

Carica certificato personalizzato in Cisco Business Wireless Access Point

Obiettivo

L'obiettivo di questo documento è mostrare come caricare un certificato personalizzato sul proprio Cisco Business Wireless (CBW) Access Point (AP).

Dispositivi interessati | Versione software

- Access point Cisco Business Wireless 140AC | 10.6.1.0 ([scarica la versione più recente](#))
- Access point Cisco Business Wireless 145AC | 10.6.1.0 ([scarica la versione più recente](#))
- Access point Cisco Business Wireless 240AC | 10.6.1.0 ([scarica la versione più recente](#))

Introduzione

Nella versione 10.6.1.0 e successive del firmware degli access point CBW è ora possibile importare i propri certificati WEBAUTH (che gestisce la pagina del portale vincolato) o WEBADMIN (pagina di gestione dell'access point primario CBW) nell'interfaccia utente Web che potrebbe essere considerata attendibile dai dispositivi e dai sistemi interni. Per impostazione predefinita, le pagine WEBAUTH e WEBADMIN utilizzano certificati autofirmati che in genere non sono attendibili e possono generare avvisi sui certificati quando si tenta di connettersi al dispositivo.

Questa nuova funzionalità consente di caricare facilmente certificati personalizzati nell'access point CBW. Iniziamo.

Prerequisiti

- Accertarsi di aver aggiornato il firmware dell'access point CBW alla versione 10.6.1.0. [Fare clic per istruzioni dettagliate sull'aggiornamento del firmware.](#)
- Per rilasciare i certificati WEBAUTH o WEBADMIN necessari per CBW, è necessaria un'autorità di certificazione (CA) privata o interna. I certificati possono quindi essere installati in qualsiasi PC di gestione in grado di connettersi all'interfaccia utente Web CBW.
- Il certificato CA radice corrispondente deve essere installato nel browser client per utilizzare il certificato personalizzato per il portale captive o l'accesso di gestione per evitare potenziali avvisi relativi ai certificati.
- CBW utilizza un indirizzo IP 192.0.2.1 reindirizzato internamente per il reindirizzamento del portale captive. È quindi consigliabile includere questo nome come nome comune (CN) o nome alternativo soggetto (SAN) del certificato WEBAUTH.
- I requisiti di denominazione per i certificati WEBADMIN includono: CN-cisobusiness.cisco; La SAN deve essere dns-cisobusiness.cisco; se si utilizza un indirizzo IP statico, la SAN può includere anche dns=<indirizzo ip>.

Carica certificati

Passaggio 1

Accedere all'interfaccia utente Web dell'access point CBW.



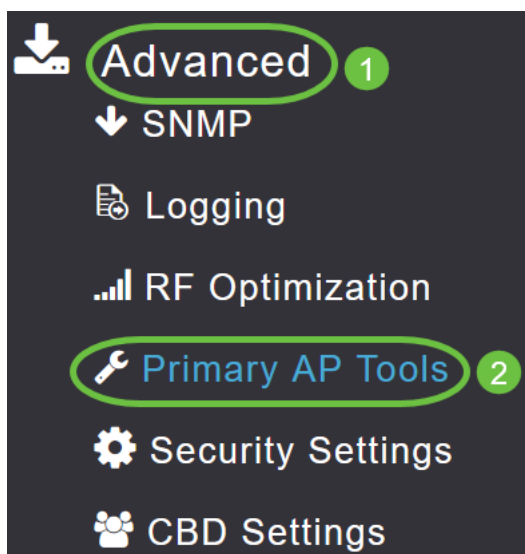
Cisco Business Wireless Access Point

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



Passaggio 2

Per caricare i certificati, passare a **Avanzate > Strumenti PA principali**.

