

Aangepaste 802.1X instellingen voor een draadloos access point

Doel

De standaard 802.1X is ontwikkeld om beveiliging te bieden in Layer 2 van het OSI-model (Open System Interconnect). Het bestaat uit de volgende onderdelen: Leverancier, Authenticator en Verificatieserver. Een Leverancier is de client of software die op een netwerk aangesloten is zodat hij toegang heeft tot zijn bronnen. Het moet geloofsbrieven of certificaten verstrekken om een IP-adres te verkrijgen en deel uitmaken van dat specifieke netwerk. Een aanvrager kan geen toegang hebben tot de netwerkbronnen tot hij is geauthentificeerd.

Het configureren van 802.1X uitgebreide instellingen op uw Wireless Access Point (WAP) is handig om geautoriseerde apparaten achter uw WAP toe te staan om deel uit te maken van het netwerk en om toegang te hebben tot de bronnen. Tegelijkertijd voegt het ook een beveiligingslaag toe aan het netwerk.

Dit artikel toont u hoe u 802.1X uitgebreide instellingen op uw draadloos access point kunt configureren.

Toepasselijke apparaten

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

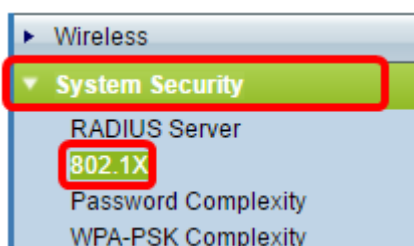
Softwareversie

- 1.0.1.2 - WAP150, WAP361
- 1.0.6.2 - WAP121, WAP321
- 1.0.2.2 - WAP131, WAP351
- 1.2.1.3 - WAP551, WAP561, WAP371
- 1.0.0.17 - WAP571, WAP571E

Aangepaste 802.1X instellingen configureren op een WAP

Stap 1. Meld u aan bij het webgebaseerde hulpprogramma van het access point en kies **stelsysteembeveiliging>802.1X**.

Opmerking: Het web-Based Nutsmenu kan variëren afhankelijk van het model van uw WAP. De onderstaande beelden zijn afkomstig van WAP361.



Opmerking: Als u andere modellen WAP gebruikt, kiest u **System Security > 802.1X Supplicant** en slaat u vervolgens over naar [Stap 3](#).

Stap 2. Controleer het vakje voor het poortnummer dat u wilt configureren en klik op **Bewerken**.

Port Table				
	Port No.	Enable	Role	
<input checked="" type="checkbox"/>	0	<input type="checkbox"/>	Supplicant ▼	Show Details
<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

Edit

Stap 3. Controleer het aanvinkvakje **Enable** en kies vervolgens **Leverancier** in de vervolgkeuzelijst. Dit is de standaardoptie.

Opmerking: Voor andere modellen WAP, controleer het aanvinkvakje **Enable** in voor de beheermodus en sla deze vervolgens over naar [Stap 5](#).

Port Table				
	Port No.	Enable	Role	
<input checked="" type="checkbox"/>	0	<input checked="" type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	1	<input type="checkbox"/>	Supplicant 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

Edit

Stap 4. Klik op de link **Details tonen** om u in staat te stellen de instellingen te bewerken.

Port Table				
	Port No.	Enable	Role	
<input checked="" type="checkbox"/>	0	<input checked="" type="checkbox"/>	Supplicant ▼	Show Details
<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

Edit

Stap 5. Kies het juiste type van de MAP-methode (Extensible Authentication Protocol) in de vervolgkeuzelijst EAP-methode.

EAP Method: (Range: 1 - 64 Characters)

Username: (Range: 1 - 64 Characters)

Password: (Range: 1 - 64 Characters)

De opties zijn:

- MD5 — MD5 is een algoritme dat wordt gebruikt om gegevens van elk formaat te versleutelen met 128 bit. Het MD5-algoritme gebruikt een openbaar cryptosysteem om gegevens te versleutelen.
- PEAP — Protected Extensible Authentication Protocol (PEAP) bevestigt draadloze LAN-clients (Local Area Network) via digitale certificaten die door de server worden uitgegeven door het maken van een versleutelde Secure Socket Layer (SSL) of Transport Layer Security (TLS)-tunnel tussen de client en de verificatieserver.
- TLS — TLS is een protocol dat beveiliging en gegevensintegriteit biedt voor communicatie via het internet. Deze zorgt ervoor dat er geen derden zijn die met het oorspronkelijke bericht knoeien.

Opmerking: In dit voorbeeld wordt MD5 gebruikt.

Stap 6. Voer uw favoriete gebruikersnaam in het veld *Gebruikersnaam* in. Dit wordt gebruikt bij het reageren op een 802.1X vericator. Het kan maximaal 64 tekens lang zijn, inclusief hoofdletters en kleine letters, getallen en speciale tekens, behalve dubbele aanhalingstekens.

