

Upload Custom Certificate in Cisco Business Wireless Access Point

Objective

The objective of this document is to show how to upload a custom certificate on your Cisco Business Wireless (CBW) Access Point (AP).

Applicable Devices | Software Version

- Cisco Business Wireless 140AC Access Point | 10.6.1.0 ([Download latest](#))
- Cisco Business Wireless 145AC Access Point | 10.6.1.0 ([Download latest](#))
- Cisco Business Wireless 240AC Access Point | 10.6.1.0 ([Download latest](#))

Introduction

In CBW APs firmware version 10.6.1.0 and above, you can now import your own WEBAUTH (that handles captive portal page) or WEBADMIN (the CBW Primary AP Management page) certificates into the web user interface (UI) that may be trusted by your internal devices and systems. By default, WEBAUTH and WEBADMIN pages use self-signed certificates that are usually not trusted and can lead to certificate warnings when you try to connect to your device.

With this new feature, you can easily upload custom certificates on your CBW AP. Let's get started.

Prerequisites

- Make sure you have upgraded the CBW AP firmware to 10.6.1.0. [Click if you would like step-by-step instructions on doing a firmware update.](#)
- A private or internal Certificate Authority (CA) is needed to issue the WEBAUTH or WEBADMIN certificates needed for CBW. The certificates can then be installed on any management PC that can connect to the CBW web UI.
- The corresponding Root CA certificate must be installed in the client browser to use the custom certificate for captive portal or management access to avoid potential certificate warnings.

- CBW uses an internally redirected IP address 192.0.2.1 for captive portal redirection. So, it is best to include this as the WEBAUTH certificate's Common Name (CN) or Subject Alternative Name (SAN).
- Naming requirements for WEBADMIN certificates include: CN-cisobusiness.cisco; SAN must be dns-cisobusiness.cisco; if a static IP address is used, then the SAN may also include dns=<ip address>.

Upload Certificates

Step 1

Login to the web UI of the CBW AP.