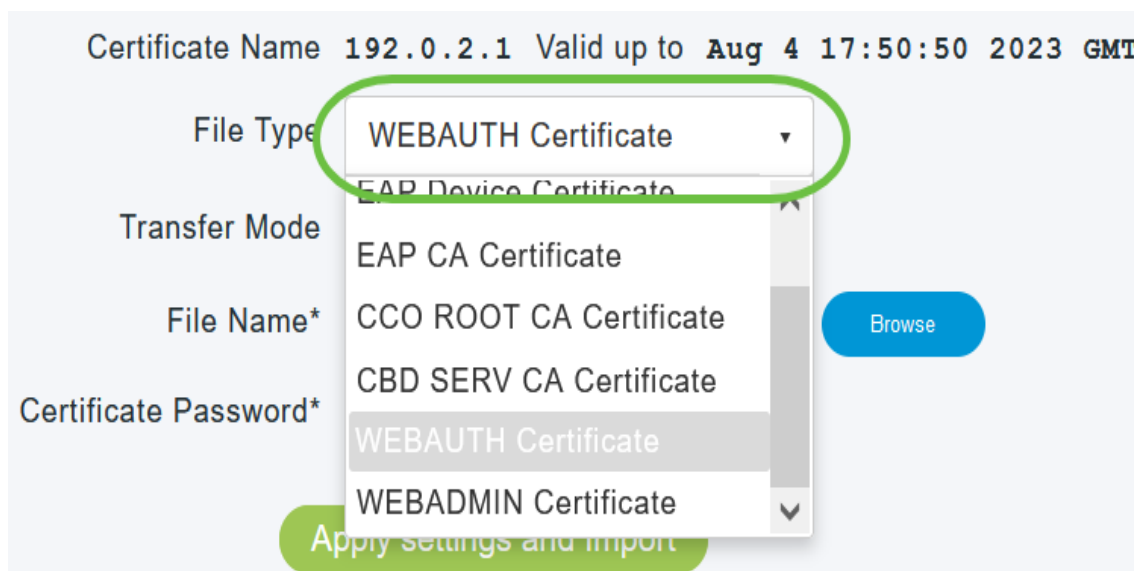


Passaggio 3

Scegliere la scheda **Carica file**.

Passaggio 4

Dal menu a discesa *Tipo di file*, scegliere *WEBAUTH* o *WEBADMIN Certificate*.



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

I file DEVONO essere in formato PEM e devono contenere le chiavi pubblica e privata. Deve inoltre essere protetto da password. I certificati WEBAUTH e WEBADMIN DEVONO avere un nome comune (CN) come ciscobusiness.cisco. Sarà quindi necessario utilizzare una CA interna per rilasciare i certificati.

Passaggio 5

Scegliere *Modalità di trasferimento* dal menu a discesa. Le opzioni sono:

- HTTP (computer locale)
- FTP
- TFTP

Nell'esempio è selezionato **HTTP**.

File Type

Transfer Mode

File Name*

Certificate Password*

Passaggio 6

Fare clic su **Sfoggia**.

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

File Type

Transfer Mode

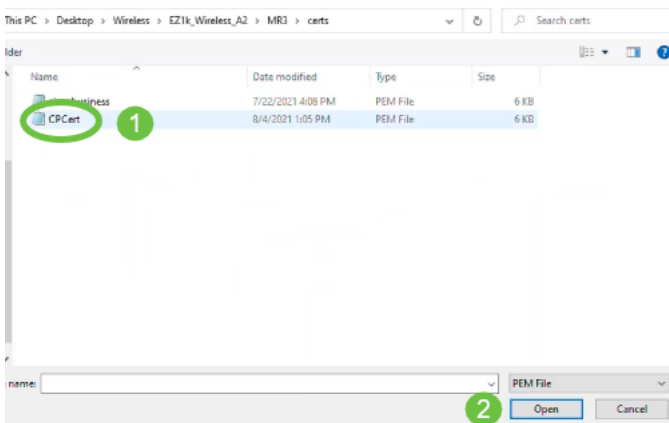
File Name*

Certificate Password*

Se la modalità di trasferimento è FTP o TFTP, immettere l'indirizzo IP del server, il percorso del file e altri campi obbligatori.

