Télécharger un certificat personnalisé dans le point d'accès sans fil professionnel Cisco

Objectif

L'objectif de ce document est de montrer comment télécharger un certificat personnalisé sur votre point d'accès (AP) Cisco Business Wireless (CBW).

Périphériques pertinents | Version logicielle

- Point d'accès Cisco Business Wireless 140AC | 10.6.1.0 (télécharger la dernière version)
- Point d'accès Cisco Business Wireless 145AC | 10.6.1.0 (télécharger la dernière version)
- Point d'accès Cisco Business Wireless 240AC | 10.6.1.0 (télécharger la dernière version)

Introduction

Dans la version 10.6.1.0 et ultérieure du microprogramme des points d'accès CBW, vous pouvez désormais importer vos propres certificats WEBAUTH (qui gère la page du portail captif) ou WEBADMIN (la page de gestion des points d'accès principaux CBW) dans l'interface utilisateur Web qui peut être approuvée par vos périphériques et systèmes internes. Par défaut, les pages WEBAUTH et WEBADMIN utilisent des certificats auto-signés qui ne sont généralement pas approuvés et peuvent générer des avertissements de certificat lorsque vous tentez de vous connecter à votre périphérique.

Avec cette nouvelle fonctionnalité, vous pouvez facilement télécharger des certificats personnalisés sur votre point d'accès CBW. Commençons tout de suite.

Conditions préalables

- Vérifiez que vous avez mis à niveau le micrologiciel du point d'accès CBW vers la

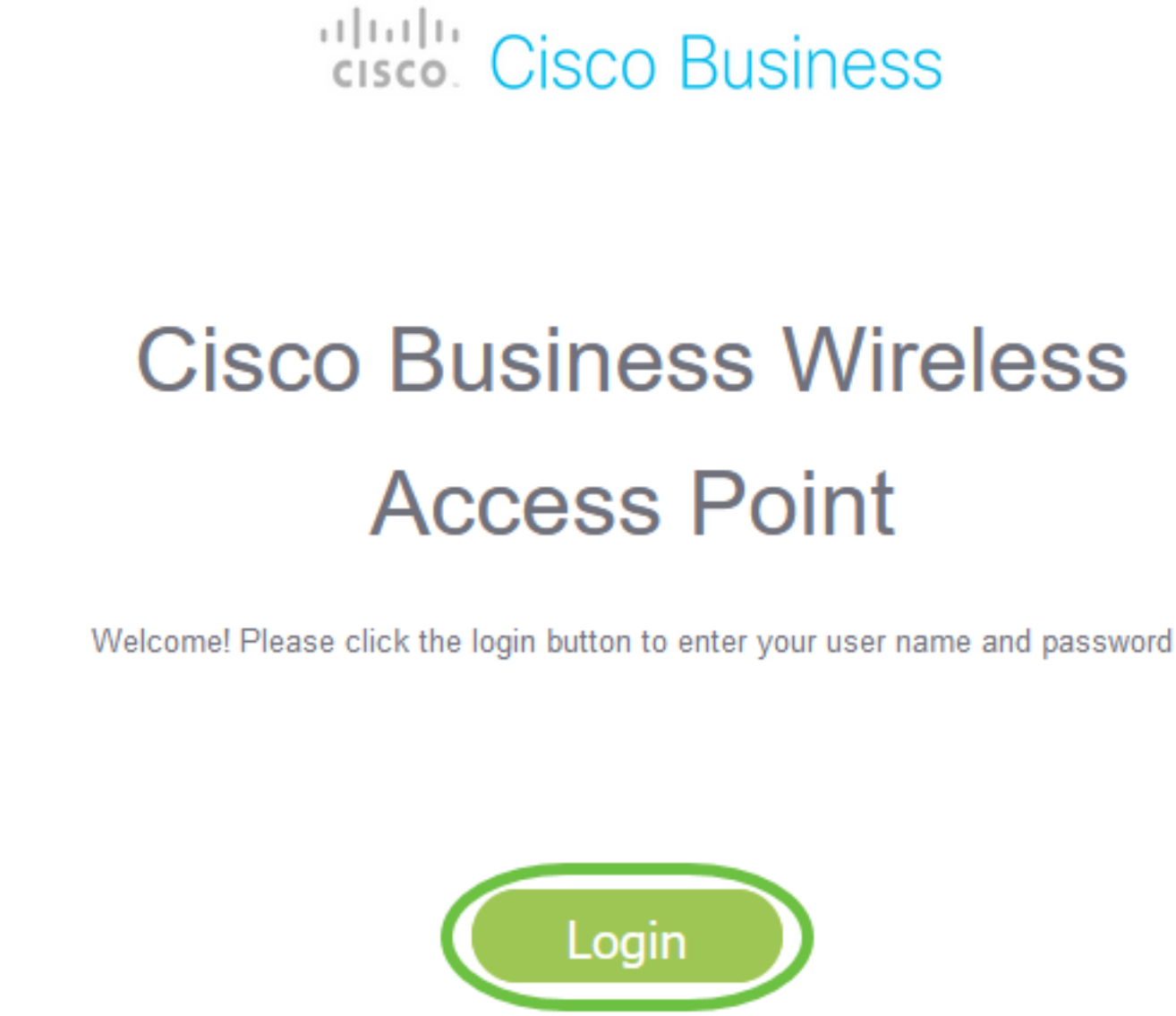
version 10.6.1.0. Cliquez sur ce bouton pour obtenir des instructions détaillées sur la mise à jour du micrologiciel.

