

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 Cisco Business Wireless (CBW).

Périphériques pertinents | Version du logiciel

- 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 micrologiciel 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 CBW principaux) 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 fiables et peuvent donner lieu à des avertissements de certificat lorsque vous essayez de vous connecter à votre périphérique.

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

Conditions préalables

- Vérifiez que vous avez mis à niveau le micrologiciel du point d'accès CBW vers 10.6.1.0. [Cliquez sur si vous souhaitez 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 du client pour utiliser le certificat personnalisé pour l'accès au portail captif ou à la gestion afin d'éviter les avertissements de certificat potentiels.
- CBW utilise une adresse IP redirigée en interne 192.0.2.1 pour la redirection du portail captif. Il est donc préférable d'inclure ce nom comme nom commun (CN) ou nom de

remplacement d'objet (SAN) du certificat WEBAUTH.

- Les exigences de dénomination des certificats WEBADMIN sont les suivantes : CN-cisobbusiness.cisco ; SAN doit être dns-ciscobusiness.cisco ; si une adresse IP statique est utilisée, le SAN peut également inclure dns=<adresse ip>.

Télécharger les certificats

Étape 1

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



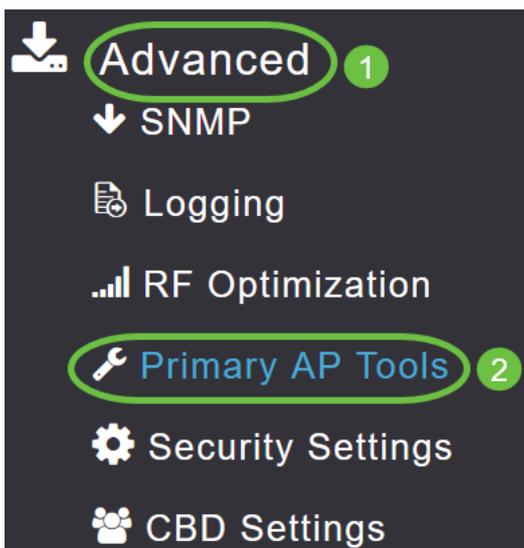
Cisco Business Wireless Access Point

Welcome! Please click the login button to enter your user name and password



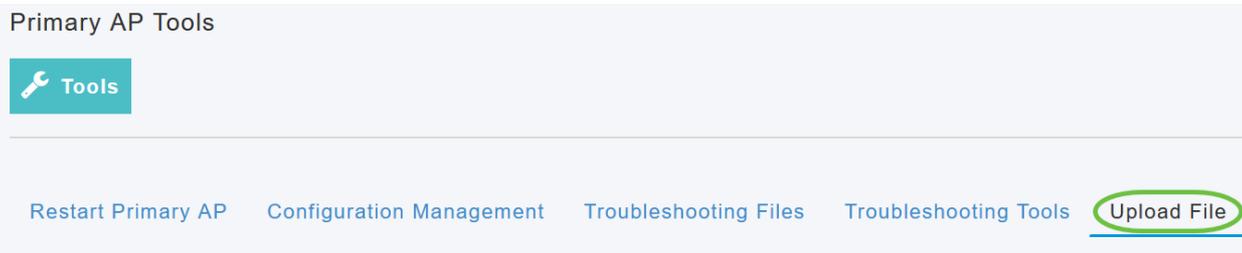
Étape 2

Pour télécharger des certificats, accédez à **Advanced > Primary AP Tools**.



