

Draadloze beveiligingsinstellingen configureren op WAP125 en WAP581

Doel

Draadloze beveiliging biedt u de mogelijkheid het draadloze netwerk te beschermen tegen toegang door onbevoegden. WAP125 en WAP 581 access points ondersteunen Static Wired Equivalent Protection (EFG), Wi-Fi Protected Access (WAP) Persoonlijk en WAP Enterprise. Deze instellingen kunnen worden ingesteld per Virtual Access Point (VAP). Wanneer u deze instellingen op hun plaats zet, levert dit netwerkbeveiliging per VAP op. Het wordt typisch gevormd wanneer het toegangspunt eerst wordt opgesteld, of wanneer updates aan de draadloze veiligheidsinstellingen van het netwerk worden gemaakt.

Dit artikel heeft als doel u te tonen hoe u draadloze beveiliging op een WAP125- of WAP581-access point kunt configureren.

Toepasselijke apparaten

- WAP125
- WAP581

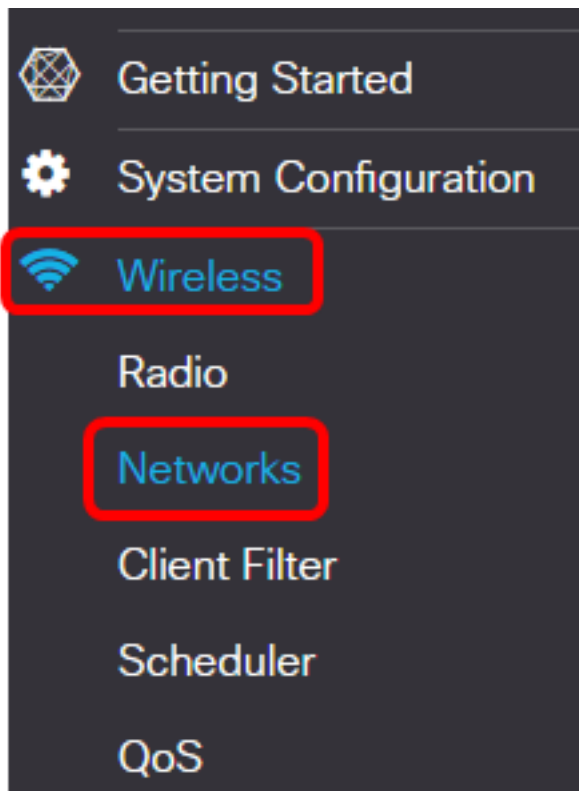
Softwareversie

- WAP125 - 1.0.0.3
- WAP581 - 1.0.0.4

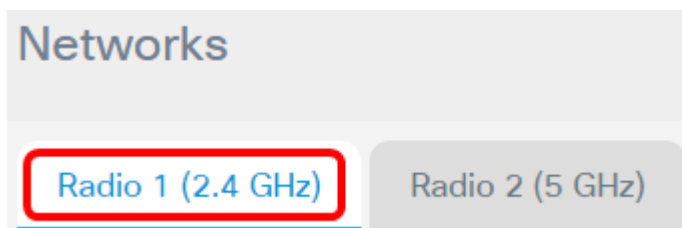
Draadloze beveiligingsinstellingen configureren

Persoonlijke beveiliging instellen

Stap 1. Meld u aan bij het webgebaseerde hulpprogramma van WAP en kies **Draadloos > netwerken**.

