Configurez les configurations de suppliant de 802.1X sur un point d'accès sans fil

Objectif

La norme de 802.1X a été développée pour fournir la Sécurité dans la couche 2 du modèle ouvert de System Interconnection (OSI). Il comprend les composants suivants : Suppliant, authentificateur, et serveur d'authentification. Un suppliant est le client ou le logiciel qui se connectent à un réseau de sorte qu'il puisse accéder à ses ressources. Il doit fournir des qualifications ou des Certificats pour obtenir une adresse IP et pour faire partie de ce réseau particulier. Un suppliant ne peut pas avoir accès aux ressources de réseau jusqu'à ce qu'il ait été authentifié.

Configurer des configurations de suppliant de 802.1X sur votre point d'accès sans fil (WAP) est utile pour permettre aux périphériques autorisés derrière votre WAP pour faire partie du réseau et pour accéder à ses ressources. En même temps, il ajoute également une couche de Sécurité au réseau.

Cet article t'affichera comment configurer des configurations de suppliant de 802.1X sur votre point d'accès sans fil.

Périphériques applicables

- Gamme WAP100
- Gamme WAP300
- Gamme WAP500

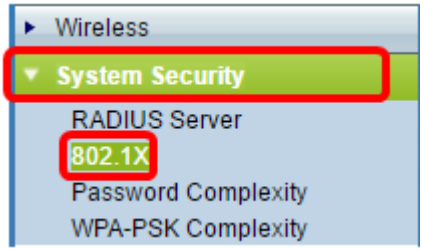
Version de logiciel

- 1.0.1.2 – WAP150, WAP361
- 1.0.6.2 – WAP121, WAP321
- 1.0.2.2 – WAP131, WAP351
- 1.2.1.3 – WAP551, WAP561, WAP371
- 1.0.0.17 – WAP571, WAP571E

Configurez les configurations de suppliant de 802.1X sur un WAP

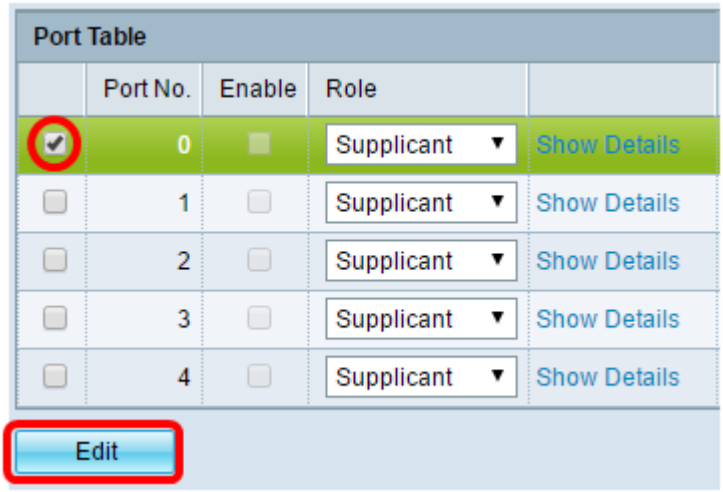
Étape 1. Ouvrez une session à l'utilitaire basé sur le WEB du Point d'accès et choisissez le **système Security>802.1X**.

Remarque: Le menu de service basé sur le WEB peut varier selon le modèle de votre WAP. Les images ci-dessous sont prises de WAP361.



