

Konfigurieren der Wireless-Sicherheitseinstellungen auf einem WAP

Einführung

Die Konfiguration der Wireless-Sicherheit auf Ihrem Wireless Access Point (WAP) ist äußerst wichtig, um Ihr Wireless-Netzwerk vor Eindringlingen zu schützen, die den Schutz Ihrer Wireless-Geräte sowie die Daten, die über Ihr Wireless-Netzwerk übertragen werden, gefährden können. Sie können die Wireless-Sicherheit in Ihrem Wireless-Netzwerk konfigurieren, indem Sie MAC Filter, Wi-Fi Protected Access (WPA/WPA2) Personal und WPA/WPA2 Enterprise einrichten.

MAC-Filterung wird verwendet, um die Wireless-Clients mithilfe ihrer MAC-Adressen für den Zugriff auf das Netzwerk zu filtern. Eine Client-Liste wird so konfiguriert, dass die Adressen in der Liste für den Zugriff auf das Netzwerk zugelassen oder blockiert werden. Dies hängt von Ihrer Präferenz ab. Weitere Informationen zur MAC-Filterung erhalten Sie [hier](#).

WPA/WPA2 Personal und WPA/WPA2 Enterprise sind Sicherheitsprotokolle, die zum Schutz der Privatsphäre verwendet werden, indem die übertragenen Daten über das Wireless-Netzwerk verschlüsselt werden. WPA/WPA2 ist mit den IEEE-Standards 802.11E und 802.11i kompatibel. Im Vergleich zum WEP-Sicherheitsprotokoll (Wired Equivalent Privacy) hat WPA/WPA2 die Authentifizierungs- und Verschlüsselungsfunktionen verbessert.

WPA/WPA2 Personal ist für den Heimgebrauch und WPA/WPA2 Enterprise für ein Netzwerk im geschäftlichen Maßstab. WPA/WPA2 Enterprise bietet im Vergleich zu WPA/WPA2 Personal mehr Sicherheit und eine zentrale Kontrolle über das Netzwerk.

In diesem Szenario wird die Wireless-Sicherheit auf dem WAP konfiguriert, um das Netzwerk mithilfe der WPA/WPA2 Personal- und Enterprise-Einstellungen vor Eindringlingen zu schützen.

Ziel

In diesem Artikel erfahren Sie, wie Sie Sicherheitsprotokolle für WPA/WPA2 Personal und Enterprise konfigurieren, um die Sicherheit und den Datenschutz Ihres Wireless-Netzwerks zu verbessern.

Hinweis: In diesem Artikel wird davon ausgegangen, dass auf dem WAP bereits ein Service Set Identifier (SSID) oder ein Wireless Local Area Network (WLAN) erstellt wurde.

Anwendbare Geräte

- WAP100-Serie
- WAP300-Serie
- WAP500-Serie

Softwareversion

- 1.0.2.14 - WAP131, WAP351

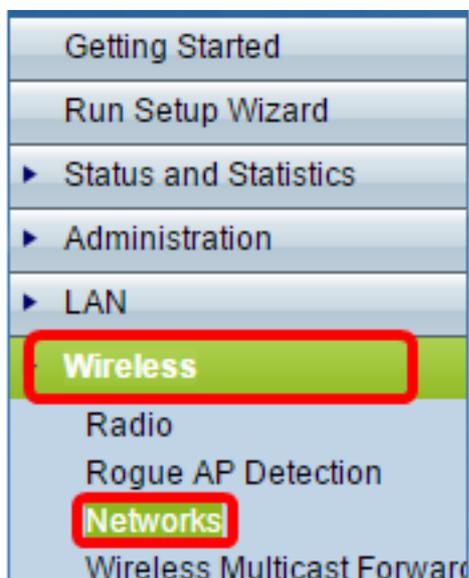
- 1.0.6.5 - WAP121, WAP321
- 1.3.0.4 - WAP371
- 1.1.0.7 - WAP150, WAP361
- 1.2.1.5 - WAP551, WAP561
- 1.0.1.11 - WAP571, WAP571E

