Configuration of 802.1X Authentication on WAP121 and WAP321 Access Points

Objective

In 802.1X authentication when a host (also known as the supplicant) tries to connect to a secured network, a network device called the authenticator checks with an authentication server that supports the security protocols, RADIUS and Extensible Authentication Protocol (EAP), to verify the identity of the supplicant. In this way, the network device provides an additional layer of security to the network.

This document explains how to configure the WAP121 and WAP321 access points as a supplicant for 802.1X authentication.

Applicable Devices

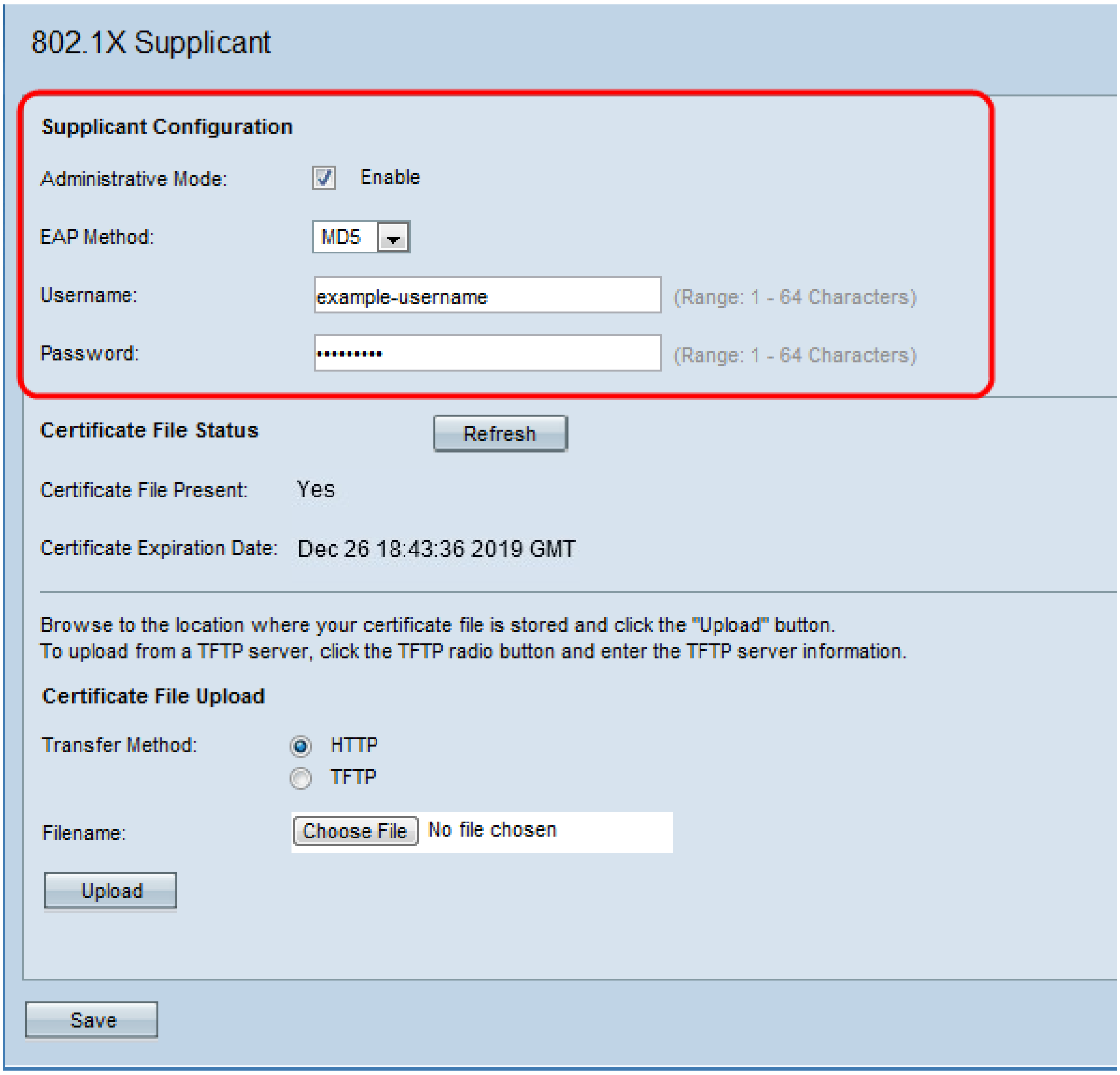
- WAP121
- WAP321

Software Version

- 1.0.3.4

802.1X Supplicant Configuration

Step 1. Log in to the web configuration utility and choose **System Security > 802.1X Supplicant**. The *Supplicant Configuration* page opens:



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

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: No file chosen

Step 2. Check **Enable** in the Administrative Mode field to enable the device to act as a supplicant in 802.1X authentication.

Step 3. Choose the appropriate type of Extensible Authentication Protocol (EAP) method from the drop-down list in the EAP Method field.

- MD5 — MD5 is an algorithm which is used to encrypt data of any size in to 128 bit, the MD5 algorithm uses public key cryptosystem to encrypt the data.

- PEAP — Protected EAP is an authentication method that provides enhanced security, PEAP authenticates wireless LAN clients through digital certificates issued by the server by creating an encrypted SSL/TLS tunnel between the client and the authentication server.

- TLS — Transport Layer Security (TLS) is a cryptographic protocol that provides security and data integrity for communication over the Internet. When a server and client communicate, TLS ensures that no third party tampers with the original message. Most of the functions of MD5 are used in TLS.

Step 4. Enter the username and password that the access point uses to get authentication from the 802.1X authenticator in the Username and Password fields. The length of the username and password must be from 1 to 64 alphanumeric and symbol characters.

Step 5. Click **Save** to save the settings.

Note: The Certificate File Status area shows whether the certificate file is present or not. The

SSL certificate is a digitally signed certificate by a certificate authority that allows the web browser to have a secure communication with the web server. To manage and configure the SSL certificate refer to the article *Secure Socket Layer (SSL) Certificate Management on WAP121 and WAP321 Access Points*.