

Hochladen eines benutzerdefinierten Zertifikats in einen Cisco Business Wireless Access Point

Ziel

In diesem Dokument wird erläutert, wie Sie ein benutzerdefiniertes Zertifikat auf Ihren Cisco Business Wireless Access Point (AP) hochladen.

Unterstützte Geräte | Software-Version

- Cisco Business Wireless Access Point 140AC | 10.6.1.0 ([Aktuelle Version herunterladen](#))
- Cisco Business Wireless Access Point 145AC | 10.6.1.0 ([Aktuelle Version herunterladen](#))
- Cisco Business Wireless Access Point 240AC | 10.6.1.0 ([Aktuelle Version herunterladen](#))

Einleitung

In der Firmware-Version 10.6.1.0 der CBW APs und höher können Sie jetzt Ihre eigenen WEBAUTH- (die Captive Portal Page behandelt) oder WEBADMIN-Zertifikate (die primäre CBW-AP-Verwaltungsseite) in die Webbenutzeroberfläche (UI) importieren, die von Ihren internen Geräten und Systemen als vertrauenswürdig eingestuft werden können. Standardmäßig verwenden WEBAUTH- und WEBADMIN-Seiten selbstsignierte Zertifikate, die in der Regel nicht vertrauenswürdig sind, und können zu Zertifikatwarnungen führen, wenn Sie versuchen, eine Verbindung mit Ihrem Gerät herzustellen.

Mit dieser neuen Funktion können Sie ganz einfach benutzerdefinierte Zertifikate auf Ihren CBW-AP hochladen. Fangen wir an.

Voraussetzungen

- Stellen Sie sicher, dass Sie die CBW AP-Firmware auf 10.6.1.0 aktualisiert haben.

[Klicken Sie, wenn Sie eine schrittweise Anleitung für ein Firmware-Update wünschen.](#)

- Eine private oder interne Zertifizierungsstelle (Certificate Authority, CA) ist erforderlich, um die für CBW erforderlichen WEBAUTH- oder WEBADMIN-Zertifikate auszustellen. Die Zertifikate können dann auf jedem Management-PC installiert werden, der eine Verbindung zur CBW-Webbenutzeroberfläche herstellen kann.
- Das entsprechende Zertifikat der Stammzertifizierungsstelle muss im Clientbrowser installiert werden, damit das benutzerdefinierte Zertifikat für den Zugriff auf das Captive Portal oder die Verwaltung verwendet werden kann, um potenzielle Zertifikatwarnungen zu vermeiden.
- CBW verwendet eine intern umgeleitete IP-Adresse 192.0.2.1 für die Captive Portal-Umleitung. Daher empfiehlt es sich, diesen Namen als Common Name (CN) oder Subject Alternative Name (SAN) des WEBAUTH-Zertifikats anzugeben.
- Benennungsanforderungen für WEBADMIN-Zertifikate sind: CN-cisobusiness.cisco
SAN muss dns-cisobusiness.cisco sein; Wenn eine statische IP-Adresse verwendet wird, kann das SAN auch dns=<IP-Adresse> enthalten.

Zertifikate hochladen

Schritt 1

Melden Sie sich bei der Webbenutzeroberfläche des CBW AP an.