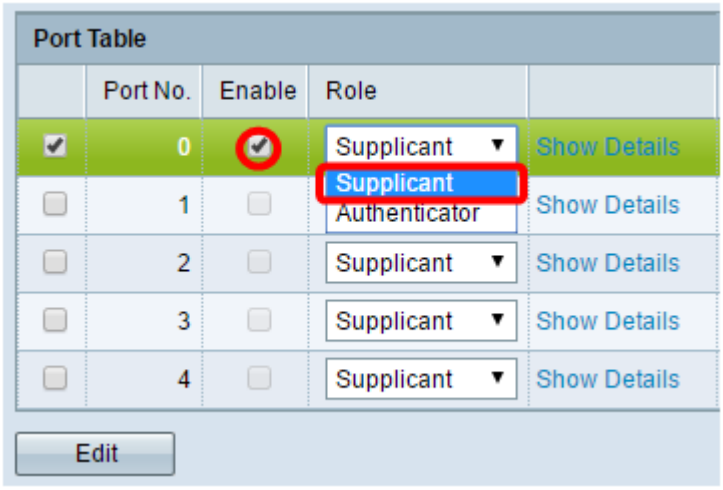
Note: Si vous utilisez d'autres modèles de WAP, choisissez le **suppliant de sécurité des systèmes > de 802.1X** alors ignorez à l'étape 3.

Étape 2. Cochez la case du numéro de port que vous souhaitez configurer et puis cliquer sur Edit.

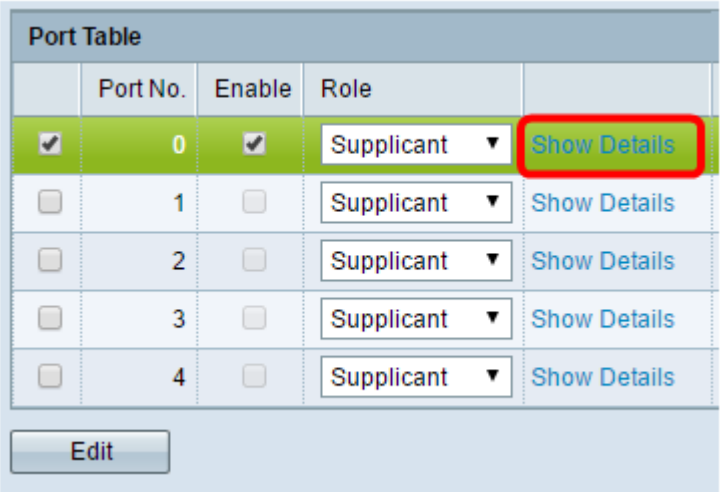


Étape 3. Cochez la case d'**enable** et puis choisissez le **suppliant de la** liste déroulante. C'est l'option par défaut.

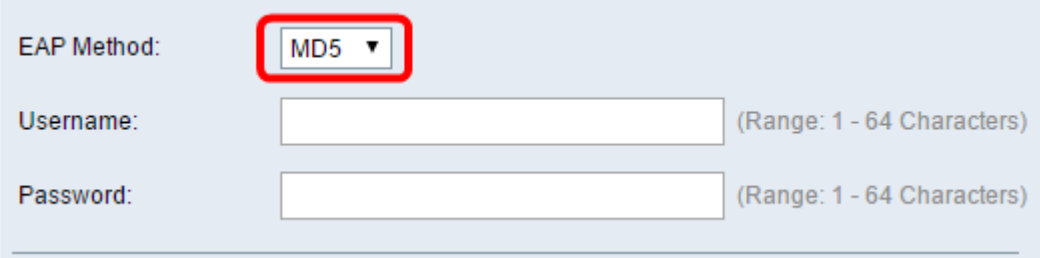
Remarque: Pour d'autres modèles de WAP, cochez la case d'**enable** pour l'Administrative Mode puis ignorez à l'étape 5.



Étape 4. Cliquez sur en fonction les **détails d'exposition** joignent pour te permettre d'éditer les configurations.



Étape 5. Choisissez le type approprié de méthode de Protocole EAP (Extensible Authentication Protocol) de la liste déroulante de méthode d'EAP.

