireless Network Mode: B/G/N-Mixed

Wireless Band Selection: ☒ 20MHz ☐ 20/40MHz

Wireless Channel: 6-2.437 GHZ

AP Management VLAN: 1

U-APSD (WMM Power Save): ☒ Enable

Wireless Table										
☐	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	Guest Network	VLAN	Wireless Isolation with SSID	WMM	WPS
☐	☒ ON	ciscosb1	☒	WPA2-Personal Mixed	Disabled	☐	1	☐	☒	☒
☐	☐ OFF	ciscosb2	☐	Disabled	Disabled	☐	1	☐	☒	☐
☐	☐ OFF	ciscosb3	☐	Disabled	Disabled	☐	1	☐	☒	☐
☐	☐ OFF	ciscosb4	☐	Disabled	Disabled	☐	1	☐	☒	☐

Edit Edit Security Mode Edit MAC Filtering Time of Day Access **Edit Guest Net** Edit WPS

Save Cancel

Schritt 2: Klicken Sie auf Gastnetzwerk bearbeiten, um das Gastnetzwerk zu konfigurieren. Die Seite Guest Net Settings wird geöffnet:

Guest Net Settings

Guest Net Name:

Guest Password: Secure

Confirm Guest Password:

Guest Access Time: 240 Minutes (Range: 30 - 1440, Default: 120)

Enable Guest Bandwidth Restriction: ☒ Enable (Enable QoS in the [Bandwidth Management page](#))

Available Bandwidth: 30 % (Range: 1 - 99, Default: 20)

Save Cancel Back

Schritt 3: Geben Sie ein Kennwort ein, das die Benutzer zur Eingabe des Gastnetzwerks im Feld "Gastkennwort" verwenden.

Schritt 4: Geben Sie das Kennwort erneut ein, das die Benutzer für die Eingabe des Gastnetzwerks verwenden, im Feld "Gastkennwort bestätigen".

Schritt 5: Geben Sie die Zeit ein, zu der Benutzer in der Guest Access Time (Zeit für Gastzugriff) mit dem Gastnetzwerk verbunden bleiben dürfen.

Schritt 6: Aktivieren Sie die Option Enable Guest Bandwidth Restriction, um die Bandbreite einzuschränken, die das Gastnetzwerk erhält.

Anmerkung: Die Bandbreitenverwaltung muss auf der Seite Bandbreitenverwaltung aktiviert werden.

Schritt 7: Geben Sie im Feld "Verfügbare Bandbreite" den Prozentsatz der Bandbreite ein, die für das Gastnetzwerk verfügbar sein soll.

Schritt 8: Klicken Sie auf Save (Speichern).

WPS-Methode 1 konfigurieren

Wi-Fi Protected Setup (WPS) ist eine Funktion, die eine einfache und sichere Einrichtung des Wireless-Netzwerks ermöglicht. Um eine Verbindung mit WPS herstellen zu können, muss das Verbindungsgerät WPS unterstützen und mit der WPA-Sicherheit kompatibel sein. Die erste Konfigurationsmethode ist eine einfache Methode, bei der die RV215W WPS-Taste und die Client-

Gerätetaste gedrückt werden müssen. Sobald beide Tasten gedrückt sind, wird das Client-Gerät mit dem WPS-Netzwerk verbunden.

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie Wireless > Basic Settings (Wireless > Grundeinstellungen). Die Seite Grundeinstellungen wird geöffnet:

Basic Settings

Radio: ☒ Enable

Wireless Network Mode: B/G/N-Mixed

Wireless Band Selection: ☒ 20MHz ☐ 20/40MHz

Wireless Channel: 6-2.437 GHZ

AP Management VLAN: 1

U-APSD (WMM Power Save): ☒ Enable

Wireless Table										
☐	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	Guest Network	VLAN	Wireless Isolation with SSID	WMM	WPS
☐	☒ ON	ciscosb1	☒	WPA2-Personal Mixed	Disabled	☐	1	☐	☒	☒
☐	☐ OFF	ciscosb2	☐	Disabled	Disabled	☐	1	☐	☒	☐
☐	☐ OFF	ciscosb3	☐	Disabled	Disabled	☐	1	☐	☒	☐
☐	☐ OFF	ciscosb4	☐	Disabled	Disabled	☐	1	☐	☒	☐

Edit Edit Security Mode Edit MAC Filtering Time of Day Access Edit Guest Net **Edit WPS**

Save Cancel

Schritt 2: Klicken Sie auf WPS bearbeiten, um WPS zu konfigurieren. Die Seite WPS wird geöffnet:

Anmerkung: Auf die WPS-Seite kann auch über Wireless > WPS zugegriffen werden.