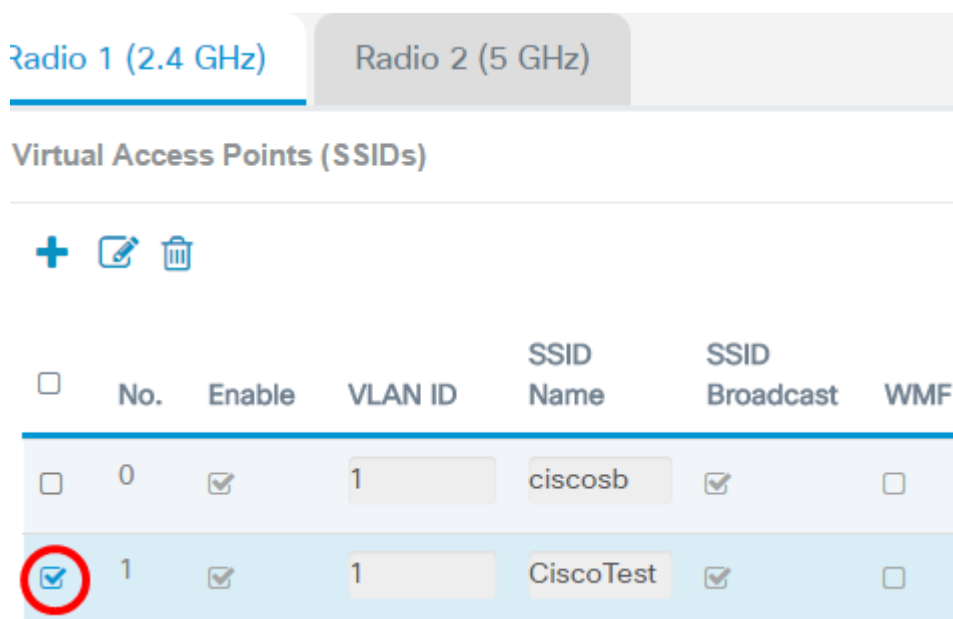


Stap 2. Kies de radio waarvan de draadloze beveiligingsinstellingen moeten worden geconfigureerd.




Opmerking: In dit voorbeeld wordt Radio 1 (2,4 GHz) gekozen.

Stap 3. Controleer het aankruisvakje voor de VAP waarvan de draadloze beveiligingsinstellingen moeten worden geconfigureerd.



Opmerking: In dit voorbeeld wordt VAP 1 gekozen.

Stap 3. Klik op **Bewerken**.

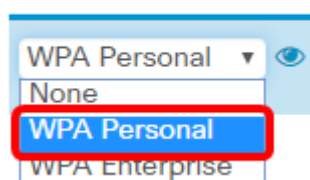



<input type="checkbox"/>	No.	Enable	VLAN ID	SSID Name	SSID Broadcast	WMF
<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	1	ciscosb	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	1	CiscoTest	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Stap 5. Kies een beveiligingsmodus in de vervolgkeuzelijst Beveiliging. De opties zijn:

- **Geen** — Met deze optie worden de draadloze beveiligingsinstellingen van de geselecteerde VAP gedeactiveerd. De veiligheidsmodus uitschakelen opent het draadloze netwerk en maakt iedereen met een draadloos apparaat in staat om verbinding te maken met uw netwerk en de bronnen ervan. Hoewel deze modus niet wordt aanbevolen, kan deze handig zijn voor netwerken op afgelegen locaties.
- **Persoonlijk WAP** - Deze optie implementeert WAP-beveiliging op het draadloze netwerk. Hiermee kunt u de TKIP-algoritmen (Temporal Key Integrity Protocol) of de Advanced Encryption Standard (AES) gebruiken. Als het wordt gemengd, zal het apparaten die het AES algoritme niet steunen in staat stellen om aan het netwerk te verbinden. Met behulp van een wachtwoord dat alfanumeriek is, kunt u maximaal 64 tekens lang gebruiken. Persoonlijk van WAP wordt gewoonlijk gebruikt in kantoren waar een RADIUS-server (Dial-In User Service) op afstand niet wordt gebruikt.
- **WAP Enterprise** — Met deze optie kunt u de beveiligingsfuncties combineren die worden aangeboden door WAP, terwijl u ook een RADIUS-server gebruikt. Dit wordt doorgaans gebruikt in omgevingen waar een RADIUS-server wordt gebruikt. Als u deze optie kiest, klikt u [hier](#).