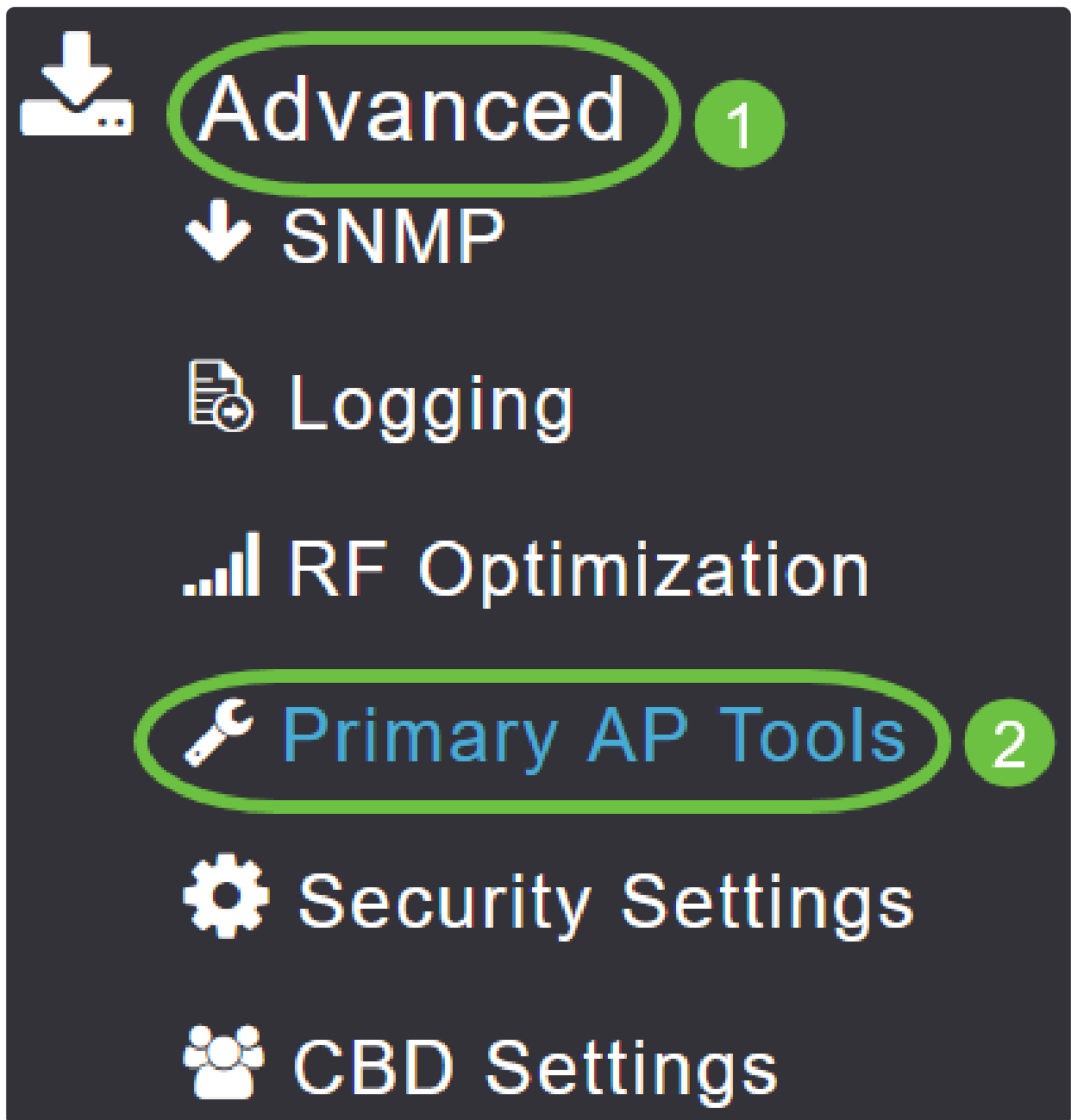
Cisco Business Wireless Access Point

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



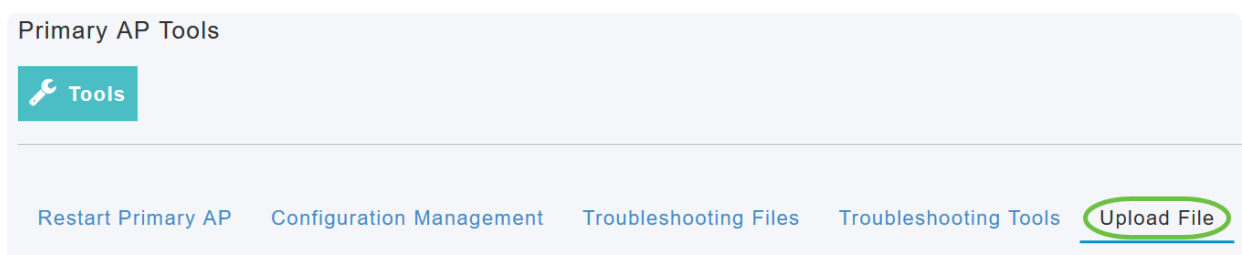
Schritt 2

Um Zertifikate hochzuladen, gehen Sie zu Erweitert > Primäre AP-Tools.



Schritt 3

Wählen Sie die Registerkarte Upload File (Datei hochladen).



Schritt 4

Wählen Sie im Dropdown-Menü Dateityp die Option WEBAUTH oder WEBADMIN Certificate aus.

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

File Type WEBAUTH Certificate

Transfer Mode

