# Konfiguration der 802.1X-Authentifizierung bei WAP121- und WAP321-Access Points

## Ziel

Bei der 802.1X-Authentifizierung, wenn ein Host (auch als Supplicant bezeichnet) versucht, eine Verbindung zu einem gesicherten Netzwerk herzustellen, überprüft ein Netzwerkgerät namens Authentifizierer mit einem Authentifizierungsserver, der die Sicherheitsprotokolle RADIUS und Extensible Authentication Protocol (EAP) unterstützt, um die Identität des Supplicant zu überprüfen. Auf diese Weise bietet das Netzwerkgerät eine zusätzliche Sicherheitsebene für das Netzwerk.

In diesem Dokument wird erläutert, wie die WAP121- und WAP321-Access Points als Komponente für die 802.1X-Authentifizierung konfiguriert werden.

## Anwendbare Geräte

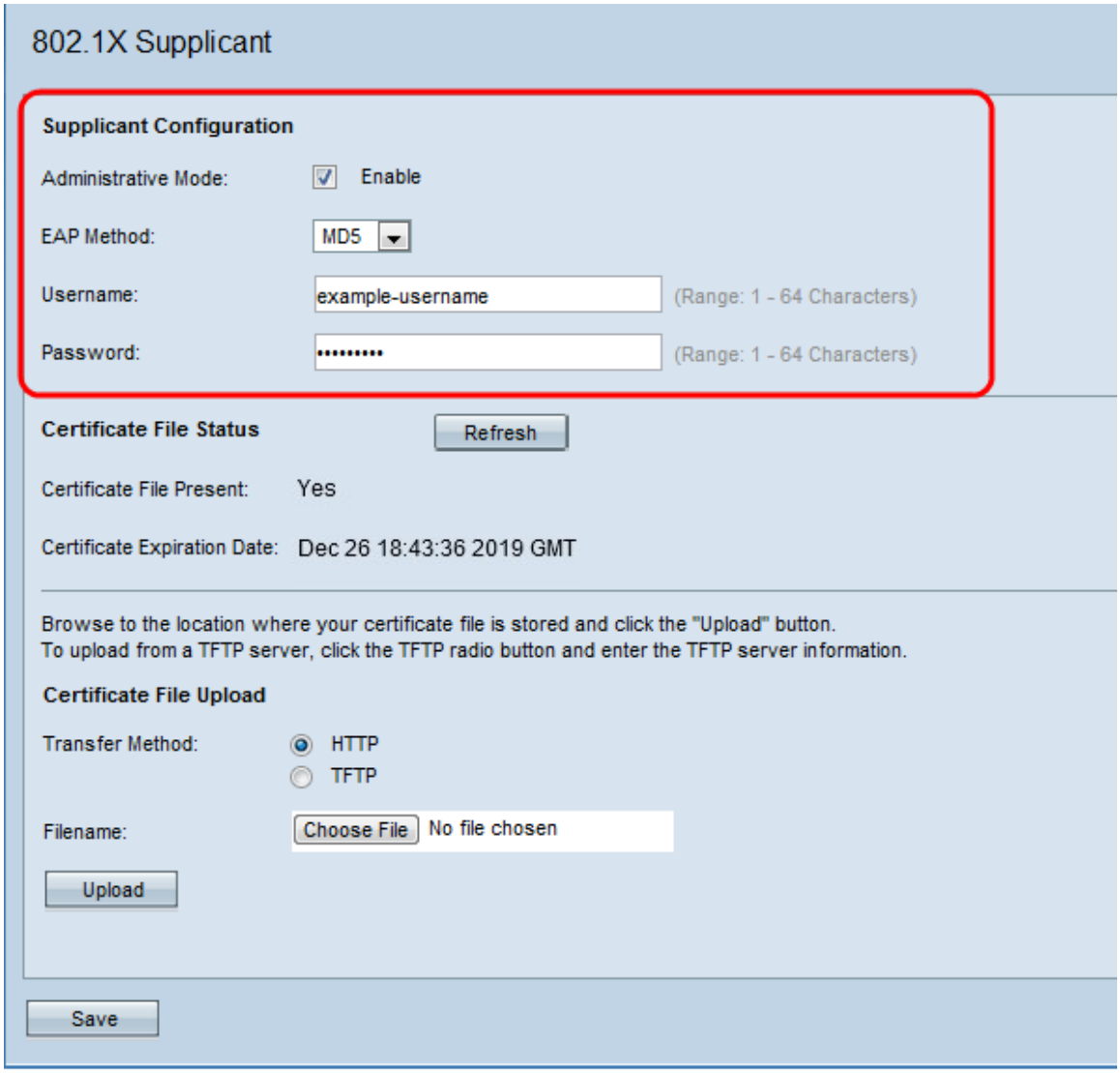
WAP121
WAP321

## Softwareversion

·1,0/3,4

## 802.1X-Komponentenkonfiguration

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Systemsicherheit > 802.1X Supplicant aus**. Die Seite *"Supplicant Configuration*" wird geöffnet:




Schritt 2: Aktivieren Sie im Feld Verwaltungsmodus die **Option Aktivieren**, um das Gerät als Komponente bei der 802.1X-Authentifizierung zu aktivieren.

Schritt 3: Wählen Sie in der Dropdown-Liste im Feld "EAP-Methode" den entsprechenden Typ der Extensible Authentication Protocol (EAP)-Methode aus.

·MD5 — MD5 ist ein Algorithmus, der zur Verschlüsselung von Daten jeder Größe bis zu 128 Bit verwendet wird. Der MD5-Algorithmus verwendet das öffentliche Schlüsselkryptosystem, um die Daten zu verschlüsseln.

·PEAP - Protected EAP ist eine Authentifizierungsmethode, die erweiterte Sicherheit bietet, PEAP authentifiziert WLAN-Clients mithilfe digitaler Zertifikate, die vom Server ausgegeben werden, indem ein verschlüsselter SSL/TLS-Tunnel zwischen dem Client und dem Authentifizierungsserver erstellt wird.

·TLS - Transport Layer Security (TLS) ist ein kryptografisches Protokoll, das Sicherheit und Datenintegrität für die Kommunikation über das Internet bietet. Wenn ein Server und ein Client kommunizieren, stellt TLS sicher, dass keine Manipulationen von Drittanbietern an der ursprünglichen Nachricht vorliegen. Die meisten MD5-Funktionen werden in TLS verwendet.

Schritt 4: Geben Sie den Benutzernamen und das Kennwort ein, mit dem der Access Point die Authentifizierung vom 802.1X-Authentifizierer in den Feldern Benutzername und Kennwort abruft. Benutzername und Kennwort müssen zwischen 1 und 64 alphanumerische

Zeichen und Symbolzeichen lang sein.

Schritt 5: Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

**Hinweis:** Im Bereich Status der Zertifikatsdatei wird angezeigt, ob die Zertifikatsdatei vorhanden ist oder nicht. Das SSL-Zertifikat ist ein digital signiertes Zertifikat von einer Zertifizierungsstelle, das dem Webbrowser eine sichere Kommunikation mit dem Webserver ermöglicht. Informationen zum Verwalten und Konfigurieren des SSL-Zertifikats finden Sie im Artikel *Secure Socket Layer (SSL) Certificate Management auf WAP121 und WAP321 Access Points*.