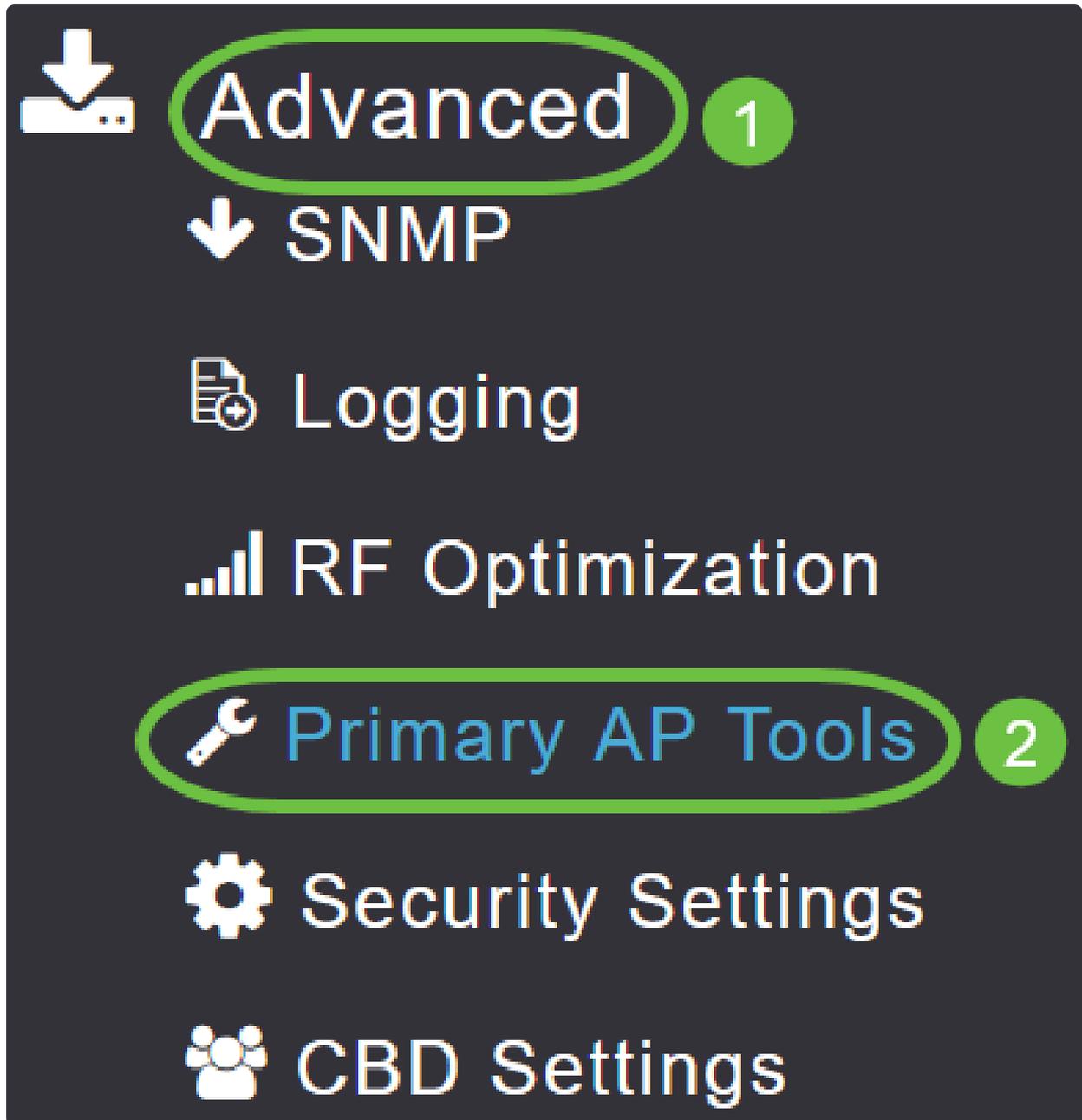
Cisco Business Wireless Access Point

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



Step 2

To upload certificates, go to **Advanced** > **Primary AP Tools**.



Step 3

Choose the **Upload File** tab.

Primary AP Tools



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

Step 4

From the *File Type* drop-down menu, choose *WEBAUTH* or *WEBADMIN Certificate*.

The screenshot shows the Primary AP Tools interface. At the top, there is a 'Tools' button. Below it, there are several navigation links: 'Restart Primary AP', 'Configuration Management', 'Troubleshooting Files', 'Troubleshooting Tools', and 'Upload File'. The 'Upload File' link is circled in green. Below the navigation links, there is a form for uploading a certificate. The form includes the following fields and options:

- Certificate Name:** 192.0.2.1
- Valid up to:** Aug 4 17:50:50 2023 GMT
- File Type:** A dropdown menu is open, showing the following options: WEBAUTH Certificate (highlighted with a green circle), EAP Device Certificate, EAP CA Certificate, CCO ROOT CA Certificate, CBD SERV CA Certificate, WEBAUTH Certificate, and WEBADMIN Certificate.
- Transfer Mode:** (Label visible, but no value selected)
- File Name*:** (Label visible, but no value entered)
- Certificate Password*:** (Label visible, but no value entered)
- Browse:** A blue button to the right of the File Name field.
- Apply settings and import:** A green button at the bottom of the form.

Note:

