

Configurer le pont de groupe de travail sur les points d'accès WAP121 et WAP321

Objectif

La fonctionnalité de pont de groupe de travail permet au point d'accès sans fil (WAP) de relier le trafic entre un client distant et le réseau local sans fil connecté au mode pont de groupe de travail. Le périphérique WAP associé à l'interface distante est appelé interface de point d'accès et celui associé au réseau local sans fil est appelé interface d'infrastructure. Cette fonctionnalité est recommandée lorsque la fonctionnalité WDS n'est pas utilisable, car la fonctionnalité WDS est une solution de pont préférée pour les WAP121 et WAP321. Lorsque la fonctionnalité de pont de groupe de travail est activée, la fonctionnalité de pont WDS ne fonctionne pas. Pour savoir comment le pont WDS est configuré, reportez-vous à l'article *Wireless Distribution System (WDS) Bridge Configuration sur les points d'accès WAP121 et WAP321*.

Cet article explique comment configurer le pont de groupe de travail sur les points d'accès WAP121 et WAP321.

Périphériques pertinents

- WAP121
- WAP321

Version du logiciel

- 1.0.3.4

Configurer le pont de groupe de travail

Note: Pour pouvoir activer le pont de groupe de travail, le clustering doit être activé dans le WAP. Si elle est désactivée, vous devez désactiver la configuration par point unique, qui à son tour active la mise en grappe. Tous les périphériques WAP qui participent au pont de groupe de travail doivent avoir des paramètres communs pour la radio, le mode IEEE 802.11, la bande passante du canal et le canal (audio non recommandé). Pour vous assurer que ces paramètres sont identiques sur tous les périphériques, recherchez les paramètres radio. Pour configurer ces paramètres, reportez-vous à l'article *Configuration des paramètres radio sans fil de base sur les points d'accès WAP121 et WAP321*.

Étape 1. Connectez-vous à l'utilitaire de configuration du point d'accès et choisissez **Wireless > Work Group Bridge**. La page *WorkGroup Bridge* s'ouvre :

WorkGroup Bridge

WorkGroup Bridge Mode: Enable

Infrastructure Client Interface

SSID: (Range: 2-32 Characters)

Security: (+)

VLAN ID: (Range: 1 - 4094, Default: 1)

Connection Status: Disconnected

Access Point Interface

Status: Enable

SSID: (Range: 2-32 Characters)

SSID Broadcast: Enable

Security: (+)

MAC Filtering:

VLAN ID: (Range: 1 - 4094, Default: 1)

Étape 2. Cochez **Enable** dans le champ *WorkGroup Bridge Mode* pour activer la fonctionnalité de pont de groupe de travail.

WorkGroup Bridge

WorkGroup Bridge Mode: Enable

Infrastructure Client Interface

SSID: (Range: 2-32 Characters)

Security: (+)

VLAN ID: (Range: 1 - 4094, Default: 1)

Connection Status: Disconnected

Access Point Interface

Status: Enable

SSID: (Range: 2-32 Characters)

SSID Broadcast: Enable

Security: (+)

MAC Filtering:

VLAN ID: (Range: 1 - 4094, Default: 1)


Étape 3. Entrez le nom SSID (Service Set Identifier) dans le champ *SSID* pour l'interface client de l'infrastructure.

WorkGroup Bridge

Refresh

WorkGroup Bridge Mode: Enable

Infrastructure Client Interface

SSID: (Range: 2-32 Characters) 

Security:

VLAN ID: (Range: 1 - 4094, Default: 1)

Connection Status: Disconnected

Access Point Interface

Status: Enable

SSID: (Range: 2-32 Characters)

SSID Broadcast: Enable

Security:

MAC Filtering:

VLAN ID: (Range: 1 - 4094, Default: 1)

Save

MAC Address	SSID
08:00:27:00:00:00	WPSU-Guest
08:00:27:00:00:00	(Non Broadcasting)
08:00:27:00:00:00	WPSU-Guest
08:00:27:00:00:00	WPSU-Guest
08:00:27:00:00:00	WPSU-Guest
08:00:27:00:00:00	WPSU-Guest
08:00:27:00:00:00	WPSU-Guest
08:00:27:00:00:00	WPSU-Guest
08:00:27:00:00:00	WPSU-Guest
08:00:27:00:00:00	(Non Broadcasting)
08:00:27:00:00:00	WPSU-Guest
08:00:27:00:00:00	(Non Broadcasting)
08:00:27:00:00:00	WPSU-Guest

Astuce : Vous pouvez également cliquer sur l'icône **Flèche** en regard du champ *SSID* pour rechercher des SSID voisins similaires. Cette option est activée uniquement si la détection des points d'accès est activée dans la détection des points d'accès indésirables, qui est désactivée par défaut. Reportez-vous à l'article *Détection des points d'accès non fiables sur les points d'accès WAP121 et WAP321* pour activer la détection des points d'accès non fiables.