Konfigurieren der Wireless-Sicherheitseinstellungen

WPA/WPA2 Personal konfigurieren

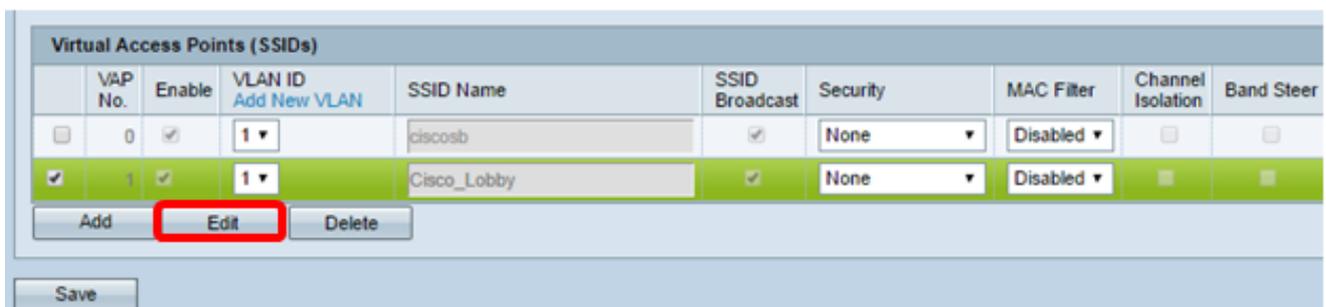
Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm des Access Points an, und wählen Sie **Wireless > Networks** aus.

Hinweis: In der Abbildung unten wird das webbasierte Dienstprogramm des WAP361 als Beispiel verwendet. Die Menüoptionen können je nach Gerät variieren.



Schritt 2: Aktivieren Sie im Bereich Virtual Access Points (SSIDs) das Kontrollkästchen der SSID, die Sie konfigurieren möchten, und klicken Sie auf **Edit**.

Hinweis: In diesem Beispiel wird VAP1 ausgewählt.



Schritt 3: Klicken Sie in der Dropdown-Liste "Sicherheit" auf **WPA Personal**.

Virtual Access Points (SSIDs)							
VAP No.	Enable	VLAN ID <small>Add New VLAN</small>	SSID Name	SSID Broadcast	Security		
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	ciscosb	<input checked="" type="checkbox"/>	None		
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	Cisco_Lobby	<input checked="" type="checkbox"/>	None	<div style="border: 2px solid red; padding: 2px;"> None None WPA Personal WPA Enterprise </div>	

Schritt 4: Aktivieren Sie das Kontrollkästchen, um die WPA-Version (WPA-TKIP oder WPA2-AES) auszuwählen. Zwei können gleichzeitig ausgewählt werden.

- WPA-TKIP - Wi-Fi Protected Access-Temporal Key Integrity Tool. Das Netzwerk verfügt über einige Client-Stationen, die nur das ursprüngliche WPA- und TKIP-Sicherheitsprotokoll unterstützen. Beachten Sie, dass die Wahl von nur WPA-TKIP für Access Points gemäß den neuesten Anforderungen der Wi-Fi Alliance nicht zulässig ist.
- WPA2-AES - Wi-Fi Protected Access-Advanced Encryption Standard. Alle Client-Stationen im Netzwerk unterstützen das Verschlüsselungs-/Sicherheitsprotokoll WPA2 und AES-CCMP. 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.

Hinweis: In diesem Beispiel sind beide Kontrollkästchen aktiviert.

WPA Versions: WPA-TKIP WPA2-AES

Key: (Range: 8-63 Characters)

Show Key as Clear Text

Key Strength Meter: Below Minimum

Broadcast Key Refresh Rate Sec (Range: 0-86400, 0 =

Schritt 5: Erstellen Sie ein Kennwort mit 8 bis 63 Zeichen, und geben Sie es in das Feld *Schlüssel* ein.

WPA Versions: WPA-TKIP WPA2-AES

Key: (Range: 8-63 Characters)

Show Key as Clear Text

Key Strength Meter: Strong

Hinweis: Sie können das Feld **Schlüssel als Klartext anzeigen** aktivieren, um das von Ihnen erstellte Kennwort anzuzeigen.

WPA Versions: WPA-TKIP WPA2-AES

Key: (Range: 8-63 Characters)

Show Key as Clear Text

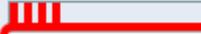
Key Strength Meter:  Strong

Schritt 6: (Optional) Geben Sie im Feld *Broadcast Key Refresh Rate (Aktualisierungsrate für Sendeschlüssel)* einen Wert oder das Intervall ein, in dem der Schlüssel Broadcast (Gruppe) für Clients aktualisiert wird, die diesem VAP zugeordnet sind. Der Standardwert ist 300 Sekunden, und der gültige Bereich liegt zwischen 0 und 86.400 Sekunden. Ein Wert von 0 gibt an, dass der Broadcast-Schlüssel nicht aktualisiert wird.

