

Instellingen 802.1X instellen op WAP351

Doel

Dankzij de IEEE 802.1X-verificatie kan het WAP-apparaat toegang krijgen tot een beveiligd bekabeld netwerk. U kunt het WAP-apparaat configureren als een 802.1X smeebede (client) op het bekabelde netwerk. WAP351 kan ook als authenticator worden geconfigureerd. Een versleutelde naam en wachtwoord kunnen worden ingesteld zodat het WAP-apparaat kan worden geauthenticeerd met 802.1X.

Op de netwerken die IEEE 802.1X poortgebaseerde netwerktoegangscontrole gebruiken, kan een aanvrager geen toegang tot het netwerk verkrijgen tot de 802.1X-authenticator toegang verleent. Als uw netwerk 802.1X gebruikt, moet u 802.1X authenticatie informatie op het WAP apparaat configureren zodat het aan de authenticator kan leveren.

Het doel van dit document is om u te tonen hoe u 802.1X uitgebreide instellingen op WAP351 moet configureren.

Toepasselijke apparaten

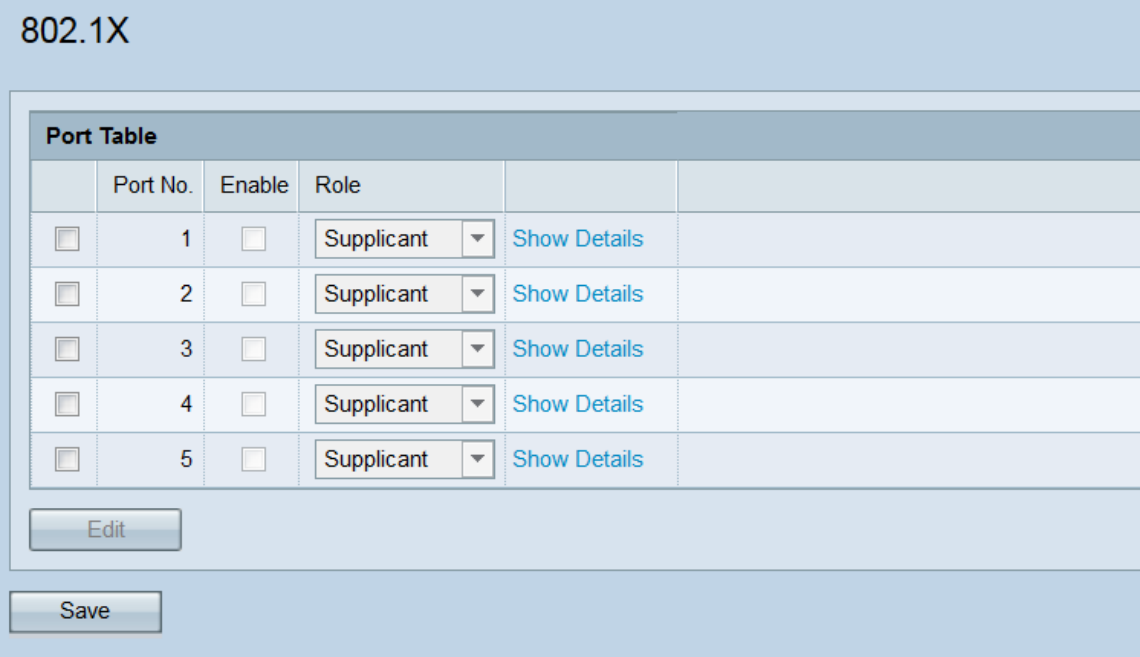
- WAP351

Softwareversie

- v1.0.1.3

Aangepaste 802.1X-instellingen configureren

Stap 1. Meld u aan bij het web configuratieprogramma en kies **Systeembeveiliging > 802.1X**. De pagina *802.1X* wordt geopend.



802.1X

Port Table					
	Port No.	Enable	Role		
<input type="checkbox"/>	1	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	2	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	3	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	4	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	5	<input type="checkbox"/>	Supplicant	Show Details	

Edit

Save

Stap 2. De *poorttabel* toont vijf LAN-interfaces die kunnen worden geconfigureerd voor

802.1X-verificatie. Controleer het/de aanvinkvakje(s) dat/de poorten die u wilt bewerken.