File Name* CCO ROOT CA Certificate

Certificate Password* CBD SERV CA Certificate

WEBAUTH Certificate

WEBADMIN Certificate

Browse

Apply settings and import

Note:

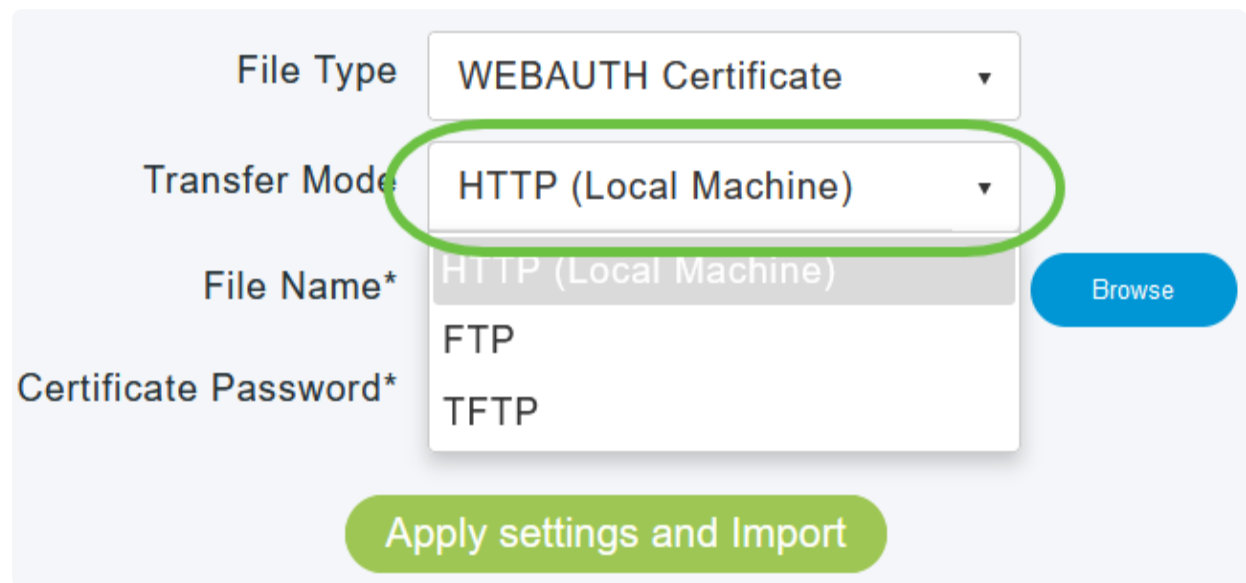
Die Dateien MÜSSEN das PEM-Format haben und sowohl den öffentlichen als auch den privaten Schlüssel enthalten. Es sollte auch passwortgeschützt sein. WEBAUTH- und WEBADMIN-Zertifikate MÜSSEN den Common Name (CN) ciscobusiness.cisco aufweisen. Sie müssen also eine interne Zertifizierungsstelle verwenden, um Zertifikate auszustellen.