- Une autorité de certification (CA) privée ou interne est nécessaire pour émettre les certificats WEBAUTH ou WEBADMIN nécessaires pour CBW. Les certificats peuvent ensuite être installés sur n'importe quel PC de gestion qui peut se connecter à l'interface utilisateur Web de CBW.
- Le certificat d'autorité de certification racine correspondant doit être installé dans le navigateur client pour utiliser le certificat personnalisé pour un accès captif au portail ou à la gestion afin d'éviter les avertissements de certificat potentiels.
- CBW utilise une adresse IP 192.0.2.1 redirigée en interne pour la redirection du portail captif. Il est donc préférable d'inclure ce nom sous le nom commun (CN) ou le nom alternatif du sujet (SAN) du certificat WEBAUTH.
- Les certificats WEBADMIN doivent être nommés comme suit : CN-cisobusiness.cisco ; SAN doit être dns-ciscobusiness.cisco ; si une adresse IP statique est utilisée, le SAN peut également inclure dns=<adresse ip>.

Télécharger des certificats

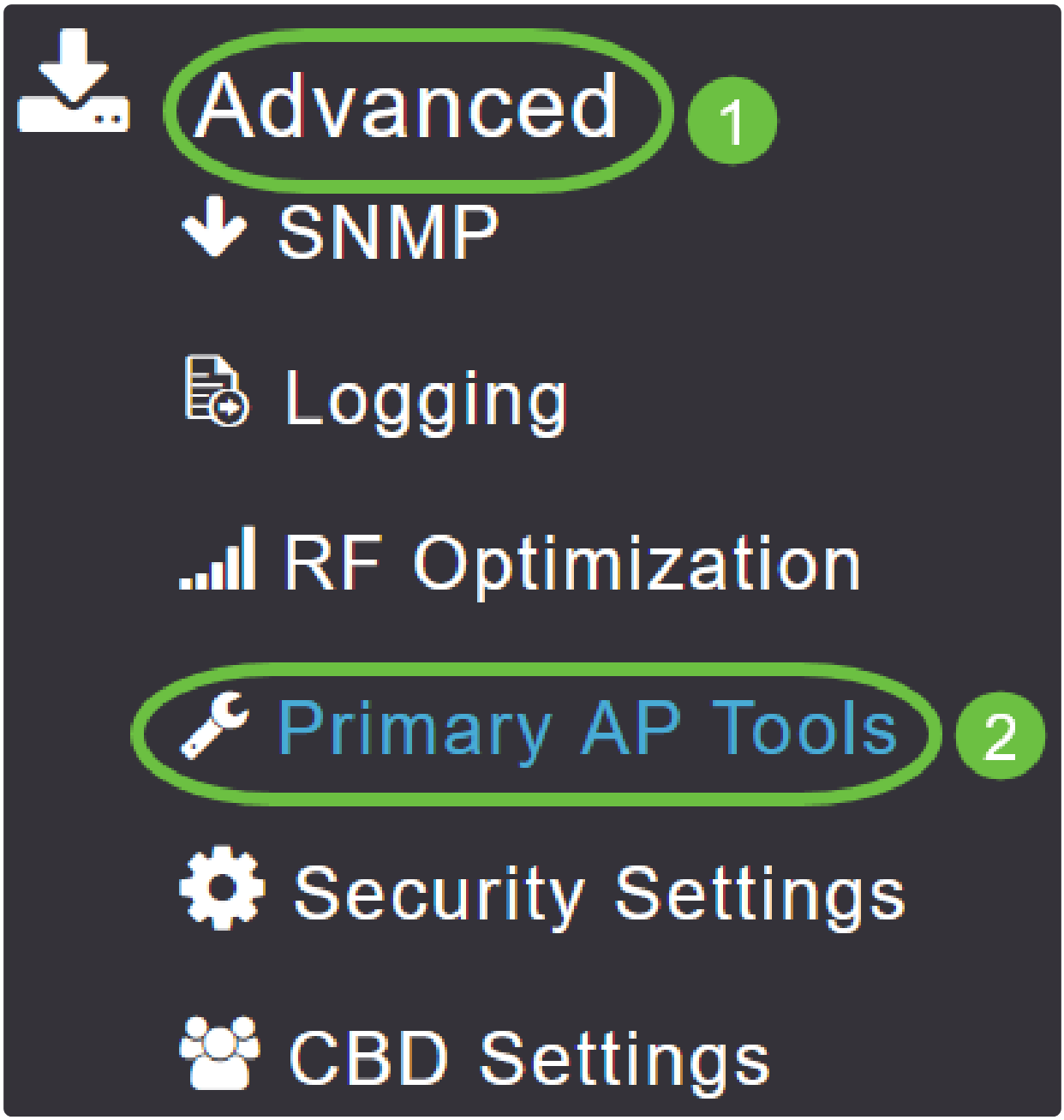
Étape 1

Connectez-vous à l'interface utilisateur Web du point d'accès CBW.



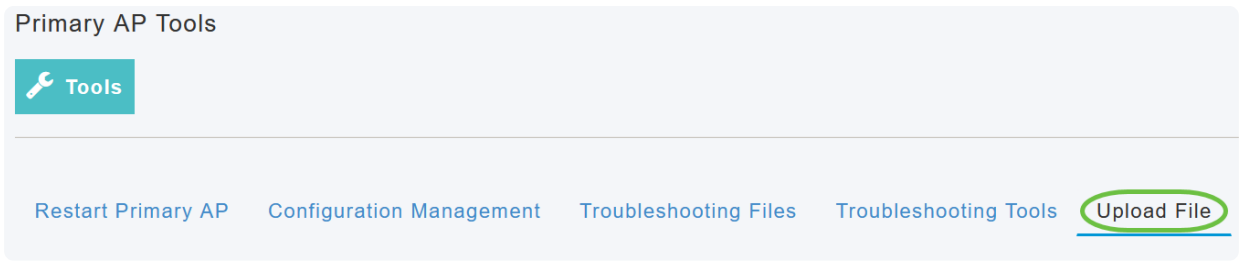
Étape 2

Pour télécharger des certificats, accédez à Avancé > Outils du point d'accès principal.