WPA Versions: WPA-TKIP WPA2-AES

Key: (Range: 8-63 Characters)

Show Key as Clear Text

Key Strength Meter:  Session Key Refresh Rate

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)

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

Virtual Access Points (SSIDs)				
	VAP No.	Enable	VLAN ID <small>Add New VLAN</small>	SSID Name
<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	1	ciscosb
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	1	Cisco_Lobby

Add Edit Delete

Save

Sie haben jetzt WPA Personal auf Ihrem WAP konfiguriert.

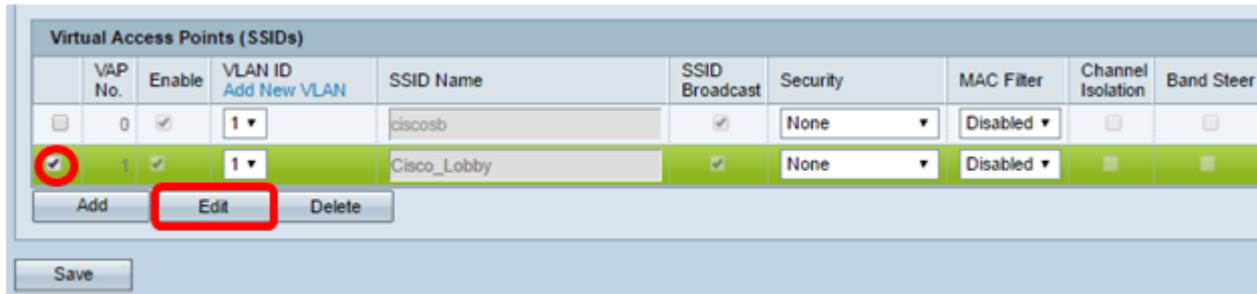
WPA/WPA2 Enterprise konfigurieren

Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm des Access Points an, und wählen Sie **Wireless > Networks** aus.

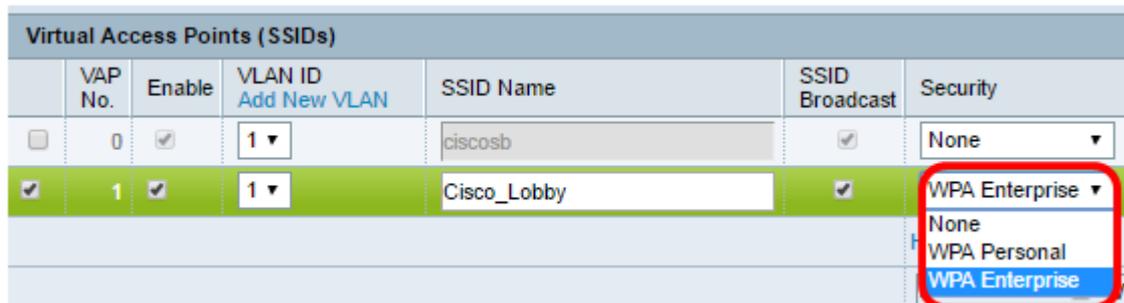
Hinweis: In der Abbildung unten wird das webbasierte Dienstprogramm des WAP361 als Beispiel verwendet.

- Getting Started
- Run Setup Wizard
- ▶ Status and Statistics
- ▶ Administration
- ▶ LAN
- Wireless**
- Radio
- Rogue AP Detection
- Networks**
- Wireless Multicast Forward

Schritt 2: Aktivieren Sie im Bereich Virtual Access Points (SSIDs) die SSID, die Sie konfigurieren möchten, und klicken Sie unten auf die Schaltfläche **Bearbeiten**.



Schritt 3: Wählen Sie **WPA Enterprise** aus der Dropdown-Liste Security (Sicherheit) aus.



Schritt 4: Wählen Sie die WPA-Version (WPA-TKIP, WPA2-AES und Enable Pre-Authentication) aus.

