

Draadloze beveiligingsinstellingen op een WAP configureren

Inleiding

Het configureren van de draadloze beveiliging op uw Wireless Access Point (WAP) is zeer essentieel om uw draadloze netwerk te beschermen tegen indringers die de privacy van uw draadloze apparaten evenals de gegevensoverdracht via uw draadloze netwerk in gevaar kunnen brengen. U kunt de draadloze beveiliging van uw draadloze netwerk configureren door MAC Filter, Wi-Fi Protected Access (WAP/WAP2) Persoonlijk en WAP/WAP2 Enterprise in te stellen.

MAC Filtering wordt gebruikt om de draadloze clients te filteren om het netwerk te bereiken met behulp van hun MAC-adressen. Een clientlijst is ingesteld om de adressen in de lijst toe te staan of te blokkeren, afhankelijk van uw voorkeur. Om meer te weten te komen over MAC Filtering, klik [hier](#).

Persoonlijk en de Persoonlijke en WAP/WAP2 Enterprise zijn veiligheidsprotocollen die gebruikt worden om de privacy te beschermen door de verzonden gegevens via het draadloze netwerk te versleutelen. WAP/WAP2 is compatibel met IEEE 802.11E en 802.11i. Vergeleken met het beveiligingsprotocol met Wired Equivalent Privacy (EVP), hebben WAP/WAP2 de verificatie en coderingsfuncties verbeterd.

Persoonlijk WAP/WAP2 is voor huisgebruik en WAP/WAP2 Enterprise is voor netwerk op bedrijfsniveau. WAP/WAP2 Enterprise biedt grotere beveiliging en gecentraliseerde controle over het netwerk vergeleken met Persoonlijk WAP/WAP2.

In dit scenario zal draadloze beveiliging op WAP worden geconfigureerd om het netwerk tegen indringers te beschermen met behulp van de instellingen voor WAP/WAP2 en Enterprise.

Doel

Dit artikel is bedoeld om u te tonen hoe u de Persoonlijke en de Veiligheid van de Persoonlijke en de Veiligheid van de Bedrijf te vormen om de veiligheid en de privacy van uw draadloos netwerk te verbeteren.

Opmerking: Dit artikel gaat ervan uit dat een Service Set-Identificer (SSID) of een Wireless Local Area Network (WLAN) al op uw WAP is gemaakt.

Toepasselijke apparaten

- WAP100 Series switch
- WAP300 Series-switches
- WAP500 Series-switches

Softwareversie

- 1.0.2.14 - WAP131, WAP351

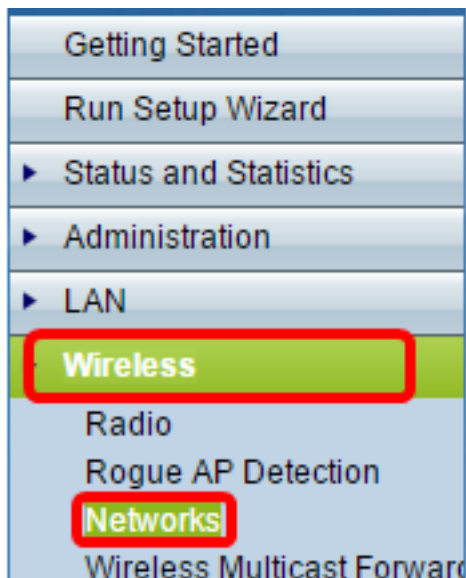
- 1.0.6.5 - WAP121, WAP321
- 1.3.0.4 - WAP371
- 1.1.0.7 - WAP150, WAP361
- 1.2.1.5 - WAP551, WAP561
- 1.0.1.11 - WAP571, WAP571E

Draadloze beveiligingsinstellingen configureren

Persoonlijk WAP/WAP2 configureren

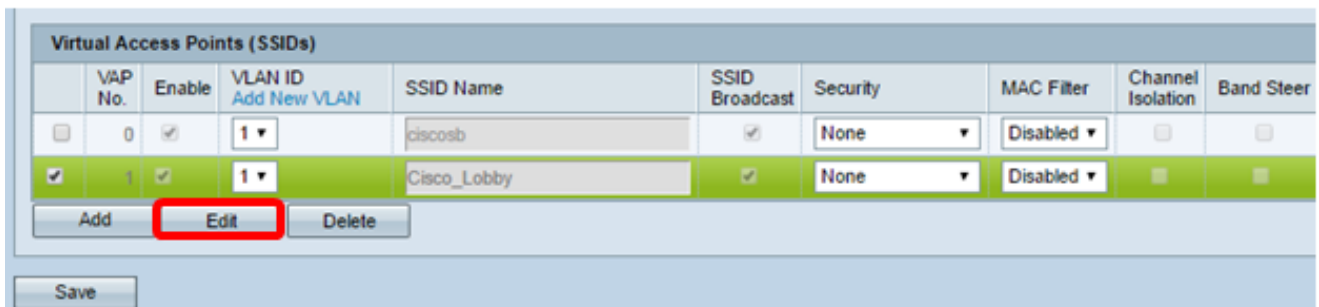
Stap 1. Meld u aan bij het webgebaseerde hulpprogramma van uw access point en kies **Wireless > netwerken**.