Étape 4. Choisissez le type de sécurité pour authentifier une station client sur le périphérique WAP en amont (Infrastructure Client Interface) dans la liste déroulante *Sécurité*. Les valeurs possibles sont les suivantes :

WorkGroup Bridge

Refresh

WorkGroup Bridge Mode: Enable

Infrastructure Client Interface

SSID: (Range: 2-32 Characters)

Security:

-
-
-
-
 (+)

VLAN ID: (Range: 1 - 4094, Default: 1)

Connection Status:

Access Point Interface

Status: Enable

SSID: (Range: 2-32 Characters)

SSID Broadcast: Enable

Security: (+)

MAC Filtering:

VLAN ID: (Range: 1 - 4094, Default: 1)

Save

·Aucun : ouvrez ou non la sécurité. C'est la valeur par défaut. Si vous choisissez cette option, passez à l'étape 5.

·Static WEP : le WEP statique est la sécurité minimale et peut prendre en charge jusqu'à 4 clés de 64 à 128 bits. La même clé doit être utilisée dans tous les noeuds. Pour la configuration du WEP statique, accédez à [Static WEP](#).

·WPA Personal : WPA Personal est plus avancé que WEP et peut prendre en charge des clés de 8 à 63 caractères. La méthode de cryptage est RC4 pour WPA et Advanced Encryption Standard (AES) pour WPA2. WPA2 est recommandé car il dispose d'une norme de cryptage plus puissante. Pour la configuration de WPA personal, accédez à [WPA Personal for Client Interface](#).

·WPA Enterprise - WPA Enterprise est la sécurité la plus avancée et recommandée. Il utilise le protocole PEAP (Protected Extensible Authentication Protocol) dans lequel chaque utilisateur sans fil sous WAP est autorisé avec des noms d'utilisateur et des mots de passe individuels pouvant même prendre en charge les normes de cryptage AES. Il utilise également la sécurité de la couche de transport (TLS) en plus du protocole PEAP, dans lequel chaque utilisateur doit également fournir un certificat supplémentaire pour accéder au protocole. La méthode de cryptage est RC4 pour WPA et Advanced Encryption Standard (AES) pour WPA2. Pour la configuration de WPA Enterprise, accédez à [WPA Enterprise](#).

Note: En fonction du mode IEEE 802.11 choisi, la disponibilité des options ci-dessus peut varier.

Étape 5. Entrez l'ID de VLAN dans le champ *ID de VLAN* de l'interface client de l'infrastructure.

WorkGroup Bridge

WorkGroup Bridge Mode: Enable

Infrastructure Client Interface

SSID: (Range: 2-32 Characters)

Security: (+)

VLAN ID: (Range: 1 - 4094, Default: 1)

Connection Status: Disconnected

Access Point Interface

Status: Enable

SSID: (Range: 2-32 Characters)

SSID Broadcast: Enable

Security: (+)

MAC Filtering:

VLAN ID: (Range: 1 - 4094, Default: 1)

Étape 6. Cochez **Enable** dans le champ *Status* pour activer le pontage sur l'interface du point d'accès.

WorkGroup Bridge

WorkGroup Bridge Mode: Enable

Infrastructure Client Interface

SSID: (Range: 2-32 Characters)

Security: (+)

VLAN ID: (Range: 1 - 4094, Default: 1)

Connection Status: Disconnected

Access Point Interface

Status: Enable

SSID: (Range: 2-32 Characters)

SSID Broadcast: Enable

Security: (+)

MAC Filtering:

VLAN ID: (Range: 1 - 4094, Default: 1)

Étape 7. Entrez le SSID (Service Set Identifier) dans le nom de champ *SSID* de l'interface de point d'accès.

Étape 8. (Facultatif) Si vous souhaitez diffuser le SSID en aval, cochez la case **Activer** dans le champ *Diffusion SSID* à diffuser. Il est activé par défaut.