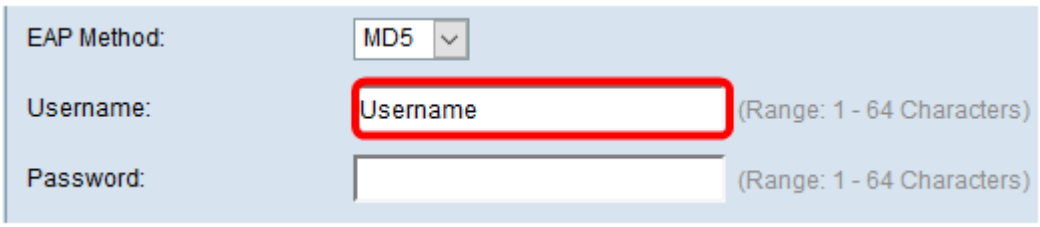


Les options sont :

- MD5 — Le MD5 est un algorithme qui est utilisé pour chiffrer des données de n'importe quelle taille dans le bit 128. L'algorithme de MD5 emploie un système cryptographique public pour chiffrer des données.
- PEAP — Le Protected Extensible Authentication Protocol (PEAP) authentifie des clients de réseau local sans fil (RÉSEAU LOCAL) par des Certificats numériques délivrés par le serveur en créant un tunnel chiffré de Secure Sockets Layer (SSL) ou de Transport Layer Security (TLS) entre le client et le serveur d'authentification.
- TLS — Le TLS est un protocole qui fournit la Sécurité et l'intégrité des données pour la transmission au-dessus de l'Internet. Il s'assure qu'aucun tiers ne trifouille le premier message.

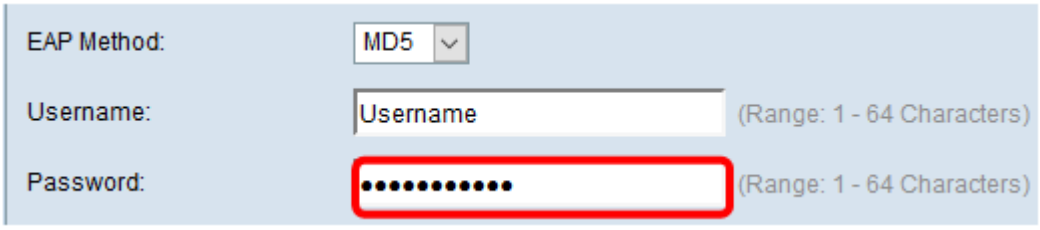
Remarque: Dans cet exemple, le MD5 est utilisé.

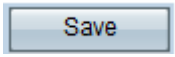
Étape 6. Écrivez votre nom d'utilisateur préféré dans le domaine de *nom d'utilisateur*. Ceci sera utilisé quand répondant à un authentificateur de 802.1X. Ce peut être jusqu'à 64 caractères longs, peut inclure les lettres majuscules et minuscules, les nombres, et les caractères particuliers excepté de doubles guillemets.



Étape 7. Entrez votre mot de passe préféré dans le domaine de *mot de passe*. Ce mot de

passe de MD5 est utilisé en répondant à un authentificateur de 802.1X. Le mot de passe peut être jusqu'à 64 caractères longs, peut inclure les lettres majuscules et minuscules, les nombres, et les caractères particuliers excepté des guillemets.



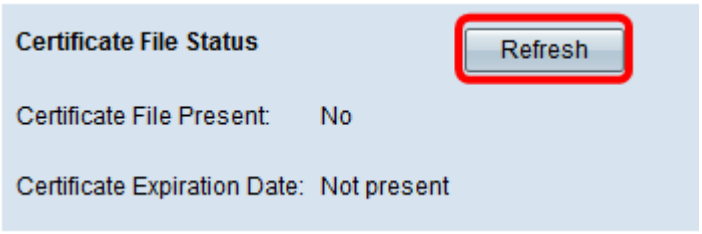
Étape 8. Cliquez sur  le bouton.

Vous devriez maintenant avoir configuré les configurations de suppliant de 802.1X sur votre WAP.

Configurations de fichier du certificat de vue

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.

Étape 1. Pour visualiser l'état actuel du fichier du certificat, le clic **régénèrent**.

