

# Configurer les paramètres du demandeur 802.1X sur un WAP125 ou WAP581

## Objectif

Un demandeur est l'un des trois rôles de la norme IEEE 802.1X. La norme 802.1X a été développée pour assurer la sécurité de la couche 2 du modèle OSI. Il se compose des composants suivants : Serveur de demandeur, d'authentificateur et d'authentification. Un demandeur est le client ou le logiciel qui se connecte à un réseau pour qu'il puisse accéder à ses ressources. Il doit fournir des informations d'identification ou des certificats pour obtenir une adresse IP et faire partie de ce réseau particulier. Un demandeur ne peut pas avoir accès aux ressources réseau tant qu'il n'a pas été authentifié.

Cet article explique comment configurer le point d'accès WAP125 ou WAP581 en tant que demandeur 802.1X.

**Note:** Pour savoir comment configurer les informations d'identification du demandeur 802.1X sur votre commutateur, cliquez [ici](#).

## Périphériques pertinents

- WAP125
- WAP581

## Version du logiciel

- 1.0.0.4 - WAP581
- 1.0.0.5 - WAP125

## Configurer le demandeur 802.1X

### Configurer les informations d'identification du demandeur

Étape 1. Connectez-vous à l'utilitaire Web de votre WAP. Le nom d'utilisateur et le mot de passe par défaut sont cisco/cisco.



## Wireless Access Point

cisco

.....|

English

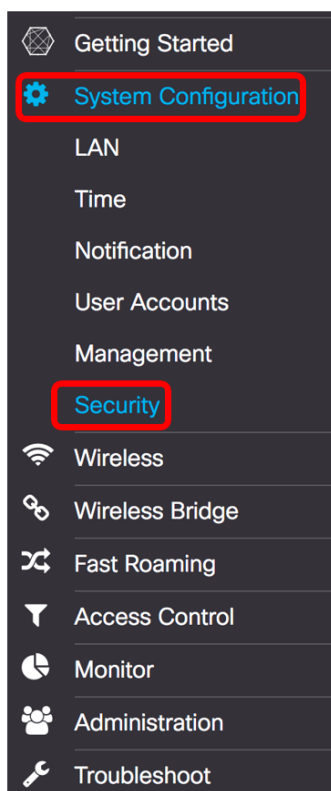
Login

©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.

**Note:** Si vous avez déjà modifié le mot de passe ou créé un nouveau compte, saisissez plutôt vos nouvelles informations d'identification.

Étape 2. Choisissez **Configuration du système > Sécurité**.



Étape 3. Cochez la case **Activer** pour activer le mode d'administration. Cela permet au WAP d'agir en tant que demandeur de l'authentificateur.

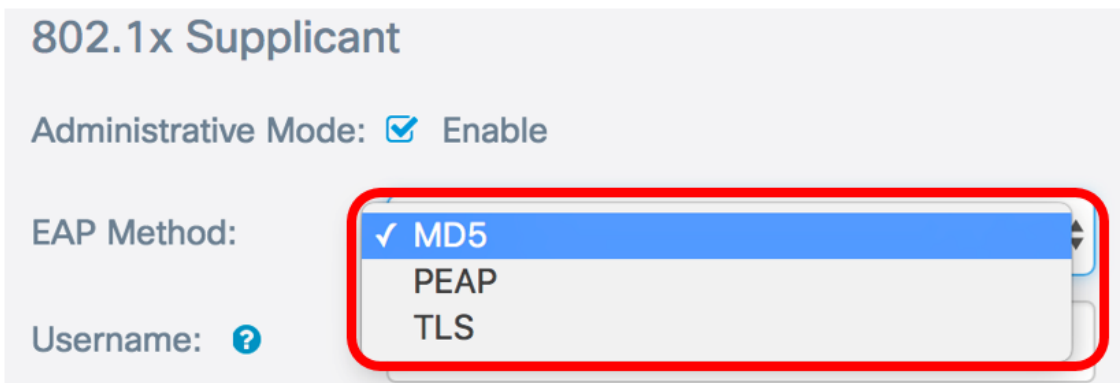
# 802.1x Supplicant

Administrative Mode:  Enable

Étape 4. Choisissez le type approprié de méthode EAP (Extensible Authentication Protocol) qui sera utilisé pour chiffrer les noms d'utilisateur et les mots de passe dans la liste déroulante *Méthode EAP*. Les options sont les suivantes :

