# Configuration des paramètres du demandeur 802.1X sur les WAP131 et WAP371

# Objectif

L'authentification IEEE 802.1X permet au périphérique WAP d'accéder à un réseau câblé sécurisé. Vous pouvez activer le périphérique WAP en tant que demandeur 802.1X (client) sur le réseau câblé. Un nom d'utilisateur et un mot de passe chiffrés peuvent être configurés pour permettre au périphérique WAP de s'authentifier à l'aide de la norme 802.1X.

Sur les réseaux qui utilisent le contrôle d'accès réseau basé sur les ports IEEE 802.1X, un demandeur ne peut pas accéder au réseau tant que l'authentificateur 802.1X n'a pas accordé l'accès. Si votre réseau utilise 802.1X, vous devez configurer les informations d'authentification 802.1X sur le périphérique WAP, afin qu'il puisse les fournir à l'authentificateur.

L'objectif de ce document est de vous montrer comment configurer les paramètres du demandeur 802.1X sur les WAP131 et WAP371.

# Périphériques pertinents

·WAP131

·WAP371

## Version du logiciel

·v1.0.0.39 (WAP131)

·v1.2.0.2 (WAP371)

## Configuration des paramètres du demandeur 802.1X

Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez **Sécurité du** système > Supplicant 802.1X. La page *802.1X Supplicant* s'ouvre.

802.1X Supplicant		
Supplicant Configuration		
Administrative Mode:	Enable	
EAP Method:	MD5 💌	
Username:		(Range: 1 - 64 Characters)
Password:		(Range: 1 - 64 Characters)
Certificate File Status	Refresh	
Certificate File Present:	No	
Certificate Expiration Date:	Not present	
Browse to the location whe To upload from a TFTP ser	re your certificate file is stored and click th ver, click the TFTP radio button and enter t	e "Upload" button. he TFTP server information.
Certificate File Upload		
Transfer Method:	<ul><li>HTTP</li><li>TFTP</li></ul>	
Filename:	Browse No file selected.	
Upload		
Save		

#### Configuration du demandeur

Étape 1. Accédez à la zone *Configuration du demandeur*. Dans le champ *Mode administratif* , cochez la case **Activer** pour activer la fonctionnalité de demandeur 802.1X.

Supplicant Configuration		
Administrative Mode:	Enable	
EAP Method:	MD5 💌	
Username:		(Range: 1 - 64 Characters)
Password:		(Range: 1 - 64 Characters)

Étape 2. Dans la liste déroulante *Méthode EAP*, sélectionnez l'algorithme qui sera utilisé pour chiffrer les noms d'utilisateur et les mots de passe. EAP est l'acronyme de Extensible Authentication Protocol et est utilisé comme base pour les algorithmes de chiffrement.

Supplicant Configuration		
Administrative Mode:	Enable	
EAP Method:	MD5 🔽	
Username <sup>.</sup>	MD5 PEAP	(Range: 1 - 64 Characters)
	TLS	(Runge, Frontendrotoro)
Password:		(Range: 1 - 64 Characters)

Les options disponibles sont les suivantes :

·MD5 — L'algorithme MD5 Message-Digest utilise une fonction de hachage pour fournir une sécurité de base. Cet algorithme n'est pas recommandé, car les deux autres ont une sécurité supérieure.

·PEAP : PEAP signifie Protected Extensible Authentication Protocol. Il encapsule le protocole EAP et fournit une sécurité supérieure à MD5 en utilisant un tunnel TLS pour transmettre des données.

·TLS : TLS est l'acronyme de Transport Layer Security, et est une norme ouverte offrant une sécurité élevée.

Étape 3. Dans le champ *Nom d'utilisateur*, saisissez le nom d'utilisateur que le périphérique WAP utilisera lors de la réponse aux demandes d'un authentificateur 802.1X. Le nom d'utilisateur doit comporter entre 1 et 64 caractères et peut inclure des caractères alphanumériques et spéciaux.