802.1X

Port Table					
	Port No.	Enable	Role		
<input checked="" type="checkbox"/>	1	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	2	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	3	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	4	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	5	<input type="checkbox"/>	Supplicant	Show Details	

Edit

Save

Stap 3. Klik op de knop **Bewerken**. De gecontroleerde poort(en) is nu beschikbaar voor het bewerken.

802.1X

Port Table					
	Port No.	Enable	Role		
<input checked="" type="checkbox"/>	1	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	2	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	3	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	4	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	5	<input type="checkbox"/>	Supplicant	Show Details	

Edit

Save

Stap 4. Controleer in het veld *Inschakelen* het/de aankruisvakje(s) van de poort(s) waarop u 802.1X-instellingen wilt inschakelen.

802.1X

Port Table					
	Port No.	Enable	Role		
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	2	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	3	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	4	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	5	<input type="checkbox"/>	Supplicant	Show Details	

Edit

Save

Stap 5. In de vervolgkeuzelijst *RoI* selecteert u of de corresponderende poort is ingesteld als een **smeekbede** of een **verificator**. Als u Aanvoerder hebt gekozen, gaat u naar het gedeelte [Instellingen Aanvraagt](#). Als u Authenticator kiest, gaat u naar het gedeelte [Verificator Instellingen](#) configuratie. Een verificator ligt in tussen de client (Leverancier) die toegang tot het netwerk en de RADIUS-server zelf wenst te verkrijgen. Het is verantwoordelijk voor de afhandeling van alle communicatie tussen de twee. Een Leverancier verstrekt geloofsbrieven aan een Verificator om toegang tot het netwerk te krijgen. Een typische instelling op WAP351 zou de WAN-poort als Leverancier hebben (zodat WAP toegang heeft tot het netwerk) en de LAN-poorten als Verificators hebben (dus kan WAP apparaten eronder autoriseren).

Port Table					
	Port No.	Enable	Role		
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	Supplicant ▼	Show Details	
<input type="checkbox"/>	2	<input type="checkbox"/>	Supplicant Authenticator	Show Details	
<input type="checkbox"/>	3	<input type="checkbox"/>	Supplicant ▼	Show Details	
<input type="checkbox"/>	4	<input type="checkbox"/>	Supplicant ▼	Show Details	
<input type="checkbox"/>	5	<input type="checkbox"/>	Supplicant ▼	Show Details	

Configuratie van leveranciers

Stap 1. Klik op **Show Details** om de informatie over de flexibele instellingen weer te geven.

Port Table					
	Port No.	Enable	Role		
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	Supplicant ▼	Hidden Details	
<p>EAP Method: <input type="text" value="MD5"/> ▼</p> <p>Username: <input type="text"/> (Range: 1 - 64 Characters)</p> <p>Password: <input type="text"/> (Range: 1 - 64 Characters)</p> <hr/> <p>Certificate File Status <input type="button" value="Refresh"/></p> <p>Certificate File Present: No</p> <p>Certificate Expiration Date: Not Present</p> <hr/> <p>Browse to the location where your certificate file is stored and click the "Upload" button. To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.</p> <p>Certificate File Upload</p> <p>Transfer Method: <input checked="" type="radio"/> HTTP <input type="radio"/> TFTP</p> <p>Filename <input type="button" value="Browse..."/> No file selected.</p> <p><input type="button" value="Upload"/></p>					
<input type="checkbox"/>	2	<input type="checkbox"/>	Supplicant ▼	Show Details	

Opmerking: Deze informatie kan automatisch worden geopend nadat u in het veld *Modus*

een selectie hebt gemaakt.

Stap 2. Kies in de vervolgkeuzelijst *EAP-methode* het algoritme dat zal worden gebruikt om gebruikersnamen en wachtwoorden te versleutelen. EAP staat voor Extensible Authentication Protocol, en wordt gebruikt als basis voor encryptie-algoritmen.