Étape 9. Sélectionnez le type de sécurité pour authentifier les stations clientes en aval sur le périphérique WAP (Access Point Interface) dans la liste déroulante Sécurité. Les valeurs possibles sont les suivantes :

WorkGroup Bridge

Refresh

WorkGroup Bridge Mode: Enable

Infrastructure Client Interface

SSID: (Range: 2-32 Characters)

Security: (+)

VLAN ID: (Range: 1 - 4094, Default: 1)

Connection Status: Disconnected

Access Point Interface

Status: Enable

SSID: (Range: 2-32 Characters)

SSID Broadcast: Enable

Security: (+)

MAC Filtering:

VLAN ID: (Range: 1 - 4094, Default: 1)

Save

·Aucun : ouvrez ou non la sécurité. C'est la valeur par défaut. Ignorez l'étape 10 si vous choisissez cette option.

·Static WEP : le WEP statique est la sécurité minimale et peut prendre en charge jusqu'à 4 clés de 64 à 128 bits. Pour la configuration du WEP statique, accédez à [Static WEP](#)

·WPA Personal : WPA Personal est plus avancé que WEP et peut prendre en charge des clés de 8 à 63 caractères. La méthode de cryptage est TKIP (Temporal Key Integrity Protocol) ou Counter Cipher Mode avec CCMP (Block Chaining Message Authentication Code Protocol). WPA2 avec CCMP est recommandé car il possède une norme de cryptage AES (Advanced Encryption Standard) plus puissante que la norme TKIP qui utilise uniquement une norme RC4 64 bits. Pour la configuration de WPA personal, accédez à [WPA Personal for Access Point Interface](#).

Étape 10. Choisissez le type de filtrage MAC que vous souhaitez configurer pour l'interface de point d'accès dans la liste déroulante *Filtrage MAC*. Lorsqu'elle est activée, l'accès au WAP est accordé ou refusé aux utilisateurs en fonction de l'adresse MAC du client qu'ils utilisent. Les valeurs possibles sont les suivantes :

WorkGroup Bridge

Refresh

WorkGroup Bridge Mode: Enable

Infrastructure Client Interface

SSID: (Range: 2-32 Characters)

Security: (+)

VLAN ID: (Range: 1 - 4094, Default: 1)

Connection Status: Disconnected

Access Point Interface

Status: Enable

SSID: (Range: 2-32 Characters)

SSID Broadcast: Enable

Security: (+)

MAC Filtering: (Dropdown menu with options: Disabled, Local, RADIUS)

VLAN ID: (Range: 1 - 4094, Default: 1)

Save

·désactivé : tous les clients peuvent accéder au réseau en amont. C'est la valeur par défaut.

·local : l'ensemble de clients qui peuvent accéder au réseau en amont est limité aux clients spécifiés dans une liste d'adresses MAC définie localement.

·Radius : l'ensemble de clients qui peuvent accéder au réseau en amont est limité aux clients spécifiés dans une liste d'adresses MAC sur un serveur RADIUS.

Étape 11. Saisissez l'ID VLAN dans le champ VLAN ID de l'interface client du point d'accès.

WorkGroup Bridge

WorkGroup Bridge Mode: Enable

Infrastructure Client Interface

SSID: (Range: 2-32 Characters)

Security: (+)

VLAN ID: (Range: 1 - 4094, Default: 1)

Connection Status: Disconnected

Access Point Interface

Status: Enable

SSID: (Range: 2-32 Characters)

SSID Broadcast: Enable

Security: (+)

MAC Filtering:

VLAN ID: (Range: 1 - 4094, Default: 1)

Note: Pour permettre le pontage des paquets, la configuration VLAN pour l'interface de point d'accès et l'interface filaire doit correspondre à celle de l'interface client de l'infrastructure.

Étape 12. Cliquez sur **Save** pour enregistrer les paramètres.

[WEP statique](#)

Infrastructure Client Interface

SSID: (Range: 2-32 Characters)

Security:

Transfer Key Index:

Key Length: 64 bits 128 bits

Key Type: ASCII Hex

WEP Keys: (Required: 26)

1:

2:

3:

4:

VLAN ID: (Range: 1 - 4094, Default: 1)

Connection Status: **Disconnected**

Étape 1. Lorsque vous sélectionnez Static WEP, des champs supplémentaires s'affichent. Dans la liste déroulante du champ *Index de clé de transfert*, sélectionnez un index de clé. Les valeurs disponibles sont 1, 2, 3 et 4. La valeur par défaut est 1. L'index de clé est différent pour les différents WLAN. Les périphériques connectés à un réseau local sans fil particulier doivent avoir le même index de clé. Cette clé est utilisée pour chiffrer les données à des fins de communication.