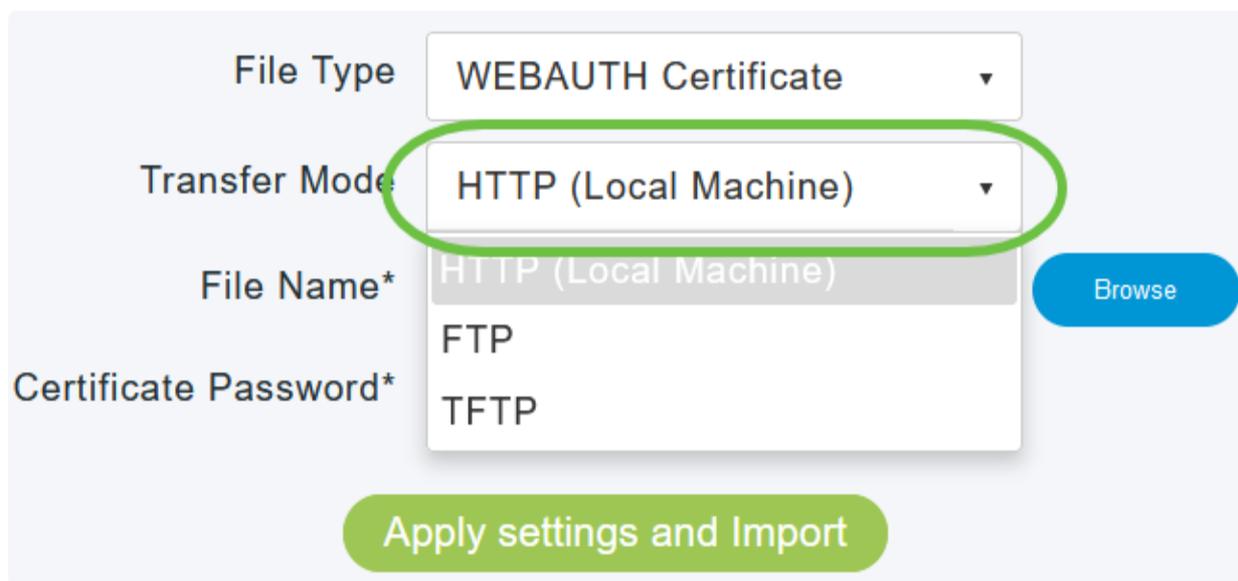
The files **MUST** be in PEM format and should contain both the Public and Private keys. It should also be password protected. Both WEBAUTH and WEBADMIN certificates **MUST** have a Common Name (CN) as ciscobusiness.cisco. So, you will need to use an internal CA to issue certificates.

Step 5

Choose the *Transfer Mode* from the drop-down menu. The options are:

- *HTTP (Local Machine)*
- *FTP*
- *TFTP*

In this example, **HTTP** is selected.



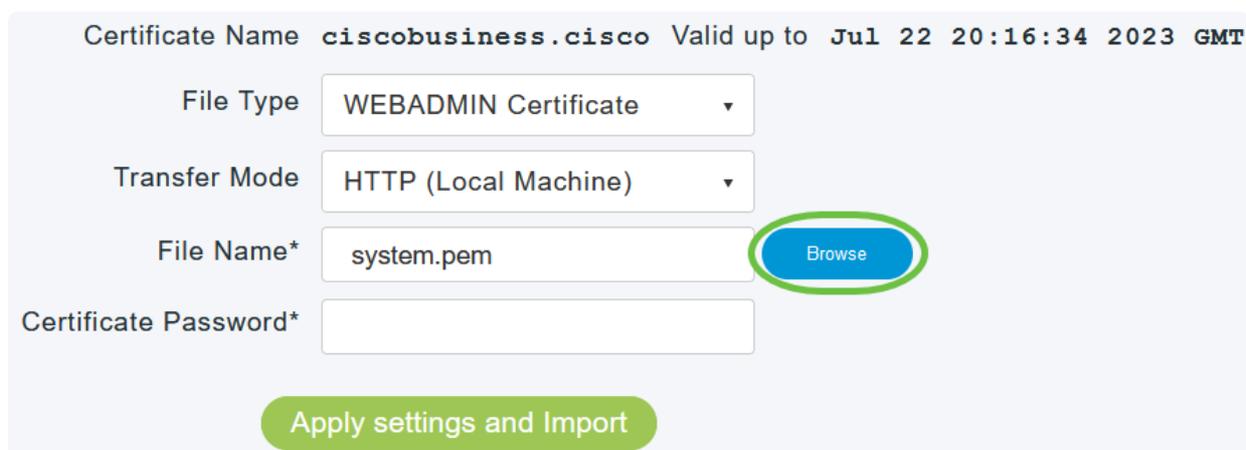
The screenshot shows a configuration form with the following fields and options:

- File Type:** WEBAUTH Certificate
- Transfer Mode:** HTTP (Local Machine) (highlighted with a green oval)
- File Name*:** HTTP (Local Machine) (highlighted with a green oval)
- Certificate Password*:** (empty)

Buttons: **Browse** (blue), **Apply settings and Import** (green)

Step 6

Click **Browse**.