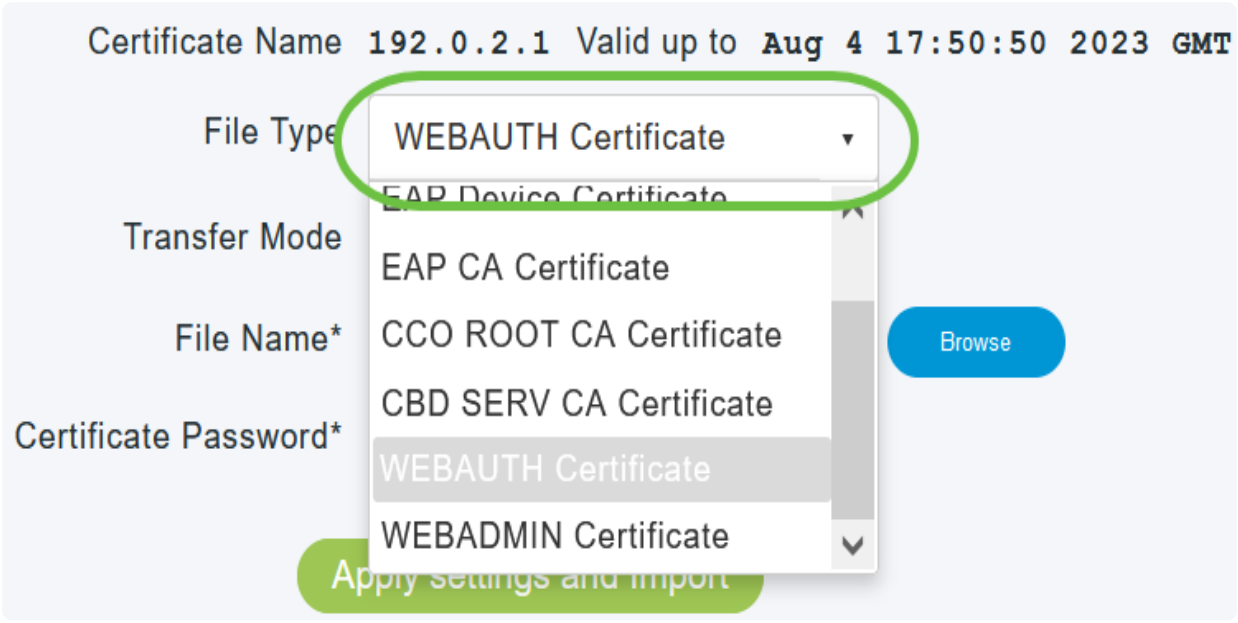
Étape 3

Sélectionnez l'onglet Télécharger un fichier.



Étape 4

Dans le menu déroulant File Type, choisissez WEBAUTH ou WEBADMIN Certificate.