Security



WPA Personal ▼ 

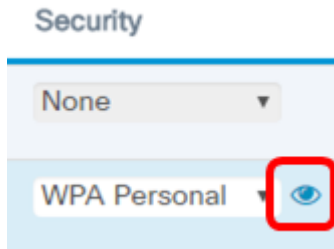
None

WPA Personal

WPA Enterprise

Opmerking: In dit voorbeeld, wordt de Persoonlijke van WAP gekozen.

Stap 6. Klik op de knop Bekijken om de persoonlijke parameters van WAP te configureren.



Stap 7. Kies uw WAP-versie in het gebied WAP-versies. De opties zijn:

- WAP-TKIP — Deze optie implementeert gemengde beveiliging op het draadloze netwerk. Het is ideaal voor netwerken met gemengde draadloze klanten. Deze optie is standaard uitgeschakeld.
- WAP2-AES - Deze optie implementeert WAP2-AES beveiliging op het netwerk. Dit is ideaal voor draadloze netwerken met klanten die de veiligheid van WAP2 ondersteunen.

Security Setting

WPA Versions: WPA-TKIP WPA2-AES

Key:

Show Key as Clear Text

Key Strength Meter: Below Minimum


Broadcast Key Refresh Rate

Opmerking: In dit voorbeeld is WAP-TKIP ingeschakeld.


Stap 8. Voer het netwerkwachtwoord in het veld *Key*. De toets kan een combinatie zijn van letters en cijfers, van 8 tot 63 tekens lang.


Security Setting

WPA Versions: WPA-TKIP WPA2-AES

Key: 

Show Key as Clear Text

Key Strength Meter:  Below Minimum


Broadcast Key Refresh Rate 

Opmerking: In dit voorbeeld wordt Cisco!@#\$\$%^&*() ingevoerd.


Stap 9. (Optioneel) Controleer de **sleutel tonen als** het vakje **Tekst wissen** om de toets in onbewerkte tekst te bekijken.


Security Setting

WPA Versions: WPA-TKIP WPA2-AES

Key: 

Show Key as Clear Text

Key Strength Meter:  Below Minimum

Broadcast Key Refresh Rate 

Opmerking: In dit voorbeeld, toon sleutel als de Duidelijke Tekst wordt gecontroleerd.

Stap 10. Voer het aantal seconden in totdat uw beveiligingstoets wordt vervangen door een nieuwe gegenereerd toets in het veld *Broadcast Key Refresh Rate*. De standaardwaarde is 86400.

Security Setting

WPA Versions:

WPA-TKIP

WPA2-AES

Key: [?](#)

Cisco!@#\$\$%^&*()

Show Key as Clear Text

Key Strength Meter:



Below Minimum

Broadcast Key Refresh Rate [?](#)

86400

OK

cancel

Stap 1. Klik op OK.

Security Setting

WPA Versions:

WPA-TKIP

WPA2-AES

Key: [?](#)

Cisco!@#\$\$%^&*()

Show Key as Clear Text

Key Strength Meter:



Below Minimum

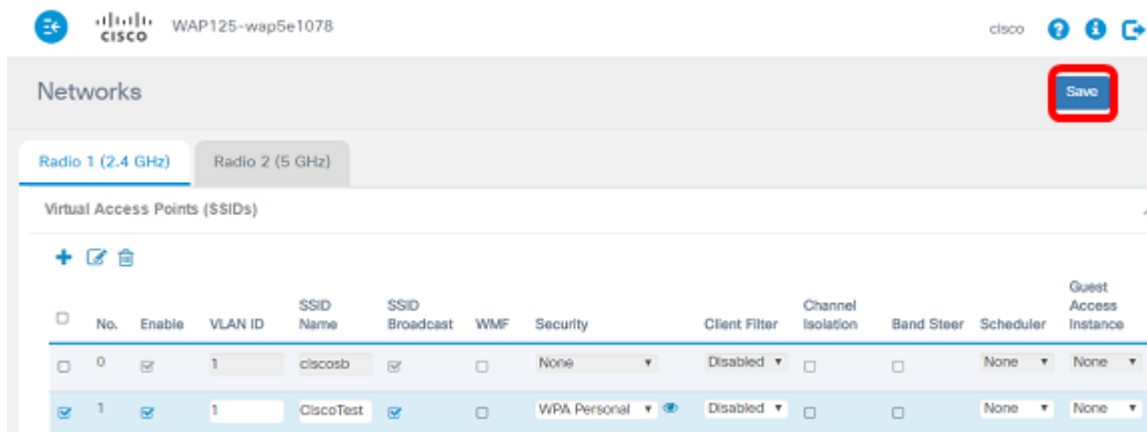
Broadcast Key Refresh Rate [?](#)