The screenshot shows the configuration form with the following fields and options:

- Certificate Name:** ciscobusiness.cisco
- Valid up to:** Jul 22 20:16:34 2023 GMT
- File Type:** WEBADMIN Certificate
- Transfer Mode:** HTTP (Local Machine)
- File Name*:** system.pem
- Certificate Password*:** (empty)

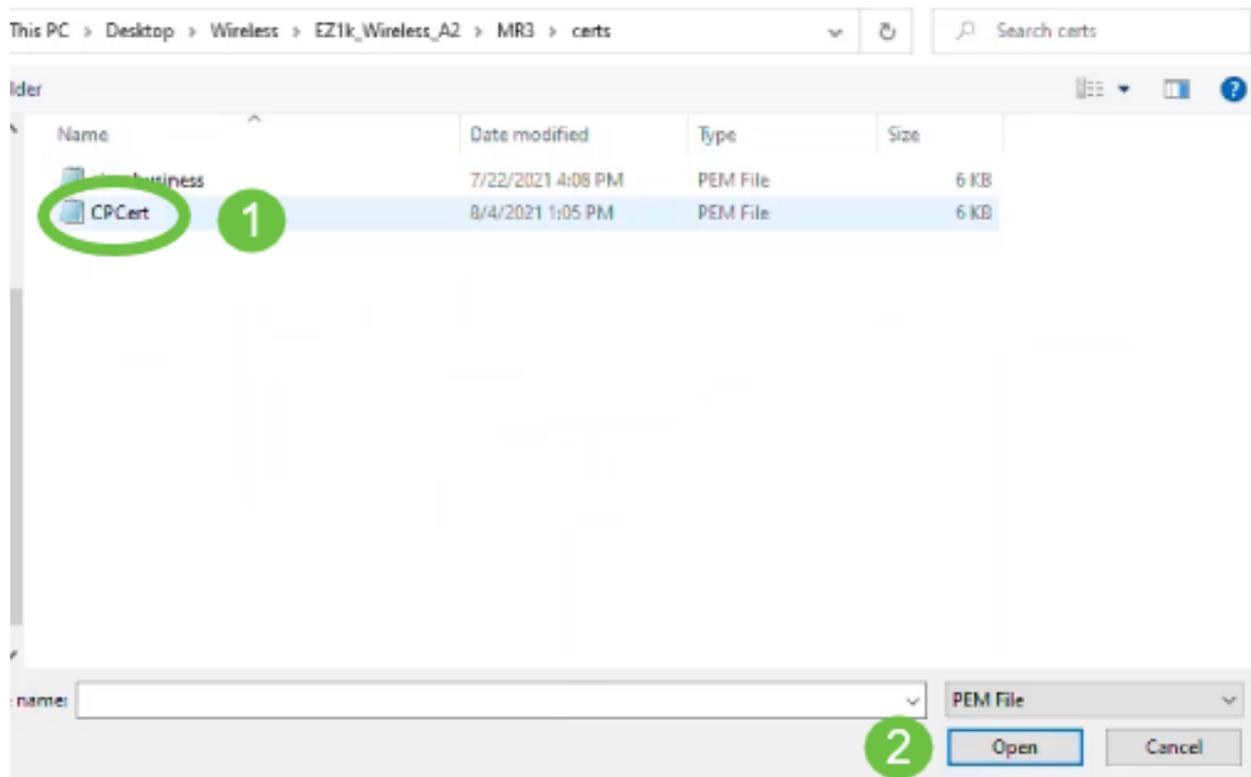
Buttons: **Browse** (blue, highlighted with a green oval), **Apply settings and Import** (green)

Note:

If the *Transfer Mode* is *FTP* or *TFTP*, then enter the *Server IP Address*, *File path*, and other required fields.

Step 7

Upload the file from your local PC by navigating to the folder containing the custom certificate. Select the certificate file and click **Open**.

