

Configuratie van 802.1X verificatie op WAP121 en WAP321 access points

Doel

Bij 802.1X-verificatie wanneer een host (ook bekend als de aanvrager) probeert verbinding te maken met een beveiligd netwerk, wordt een netwerkkapparaat de authenticator-controles genoemd met een verificatieserver die de beveiligingsprotocollen, RADIUS en Extensible Authentication Protocol (EAP) ondersteunt, om de identiteit van de aanvrager te controleren. Op deze manier biedt het netwerkkapparaat een extra beveiligingslaag voor het netwerk.

Dit document legt uit hoe u de WAP121- en WAP321-access points kunt configureren als een aanvraag voor 802.1X-verificatie.

Toepasselijke apparaten

- WAP121
- WAP321

Softwareversie

- 1.0.3.4

Configuratie van 802.1X aanvragen

Stap 1. Meld u aan bij het web configuratie hulpprogramma en kies **systeembeveiliging > 802.1X smeekbede**. De pagina *Aangepaste configuratie* wordt geopend:

802.1X Supplicant

Supplicant Configuration

Administrative Mode: ☒ Enable

EAP Method: MD5

Username: example-username (Range: 1 - 64 Characters)

Password: (Range: 1 - 64 Characters)

Certificate File Status Refresh

Certificate File Present: Yes

Certificate Expiration Date: Dec 26 18:43:36 2019 GMT

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: Choose File No file chosen

Upload

Save

Stap 2. Controleer het veld Administratieve modus in om het apparaat in staat te stellen om als aanvrager op 802.1X-verificatie te reageren.

Stap 3. Kies het juiste type van de MAP-methode (Extensible Authentication Protocol) in de vervolgkeuzelijst in het veld EAP-methode.

- MD5 — MD5 is een algoritme dat wordt gebruikt om gegevens van elke grootte in een bit van 128 te versleutelen, het MD5-algoritme gebruikt openbare sleutelcryptosysteem om de gegevens te versleutelen.
- PEAP — Protected EAP is een authenticatiemethode die grotere veiligheid biedt, PEAP verifieert draadloze LAN-klanten door middel van digitale certificaten die door de server worden uitgegeven door een versleutelde SSL/TLS-tunnel te maken tussen de client en de authenticatieserver.
- TLS — Transport Layer Security (TLS) is een cryptografisch protocol dat beveiliging en gegevensintegriteit biedt voor communicatie via het internet. Wanneer een server en client communiceren, zorgt TLS ervoor dat geen derde partij met het oorspronkelijke bericht knoeien. De meeste functies van MD5 worden gebruikt in TLS.

Stap 4. Voer de gebruikersnaam en het wachtwoord in die het access point gebruikt om verificatie te krijgen van de 802.1X-authenticator in de velden Gebruikersnaam en Wachtwoord. De lengte van de gebruikersnaam en het wachtwoord moet van 1 tot 64 alfanumerieke tekens en symbolische tekens zijn.

Stap 5. Klik op **Opslaan** om de instellingen op te slaan.

Opmerking: 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. Om het SSL-certificaat te beheren en te configureren verwijst u naar het artikel [Secure Socket Layer \(SSL\) certificaatbeheer op WAP121 en WAP321 access points](#).