WPS

Wi-Fi Protected Setup™

WPS: ciscosb1

Use one of the following for each Wi-Fi Protected Setup supported device:

1. If your client device has a Wi-Fi Protected Setup button, click or press that button and then click the button on the right.



OR

2. If your client device has a Wi-Fi protected Setup PIN number, enter that number here and then click

OR

3. If your client asks for the Router's PIN number, enter Device PIN below in your client device.

Device PIN Status: Active

Device PIN:

PIN Lifetime:

Wi-Fi Protected Setup Status: Configured

Network Name (SSID): ciscosb1

Security: WPA2-Personal

Schritt 3: Klicken Sie auf Bearbeiten, um das Wireless-Netzwerk auszuwählen, in dem WPS aktiviert werden soll.

WPS

Wi-Fi Protected Setup™

WPS: ciscosb1

Use one of the following for each Wi-Fi Protected Setup supported device:

1. If your client device has a Wi-Fi Protected Setup button, click or press that button and then click the button on the right.



OR

2. If your client device has a Wi-Fi protected Setup PIN number, enter that number here 19582493 and then click

OR

3. If your client asks for the Router's PIN number, enter Device PIN below in your client device.

Device PIN Status: Active

Device PIN: 47083578

PIN Lifetime: 4 Hours ▼

Wi-Fi Protected Setup Status: Configured

Network Name (SSID): ciscosb1

Security: WPA2-Personal

Schritt 4: Klicken Sie auf die Schaltfläche WPS auf der Seite WPS.

Schritt 5: Klicken Sie auf die WPS-Schaltfläche auf dem Client-Gerät oder auf einem Dienstprogrammbildschirm des Client-Geräts, um das Client-Gerät mit dem WPS-Netzwerk zu verbinden.

In den folgenden Feldern werden Informationen zur WPS-Konfiguration angezeigt.

- Wi-Fi Protected Setup Status - Der Status der WPS-Konfiguration.
- Netzwerkname (SSID) - Der Netzwerkname, der der WPS-Konfiguration vom RV215W zugewiesen wurde.
- WPA2-Personal - Der Sicherheitstyp, den die WPS-Konfiguration verwendet.

WPS-Methode 2 konfigurieren

Wi-Fi Protected Setup (WPS) ist eine Funktion, die eine einfache und sichere Einrichtung des Wireless-Netzwerks ermöglicht. Um eine Verbindung mit WPS herstellen zu können, muss das Verbindungsgerät WPS unterstützen und mit der WPA-Sicherheit kompatibel sein. Bei der zweiten Methode muss die PIN-Nummer des Client-Geräts angegeben werden. Nachdem die PIN-Nummer auf der WPS-Seite eingegeben wurde, stellt das Client-Gerät eine Verbindung zum WPS-Netzwerk her.

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie Wireless > Basic Settings (Wireless > Grundeinstellungen). Die Seite Grundeinstellungen wird geöffnet:

Basic Settings

Radio: ☒ Enable

Wireless Network Mode: B/G/N-Mixed

Wireless Band Selection: ☒ 20MHz ☐ 20/40MHz

Wireless Channel: 6-2.437 GHZ

AP Management VLAN: 1

U-APSD (WMM Power Save): ☒ Enable

Wireless Table										
☐	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	Guest Network	VLAN	Wireless Isolation with SSID	WMM	WPS
☐	☒ ON	ciscosb1	☒	WPA2-Personal Mixed	Disabled	☐	1	☐	☒	☒
☐	☐ OFF	ciscosb2	☐	Disabled	Disabled	☐	1	☐	☒	☐
☐	☐ OFF	ciscosb3	☐	Disabled	Disabled	☐	1	☐	☒	☐
☐	☐ OFF	ciscosb4	☐	Disabled	Disabled	☐	1	☐	☒	☐

Edit Edit Security Mode Edit MAC Filtering Time of Day Access Edit Guest Net **Edit WPS**

Save Cancel

Schritt 2: Klicken Sie auf WPS bearbeiten, um WPS zu konfigurieren. Die Seite WPS wird geöffnet:

Anmerkung: Auf die WPS-Seite kann auch über Wireless > WPS zugegriffen werden.

WPS

Wi-Fi Protected Setup™

WPS: ciscosb1

Use one of the following for each Wi-Fi Protected Setup supported device:

1. If your client device has a Wi-Fi Protected Setup button, click or press that button and then click the button on the right.



OR

2. If your client device has a Wi-Fi protected Setup PIN number, enter that number here 19582493 and then click

OR

3. If your client asks for the Router's PIN number, enter Device PIN below in your client device.

Device PIN Status: Active

Device PIN: 47083578

PIN Lifetime: 4 Hours ▼

Wi-Fi Protected Setup Status: Configured

Network Name (SSID): ciscosb1

Security: WPA2-Personal

Schritt 3: Klicken Sie auf Bearbeiten, um das Wireless-Netzwerk auszuwählen, in dem WPS aktiviert werden soll.