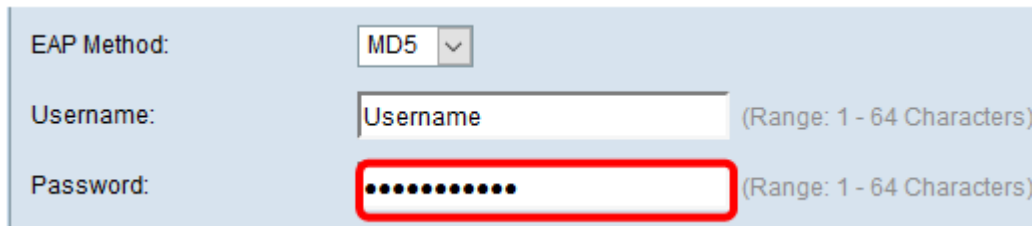
EAP Method:

Username: (Range: 1 - 64 Characters)

Password: (Range: 1 - 64 Characters)

Stap 7. Voer in het veld *Wachtwoord* uw gewenste wachtwoord in. Dit MD5 wachtwoord

wordt gebruikt bij het reageren op een 802.1X verificator. Het wachtwoord kan maximaal 64 tekens lang zijn, inclusief hoofdletters, kleine letters, getallen en speciale tekens, behalve aanhalingstekens.



The screenshot shows a configuration form with three fields: 'EAP Method' with a dropdown menu set to 'MD5', 'Username' with a text input field containing 'Username' and a range note '(Range: 1 - 64 Characters)', and 'Password' with a masked text input field containing ten dots and a range note '(Range: 1 - 64 Characters)'. A red rectangle highlights the password field.

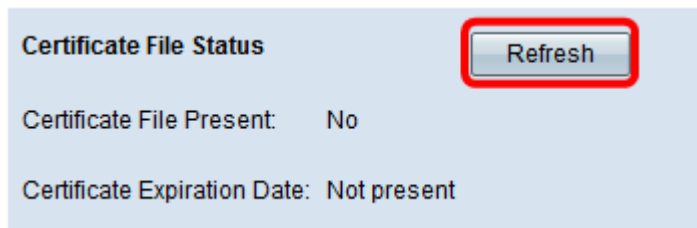
Stap 8. Klik op de  knop.

U dient nu de instellingen voor 802.1X superieur op uw WAP te hebben ingesteld.

Instellingen certificaatbestand weergeven

De status certificaatbestand toont aan of het certificaatbestand al dan niet aanwezig is. Het SSL-certificaat is een digitaal ondertekend certificaat door een certificeringsinstantie waarmee de webbrowser een veilige communicatie met de webserver kan hebben.

Stap 1. Klik op **Vernieuwen** om de huidige status van het certificaatbestand te weergeven.



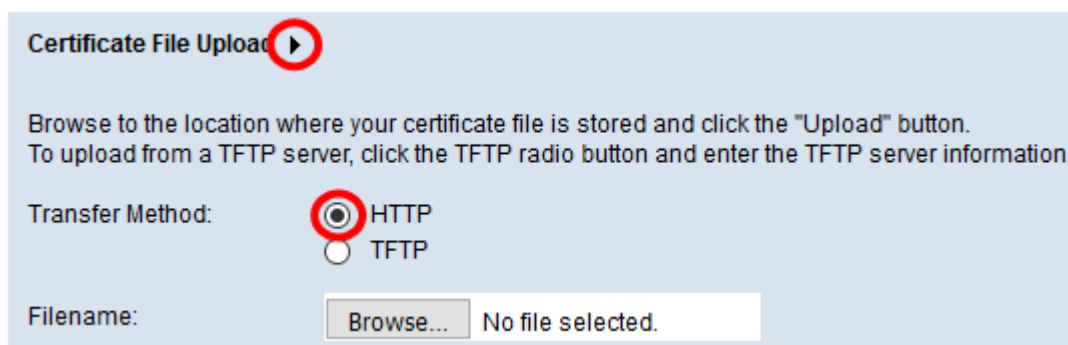
The screenshot shows a 'Certificate File Status' section with a 'Refresh' button highlighted by a red rectangle. Below the button, the status is displayed as 'Certificate File Present: No' and 'Certificate Expiration Date: Not present'.

De status van het certificaatbestand heeft de volgende velden:

- Aanwezigheid van certificaat - hiermee wordt aangegeven of het certificaatbestand al dan niet aanwezig is.
- Vervaldatum certificaat - Hier wordt de verloopdatum van het huidige certificaatbestand weergegeven.

Een certificaatbestand uploaden

Stap 1. Klik op het pijltje naast certificaatbestand uploaden en kies vervolgens de gewenste radioknop in de overdrachtmethode.