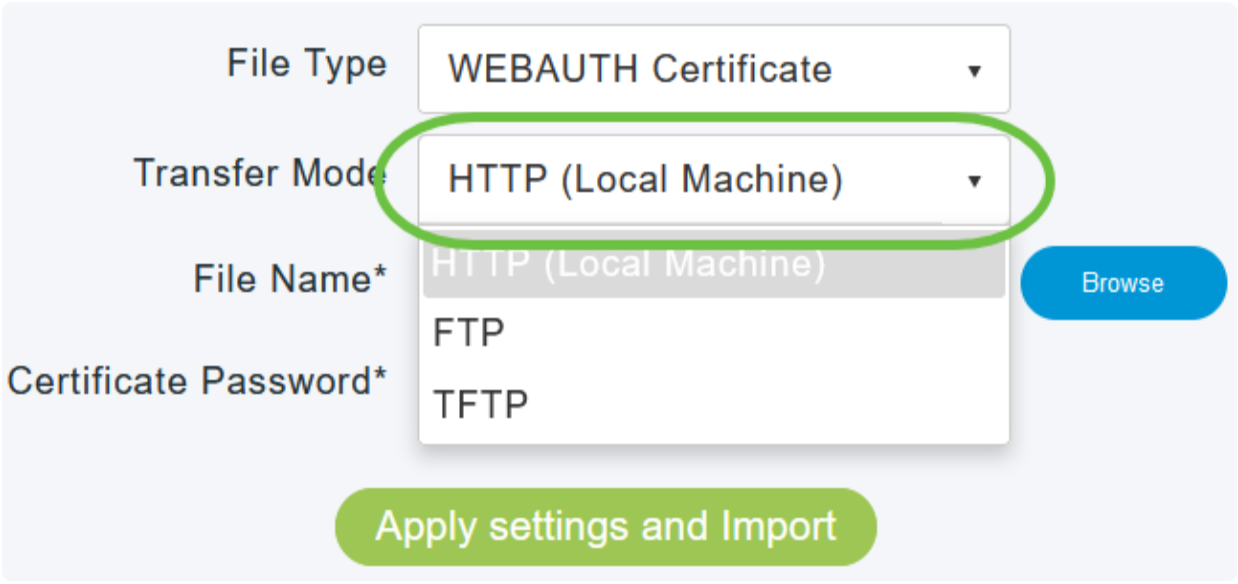
> ⓘ Note:
> Les fichiers DOIVENT être au format PEM et contenir les clés publique et privée. Il doit également être protégé par mot de passe. Les certificats WEBAUTH et WEBADMIN DOIVENT avoir un nom commun (CN) sous le nom ciscobusiness.cisco. Vous devrez donc utiliser une autorité de certification interne pour émettre des certificats.

Étape 5

Choisissez le Mode de transfert dans le menu déroulant. Les options sont les suivantes :

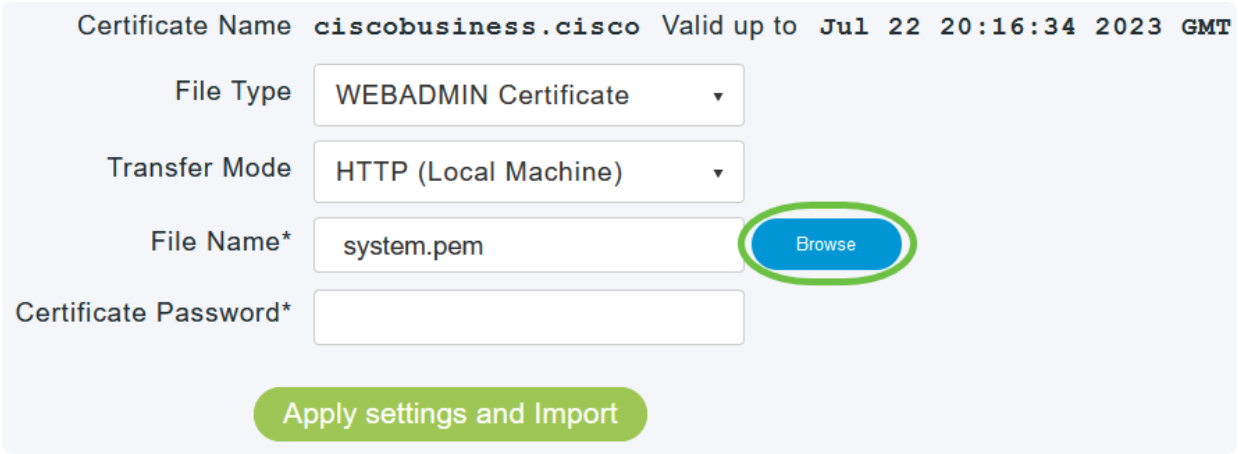
- HTTP (ordinateur local)
- FTP
- TFTP

Dans cet exemple, HTTP est sélectionné.



Étape 6

Cliquez sur Browse.