Opmerking: In de onderstaande afbeelding wordt het op internet gebaseerde nut van WAP361 als voorbeeld gebruikt. De menuopties kunnen variëren afhankelijk van het model van het apparaat.



Stap 2. Onder het gebied Virtual Access Point (SSID's) controleert u het aankruisvakje van de SSID die u wilt configureren en klikt op **Bewerken**.

Opmerking: In dit voorbeeld wordt VAP1 geselecteerd.



Stap 3. Klik in de vervolgkeuzelijst Security op **WAP Persoonlijk**.

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>

Stap 4. Kies de WAP-versie (WPA-TKIP of WPA2-AES) door het aankruisvakje te controleren. Twee kunnen tegelijk worden gekozen.

- WPA-TKIP — Wi-Fi beschermde access-tijdelijke toetsingstool. Het netwerk heeft bepaalde clientstations die alleen het oorspronkelijke protocol voor WAP- en TKIP-beveiliging ondersteunen. Merk op dat het kiezen van alleen WPA-TKIP voor access point niet is toegestaan volgens de laatste Wi-Fi Alliance vereiste.
- WPA2-AES — Wi-Fi beschermde access-geavanceerde encryptie-standaard. Alle clientstations op de netwerkondersteuning van WPA2 en AES-CCMP-algoritme/beveiligingsprotocol. Deze WAP-versie biedt de beste beveiliging volgens de IEEE 802.11i-standaard. Volgens de laatste Wi-Fi Alliance-eis moet WAP deze modus voortdurend ondersteunen.

Opmerking: In dit voorbeeld worden beide vinkjes gecontroleerd.

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 =

Stap 5. Maak een wachtwoord dat uit 8-63 tekens bestaat, en voer het in het veld Key in.

WPA Versions: WPA-TKIP WPA2-AES

Key: (Range: 8-63 Characters)

Show Key as Clear Text


Key Strength Meter: Strong

Opmerking: U kunt de sleutel tonen als het vakje Tekst wissen controleren om het wachtwoord weer te geven dat u hebt gemaakt.

WPA Versions: WPA-TKIP WPA2-AES

Key: (Range: 8-63 Characters)

Show Key as Clear Text

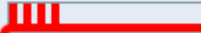
Key Strength Meter:  Strong

Stap 6. (Optioneel) In het veld *Broadcast Key Refresh Rate* voert u een waarde in of het interval in waarmee de uitzending (groep)-toets wordt teruggestuurd voor klanten die bij deze VAP zijn gekoppeld. De standaardinstelling is 300 seconden en het geldige bereik is van 0 tot 86400 seconden. Een waarde van 0 geeft aan dat de uitzending-toets niet wordt vernieuwd.

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)

Stap 7. Klik op **Opslaan**.

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

U hebt nu WAP Persoonlijk op uw WAP ingesteld.

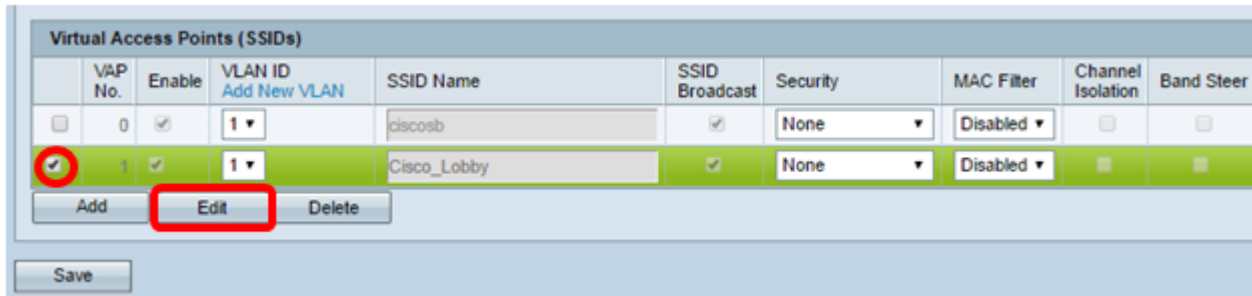
WAP2-ondernemingen configureren

Stap 1. Meld u aan bij het webgebaseerde hulpprogramma van uw access point en kies **Wireless > Networks**.