Étape 2. Dans le champ *Longueur de clé*, sélectionnez la case d'option **64 bits** ou **128 bits**. Indique la longueur de la clé utilisée.

Étape 3. Cliquez sur la case d'option souhaitée dans le champ *Type de clé*. Les clés WEP sont généralement en hexadécimal.

- ASCII — ASCII (American Standard Code for Information Interchange) est un système de codage de caractères basé sur l'alphabet anglais codé en 128 caractères spécifiés.

- HEX — HEX (hexadécimal) est un système de numération pondérée avec la base 16. Il utilise 16 symboles distincts 0-9 pour les nombres de 0 à 9 et A, B, C, D, E, F pour représenter des valeurs comprises entre 10 et 15. Chaque hexadécimal représente quatre chiffres binaires.

Étape 4. Entrez jusqu'à quatre clés WEP dans les quatre champs suivants marqués comme 1,2,3 et 4 sous le champ *Clé WEP*. Il s'agit d'une chaîne entrée comme clé. La longueur de la clé varie selon la longueur et le type de la clé. La longueur requise est indiquée en regard du champ WEP Key (Clé WEP). Les chaînes de clé WEP doivent correspondre dans tous les noeuds WAP (AP et clients) et doivent être situées dans le même champ. Cela signifie que si la chaîne 1 est la clé 1 dans un périphérique, la chaîne 1 doit également être la clé 1 dans les autres périphériques du pont de groupe de travail.

WPA Personal pour interface client

Infrastructure Client Interface

SSID: test (Range: 2-32 Characters)

Security: WPA Personal

WPA Versions: WPA WPA2

Key: (Range: 8-63 Characters)

VLAN ID: 1 (Range: 1 - 4094, Default: 1)

Connection Status: Disconnected

Étape 1. Vérifiez les versions WPA souhaitées dans le champ *WPA Versions*. Généralement, WPA est choisi uniquement si certains des WAP du système de pont ne prennent pas en charge WPA2. WPA2 est le plus avancé et recommandé.

·WPA : si le réseau comporte des stations clientes qui prennent en charge la version originale de WPA.

·WPA2 : si toutes les stations clientes du réseau prennent en charge WPA2. Cette version de protocole fournit la meilleure sécurité selon la norme IEEE 802.11i.

Étape 2. Entrez la clé WPA partagée dans le champ *Key*. La clé peut inclure des caractères alphanumériques, des majuscules et des minuscules et des caractères spéciaux.

WPA personnel pour l'interface de point d'accès

Security: WPA Personal

WPA Versions: WPA WPA2

Cipher Suites: TKIP CCMP (AES)

Key: (Range: 8-63 Characters)

Broadcast Key Refresh Rate: 300 (Range: 0-86400)

Étape 1. Vérifiez les versions WPA souhaitées dans le champ *WPA Versions*. Généralement, WPA est choisi uniquement si certains des WAP concernés ne prennent pas en charge WPA2 ; sinon, WPA2 est recommandé.

·WPA : si le réseau comporte des stations clientes qui prennent en charge la version originale de WPA.

·WPA2 : si toutes les stations clientes du réseau prennent en charge WPA2. Cette version de protocole fournit la meilleure sécurité selon la norme IEEE 802.11i.

Note: Si le réseau est un mélange de clients WPA et WPA2, cochez les deux cases. Cela permet aux stations client WPA et WPA2 de s'associer et de s'authentifier, mais utilise le

WPA2 plus robuste pour les clients qui le prennent en charge.

Étape 2. Choisissez les suites de chiffrement souhaitées dans le champ *Suites de chiffrement*.

·TKIP : le protocole TKIP (Temporal Key Integrity Protocol) utilise uniquement une norme RC4 64 bits.

