

Aangepast certificaat uploaden via Cisco draadloos access point voor bedrijven

Doel

Het doel van dit document is om te laten zien hoe u een aangepast certificaat op uw Cisco Business Wireless (CBW) access point (AP) kunt uploaden.

Toepasselijke apparaten | Software versie

- Cisco Business Wireless 140 AC access point | 10.6.1.0 ([laatste download](#))
- Cisco Business Wireless 145 AC access point | 10.6.1.0 ([laatste download](#))
- Cisco Business Wireless-240 AC access point | 10.6.1.0 ([laatste download](#))

Inleiding

In CBW APs firmware versie 10.6.1.0 en hoger kunt u nu uw eigen WEBAUTH (dat een interne portal pagina verwerkt) of WEBADMIN (het CBW Primaire AP Management-pagina)-certificaten importeren naar de web user interface (UI) die kan worden vertrouwd door uw interne apparaten en systemen. Standaard gebruiken WEBAUTH- en WEBADMIN-pagina's zelfondertekende certificaten die meestal niet worden vertrouwd en die kunnen leiden tot certificeringswaarschuwingen wanneer u probeert verbinding te maken met uw apparaat.

Met deze nieuwe functie kunt u eenvoudig aangepaste certificaten op uw CBW AP uploaden. Laten we beginnen.

Voorwaarden

- Zorg ervoor dat u de CBW AP firmware hebt bijgewerkt tot 10.6.1.0. [Klik als u stap voor stap instructies wilt doen voor een firmware-update](#).
- Er is een particuliere of interne certificeringsinstantie (CA) nodig om de WEBAUTH- of WEBADMIN-certificaten af te geven die nodig zijn voor CBW. De certificaten kunnen dan worden geïnstalleerd op elke beheerpc die verbinding kan maken met het CBW web UI.
- Het corresponderende Root CA-certificaat moet in de browser van de client worden geïnstalleerd om het aangepaste certificaat voor een portal of beheertoegang te gebruiken om potentiële certificeringswaarschuwingen te voorkomen.
- CBW gebruikt een intern opnieuw gericht IP-adres 192.0.2.1 voor een poortadapter-omleiding. Het is dus het beste om dit op te nemen als de gemeenschappelijke naam (GN) van het WEBAUTH-certificaat of de Onderwerp Alternative Name (SAN).
- Namen voor WEBADMIN-certificaten omvatten: GN-cisobusiness.cisco; SAN moet dns-cisobusiness.cisco zijn; Als een statisch IP-adres wordt gebruikt, kan de SAN ook dns=<ip-adres> bevatten.

Uploadcertificaten

Stap 1

Meld u aan bij het web UI van het CBW AP.



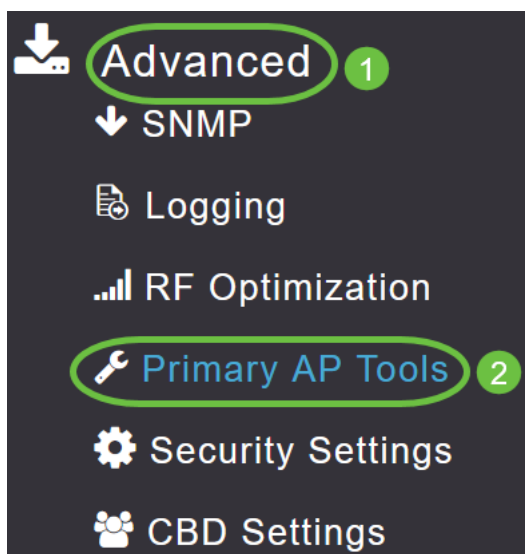
Cisco Business Wireless Access Point

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



Stap 2

Als u certificaten wilt uploaden, gaat u naar **Geavanceerd > Primaire AP-tools**.



Stap 3

Kies het tabblad **Upload File**.

Stap 4

Kies in het vervolgkeuzemenu *File Type* de optie *WEBAUTH* of het *WEBADMIN-certificaat*.

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

File Type WEBAUTH Certificate

Transfer Mode

File Name* Browse

Certificate Password*

Apply settings and import

De bestanden moeten in PEM-indeling zijn en zowel de openbare als de particuliere sleutels bevatten. Het wachtwoord moet ook worden beveiligd. Zowel WEBAUTH- als WEBADMIN-certificaten moeten een gezamenlijke naam (CN) hebben als ciscobusiness.cisco. U moet dus een interne CA gebruiken om certificaten af te geven.

Stap 5

Kies de *Overoverdrachtmodus* in het vervolgkeuzemenu. De opties zijn:

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

In dit voorbeeld is **HTTP** geselecteerd.

File Type

Transfer Mode

File Name*

Certificate Password*

Stap 6

Klik op **Bladeren**.