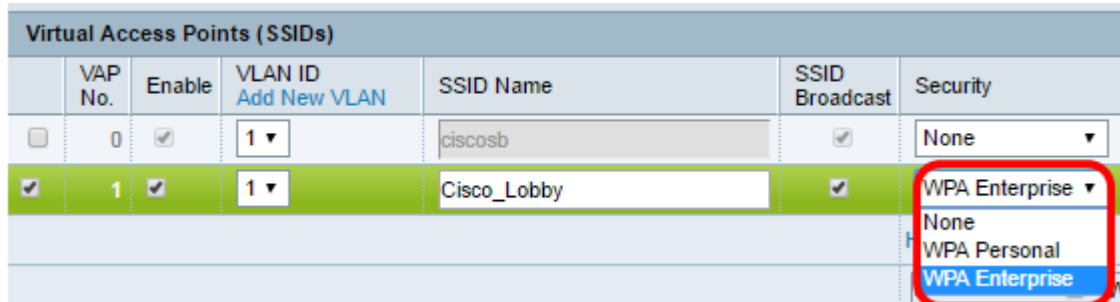
Opmerking: In de onderstaande afbeelding wordt het op internet gebaseerde nut van WAP361 als voorbeeld gebruikt.

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

Stap 2. Onder het gebied Virtual Access Point (SSID's) controleert u de SSID's die u wilt configureren en klikt op de knop **Bewerken** hieronder.



Stap 3. Kies **WAP Enterprise** uit de vervolgkeuzelijst Beveiligingsinstellingen.



Stap 4. Kies de WAP-versie (WAP-TKIP, WAP2-AES en pre-verificatie inschakelen).

- Schakel pre-verificatie in - Als u alleen voor WAP2-AES of zowel voor WAP-TKIP als voor WAP2-AES kiest, kunt u pre-verificatie voor de WAP2-AES clients inschakelen. Controleer deze optie als u wilt dat de WAP2 draadloze klanten de pre-authenticatie pakketten verzenden. De informatie van vóór de verificatie wordt via het WAP-apparaat doorgegeven dat de client momenteel gebruikt voor het WAP-doelapparaat. Het inschakelen van deze functie kan ertoe bijdragen de authenticatie van roamende klanten te versnellen die verbinding maken met meerdere access points (AP).

Opmerking: Deze optie is niet van toepassing als u WAP-TKIP voor WAP-versies hebt geselecteerd omdat het oorspronkelijke WAP deze optie niet ondersteunt.

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)

Stap 5. (Optioneel) Schakel het aankruisvakje voor **global RADIUS-serverinstellingen gebruiken** uit om de instellingen te bewerken.

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)

Stap 6. (Optioneel) Klik op de radioknop voor het juiste **IP-adrestype voor de server**.

Opmerking: Bij dit voorbeeld wordt IPv4 geselecteerd.

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)

Stap 7. Voer het IP-adres van de RADIUS-server in het veld *IP-adres van de server*.

Opmerking: Voor dit voorbeeld wordt 192.168.1.101 gebruikt.

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)

Stap 8. Voer in het veld *Key* in de wachtwoordtoets die overeenkomt met uw RADIUS-server die de WAP gebruikt om de RADIUS-server te authenticeren. U kunt gebruikmaken van 1 tot 64 standaard alfanumerieke en speciale tekens.

Opmerking: De toetsen zijn hoofdlettergevoelig en moeten overeenkomen met de toetsen die op de RADIUS-server zijn ingesteld.

Stap 9. (Optioneel) Herhaal stappen 7-8 voor elke RADIUS-server in uw netwerk waarmee u de WAP wilt communiceren.

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)

Stap 10. (Optioneel) Controleer het aankruisvakje **EnableRADIUS-accounting** om het volgen en meten van de bronnen die een gebruiker heeft verbruikt mogelijk te maken (systeemtijd, de hoeveelheid verzonden gegevens). Door deze functie in te schakelen, kan RADIUS-accounting voor zowel de primaire als de reserveservers mogelijk maken.

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)

Stap 1. Klik op .

U hebt nu een WAP/WAP2 Enterprise-beveiliging ingesteld op uw WAP.