EAP Method: MD5 (selected)
MD5
PEAP
TLS

Username: (Range: 1 - 64 Characters)

Password: (Range: 1 - 64 Characters)

Certificate File Status Refresh

Certificate File Present: No

Certificate Expiration Date: Not Present

Browse to the location where your certificate file is stored and click the "Upload" button.
To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.

Certificate File Upload

Transfer Method: HTTP TFTP

Filename: Browse... No file selected.

Upload

De beschikbare opties zijn:

- MD5 — Het MD5 bericht-digest-algoritme gebruikt een hashfunctie om basisbeveiliging te bieden. Dit algoritme wordt niet aanbevolen, omdat de andere twee een hogere veiligheid hebben.
- PEAP — PEAP staat voor Protected Extensible Verification Protocol. Het kapselt EAP in en biedt meer veiligheid dan MD5 door gebruik te maken van een TLS-tunnel om gegevens te verzenden.
- TLS — TLS staat voor Transport Layer Security en is een open standaard die hoge beveiliging biedt.

Stap 3. In het veld *Gebruikersnaam* voert u de gebruikersnaam in die het WAP-apparaat gebruikt bij het beantwoorden van verzoeken van een 802.1X-authenticator. De gebruikersnaam moet 1 - 64 tekens lang zijn, en kan alfanumerieke en speciale tekens bevatten.

EAP Method: MD5 ▼

Username: (Range: 1 - 64 Characters)

Password: (Range: 1 - 64 Characters)

Certificate File Status

Certificate File Present: No

Certificate Expiration Date: Not Present

Browse to the location where your certificate file is stored and click the "Upload" button.
To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.

Certificate File Upload

Transfer Method: HTTP
 TFTP

Filename No file selected.

Stap 4. Voer in het veld *Wachtwoord* in het wachtwoord dat het WAP-apparaat gebruikt bij het beantwoorden van verzoeken van een 802.1X-authenticator. De gebruikersnaam moet 1 - 64 tekens lang zijn, en kan alfanumerieke en speciale tekens bevatten.

EAP Method: MD5 ▾

Username: username1 (Range: 1 - 64 Characters)

Password: ●●●●●●●● (Range: 1 - 64 Characters)

Certificate File Status Refresh

Certificate File Present: No

Certificate Expiration Date: Not Present

Browse to the location where your certificate file is stored and click the "Upload" button.
To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.

Certificate File Upload

Transfer Method: HTTP
 TFTP

Filename Browse... No file selected.

Upload

Stap 5. Het gebied met de *status van het certificaatbestand* toont aan of er een HTTP SSL-certificaatbestand op het WAP-apparaat bestaat. Het veld *certificaatbestand bevat* "Ja" als er een certificaat is; de standaardinstelling is "Nee". Indien er een certificaat aanwezig is, zal de *vervaldatum van het certificaat* aangeven wanneer deze verstrijkt; anders is de standaardinstelling "Niet aanwezig". Als u de laatste informatie wilt weergeven, klikt u op de knop **Vernieuwen** om de meest recente certificaatinformatie te ontvangen.

EAP Method: MD5 ▼

Username: username1 (Range: 1 - 64 Characters)

Password: ●●●●●●●● (Range: 1 - 64 Characters)

Certificate File Status Refresh

Certificate File Present: No

Certificate Expiration Date: Not Present

Browse to the location where your certificate file is stored and click the "Upload" button.
To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.

Certificate File Upload

Transfer Method: HTTP
 TFTP

Filename No file selected.

Stap 6. Als u geen HTTP-SSL-certificeringsbestand wilt uploaden, slaat u de [Stap 12](#) over. Anders selecteert u de **HTTP**- of **TFTP**-radioknoppen in het veld *Transfer Methode* om te kiezen welk protocol u wilt gebruiken om het certificaat te uploaden.

EAP Method: MD5 ▼

Username: username1 (Range: 1 - 64 Characters)

Password: ●●●●●●●● (Range: 1 - 64 Characters)

Certificate File Status Refresh

Certificate File Present: No

Certificate Expiration Date: Not Present

Browse to the location where your certificate file is stored and click the "Upload" button.
To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.