Passaggio 7

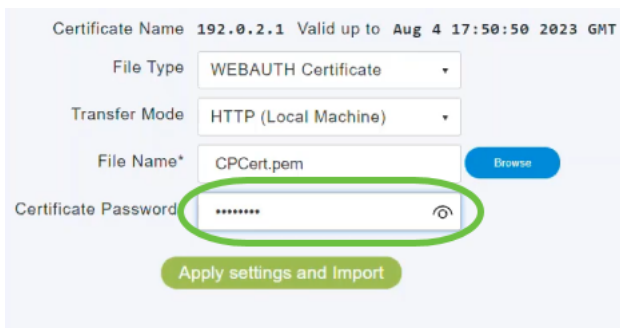
Caricare il file dal PC locale passando alla cartella contenente il certificato personalizzato. Selezionare il file del certificato e fare clic su **Apri**.



Il certificato deve essere un file PEM.

Passaggio 8

Immettere la *password* del *certificato*.



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)

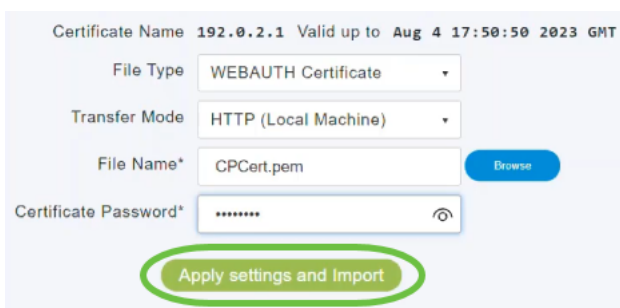
File Name* CPCert.pem [Browse](#)

Certificate Password* [password] [🔍](#)

[Apply settings and import](#)

Passaggio 9

Fare clic su **Applica impostazioni e Importa**.



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)

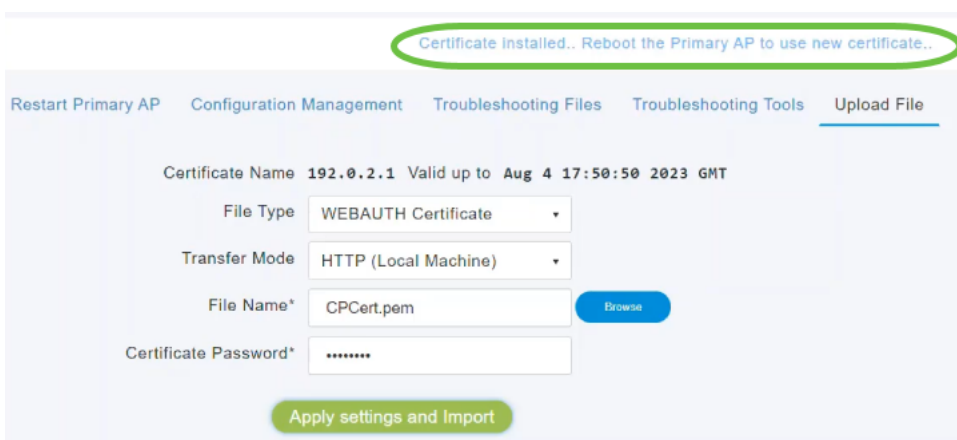
File Name* CPCert.pem [Browse](#)

Certificate Password* [password] [🔍](#)

[Apply settings and import](#)

Passaggio 10

Una volta installato correttamente il certificato, verrà visualizzata una notifica. Riavviare l'access point primario.



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* [password]

[Apply settings and import](#)

Per modificare il certificato, caricarne uno nuovo. Il certificato precedentemente installato verrà sovrascritto. Per tornare al certificato autofirmato predefinito, è necessario reimpostare il punto di accesso primario.

Conclusioni

È tutto pronto! Caricamento dei certificati personalizzati nell'access point CBW completato.