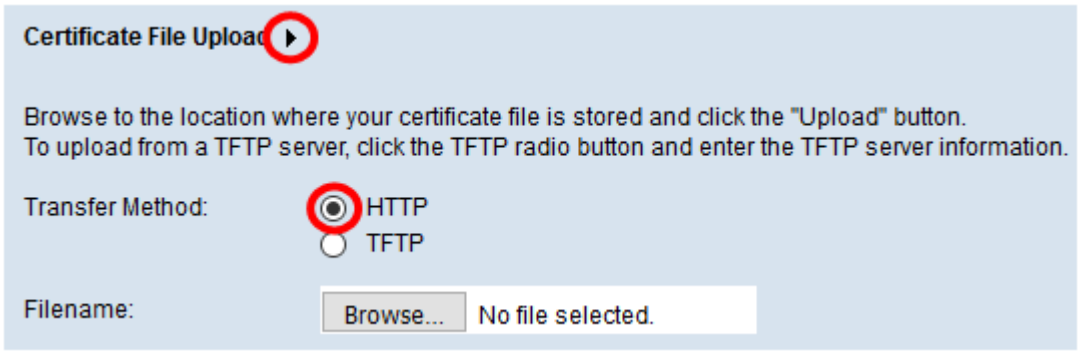


La région d'état de fichier du certificat a les champs suivants :

- Fichier du certificat actuel – Affiche, que le fichier du certificat soit présent ou pas.
- Date d'expiration de certificat – Affiche la date d'expiration du fichier de certificat valable.

Téléchargez un fichier du certificat

Étape 1. Cliquez sur la flèche près du téléchargement de fichier du certificat puis choisissez la case d'option désirée de la méthode de transfert.

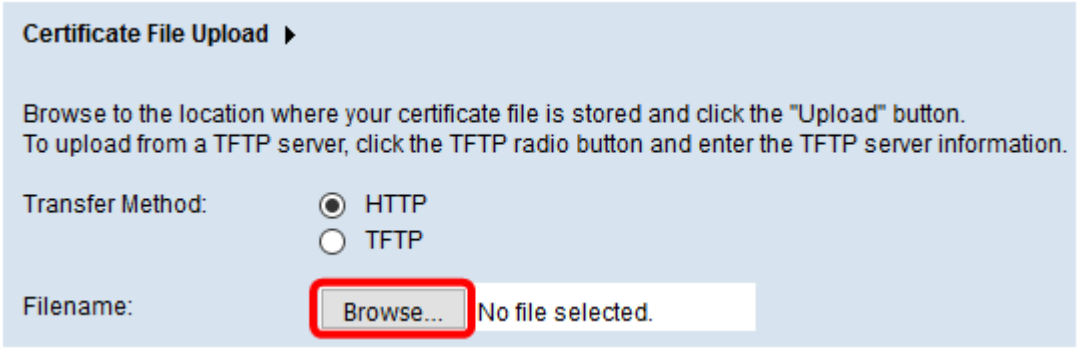


Il y a deux méthodes de transfert en téléchargeant le fichier :

- Protocole HTTP (Hypertext Transfer Protocol)
- **Trivial File Transfer Protocol (TFTP)**

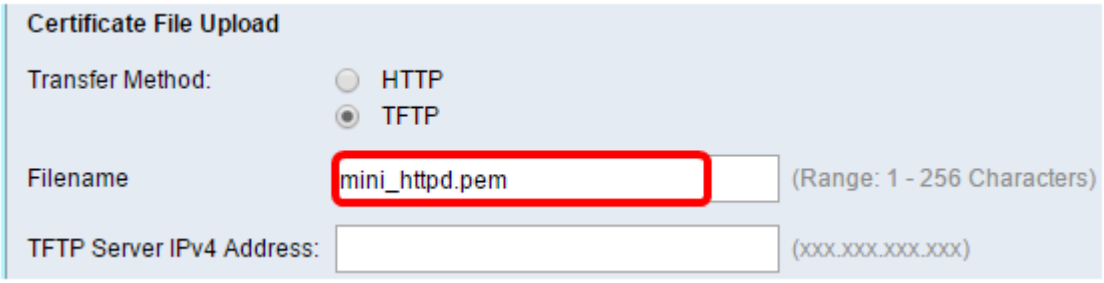
Remarque: Dans cet exemple, le HTTP est choisi.