Certificate File Upload

Transfer Method: HTTP TFTP

Filename Browse... No file selected.

Upload

Stap 7. Als u **TFTP** hebt geselecteerd, ga verder met Stap 8. Als u **HTTP** hebt geselecteerd, klikt u op de knop Bladeren... om het certificaatbestand op uw PC te vinden. Naar [Stap 10](#).

EAP Method: MD5 ▼

Username: username1 (Range: 1 - 64 Characters)

Password: ●●●●●●●● (Range: 1 - 64 Characters)

Certificate File Status Refresh

Certificate File Present: No

Certificate Expiration Date: Not Present

Browse to the location where your certificate file is stored and click the "Upload" button.
To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.

Certificate File Upload

Transfer Method: HTTP
 TFTP

Filename No file selected.

Upload

Stap 8. Als u **TFTP** hebt geselecteerd in het veld *Overdrachtmethode*, typt u de bestandsnaam van het certificaat in het veld *Bestandsnaam*.

EAP Method: (Range: 1 - 64 Characters)

Username: (Range: 1 - 64 Characters)

Password: (Range: 1 - 64 Characters)

Certificate File Status

Certificate File Present: No

Certificate Expiration Date: Not Present

Browse to the location where your certificate file is stored and click the "Upload" button.
To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.

Certificate File Upload

Transfer Method: HTTP TFTP

Filename: (Range: 1 - 256 Characters)

TFTP Server IPv4 Address: (xxx.xxx.xxx.xxx)

Opmerking: Het bestand moet eindigen op .pem.

Stap 9. Voer het IP-adres van de TFTP-server in het veld *IPv4-adres van de TFTP-server*.

EAP Method: MD5 ▼

Username: username1 (Range: 1 - 64 Characters)

Password: ●●●●●●●● (Range: 1 - 64 Characters)

Certificate File Status Refresh

Certificate File Present: No

Certificate Expiration Date: Not Present

Browse to the location where your certificate file is stored and click the "Upload" button.
To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.

Certificate File Upload

Transfer Method: HTTP TFTP

Filename: certificate.pem (Range: 1 - 256 Characters)

TFTP Server IPv4 Address: 192.0.2.100 (xxx.xxx.xxx.xxx)

Upload

[Step 10](#). Klik op Upload.

EAP Method: MD5 ▼

Username: username1 (Range: 1 - 64 Characters)

Password: ●●●●●●●● (Range: 1 - 64 Characters)

Certificate File Status Refresh

Certificate File Present: No

Certificate Expiration Date: Not Present

Browse to the location where your certificate file is stored and click the "Upload" button.
To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.