Schritt 5

Wählen Sie den Übertragungsmodus aus dem Dropdown-Menü aus. Folgende Optionen sind verfügbar:

- HTTP (Lokaler Computer)
- FTP
- TFTP

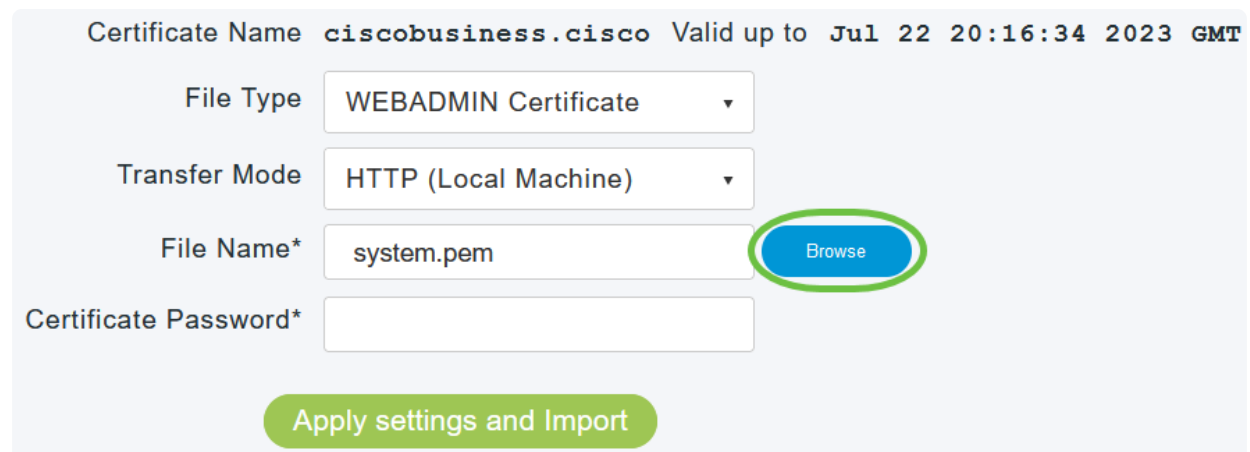
In diesem Beispiel ist HTTP ausgewählt.



The screenshot shows a configuration form for a certificate. The 'File Type' is set to 'WEBAUTH Certificate'. The 'Transfer Mode' dropdown menu is open, showing three options: 'HTTP (Local Machine)' (which is highlighted with a green oval), 'FTP', and 'TFTP'. The 'File Name*' field contains 'HTTP (Local Machine)'. The 'Certificate Password*' field is empty. A blue 'Browse' button is located to the right of the 'File Name*' field. At the bottom, there is a green button labeled 'Apply settings and Import'.

Schritt 6

Klicken Sie auf Durchsuchen.