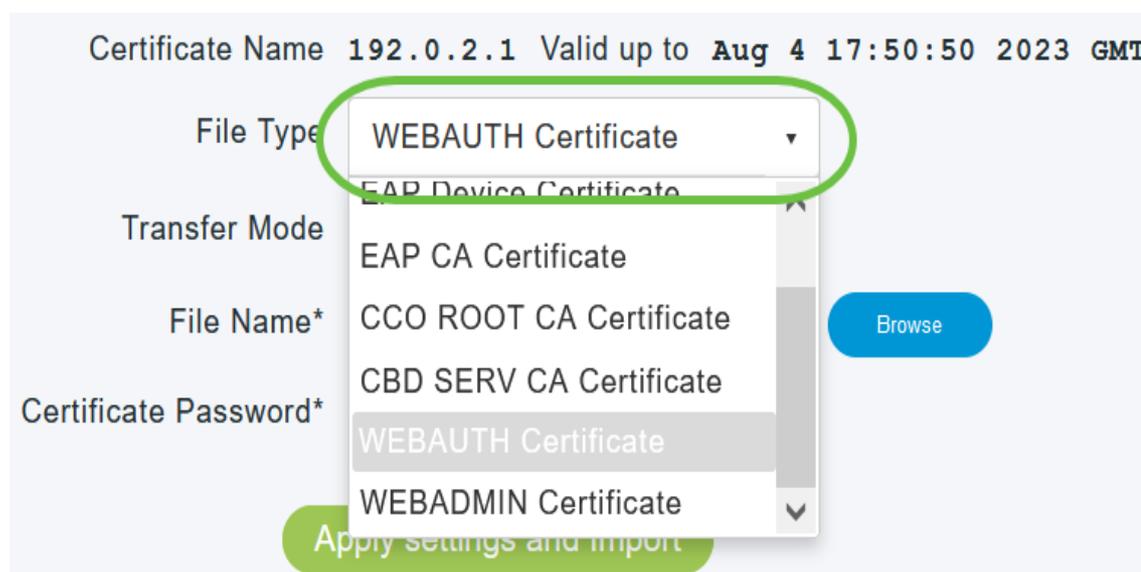
Étape 3

Sélectionnez l'onglet **Télécharger le fichier**.



Étape 4

Dans le menu déroulant *Type de fichier*, sélectionnez *WEBAUTH* ou *WEBADMIN Certificate*.



Les fichiers DOIVENT être au format PEM et contenir les clés Public et Private. Il doit également être protégé par mot de passe. Les certificats WEBAUTH et WEBADMIN DOIVENT avoir un nom commun (CN) en tant que ciscobusiness.cisco. Vous devez donc utiliser une autorité de certification interne pour émettre des certificats.

Étape 5

Sélectionnez le *mode de transfert* dans le menu déroulant. Les options sont les suivantes :

- *HTTP (machine locale)*
- *FTP*
- *TFTP*

Dans cet exemple, **HTTP** est sélectionné.

File Type

Transfer Mode:

File Name*

Certificate Password*

Étape 6

Cliquez sur **Browse**.

Certificate Name `ciscobusiness.cisco` Valid up to `Jul 22 20:16:34 2023 GMT`

File Type

Transfer Mode

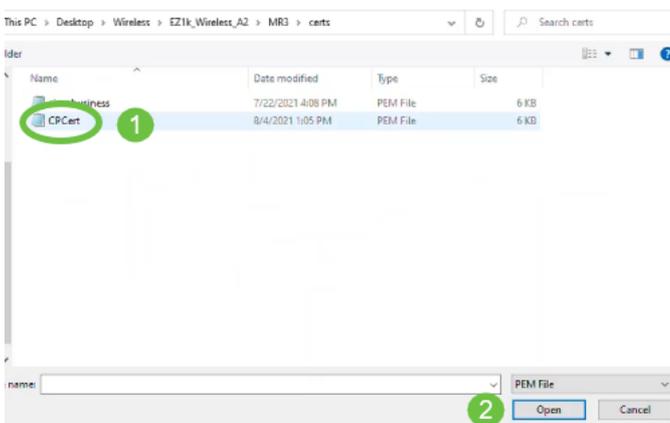
File Name*

Certificate Password*

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

Étape 7

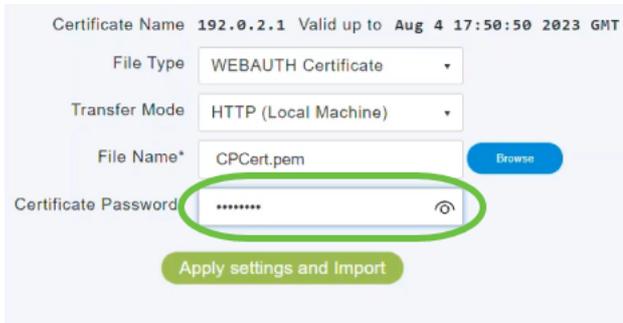
Téléchargez le fichier à partir de votre ordinateur local en accédant au dossier contenant le certificat personnalisé. Sélectionnez le fichier de certificat et cliquez sur **Ouvrir**.