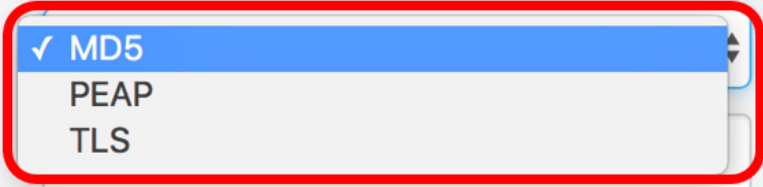
- MD5 : utilise une méthode de cryptage 128 bits. L'algorithme MD5 utilise un système de chiffrement public pour chiffrer les données.
- PEAP : le protocole PEAP (Protected Extensible Authentication Protocol) authentifie les clients LAN sans fil via des certificats numériques émis par le serveur en créant un tunnel SSL/TLS chiffré entre le client et le serveur d'authentification.
- TLS : TLS (Transport Layer Security) est un protocole qui assure la sécurité et l'intégrité des données pour les communications sur Internet. Il garantit qu'aucun tiers ne modifie le message d'origine.


**Note:** Dans cet exemple, MD5 est utilisé.



802.1x Supplicant

Administrative Mode:  Enable

EAP Method: 

Username: 

Étape 5. Entrez un nom d'utilisateur dans le champ *Nom d'utilisateur*. Il s'agit du nom d'utilisateur configuré sur l'authentificateur et utilisé pour répondre à l'authentificateur 802.1X. Il peut comporter entre un et 64 caractères, des majuscules et des minuscules, des chiffres et des caractères spéciaux, à l'exception des guillemets doubles.

**Note:** Dans cet exemple, UserAccess\_1 est utilisé.

### 802.1x Supplicant

Administrative Mode:  Enable

EAP Method: MD5

Username:

Étape 6. Entrez un mot de passe associé au nom d'utilisateur dans le champ *Mot de passe*. Ce mot de passe MD5 est utilisé pour répondre à l'authentificateur 802.1X. Le mot de passe peut comporter entre un et 64 caractères, des majuscules et des minuscules, des chiffres et des caractères spéciaux, à l'exception des guillemets.

### 802.1x Supplicant

Administrative Mode:  Enable

EAP Method: MD5

Username:

Password:

Étape 7. Cliquez sur le bouton **Enregistrer** pour enregistrer les paramètres configurés.

# Security

**Save**

## 802.1x Supplicant

Administrative Mode:  Enable

EAP Method: MD5

Username:

Password:

Vous devez maintenant configurer les paramètres du demandeur 802.1X sur le WAP.

### Téléchargement du fichier de certificat

Étape 1. Dans la méthode de transfert, choisissez une méthode que le WAP utilisera pour obtenir le certificat SSL. Le certificat SSL est un certificat signé numériquement par une autorité de certification qui permet au navigateur Web d'avoir une communication sécurisée avec le serveur Web. Les options sont les suivantes :

- HTTP : le certificat est téléchargé via le protocole HTTP (Hyper Text Transfer Protocol) ou via le navigateur.
- TFTP : le certificat est téléchargé via un serveur TFTP (Trivial File Transfer Protocol). Si cette option est sélectionnée, passez à l'[étape 3](#). Vous devrez entrer le nom de fichier et l'adresse TFTP.