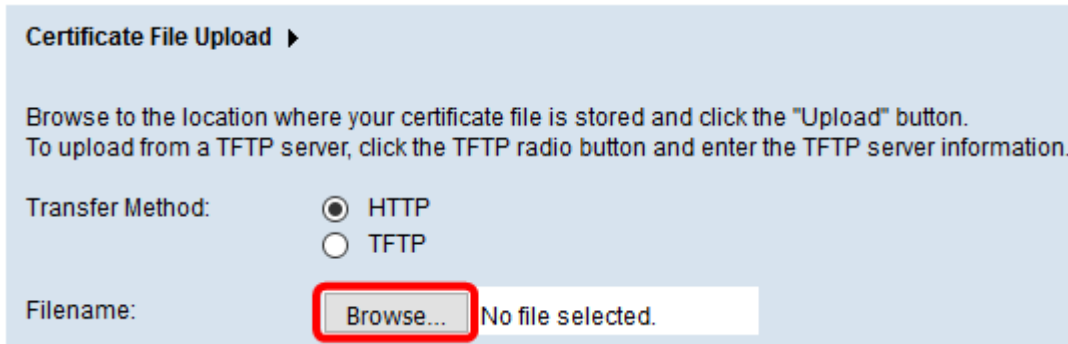
The screenshot shows a 'Certificate File Upload' section with a play button icon circled in red. Below the icon, there is instructional text: 'Browse to the location where your certificate file is stored and click the "Upload" button. To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.' Under 'Transfer Method:', the 'HTTP' radio button is selected and circled in red, while the 'TFTP' radio button is unselected. At the bottom, the 'Filename:' field contains a 'Browse...' button and the text 'No file selected.'

Er zijn twee methoden voor overdracht van het bestand:

- Hypertext Transfer Protocol (HTTP)-protocol
- Trial File Transfer Protocol (TFTP)

Opmerking: In dit voorbeeld wordt HTTP gekozen.

Stap 2. (Optioneel) Als HTTP is geselecteerd, klikt u op **Bladeren** om het certificaatbestand van uw computer te kiezen en vervolgens overslaat u naar [Stap 5](#).



Certificate File Upload ▶

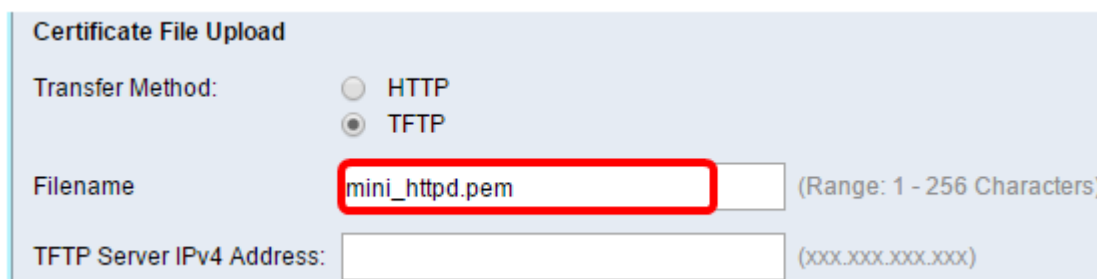
Browse to the location where your certificate file is stored and click the "Upload" button. To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.

Transfer Method: HTTP
 TFTP

Filename: No file selected.

Stap 3. (Optioneel) Als u in Stap 1 TFTP hebt gekozen, voert u de naam van het certificaatbestand in het veld *Bestandsnaam* in. De TFTP-server wordt gebruikt om beginbestanden automatisch binnen apparaten over te dragen en is zeer eenvoudig.

Opmerking: In dit voorbeeld wordt *mini_httpd.pem* gebruikt als bestandsnaam.



Certificate File Upload

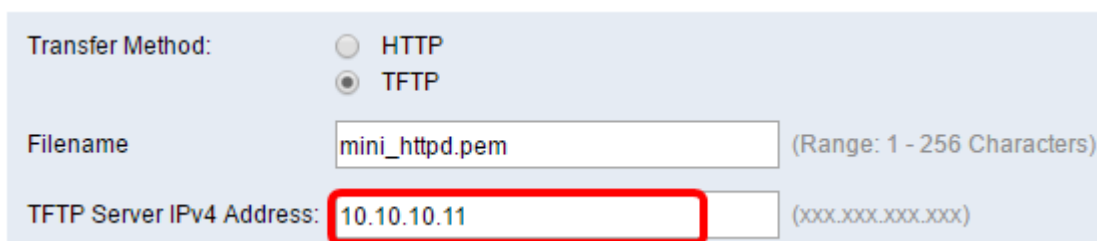
Transfer Method: HTTP
 TFTP

Filename (Range: 1 - 256 Characters)

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

Stap 4. Voer het IP-adres van de TFTP-server in het veld *IPv4-adres van de TFTP-server* in.

Opmerking: In dit voorbeeld wordt 10.10.10.11 gebruikt als het IPv4-adres van de TFTP-server.



Transfer Method: HTTP
 TFTP

Filename (Range: 1 - 256 Characters)

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

Stap 5. Klik op **Update**.

Certificate File Upload

Transfer Method: HTTP
 TFTP

Filename (Range: 1 - 256 Characters)

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

Opmerking: Als u andere WAP-modellen gebruikt, klikt u op **Upload**.

Stap 6. Klik op de knop om uw instellingen op te slaan.

U moet nu met succes een certificaatbestand op uw WAP hebben geüpload.