Le certificat doit être un fichier PEM.

Étape 8

Entrez le *mot de passe du certificat*.



Certificate Name 192.0.2.1 Valid up to Aug 4 17:50:50 2023 GMT

File Type WEBAUTH Certificate

Transfer Mode HTTP (Local Machine)

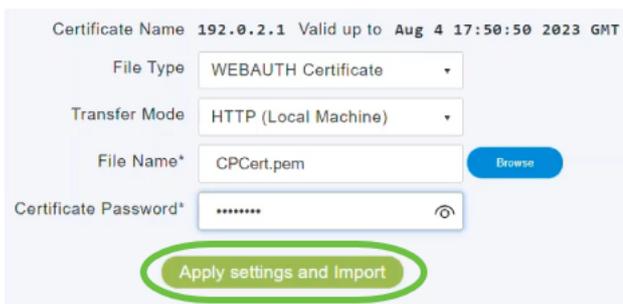
File Name* CPCert.pem [Browse](#)

Certificate Password* [👁](#)

[Apply settings and Import](#)

Étape 9

Cliquez sur **Appliquer les paramètres et Importer**.



Certificate Name 192.0.2.1 Valid up to Aug 4 17:50:50 2023 GMT

File Type WEBAUTH Certificate

Transfer Mode HTTP (Local Machine)

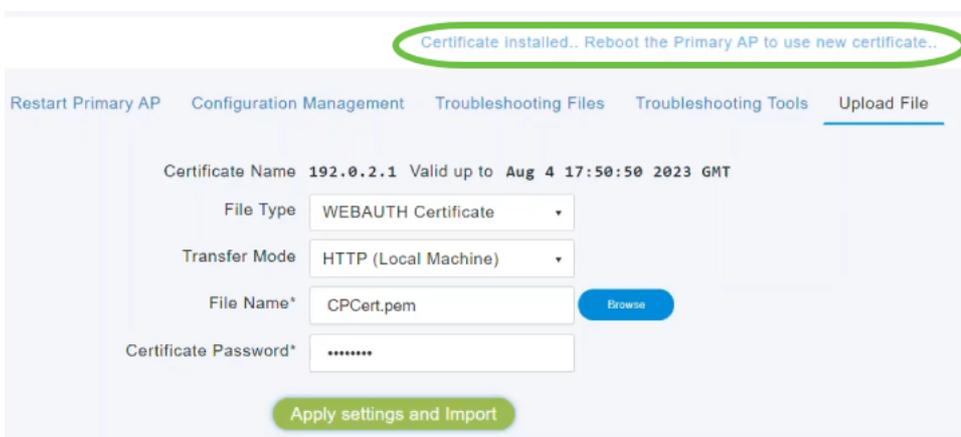
File Name* CPCert.pem [Browse](#)

Certificate Password* [👁](#)

[Apply settings and Import](#)

Étape 10

Une notification s'affiche une fois le certificat installé. Redémarrez le point d'accès principal.



Certificate installed.. Reboot the Primary AP to use new certificate..

[Restart Primary AP](#) [Configuration Management](#) [Troubleshooting Files](#) [Troubleshooting Tools](#) [Upload File](#)

Certificate Name 192.0.2.1 Valid up to Aug 4 17:50:50 2023 GMT

File Type WEBAUTH Certificate

Transfer Mode HTTP (Local Machine)

File Name* CPCert.pem [Browse](#)

Certificate Password* [👁](#)

[Apply settings and Import](#)

Pour modifier le certificat, il suffit de télécharger un nouveau certificat. Ceci écrasera le certificat précédemment installé. Si vous voulez revenir au certificat auto-signé par défaut, vous devez réinitialiser l'AP principal en usine.

Conclusion

Vous êtes tous prêts ! Vous avez maintenant téléchargé les certificats personnalisés sur votre point d'accès CBW.