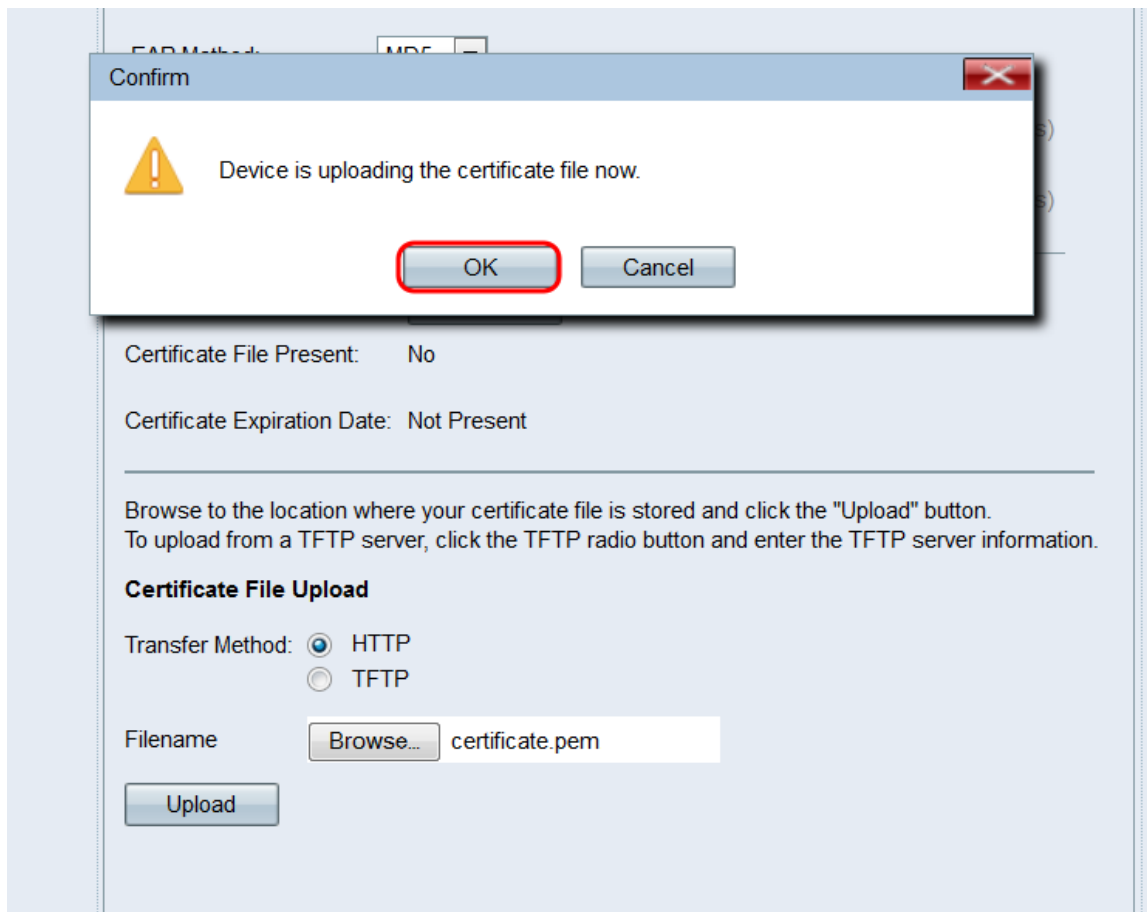
Certificate File Upload

Transfer Method: HTTP
 TFTP

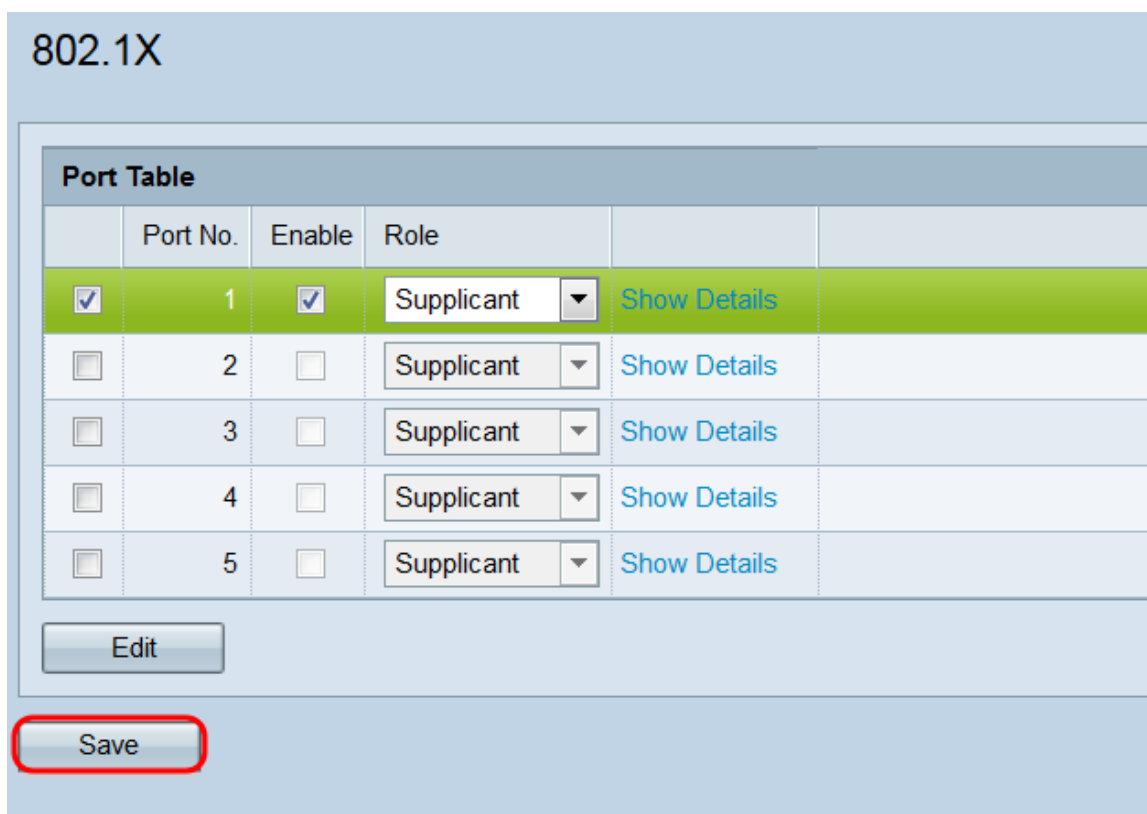
Filename Browse... certificate.pem

Upload

Stap 11. Er verschijnt een bevestigingsvenster. Klik op **OK** om te beginnen met het uploaden.



[Stap 12](#). Herhaal deze sectie voor elke poort die u wilt configureren als een 802.1X smeekbede. Klik vervolgens op **Opslaan**.



[Configuratie van verificatieinstellingen](#)

Stap 1. Klik op **Details** om de informatie over de vericatorinstellingen weer te geven.

Port Table																							
Port No.	Enable	Role																					
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Authenticator	Hidden Details																				
<input checked="" type="checkbox"/> Use global RADIUS server settings Server IP Address Type: <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6 <table border="1"> <thead> <tr> <th>No.</th> <th>Server IP Address (xxx.xxx.xxx.xxx)</th> <th>Key (Range: 1 - 64 Characters)</th> <th>Authentication Port (Range: 0 - 65535, Default: 1812)</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>0.0.0.0</td> <td></td> <td>1812</td> </tr> <tr> <td>2</td> <td></td> <td></td> <td>1812</td> </tr> <tr> <td>3</td> <td></td> <td></td> <td>1812</td> </tr> <tr> <td>4</td> <td></td> <td></td> <td>1812</td> </tr> </tbody> </table> <input type="checkbox"/> Enable RADIUS Accounting Active Server: Server IP Address-1 Periodic Reauthentication: <input type="checkbox"/> Enable Reauthentication Period: 3600 sec. (Range: 300 - 4294967295, Default: 3600)				No.	Server IP Address (xxx.xxx.xxx.xxx)	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)	1	0.0.0.0		1812	2			1812	3			1812	4			1812
No.	Server IP Address (xxx.xxx.xxx.xxx)	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)																				
1	0.0.0.0		1812																				
2			1812																				
3			1812																				
4			1812																				
<input type="checkbox"/>	<input type="checkbox"/>	Supplicant	Show Details																				

Opmerking: Deze informatie kan automatisch worden geopend nadat u in het veld *Modus* een selectie hebt gemaakt.

Stap 2. Controleer het selectieteken voor de *globale RADIUS-serverinstellingen gebruiken* als u wilt dat de poort de globale RADIUS-instellingen tijdens verificatie gebruikt. Als u wilt dat de poort een andere RADIUS-server (of servers) gebruikt, dient u dit selectieteken uit te schakelen. in het overige geval, overslaan naar [Stap 8](#).

