Configuration de l'authentification de 802.1X sur les Points d'accès WAP121 et WAP321

Objectif

Dans l'authentification de 802.1X quand les essais d'un hôte (également connu sous le nom de suppliant) à connecter à un réseau sécurisé, un périphérique de réseau ont appelé les contrôles d'authentificateur avec un serveur d'authentification qui prend en charge les protocoles de Sécurité, RADIUS et Protocole EAP (Extensible Authentication Protocol), pour vérifier l'identité du suppliant. De cette façon, le périphérique de réseau fournit une couche de sécurité supplémentaire au réseau.

Ce document explique comment configurer les Points d'accès WAP121 et WAP321 en tant que suppliant pour l'authentification de 802.1X.

Périphériques applicables

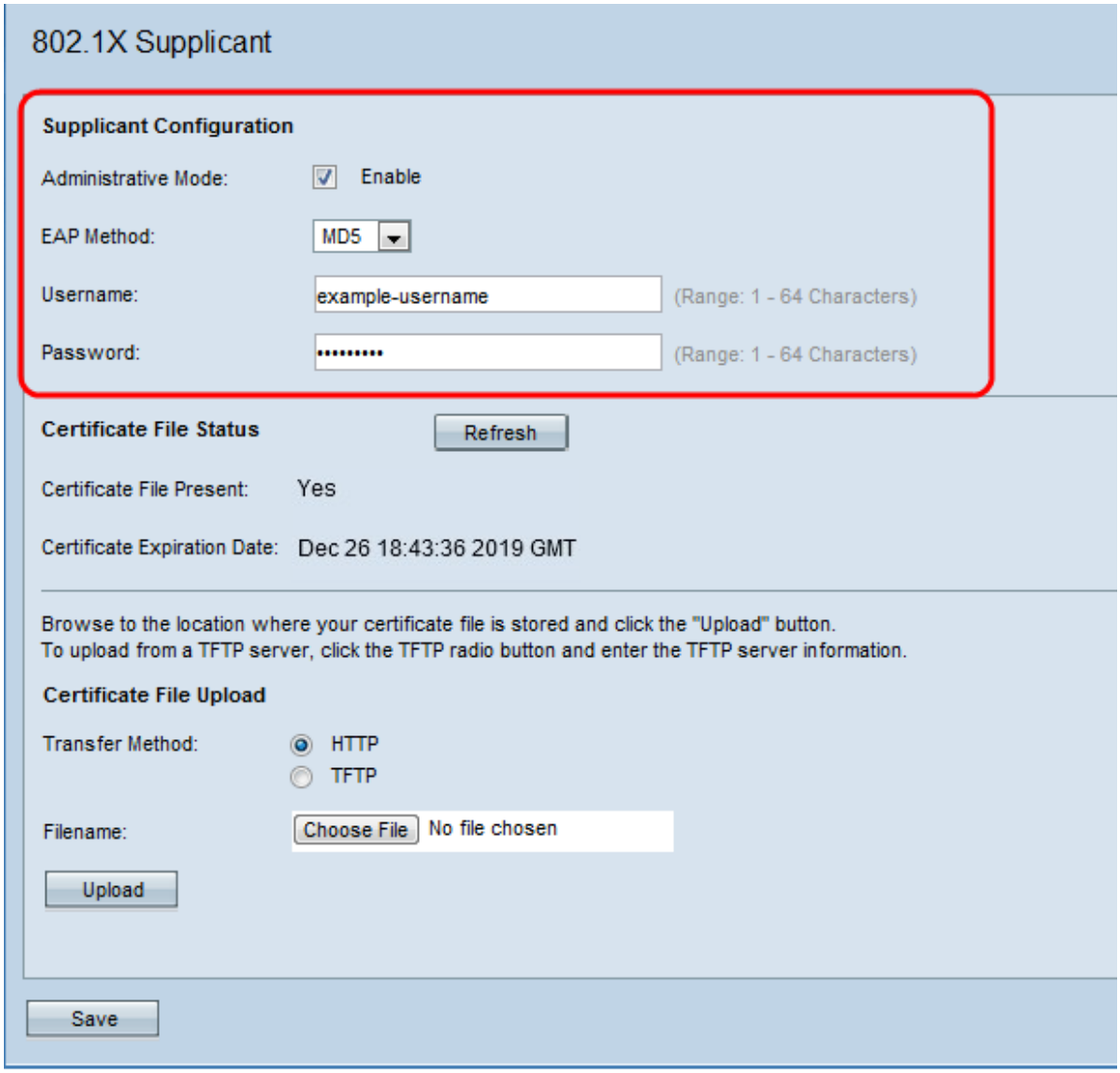
- WAP121
- WAP321

Version de logiciel

- 1.0.3.4

configuration de suppliant de 802.1X

Étape 1. Ouvrez une session à l'utilitaire de configuration Web et choisissez le **suppliant de sécurité des systèmes > de 802.1X**. La page de *configuration de suppliant* s'ouvre :



Étape 2. Enable de contrôle dans le domaine d'Administrative Mode pour permettre au périphérique d'agir en tant que suppliant dans l'authentification de 802.1X.

Étape 3. Choisissez le type approprié de méthode de Protocole EAP (Extensible Authentication Protocol) de la liste déroulante dans le domaine de méthode d'EAP.

- MD5 — Le MD5 est un algorithme qui est utilisé pour chiffrer des données de n'importe quelle taille dedans au bit 128, le système cryptographique de clé publique d'utilisations d'algorithme de MD5 pour chiffrer les données.

- PEAP — L'EAP protégé est une méthode d'authentification qui fournit la sécurité optimisée, PEAP authentifie les clients Sans fil de RÉSEAU LOCAL par des Certificats numériques délivrés par le serveur en créant un tunnel chiffré SSL/TLS entre le client et le serveur d'authentification.

- TLS — Le Transport Layer Security (TLS) est un protocole cryptographique qui fournit la Sécurité et l'intégrité des données pour la transmission au-dessus de l'Internet. Quand un serveur et un client communiquent, le TLS s'assure qu'aucun tiers ne trifouille le premier message. La plupart des fonctions du MD5 sont utilisées dans le TLS.

Étape 4. Écrivez le nom d'utilisateur et mot de passe que le Point d'accès l'utilise pour obtenir l'authentification de l'authentificateur de 802.1X dans les domaines de nom d'utilisateur et mot de passe. La longueur du nom d'utilisateur et mot de passe doit être de 1 à 64 caractères alphanumériques et de symbole.

Étape 5. **Sauvegarde de** clic pour sauvegarder les configurations.

Remarque: La région d'état de fichier du certificat affiche si le fichier du certificat est présent ou pas. Le certificat ssl est un certificat digitalement signé par une autorité de certification qui permet au navigateur Web pour avoir une communication protégée avec le web server. Pour gérer et configurer le certificat ssl référez-vous à la *Gestion de certificat de Protocole SSL (Secure Socket Layer) d'*article *sur les Points d'accès WAP121 et WAP321*.