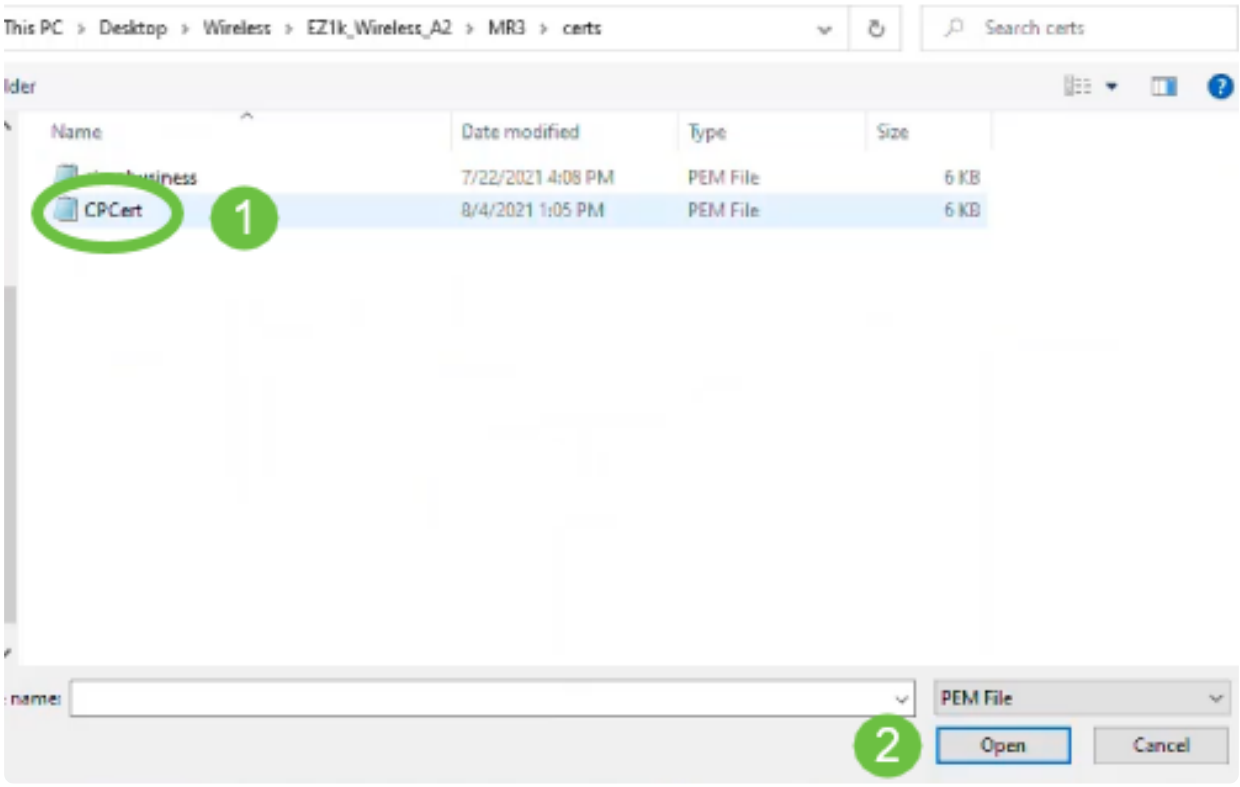


ⓘ Note:

Si le mode de transfert est FTP ou TFTP, entrez l'adresse IP du serveur, le chemin d'accès au fichier et d'autres champs obligatoires.

