

Instellen 802.1X uitgebreide instellingen op een WAP125 of WAP581

Doel

Een smeekbede is een van de drie rollen in de standaard 802.1X IEEE. 802.1X werd ontwikkeld om beveiliging in Layer 2 van het OSI-model te bieden. 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 geauthenticeerd.

Dit artikel toont u hoe u WAP125 of WAP581 access point als een 802.1X smeekbede kunt configureren.

Opmerking: Klik [hier](#) om te leren hoe u 802.1X Suppliciete Credentials op uw schakelaar kunt configureren.

Toepasselijke apparaten

- WAP125
- WAP581

Softwareversie

- 1.0.0.4 — WAP581
- 1.0.0.5 — WAP125

De 802.1X smeedster configureren

Suppliciete Credentials configureren

Stap 1. Meld u aan bij het webgebaseerde hulpprogramma van uw WAP. De standaardwaarden voor gebruikersnaam en wachtwoord zijn cisco/cisco.



Wireless Access Point

cisco

.....|

English

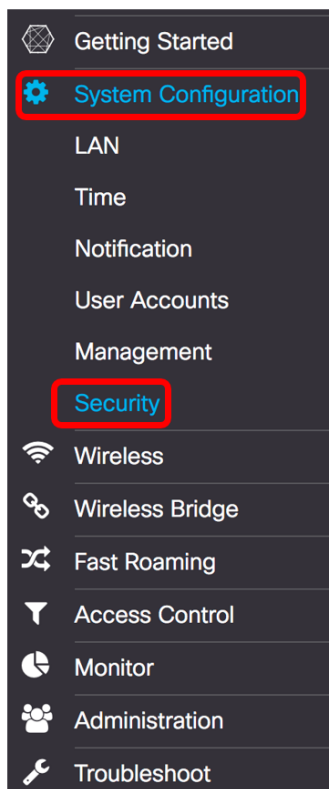
Login

©2017 Cisco Systems, Inc. All Rights Reserved.

Cisco, the Cisco Logo, and Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Opmerking: Als u het wachtwoord al hebt gewijzigd of een nieuwe account hebt aangemaakt, geeft u in plaats daarvan uw nieuwe aanmeldingsgegevens in.

Stap 2. Kies **stelsysteemconfiguratie** > **beveiliging**.



Stap 3. Controleer het aanvinkvakje **Enable** om de beheermodus in te schakelen. Hierdoor kan WAP als de aanvrager van de authenticator fungeren.

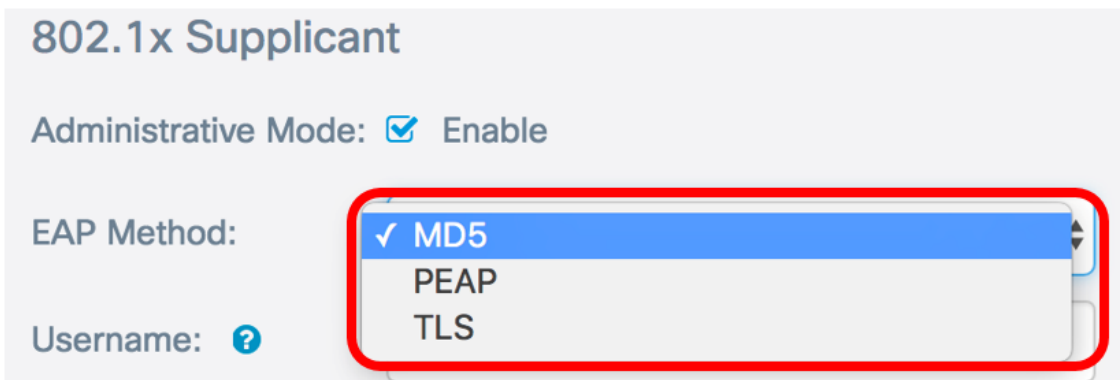
802.1x Supplicant

Administrative Mode:  Enable

Stap 4. Kies het juiste type MAP-methode (Extensible Authentication Protocol) die wordt gebruikt om gebruikersnamen en wachtwoorden te versleutelen van de vervolgkeuzelijst *EAP-methode*. De opties zijn:

- MD5 — gebruikt een 128-bits coderingsmethode. Het MD5-algoritme gebruikt een openbaar cryptosysteem om gegevens te versleutelen.
- PEAP — Protected Extensible Authentication Protocol (PEAP) bevestigt draadloze LAN-clients door middel van digitale certificaten die door de server worden uitgegeven door het maken van een versleutelde SSL/TLS-tunnel tussen de client en de verificatieserver.
- TLS — Transport Layer Security (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.



802.1x Supplicant

Administrative Mode: Enable

EAP Method: ✓ MD5
PEAP
TLS

Username: 

Stap 5. Voer een gebruikersnaam in het veld *Gebruikersnaam* in. Dit is de gebruikersnaam die is ingesteld op de verifactor en wordt gebruikt om te reageren op de 802.1X-verifactor. Het kan een tot 64 tekens lang zijn, kan hoofdletters en kleine letters, getallen en speciale tekens bevatten, behalve dubbele aanhalingstekens.

Opmerking: In dit voorbeeld wordt UserAccess_1 gebruikt.

802.1x Supplicant

Administrative Mode: Enable

EAP Method:

MD5

Username: 

UserAccess_1|

Stap 6. Voer een wachtwoord in dat aan de gebruikersnaam is gekoppeld in het veld *Wachtwoord*. Dit MD5 wachtwoord wordt gebruikt om te reageren op de 802.1X verifcator. Het wachtwoord kan één tot 64 tekens lang zijn, kan hoofdletters en kleine letters, getallen en speciale tekens behalve aanhalingstekens bevatten.