86400

OK

cancel

Stap 12. Klik op Opslaan.

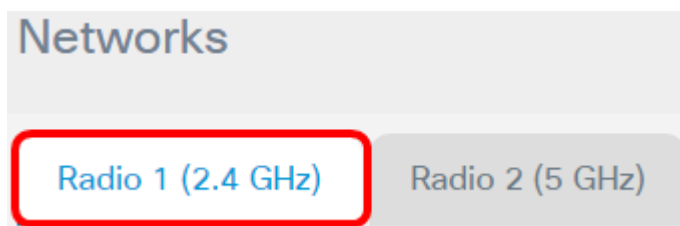


Stap 13. Klik op **OK**.

De Persoonlijke draadloze beveiligingsinstellingen van WAP zijn nu op uw WAP125 geconfigureerd.

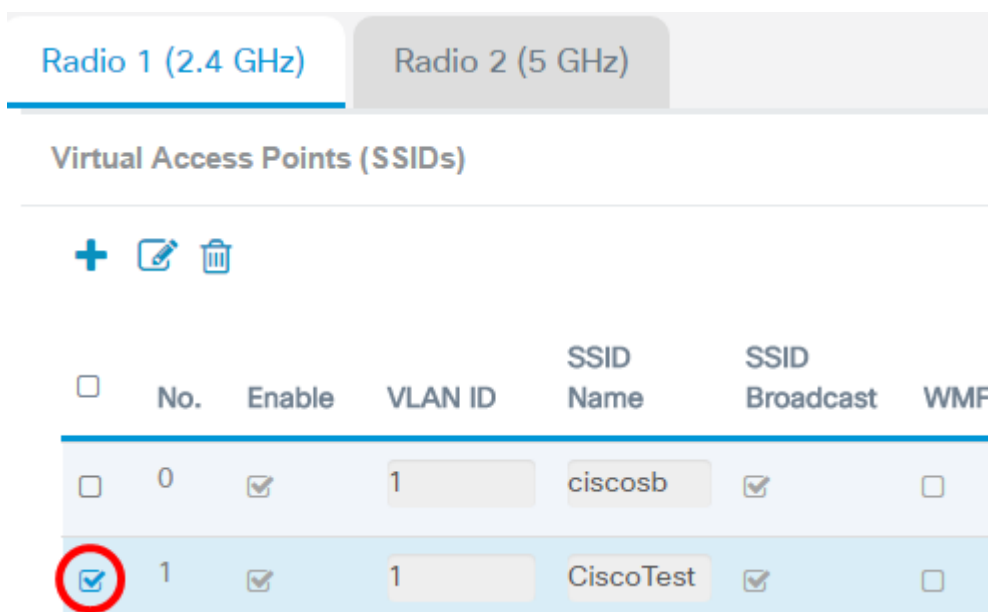
WAP Enterprise-beveiliging configureren

Stap 1. Kies de radio waarvan de draadloze beveiligingsinstellingen moeten worden geconfigureerd.



Opmerking: In dit voorbeeld wordt Radio 1 (2,4 GHz) gekozen.

Stap 2. Controleer het aankruisvakje voor de VAP waarvan de draadloze beveiligingsinstellingen moeten worden geconfigureerd.



Opmerking: In dit voorbeeld wordt VAP 1 gekozen.