- Vorauthentifizierung aktivieren: Wenn Sie nur WPA2-AES oder WPA-TKIP und WPA2-AES als WPA-Version auswählen, können Sie die Vorauthentifizierung für die WPA2-AES-Clients aktivieren. Aktivieren Sie diese Option, wenn die WPA2-Wireless-Clients die Pre-Authentication-Pakete senden sollen. Die Vorauthentifizierungsinformationen 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 Access Points (AP) verbunden sind.

Hinweis: Diese Option gilt nicht, wenn Sie WPA-TKIP für WPA-Versionen ausgewählt haben, da die ursprüngliche WPA diese Funktion nicht unterstützt.

Hide Details

WPA Versions: WPA-TKIP WPA2-AES
 Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)
 Server IP Address-2: (xxx.xxx.xxx.xxx)
 Server IP Address-3: (xxx.xxx.xxx.xxx)
 Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1 - 64 Characters)
 Key-2: (Range: 1 - 64 Characters)
 Key-3: (Range: 1 - 64 Characters)
 Key-4: (Range: 1 - 64 Characters)

Enable RADIUS Accounting

Active Server:

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)
 Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

Schritt 5: (Optional) Deaktivieren Sie das Kontrollkästchen **Globale RADIUS-Servereinstellungen verwenden**, um die Einstellungen zu bearbeiten.

WPA Versions: WPA-TKIP WPA2-AES
 Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)
 Server IP Address-2: (xxx.xxx.xxx.xxx)
 Server IP Address-3: (xxx.xxx.xxx.xxx)
 Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1 - 64 Characters)
 Key-2: (Range: 1 - 64 Characters)
 Key-3: (Range: 1 - 64 Characters)
 Key-4: (Range: 1 - 64 Characters)

Enable RADIUS Accounting

Active Server:

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)
 Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

Schritt 6: (Optional) Klicken Sie auf das Optionsfeld für den richtigen **IP-Adresstyp des Servers**.

Hinweis: In diesem Beispiel wird IPv4 gewählt.

WPA Versions: WPA-TKIP WPA2-AES
 Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)
Server IP Address-2: (xxx.xxx.xxx.xxx)
Server IP Address-3: (xxx.xxx.xxx.xxx)
Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1 - 64 Characters)
Key-2: (Range: 1 - 64 Characters)
Key-3: (Range: 1 - 64 Characters)
Key-4: (Range: 1 - 64 Characters)

Enable RADIUS Accounting

Active Server: ▼

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)
Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

Schritt 7: Geben Sie die IP-Adresse des RADIUS-Servers im Feld *Server IP Address* (*Server-IP-Adresse*) ein.

Hinweis: Für dieses Beispiel wird 192.168.1.101 verwendet.

WPA Versions: WPA-TKIP WPA2-AES
 Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)
Server IP Address-2: (xxx.xxx.xxx.xxx)
Server IP Address-3: (xxx.xxx.xxx.xxx)
Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1 - 64 Characters)
Key-2: (Range: 1 - 64 Characters)
Key-3: (Range: 1 - 64 Characters)
Key-4: (Range: 1 - 64 Characters)

Enable RADIUS Accounting

Active Server: ▼

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)
Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

Schritt 8: Geben Sie im Feld *Key* den Kennwortschlüssel für den RADIUS-Server ein, den der WAP für die Authentifizierung beim RADIUS-Server verwendet. Sie können zwischen 1 und 64 alphanumerische Standardzeichen und Sonderzeichen verwenden.

Hinweis: Bei den Tasten wird die Groß- und Kleinschreibung beachtet, und sie müssen mit dem auf dem RADIUS-Server konfigurierten Schlüssel übereinstimmen.

Schritt 9: (Optional) Wiederholen Sie die Schritte 7-8 für jeden RADIUS-Server im Netzwerk, mit dem der WAP kommunizieren soll.

WPA Versions: WPA-TKIP WPA2-AES
 Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)
Server IP Address-2: (xxx.xxx.xxx.xxx)
Server IP Address-3: (xxx.xxx.xxx.xxx)
Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1 - 64 Characters)
Key-2: (Range: 1 - 64 Characters)
Key-3: (Range: 1 - 64 Characters)
Key-4: (Range: 1 - 64 Characters)

Enable RADIUS Accounting

Active Server: ▼

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)
Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

Schritt 11: Klicken Sie .

Sie haben jetzt die WPA/WPA2 Enterprise-Sicherheit erfolgreich auf Ihrem WAP konfiguriert.