Étape 7

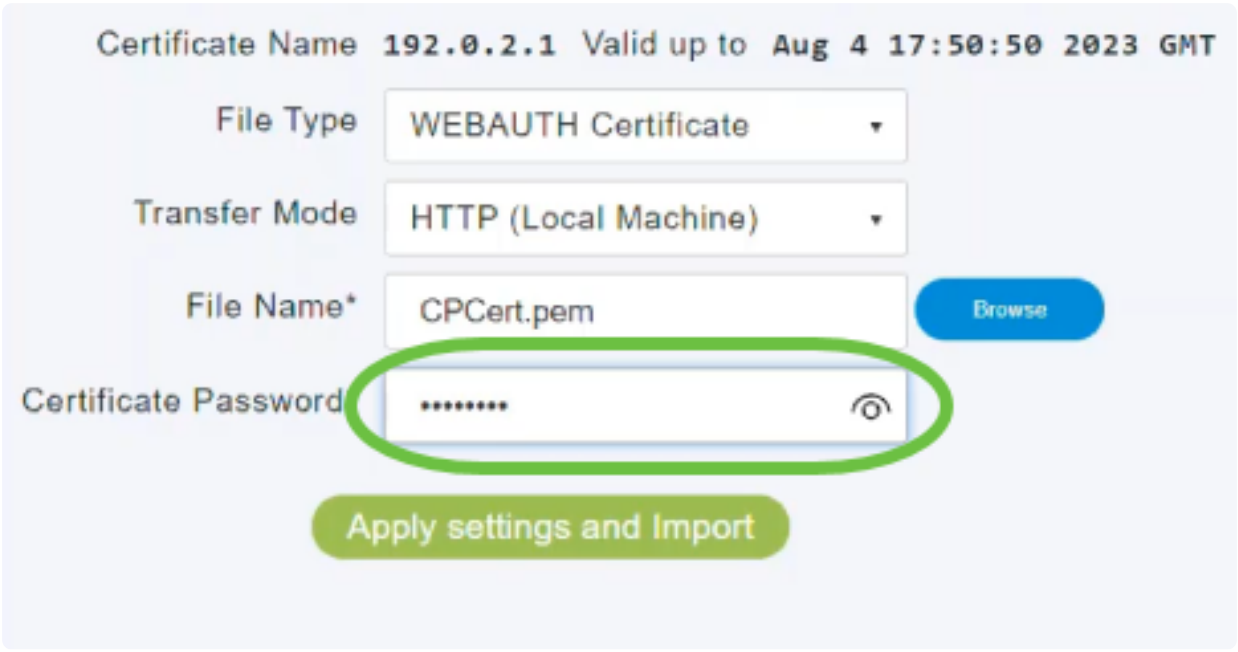
Téléchargez le fichier à partir de votre ordinateur local en naviguant jusqu'au dossier contenant le certificat personnalisé. Sélectionnez le fichier de certificat et cliquez sur Ouvrir.



> ⓘ Note:
>
> Le certificat doit être un fichier PEM. Pour télécharger correctement les certificats WEBADMIN, assurez-vous d'inclure la chaîne de certificats complète qui est le certificat du périphérique, le certificat CA émetteur et le certificat CA racine.