Schritt 4: Geben Sie die PIN-Nummer des Client-Geräts ein.

Schritt 5: Klicken Sie auf Registrieren, um das WPS-Netzwerk zu erstellen.

In den folgenden Feldern werden Informationen zur WPS-Konfiguration angezeigt.

- Wi-Fi Protected Setup Status - Der Status der WPS-Konfiguration.
- Netzwerkname (SSID) - Der Netzwerkname, der der WPS-Konfiguration vom RV215W zugewiesen wurde.

- WPA2-Personal - Der Sicherheitstyp, den die WPS-Konfiguration verwendet.

WPS-Methode 3 konfigurieren

Wi-Fi Protected Setup (WPS) ist eine Funktion, die eine einfache und sichere Einrichtung des Wireless-Netzwerks ermöglicht. Um eine Verbindung mit WPS herstellen zu können, muss das Verbindungsgerät WPS unterstützen und mit der WPA-Sicherheit kompatibel sein. Bei der dritten Methode muss der Benutzer die PIN-Nummer des RV215W auf der WPS-Konfigurationsseite des Client-Geräts eingeben.

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie Wireless > Basic Settings (Wireless > Grundeinstellungen). Die Seite Grundeinstellungen wird geöffnet:

Basic Settings

Radio: ☒ Enable

Wireless Network Mode: B/G/N-Mixed

Wireless Band Selection: ☒ 20MHz ☐ 20/40MHz

Wireless Channel: 6-2.437 GHZ

AP Management VLAN: 1

U-APSD (WMM Power Save): ☒ Enable

	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	Guest Network	VLAN	Wireless Isolation with SSID	WMM	WPS
☐	☒ ON	ciscosb1	☒	WPA2-Personal Mixed	Disabled	☐	1	☐	☒	☒
☐	☐ OFF	ciscosb2	☐	Disabled	Disabled	☐	1	☐	☒	☐
☐	☐ OFF	ciscosb3	☐	Disabled	Disabled	☐	1	☐	☒	☐
☐	☐ OFF	ciscosb4	☐	Disabled	Disabled	☐	1	☐	☒	☐

Buttons: Edit, Edit Security Mode, Edit MAC Filtering, Time of Day Access, Edit Guest Net, **Edit WPS** (highlighted), Save, Cancel

Schritt 2: Klicken Sie auf WPS bearbeiten, um WPS zu konfigurieren. Die Seite WPS wird geöffnet:

Anmerkung: Auf die WPS-Seite kann auch über Wireless > WPS zugegriffen werden.

WPS

Wi-Fi Protected Setup™

WPS: ciscosb1

Use one of the following for each Wi-Fi Protected Setup supported device:

1. If your client device has a Wi-Fi Protected Setup button, click or press that button and then click the button on the right.



OR

2. If your client device has a Wi-Fi protected Setup PIN number, enter that number here 19582493 and then click

OR

3. If your client asks for the Router's PIN number, enter Device PIN below in your client device.

Device PIN Status: Active

Device PIN: 47083578

PIN Lifetime: 4 Hours ▼

Wi-Fi Protected Setup Status: Configured

Network Name (SSID): ciscosb1

Security: WPA2-Personal

Schritt 3: Klicken Sie auf Bearbeiten, um das Wireless-Netzwerk auszuwählen, in dem WPS aktiviert werden soll.

Schritt 4: Klicken Sie auf Generate (Generieren), um eine PIN-Nummer für den RV215W zu generieren.

Schritt 5: Wählen Sie aus der Dropdown-Liste "PIN-Lebensdauer" die Zeit aus, die vergeht, bevor eine neue PIN generiert wird.

Schritt 6: Geben Sie die angegebene RV215W PIN-Nummer in die Client-Gerätekonfiguration ein. Das Client-Gerät stellt eine Verbindung zum WPS-Netzwerk her.

In den folgenden Feldern werden Informationen zur WPS-Konfiguration angezeigt.

- Wi-Fi Protected Setup Status - Der Status der WPS-Konfiguration.
- Netzwerkname (SSID) - Der Netzwerkname, der der WPS-Konfiguration vom RV215W zugewiesen wurde.
- WPA2-Personal - Der Sicherheitstyp, den die WPS-Konfiguration verwendet.

Wenn Sie weitere Dokumentation zum RV215W-Router sehen möchten, klicken Sie [hier](#).



Video zu diesem Artikel anzeigen ...

[Klicken Sie hier, um weitere Tech Talks von Cisco anzuzeigen.](#)

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.