802.1x Supplicant

Administrative Mode: Enable

EAP Method:

MD5

Username: 

UserAccess_1

Password: 

.....

Stap 7. Klik op de knop **Opslaan** om de geconfigureerde instellingen op te slaan.

Security

Save

802.1x Supplicant

Administrative Mode: Enable

EAP Method: MD5

Username:

Password:

U moet nu 802.1X uitgebreide instellingen voor WAP hebben ingesteld.

certificaatbestand uploaden

Stap 1. Kies een methode die door de WAP wordt gebruikt om het SSL-certificaat te verkrijgen. Het SSL-certificaat is een digitaal ondertekend certificaat door een certificeringsinstantie waarmee de webbrowser een veilige communicatie met de webserver kan hebben. De opties zijn:

- HTTP — Certificaat wordt geüpload via het Hyper-Text Transfer Protocol (HTTP) of via de browser.
- TFTP — Certificaat wordt geüpload via een TFTP-server (Trial File Transfer Protocol). Als dit geselecteerd is, slaat u over naar [Stap 3](#). U moet de bestandsnaam en het TFTP-adres invoeren.

Opmerking: In dit voorbeeld wordt HTTP gekozen.

Certificate File Upload

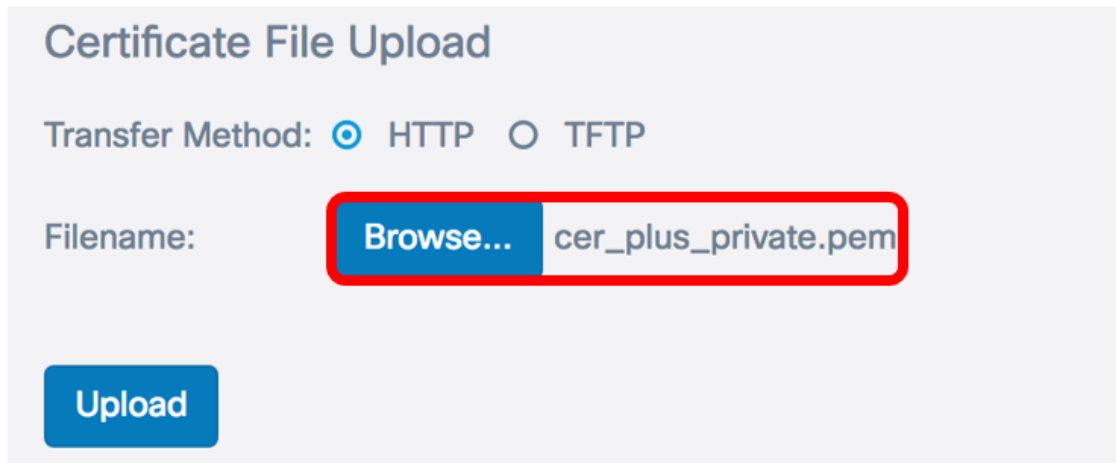
Transfer Method: HTTP TFTP

Filename: cer_plus_private.pem

HTTP-overdrachtmethode

Stap 2. (Optioneel) Als u HTTP hebt gekozen, klikt u op **Bladeren...** en kies het SSL-certificaat.

Opmerking: In dit voorbeeld wordt cer_plus_private.pem gebruikt.



Certificate File Upload

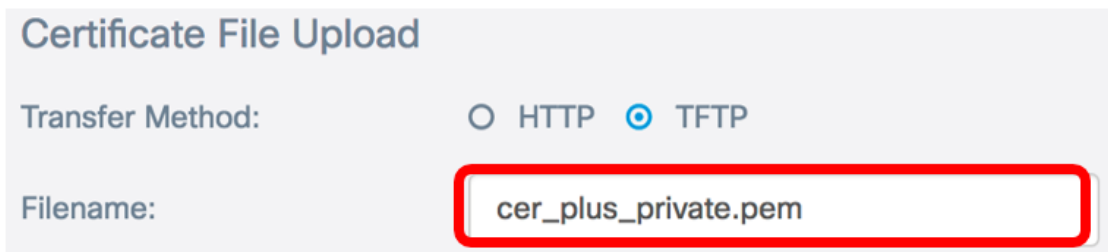
Transfer Method: HTTP TFTP

Filename: cer_plus_private.pem

TFTP-overdrachtmethode

[Stap 3](#) . Als u in Stap 1 voor TFTP hebt gekozen, voert u de naam van het bestand in het veld Bestandsnaam in.

Opmerking: In dit voorbeeld wordt cer_plus_private.pem gebruikt.



Certificate File Upload

Transfer Method: HTTP TFTP

Filename:

Stap 4. (Optioneel) Als TFTP als overdrachtmethode is gekozen, voert u het IPv4-adres van de TFTP-server in het veld *IPv4-adres van de TFTP-server in*. Dit is het pad dat de WAP zal gebruiken om het certificaat op te halen.

Opmerking: In dit voorbeeld wordt 10.21.52.101 gebruikt.



Certificate File Upload

Transfer Method: HTTP TFTP

Filename:

TFTP Server IPv4 Address:

Stap 5. Klik op **Upload**.

802.1x Supplicant

Administrative Mode: Enable

EAP Method:

Username:

Password:

Certificate File Upload

Transfer Method: HTTP TFTP

Filename:

TFTP Server IPv4 Address:

U moet nu een certificaat op de WAP hebben geüpload.