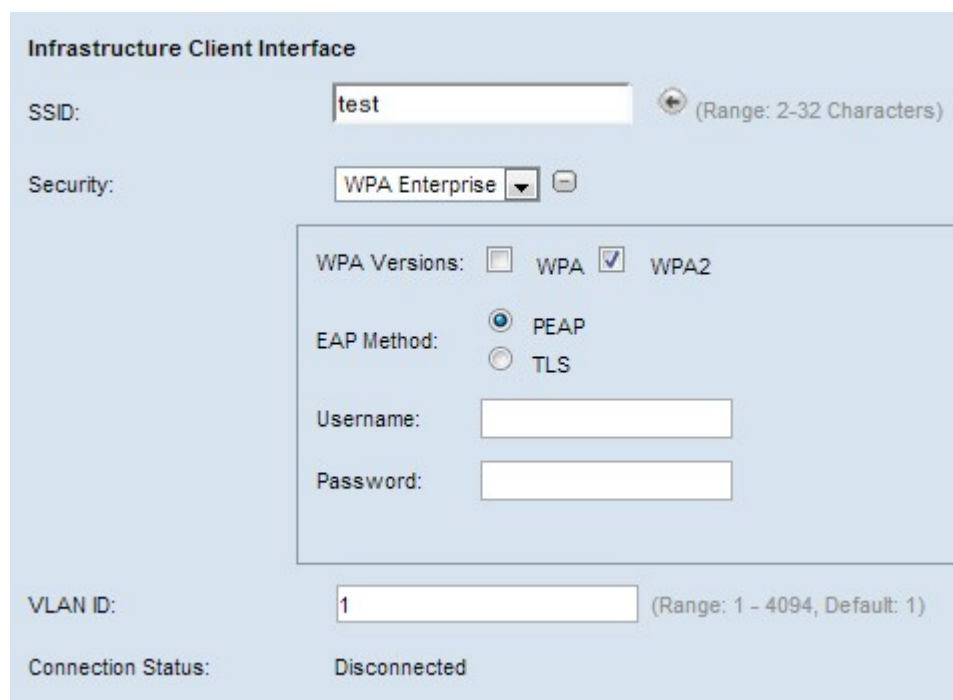
·CCMP (AES) : le mode de chiffrement de compteur avec le protocole CCMP (Block Chaining Message Authentication Code Protocol) est le protocole de sécurité utilisé par AES (Advanced Encryption Standard). WPA2 avec CCMP est recommandé car il dispose d'une norme de cryptage plus puissante.

Note: Vous pouvez choisir l'un ou l'autre ou les deux. Les clients TKIP et AES peuvent être associés au périphérique WAP.

Étape 3. Entrez la clé WPA partagée dans le champ *Key*. La clé peut inclure des caractères alphanumériques, des majuscules et des minuscules et des caractères spéciaux.

Étape 4. Entrez le taux dans le champ *Broadcast Key Refresh Rate*.

WPA Enterprise



The screenshot shows the 'Infrastructure Client Interface' configuration page. The SSID is set to 'test'. The Security is set to 'WPA Enterprise'. Under 'WPA Versions', both 'WPA' and 'WPA2' are selected. The 'EAP Method' is set to 'PEAP'. There are empty input fields for 'Username' and 'Password'. The 'VLAN ID' is set to '1'. The 'Connection Status' is 'Disconnected'.

Étape 1. Vérifiez les versions WPA souhaitées dans le champ *WPA Versions*. Généralement, WPA est choisi uniquement si certains des WAP du système de pont ne prennent pas en charge WPA2. WPA2 est le plus avancé et recommandé.

·WPA : si le réseau comporte des stations clientes qui prennent en charge la version originale de WPA.

·WPA2 : si toutes les stations clientes du réseau prennent en charge WPA2. Cette version de protocole fournit la meilleure sécurité selon la norme IEEE 802.11i.

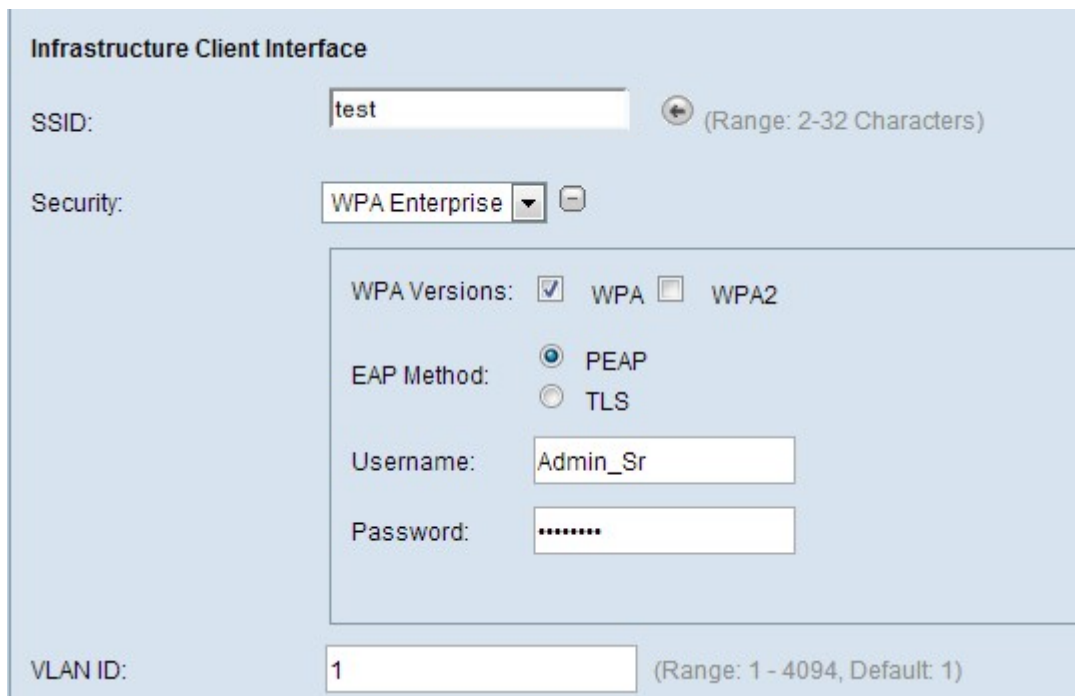
Note: Si le réseau est un mélange de clients WPA et WPA2, cochez les deux cases. Cela permet aux stations client WPA et WPA2 de s'associer et de s'authentifier, mais utilise le WPA2 plus robuste pour les clients qui le prennent en charge.