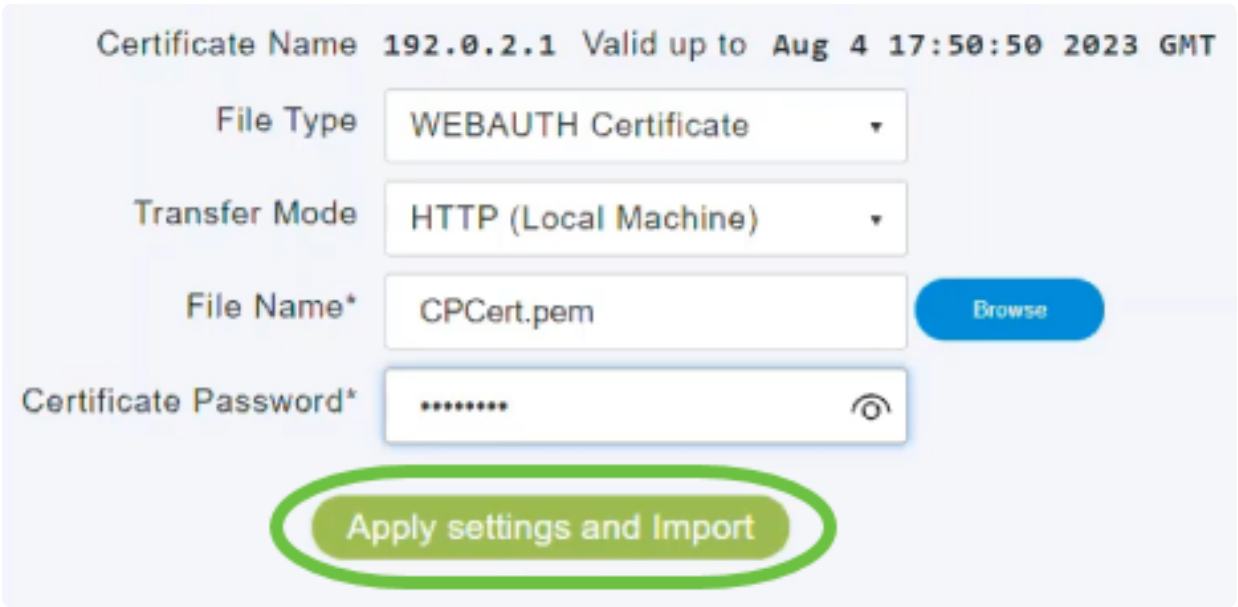
Étape 8

Saisissez le mot de passe du certificat.



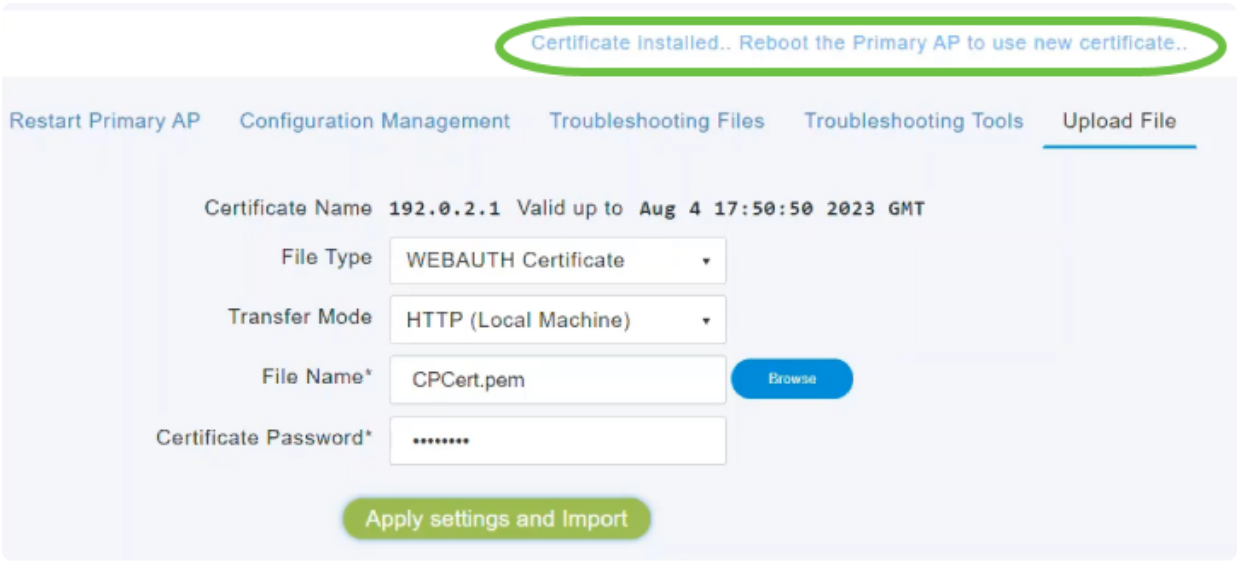
Étape 9

Cliquez sur Appliquer les paramètres et Importer.



Étape 10

Vous verrez une notification une fois que le certificat aura été correctement installé. Redémarrez le point d'accès principal.



> ⓘ Note:
>
> Pour modifier le certificat, il vous suffit de télécharger un nouveau certificat. Cette opération écrasera le certificat qui a été précédemment installé. Si vous voulez revenir au certificat auto-signé par défaut, vous devrez réinitialiser en usine l'AP principal.

Conclusion

Vous êtes tous prêts ! Vous venez de télécharger des certificats personnalisés sur votre point d'accès CBW.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.