Supplicant Configuration		
Administrative Mode:	Enable	
EAP Method:	MD5	
Username:	username1	(Range: 1 - 64 Characters)
Password:		(Range: 1 - 64 Characters)

Étape 4. Dans le champ *Mot de passe*, saisissez le mot de passe que le périphérique WAP utilisera lors de la réponse aux demandes d'un authentificateur 802.1X. Le nom d'utilisateur doit comporter entre 1 et 64 caractères et peut inclure des caractères alphanumériques et spéciaux.

Supplicant Configuration		
Administrative Mode:	Enable	
EAP Method:	MD5 <	
Username:	username1	(Range: 1 - 64 Characters)
Password:		(Range: 1 - 64 Characters)

#### Étape 5. Click Save.

Supplicant Configuration		
Administrative Mode:	Enable	
EAP Method:	MD5 💌	
Username:	username1	(Range: 1 - 64 Characters)
Password:	•••••	(Range: 1 - 64 Characters)
Certificate File Status	Refresh	
Certificate File Present:	No	
Certificate Expiration Date:	Not present	
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:	<ul><li>HTTP</li><li>TFTP</li></ul>	
Filename:	Browse No file selected.	
Upload		
Save		

#### État du fichier de certificat

Étape 1. Accédez à la zone *Statut du fichier de certificat*. Cette zone indique si un fichier de certificat SSL HTTP existe sur le périphérique WAP. Le champ *Fichier de certificat présent* indique " Oui " si un certificat est présent ; la valeur par défaut est " Non ". Si un certificat est présent, la *date d'expiration du certificat* apparaîtra à son expiration ; sinon, la valeur par défaut est " Non présent ".

Certificate File Status		Refresh
Certificate File Present:	No	
Certificate Expiration Date:	Not present	

Étape 2. Pour afficher les dernières informations, cliquez sur le bouton **Actualiser** pour obtenir les informations de certificat les plus récentes.

Certificate File Status		Refresh
Certificate File Present:	Yes	
Certificate Expiration Date:	Aug 22 16:41:51 2018 GMT	

#### Téléchargement du fichier de certificat

Étape 1. Accédez à la zone *Certificate File Upload* pour télécharger un certificat HTTP SSL sur le périphérique WAP. Dans le champ *Méthode de transfert*, sélectionnez les cases d'option **HTTP** ou **TFTP** pour choisir le protocole à utiliser pour télécharger le certificat.

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:	<ul><li>● HTTP</li><li>● TFTP</li></ul>	
Filename:	Browse No file selected.	
Upload		

Étape 2. Si vous avez sélectionné **TFTP**, passez à l'étape 3. Si vous avez sélectionné **HTTP**, cliquez sur le bouton **Parcourir...** pour rechercher le fichier de certificat sur votre ordinateur. Passez à l'<u>étape 5</u>.

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.

Étape 3. Si vous avez sélectionné **TFTP** dans le champ *Méthode de transfert*, saisissez le nom de fichier du certificat dans le champ *Nom de fichier*.

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:	<ul><li>HTTP</li><li>TFTP</li></ul>	
Filename:	certificate.pem	(Range: 1 - 256 Characters)
TFTP Server IPv4 Address:		(XXX.XXX.XXX.XXX)
Upload		

Note: Le fichier doit se terminer par .pem.

Étape 4. Entrez l'adresse IP du serveur TFTP dans le champ TFTP Server IPv4 Address.

Browse to the location where To upload from a TFTP server	your certificate file is stored and click the r, click the TFTP radio button and enter th	e "Upload" button. he TFTP server information.
Certificate File Upload		
Transfer Method:	⊙ HTTP	
	TFTP	
Filename:	certificate.pem	(Range: 1 - 256 Characters)
TFTP Server IPv4 Address:	192.168.1.100	(xxx.xxx.xxxx)
Upload		

Étape 5. Cliquez sur Upload (charger).

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: certificate.pem (Range: 1 - 256 Characters)
TFTP Server IPv4 Address: 192.168.1.100 (xxx.xxx.xxx)

Étape 6. Une fenêtre de confirmation s'affiche. Cliquez sur **OK** pour commencer le téléchargement.

Confirm	×
	Device is uploading the certificate file now.
	OK Cancel

Étape 7. Click Save.