Stap 3. Klik op **Bewerken**.

Radio 1 (2.4 GHz)

Radio 2 (5 GHz)

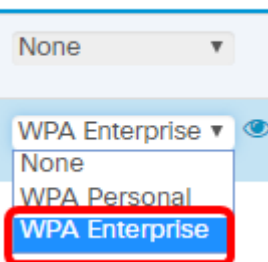
Virtual Access Points (SSIDs)



<input type="checkbox"/>	No.	Enable	VLAN ID	SSID Name	SSID Broadcast	WMF
<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	1	ciscosb	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	1	CiscoTest	<input checked="" type="checkbox"/>	<input type="checkbox"/>

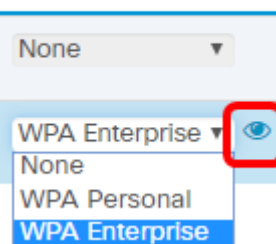
Stap 4. Kies WAP Enterprise uit de vervolgkeuzelijst Beveiliging.

Security



[Stap 5.](#) Klik op de knop om de parameters voor WAP-ondernemingen te configureren.

Security



Stap 6. Kies uw WAP-versie in het gebied WAP-versies. De opties zijn:

- WAP-TKIP — Deze optie implementeert gemengde beveiliging op het draadloze netwerk. Het is ideaal voor netwerken met gemengde draadloze klanten. Deze optie is standaard uitgeschakeld.
- WAP2-AES - Deze optie implementeert WAP2-AES beveiliging op het netwerk. Dit is ideaal voor draadloze netwerken met klanten die de veiligheid van WAP2 ondersteunen.

Security Setting



Opmerking: In dit voorbeeld is WAP-TKIP ingeschakeld.

Stap 7. (Optioneel) Controleer het selectieknop **voor** verificatie **inschakelen** om de functie te activeren. Bij controle wordt de informatie over de voorverificatie via de WAP doorgegeven dat de draadloze client momenteel is verbonden met de doelWAP. Deze optie kan de authenticatie van roamende klanten die verbinding maken met meerdere access points versnellen. Wanneer de beveiligingsmodus is uitgeschakeld, wordt deze optie ook uitgeschakeld en kan deze niet worden bewerkt.

Security Setting



Stap 8. (Optioneel) Schakel het aanvinkvakje Use global RADIUS-serverinstellingen uit om een andere set RADIUS-servers te kunnen specificeren. Standaard gebruikt elke VAP de algemene RADIUS-instellingen die voor de WAP zijn gedefinieerd.

Security Setting

WPA Versions:

WPA-TKIP

WPA2-AES

Enable pre-authentication

Use global RADIUS server settings


Server IP Address Type:

IPv4 IPv6


Server IP Address-1: 

192.168.1.1

Server IP Address-2: 

Key-1: 

.....

Key-2: 

Enable RADIUS Accounting

Active Server:

Server IP Address-1 

Broadcast Key Refresh Rate: 

86400

Session Key Refresh Rate: 

0

OK

cancel

Opmerking: In dit voorbeeld worden de instellingen van de server van de Gebruik globale RADIUS niet gecontroleerd. Als dit is ingeschakeld, gaat u naar [Stap 17](#).

Stap 9. (optioneel) Kies een IP-adrestype van de server. De opties zijn:

- IPv4 — Met deze optie kan WAP contact opnemen met de IPv4 RADIUS-server.
- IPv6 — Met deze optie kan WAP contact opnemen met de IPv6-RADIUS-server.

Security Setting

WPA Versions: WPA-TKIP WPA2-AES

Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1:

Server IP Address-2:

Key-1:

Key-2:

Enable RADIUS Accounting

Active Server:

Broadcast Key Refresh Rate:

Session Key Refresh Rate:

OK

cancel

Opmerking: In dit voorbeeld wordt IPv4 geselecteerd.

Stap 10. (Optioneel) Voer het IP-adres van de primaire RADIUS-server voor de VAP in het veld *IP-adres -1 van de server* in.