Étape 2. (facultative) si le HTTP est choisi, clic **parcourent** pour choisir le fichier du certificat à partir de votre ordinateur puis ignorent à l'étape 5.



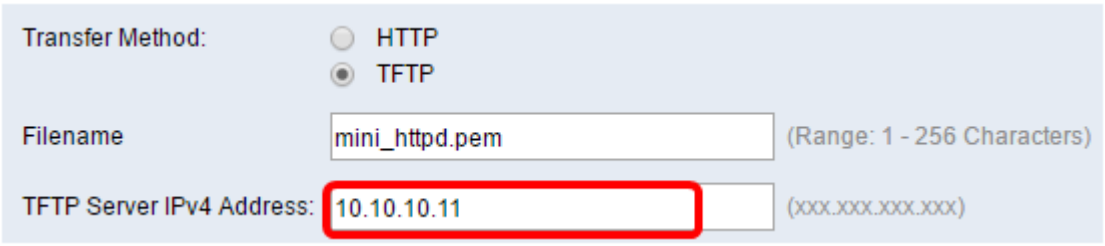
Étape 3. (facultative) si vous choisissiez le TFTP dans l'étape 1, écrivent le nom du fichier du certificat dans le *champ Filename*. Le serveur TFTP est utilisé pour transférer automatiquement des fichiers de démarrage dans des périphériques et est très simple.

Remarque: Dans cet exemple, *mini_httpd.pem* est utilisé comme nom du fichier.

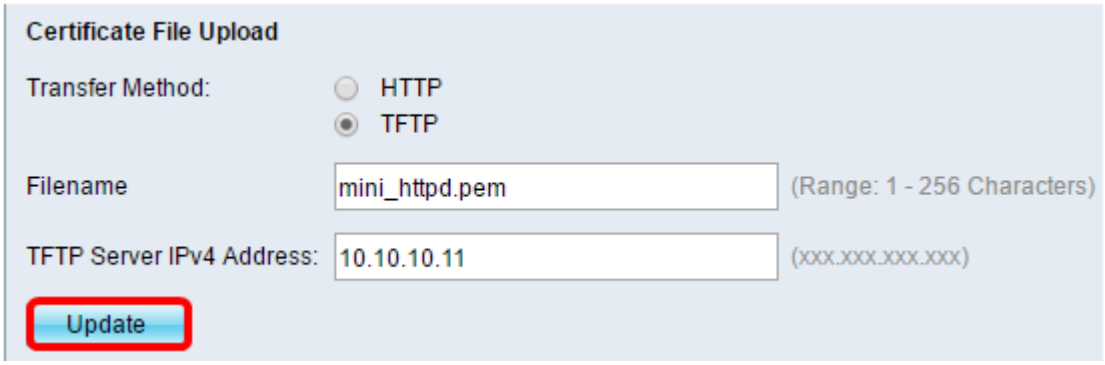


Étape 4. Écrivez l'adresse IP du serveur TFTP dans le domaine d'*ipv4 addres de serveur TFTP*.

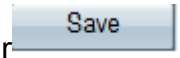
Remarque: Dans cet exemple, 10.10.10.11 est utilisé comme ipv4 addres de serveur TFTP.



Étape 5. **Mise à jour de** clic.



Note: Si vous utilisez d'autres modèles de WAP, cliquez sur Upload.

Étape 6. Cliquez sur  le bouton pour sauvegarder vos configurations.

Vous devriez avoir maintenant avec succès téléchargé un fichier du certificat sur votre WAP.