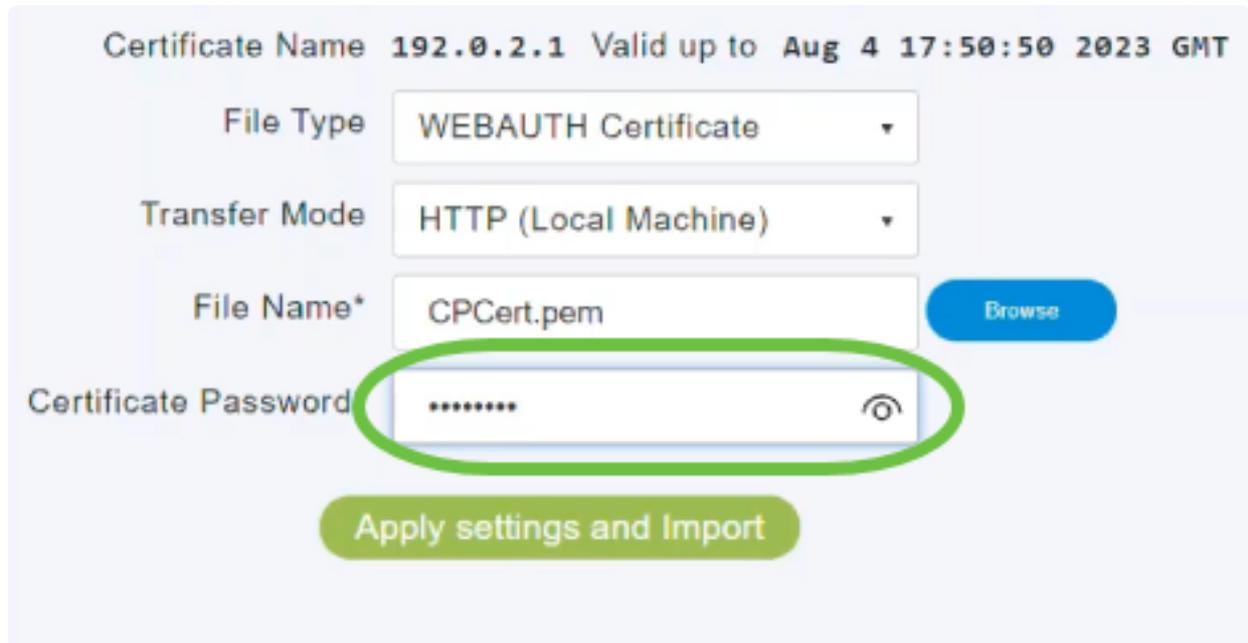


Note:

The certificate should be a PEM file. To successfully upload WEBADMIN certificates, make sure to include the full certificate chain which is the device certificate, issuing CA certificate, and root CA certificate.

Step 8

Enter the *Certificate Password*.



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) ▾

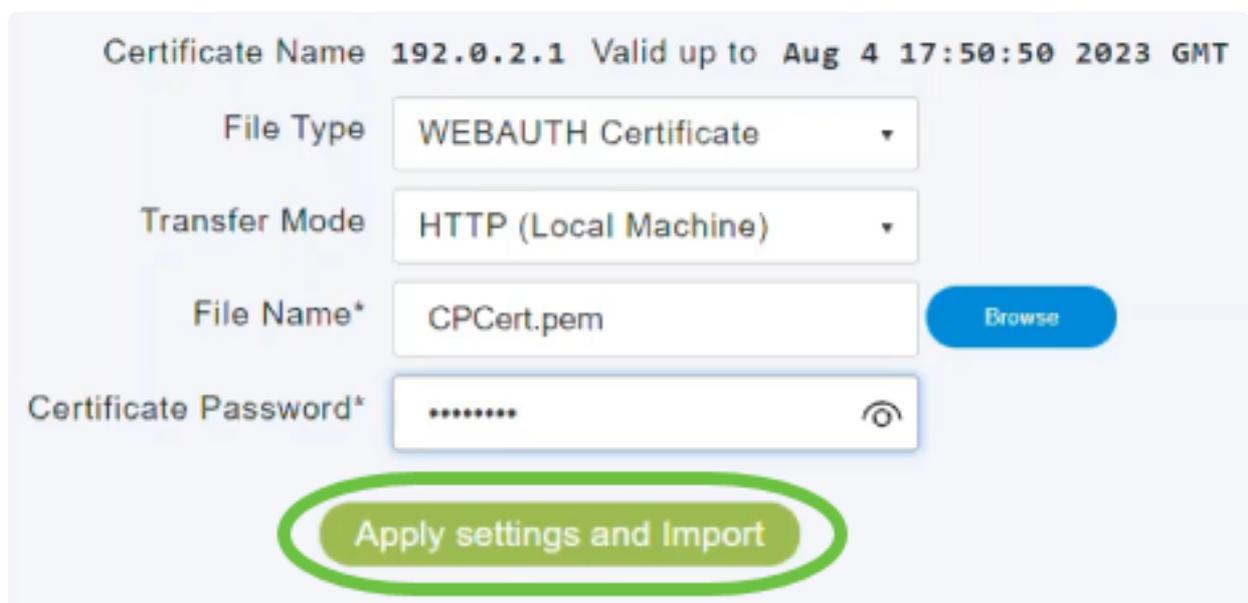
File Name* CPCert.pem [Browse](#)