Étape 2. Cliquez sur la case d'option appropriée pour choisir entre les deux méthodes EAP.

·PEAP — Protected EAP. Il s'appuie sur TLS mais évite l'installation de certificats numériques sur chaque client. Au lieu de cela, il fournit l'authentification par un nom d'utilisateur et un mot de passe. Si vous choisissez cette option, accédez à [PEAP \(Protected Extensible Authentication Protocol\)](#).

·TLS : authentification par échange de certificats numériques. Si vous choisissez cette option, accédez à [TLS \(Transport Layer Security\)](#).

[PEAP \(Protected Extensible Authentication Protocol\)](#)



The screenshot shows the 'Infrastructure Client Interface' configuration page. The SSID is set to 'test'. The Security is set to 'WPA Enterprise'. Under 'WPA Versions', 'WPA' is selected. Under 'EAP Method', 'PEAP' is selected. The Username is 'Admin_Sr' and the Password is masked with dots. The VLAN ID is set to '1'.

SSID:	test	(Range: 2-32 Characters)
Security:	WPA Enterprise	
WPA Versions:	<input checked="" type="checkbox"/> WPA	<input type="checkbox"/> WPA2
EAP Method:	<input checked="" type="radio"/> PEAP	<input type="radio"/> TLS
Username:	Admin_Sr	
Password:	*****	
VLAN ID:	1	(Range: 1 - 4094, Default: 1)

Étape 1. Entrez un nom d'utilisateur dans le champ *Nom d'utilisateur*.

Étape 2. Entrez un mot de passe dans le champ *Mot de passe*.

[TLS \(Transport Layer Security\)](#)

Infrastructure Client Interface

SSID: (Range: 2-32 Characters)

Security:

WPA Versions: WPA WPA2

EAP Method: PEAP TLS

Identity:

Private Key:

Certificate File Present:

Certificate Expiration Date:

Transfer Method: HTTP TFTP

Certificate File: No file chosen

Étape 1. Sélectionnez le mode de transfert pour télécharger un fichier de certificat pour l'authentification TLS.

·HTTP : si vous voulez télécharger le certificat à partir d'un serveur Web de PC. Si vous choisissez ceci, accédez à [HTTP](#).

·TFTP : si vous voulez télécharger le certificat à partir d'un serveur de fichiers. Si vous choisissez cette option, accédez à [TFTP](#).

[HTTP](#)

Transfer Method: HTTP TFTP

Filename: mini_httpd (2).pfx

Étape 1. Cliquez sur **Choisir un fichier** pour sélectionner un fichier de certificat. Il doit s'agir d'un fichier de type certificat avec l'extension .pem, .pfx, etc. Sinon, le téléchargement de fichier échouera.

[TFTP](#)

Transfer Method: HTTP
 TFTP

Filename

TFTP Server IPv4 Address:

Étape 1. Entrez le nom du fichier de certificat dans le champ *Nom de fichier*.

Étape 2. Saisissez l'adresse IP du serveur TFTP.

Note: Le champ Certificate File Transfer indique si un certificat est présent dans le WAP et le champ Certificate Expiration Date indique la date d'expiration du présent certificat.

Étape 3. Cliquez sur **Upload** pour télécharger le fichier sur le périphérique.