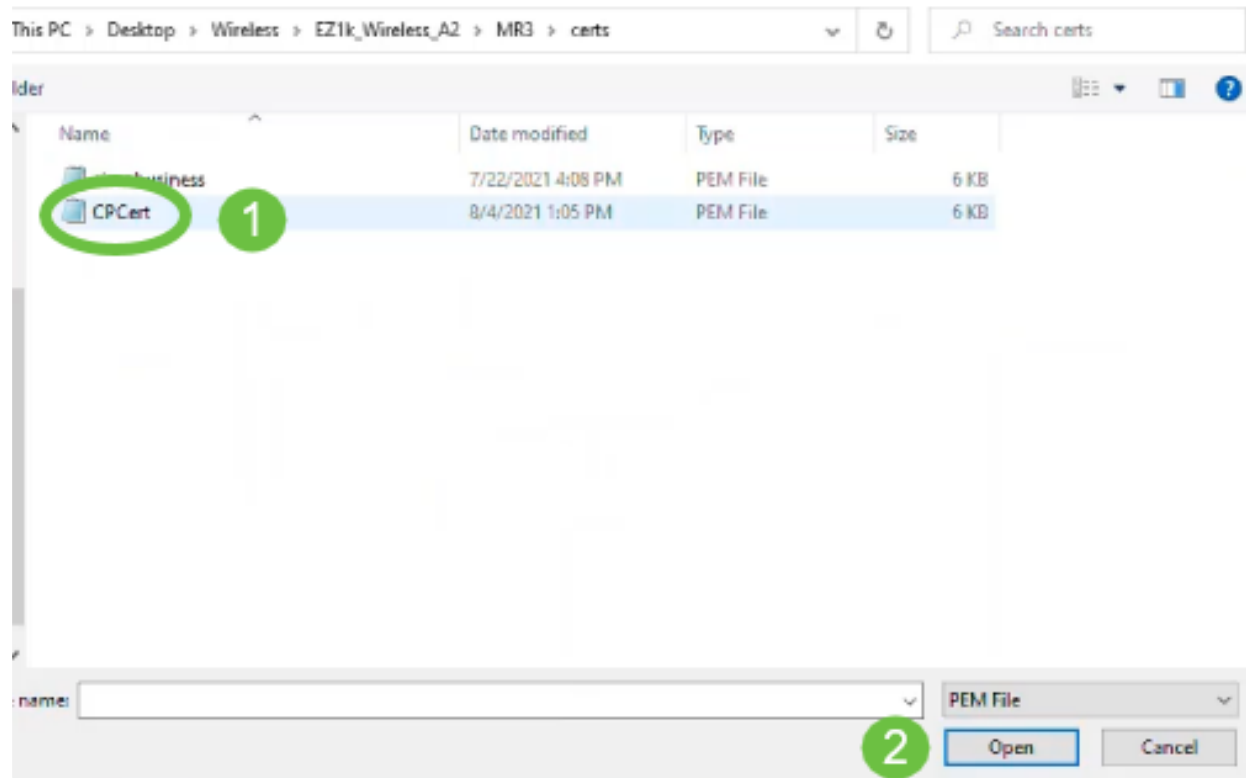
The screenshot shows the same configuration form as before, but now the 'File Name*' field contains 'system.pem'. The 'Browse' button is highlighted with a green oval. The 'Certificate Password*' field is still empty. The 'Apply settings and Import' button remains at the bottom.

Note:

Wenn der Übertragungsmodus FTP oder TFTP ist, geben Sie die Server-IP-Adresse, den Dateipfad und andere erforderliche Felder ein.

Schritt 7

Laden Sie die Datei von Ihrem lokalen PC hoch, indem Sie zu dem Ordner navigieren, der das benutzerdefinierte Zertifikat enthält. Wählen Sie die Zertifikatsdatei aus, und klicken Sie auf Öffnen.



Note:

Das Zertifikat sollte eine PEM-Datei sein. Um erfolgreich WEBADMIN-Zertifikate hochzuladen, stellen Sie sicher, dass Sie die gesamte Zertifikatskette, d. h. das Gerätezertifikat, das ausstellende Zertifizierungsstellenzertifikat und das Stammzertifizierungsstellenzertifikat, einschließen.

Schritt 8

Geben Sie das Zertifikatkennwort ein.

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](#)

Schritt 9

Klicken Sie auf Einstellungen übernehmen und Importieren.

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](#)

Schritt 10

Sobald das Zertifikat erfolgreich installiert wurde, wird eine Benachrichtigung angezeigt. Starten Sie den primären Access Point neu.

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](#)

Note:

Laden Sie einfach ein neues Zertifikat hoch, um das Zertifikat zu ändern. Dadurch wird das zuvor installierte Zertifikat überschrieben. Wenn Sie zum selbstsignierten Standardzertifikat zurückkehren möchten, müssen Sie den primären Access Point auf die Werkseinstellungen zurücksetzen.

Schlussfolgerung

Du bist fertig! Sie haben jetzt benutzerdefinierte Zertifikate erfolgreich auf Ihren CBW-AP hochgeladen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.