<input checked="" type="checkbox"/> Use global RADIUS server settings Server IP Address Type: <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6 <table border="1"> <thead> <tr> <th>No.</th> <th>Server IP Address (xxx.xxx.xxx.xxx)</th> <th>Key (Range: 1 - 64 Characters)</th> <th>Authentication Port (Range: 0 - 65535, Default: 1812)</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>0.0.0.0</td> <td></td> <td>1812</td> </tr> <tr> <td>2</td> <td></td> <td></td> <td>1812</td> </tr> <tr> <td>3</td> <td></td> <td></td> <td>1812</td> </tr> <tr> <td>4</td> <td></td> <td></td> <td>1812</td> </tr> </tbody> </table> <input type="checkbox"/> Enable RADIUS Accounting Active Server: Server IP Address-1 Periodic Reauthentication: <input type="checkbox"/> Enable Reauthentication Period: 3600 sec. (Range: 300 - 4294967295, Default: 3600)				No.	Server IP Address (xxx.xxx.xxx.xxx)	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)	1	0.0.0.0		1812	2			1812	3			1812	4			1812
No.	Server IP Address (xxx.xxx.xxx.xxx)	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)																				
1	0.0.0.0		1812																				
2			1812																				
3			1812																				
4			1812																				

Opmerking: Zie het artikel [Instellingen voor Global RADIUS-server configureren op WAP131](#)

[en WAP351.](#)

Stap 3. Selecteer in het veld *IP-adrestype voor de server* de radioknop voor de IP-versie die de RADIUS-server gebruikt. De beschikbare opties zijn **IPv4** en **IPv6**.

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

No.	Server IP Address (xxx.xxx.xxx.xxx)	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)
1	0.0.0.0		1812
2			1812
3			1812
4			1812

Enable RADIUS Accounting

Active Server: Server IP Address-1 ▼

Periodic Reauthentication: Enable

Reauthentication Period: 3600 sec. (Range: 300 - 4294967295, Default: 3600)

Opmerking: U kunt tussen de adrestypes schakelen om IPv4- en IPv6-RADIUS-adresinstellingen te configureren, maar het WAP-apparaat neemt alleen contact op met de RADIUS-server of servers met het adrestype dat u in dit veld selecteert. Het is niet mogelijk om meerdere servers verschillende adrestypes in één configuratie te hebben.

Stap 4. In het veld *IP-adres 1* of *IPv6-adres van de server* in het veld IPv4 of IPv6-adres voor de RADIUS-server, afhankelijk van het adrestype dat u in Stap 3 hebt gekozen.

Use global RADIUS server settings

Server IP Address Type: IPv4
 IPv6

No.	Server IP Address (xxx.xxx.xxx.xxx)	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)
1	192.0.2.1		1812
2			1812
3			1812
4			1812

Enable RADIUS Accounting

Active Server: ▼

Periodic Reauthentication: Enable

Reauthentication Period: sec. (Range: 300 - 4294967295, Default: 3600)

Opmerking: Het in dit veld ingevoerde adres wijst de primaire RADIUS-server van de poort aan. Adressen die zijn ingevoerd in de volgende velden (*IP-adres 2 tot en met 4*) wijzen de RADIUS-servers aan die in volgorde zullen worden geprobeerd als de verificatie niet met de primaire server verloopt.

Stap 5. In het veld *Key*, voert u de gedeelde geheime sleutel in die overeenkomt met de primaire RADIUS-server die het WAP-apparaat gebruikt om te authenticeren aan de RADIUS-server. U kunt gebruikmaken van 1 tot 64 standaard alfanumerieke en speciale tekens. Herhaal deze stap voor elke volgende RADIUS-server die u voor de poort in *Key 2* hebt ingesteld tot en met 4 velden.

Use global RADIUS server settings

Server IP Address Type: IPv4
 IPv6

No.	Server IP Address (xxx.xxx.xxx.xxx)	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)
1	192.0.2.1	••••••••	1812
2			1812
3			1812
4			1812

Enable RADIUS Accounting

Active Server: ▼

Periodic Reauthentication: Enable

Reauthentication Period: sec. (Range: 300 - 4294967295, Default: 3600)

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

Stap 6. In het veld *Verificatiepoort* voert u de poort in die de WAP gebruikt om verbinding te maken met de RADIUS-server. Herhaal deze stap voor elke RADIUS-server die u in de *verificatiepoort 2* hebt ingesteld tot en met 4 velden. De standaard is 1812.