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

File Type

Transfer Mode

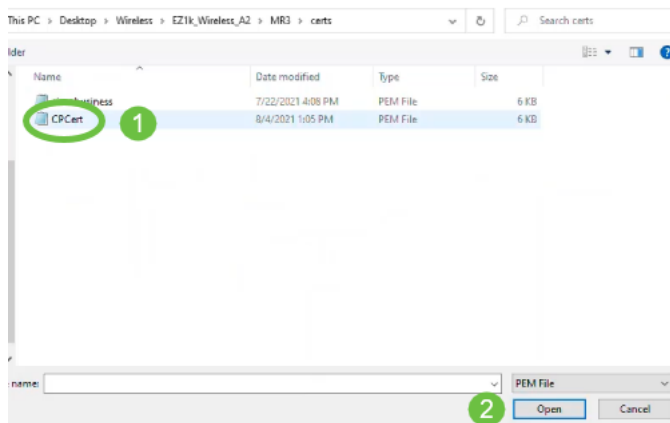
File Name*

Certificate Password*

Als de *overdrachtmodus FTP of TFTP* is, specificeert u het *IP-adres van de server, het bestandspad* en de andere benodigde velden.

Stap 7

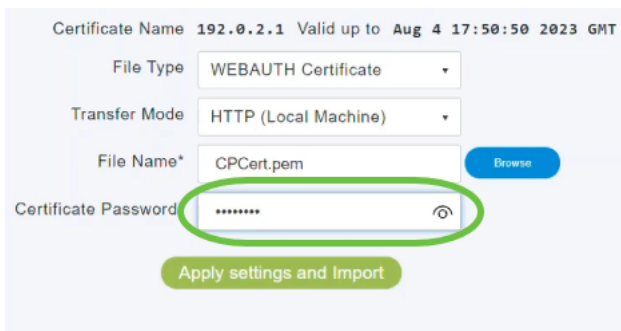
Upload het bestand vanaf uw lokale pc door naar de map te bladeren met het aangepaste certificaat. Selecteer het certificaatbestand en klik op **Openen**.



Het certificaat moet een PEM-bestand zijn.

Stap 8

Voer het *wachtwoord* in voor het certificaat.



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)

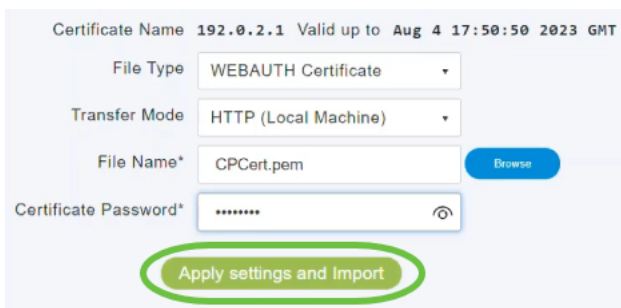
File Name* CPCert.pem [Browse](#)

Certificate Password* [🔍](#)

[Apply settings and import](#)

Stap 9

Klik op **Instellingen toepassen en Importeren**.



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)

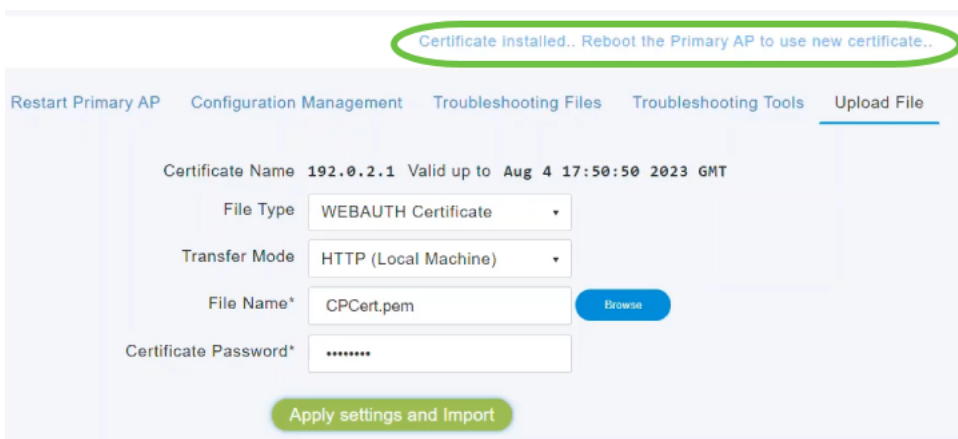
File Name* CPCert.pem [Browse](#)

Certificate Password* [🔍](#)

[Apply settings and import](#)

Stap 10

U krijgt een melding als het certificaat is geïnstalleerd. Herstart de primaire AP.



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](#)

U kunt het certificaat wijzigen door een nieuw certificaat te uploaden. Hierdoor overschrijft u het eerder geïnstalleerde certificaat. Als u wilt terugkeren naar het standaard zichzelf getekende certificaat, dient u het primaire AP opnieuw in de fabriek te zetten.

Conclusie

Jullie zijn allemaal klaar! U hebt nu met succes aangepaste certificaten op uw CBW AP geüpload.