Server IP Address Type: IPv4 IPv6

Server IP Address-1:

Server IP Address-2:

Key-1:

Key-2:

Opmerking: In dit voorbeeld wordt 192.168.1.1 ingevoerd.

Stap 1. (Optioneel) Voer het IP-adres van de RADIUS-server voor de VAP in het veld *IP-adres -2 van de server*.

Server IP Address Type: IPv4 IPv6

Server IP Address-1:

Server IP Address-2:

Key-1:

Key-2:

Opmerking: In dit voorbeeld wordt geen IP-adres voor de back-up ingevoerd.

Stap 12. (Optioneel) Voer een wachtwoord in voor het primaire serveradres in het veld *Key-1*

Server IP Address Type: IPv4 IPv6

Server IP Address-1:

Server IP Address-2:

Key-1:

Key-2:

Stap 13. (Optioneel) Voer een wachtwoord in voor het adres van de reserveserver in het veld *Key-2*.

Server IP Address Type: IPv4 IPv6

Server IP Address-1:

Server IP Address-2:

Key-1:

Key-2:

Opmerking: In dit voorbeeld wordt geen wachtwoord ingevoerd.

Stap 14. (Optioneel) Controleer het vakje **RADIUS-accounting** inschakelen. Deze optie volgt en meet de middelen die een bepaalde gebruiker heeft gebruikt, zoals de tijd en de hoeveelheid gegevens die hij heeft verzonden en ontvangen. Indien ingeschakeld, zal deze worden ingeschakeld voor de primaire en reserveservers.

Enable RADIUS Accounting

Active Server:

Broadcast Key Refresh Rate:

Session Key Refresh Rate:

Opmerking: In dit voorbeeld wordt de optie RADIUS-accounting inschakelen ingeschakeld.

Stap 15. (Optioneel) Kies een actieve server uit de vervolgkeuzelijst Actieve server.

Server IP Address Type: IPv4 IPv6

Server IP Address-1:

Server IP Address-2:

Key-1:

Key-2:

Enable RADIUS Accounting

Active Server:

Broadcast Key Refresh Rate:

Session Key Refresh Rate:

Opmerking: In dit voorbeeld wordt IP-adres-1 voor de server geselecteerd.

Stap 16. (Optioneel) Voer het aantal seconden in totdat de beveiligingstoets wordt vervangen door een nieuwe toets in het veld *Broadcast Key Refresh Rate*. De standaardwaarde is 86400.

Active Server:

Broadcast Key Refresh Rate:

Session Key Refresh Rate:

Opmerking: In dit voorbeeld wordt de Broadcast Key Refresh Rate achtergelaten op de standaardwaarde.

[Stap 17](#). Voer het interval in waarmee de WAP sessiesleutels voor elke client die aan de VAP is gekoppeld, verfrist. Het kan van 30 tot 86400 seconden zijn.

Active Server:

Broadcast Key Refresh Rate:

Session Key Refresh Rate:

Stap 18. Klik op **OK**.

Active Server:

Broadcast Key Refresh Rate:

Session Key Refresh Rate:

Stap 19. Klik op **Opslaan**.

WAP125-wap5e1078

Networks Save

Radio 1 (2.4 GHz) Radio 2 (5 GHz)

Virtual Access Points (SSIDs)

No.	Enable	VLAN ID	SSID Name	SSID Broadcast	WMF	Security	Client Filter	Channel Isolation	Band Steer	Scheduler	Guest Access Instance
0	<input type="checkbox"/>	1	ciscosb	<input type="checkbox"/>	<input type="checkbox"/>	None	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	None	None
1	<input checked="" type="checkbox"/>	1	CiscoTest	<input checked="" type="checkbox"/>	<input type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	None	None

U hebt nu de beveiliging van de WAP Enterprise op uw draadloos netwerk ingesteld.

Bekijk een video gerelateerd aan dit artikel...

[Klik hier om andere Tech Talks uit Cisco te bekijken](#)