Certificate Password* 

[Apply settings and Import](#)

Step 9

Click **Apply settings and Import**.



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) ▾

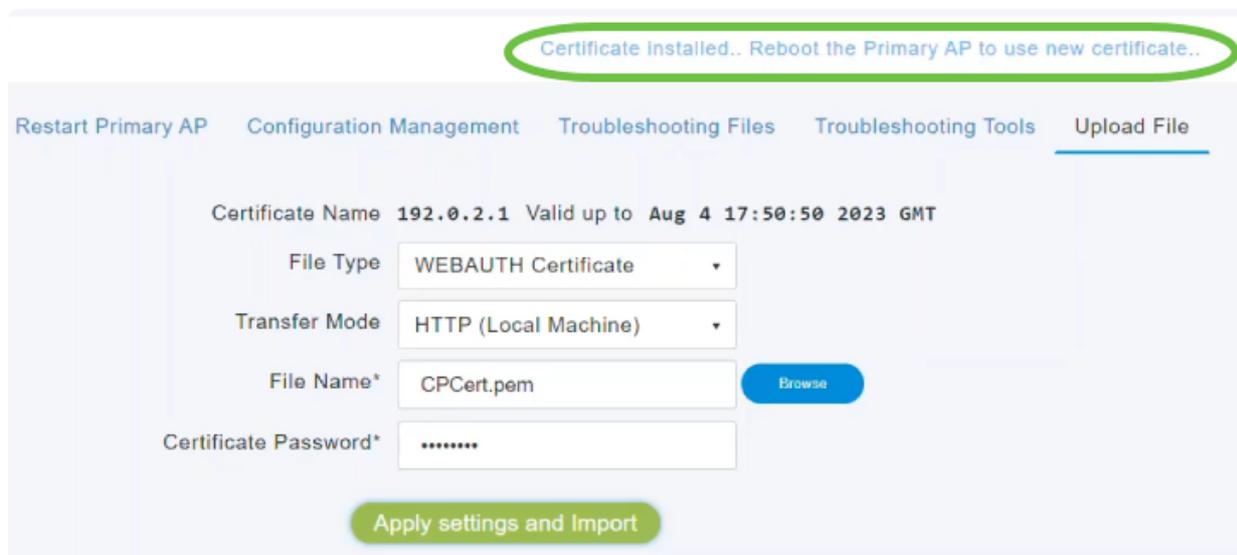
File Name* CPCert.pem [Browse](#)

Certificate Password* 

[Apply settings and Import](#)

Step 10

You will see a notification once the certificate has been successfully installed. Reboot the Primary AP.



The screenshot shows a web interface for AP configuration. At the top, a green notification bubble states: "Certificate installed.. Reboot the Primary AP to use new certificate..". Below this, a navigation bar includes "Restart Primary AP", "Configuration Management", "Troubleshooting Files", "Troubleshooting Tools", and "Upload File" (which is underlined). The main content area displays certificate details: "Certificate Name 192.0.2.1 Valid up to Aug 4 17:50:50 2023 GMT". There are four input fields: "File Type" (set to "WEBAUTH Certificate"), "Transfer Mode" (set to "HTTP (Local Machine)"), "File Name*" (set to "CPCert.pem" with a "Browse" button), and "Certificate Password*" (masked with "*****"). A green "Apply settings and Import" button is at the bottom.

Note:

To change the certificate, simply upload a new certificate. This will overwrite the certificate that was previously installed. If you want to go back to the default self-signed certificate, you will need to factory reset the primary AP.

Conclusion

You are all set! You have now successfully uploaded custom certificates on your CBW AP.