Use global RADIUS server settings

Server IP Address Type: IPv4
 IPv6

No.	Server IP Address (xxx.xxx.xxx.xxx)	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)
1	192.0.2.1	••••••••	1812
2			1812
3			1812
4			1812

Enable RADIUS Accounting

Active Server: ▼

Periodic Reauthentication: Enable

Reauthentication Period: sec. (Range: 300 - 4294967295, Default: 3600)

Stap 7. Controleer het selectieteken **met RADIUS-accounting** inschakelen om het volgen en meten van de bronnen die een gebruiker heeft verbruikt mogelijk te maken (systeemtijd,

hoeveelheid verzonden gegevens, enz.). Door dit selectieteken te controleren, kan RADIUS-accounting voor de primaire en reserveservers mogelijk zijn.

Use global RADIUS server settings

Server IP Address Type: IPv4
 IPv6

No.	Server IP Address (xxx.xxx.xxx.xxx)	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)
1	192.0.2.1	1812
2	192.0.2.2	2500
3			1812
4			1812

Enable RADIUS Accounting

Active Server: Server IP Address-1 ▼

Periodic Reauthentication: Enable

Reauthentication Period: 3600 sec. (Range: 300 - 4294967295, Default: 3600)

Stap 8. Kies in de vervolgkeuzelijst *Actieve server* een van de geconfigureerde RADIUS-servers die moet worden ingesteld als de actieve server. Deze instelling laat WAP onmiddellijk proberen om de actieve server te contacteren, in plaats van elke server achter elkaar te contacteren en de eerste beschikbare te kiezen.

Use global RADIUS server settings

Server IP Address Type: IPv4
 IPv6

No.	Server IP Address (xxx.xxx.xxx.xxx)	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)
1	192.0.2.1	1812
2	192.0.2.2	2500
3			1812
4			1812

Enable RADIUS Accounting

Active Server: Server IP Address-1 ▼

Periodic Reauthentication: Enable

Reauthentication Period: 3600 sec. (Range: 300 - 4294967295, Default: 3600)

Stap 9. In het veld *Periodieke herverificatie* controleert u het selectieteken **Toegang** tot MAP **inschakelen** om de MAP-verificatie aan te zetten. Als u geen MAP opnieuw authenticatie wilt

toestaan, sla dan over naar [stap 11](#).

Use global RADIUS server settings

Server IP Address Type: IPv4
 IPv6

No.	Server IP Address (xxx.xxx.xxx.xxx)	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)
1	192.0.2.1	••••••••	1812
2	192.0.2.2	••••••••	2500
3			1812
4			1812

Enable RADIUS Accounting

Active Server: ▼

Periodic Reauthentication: **Enable**

Reauthentication Period: sec. (Range: 300 - 4294967295, Default: 3600)

Stap 10. Als u het selectieteken **Enable** in het veld *Periodieke* echtheidscontrole hebt ingeschakeld, dient u in het veld *Verificatieperiode* binnen de MAP - periode in enkele seconden *te* noteren. De standaard is 3600. Het geldige bereik is 300 - 4294967295 seconden.

Use global RADIUS server settings

Server IP Address Type: IPv4
 IPv6

No.	Server IP Address (xxx.xxx.xxx.xxx)	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)
1	192.0.2.1	••••••~	1812
2	192.0.2.2	••~	2500
3			1812
4			1812

Enable RADIUS Accounting

Active Server: ▼

Periodic Reauthentication: Enable

Reauthentication Period: sec. (Range: 300 - 4294967295, Default: 3600)

[Stap 11](#). Herhaal deze sectie voor elke poort die u wilt configureren als een 802.1X verifiator. Klik vervolgens op **Opslaan**.

802.1X

Port Table

	Port No.	Enable	Role	
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	Authenticator ▼	Show Details
<input type="checkbox"/>	2	<input type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	3	<input type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	4	<input type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	5	<input type="checkbox"/>	Supplicant ▼	Show Details

Edit

Save