**Note:** Dans cet exemple, HTTP est choisi.

## Certificate File Upload

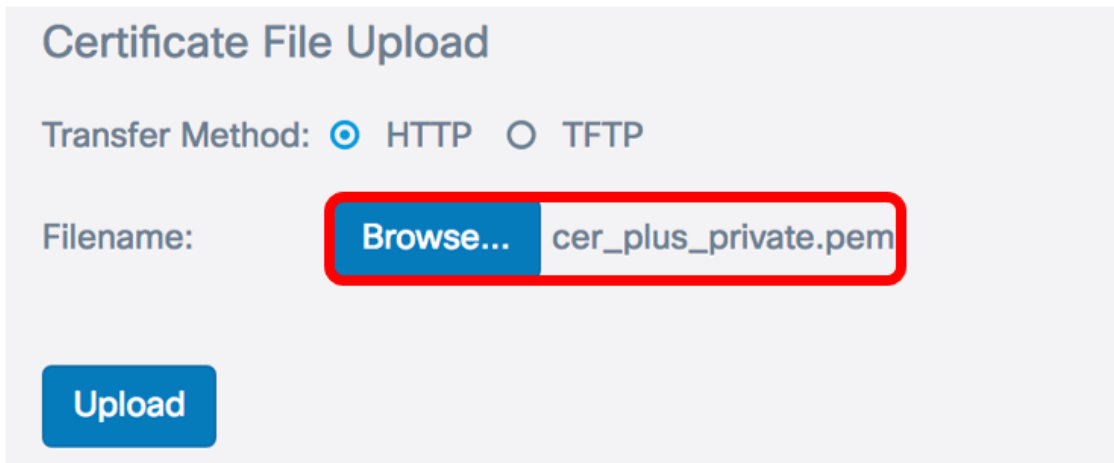
Transfer Method:  HTTP  TFTP

Filename:  cer\_plus\_private.pem

### Méthode de transfert HTTP

Étape 2. (Facultatif) Si vous avez choisi HTTP, cliquez sur **Parcourir...** et sélectionnez le certificat SSL.

**Note:** Dans cet exemple, cer\_plus\_private.pem est utilisé.



Certificate File Upload

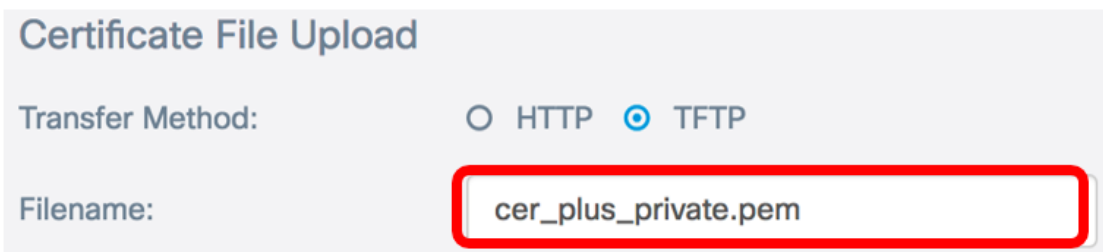
Transfer Method:  HTTP  TFTP

Filename:  cer\_plus\_private.pem

### Méthode de transfert TFTP

Étape 3. Si vous avez choisi TFTP à l'étape 1, saisissez le nom du fichier dans le champ Nom de fichier.

**Note:** Dans cet exemple, cer\_plus\_private.pem est utilisé.



Certificate File Upload

Transfer Method:  HTTP  TFTP

Filename:

Étape 4. (Facultatif) Si TFTP est choisi comme méthode de transfert, saisissez l'adresse IPv4 du serveur TFTP dans le champ *Adresse IPv4 du serveur TFTP*. Il s'agit du chemin que le WAP utilisera pour récupérer le certificat.

**Note:** Dans cet exemple, 10.21.52.101 est utilisé.



Certificate File Upload

Transfer Method:  HTTP  TFTP

Filename:

TFTP Server IPv4 Address:

Étape 5. Cliquez sur **Upload** (charger).

## 802.1x Supplicant

Administrative Mode:  Enable

EAP Method:

Username:

Password:

## Certificate File Upload

Transfer Method:  HTTP  TFTP

Filename:

TFTP Server IPv4 Address:

Vous devez maintenant avoir téléchargé un certificat sur le WAP.