



Cisco Webex Share セキュリティ

- [証明書について](#) (1 ページ)
- [証明書を生成する](#) (1 ページ)
- [証明書をダウンロードして署名する](#) (3 ページ)
- [証明書をアップロード](#) (3 ページ)
- [認証機関またはルート証明書を追加する](#) (4 ページ)
- [証明書をサポートするようにWi-Fi設定を構成する](#) (5 ページ)
- [イーサネット802.1X証明書を登録する](#) (5 ページ)
- [利用可能な証明書を表示する](#) (6 ページ)

証明書について

ほとんどの Cisco デバイスは、パスワードに加え、x.509 証明書を使用したワイヤレス接続に対応しています。会社がワイヤレス接続に証明書を使用している場合は、デバイスを起動する前に証明書を導入します。

デバイスの IP アドレスをブラウザに入力してアクセスするデバイスの設定 web ページから証明書を作成し、管理します。デバイスがコントロールハブに登録されると、設定ページがデバイスの web ページになります。設定ページが表示されない場合は、初期化を行い、デバイスを工場出荷時の状態に戻します。

導入後に証明書を使用することを決定した場合は、初期化してからコントロールハブからデバイスを削除してください。2 番目のアクティベーションコードを生成して、デバイスを再起動します。ただし、証明書の導入が完了するまでは、デバイスをコントロールハブに登録しないでください。

証明書を生成する

デバイスを起動する前に証明書を生成します。Wi-fi または 802.1 x に EAP-TLS を使用する場合は、デバイス証明書を取得してから CA 証明書をロードします。

始める前に

- デバイスをネットワークに接続します。
- デバイスのIPアドレスを取得します。

手順

ステップ 1 Webブラウザを開いて、次のURLを入力します。*IP address*はデバイスのIPアドレスです。

http://IP address

ステップ 2 設定 > をナビゲートして証明書を追加します。

ステップ 3 証明書の登録を選択します。

ステップ 4 フィールドに情報を入力します。

- 一般名: デバイスを識別するルーム名または名前。
- 組織単位名: 証明書リクエストを行う部署名。たとえば、Finance や IT などです。
- 組織名: 証明書リクエストを行う正式な企業名。Ltd. や Corp. などのサフィックスも含めません。
- ロケーション: 組織が所在する市町村。
- 都道府県: 組織が所在する正式な都道府県。短縮形を使用しないでください。
- 国: 組織が所在する国の 2 文字のISOコード。US、GB、FR など。
- キーサイズ: 2048 または 4096
- キーサイズ: 2048 または 4096
- 証明書の使用状況: 以下の 1 つ以上を確認してください。
 - **EAP / TLS** 無線接続用
 - **802.1x** 有線接続用
- 拡張キー使用オプション: 以下の拡張機能の両方を選択します。
 - サーバ認証の**serverAuth**
 - クライアント認証の**clientAuth**

ステップ 5 [生成 (Generate)]をクリックします。

次のタスク

証明書を署名する

関連トピック

[Cisco Webex Shareへの接続とアクティベーション](#)

証明書をダウンロードして署名する

証明書が生成されたら、証明書署名リクエスト(CSR)をダウンロードして、完了できるようにします。

始める前に

このデバイスの無署名証明書を生成しました。

デバイスの IP アドレスを取得します。

手順

- ステップ 1** Webブラウザを開いて、次のURLを入力します。 *IP address*はデバイスのIPアドレスです。
`http://IP address`
- ステップ 2** 設定 > をナビゲートして証明書を追加します。
- ステップ 3** 証明書の管理を選択します。
- ステップ 4** [ダウンロード (Download)] をクリックします。
コンピュータにダウンロードする証明書。
- ステップ 5** ダウンロードした証明書署名要求 (CSR) を署名してもらいます。組織通例の手順に従ってください。

次のタスク

CSRに署名したら、署名済み証明書をアップロードします。

関連トピック

[Cisco Webex Shareへの接続とアクティベーション](#)

証明書をアップロード

サーバに証明書をアップロードします。適切な権限が最初に署名されている必要があります。

始める前に

デバイスのIPアドレスを取得します。

証明書が、プライバシー強化メール (PEM) 形式であることを確認します。

手順

ステップ1 Webブラウザを開いて、次のURLを入力します。*IP address*はデバイスのIPアドレスです。

http://IP address

ステップ2 設定 > をナビゲートして証明書を追加します。

ステップ3 証明書の管理を選択します。

ステップ4 [署名付き証明書のアップロード] で、**アップロード**をクリックします。証明書の場所にナビゲートします。

間違った証明書をアップロードしてしまった場合は、正しい証明書をアップロードし直してください。

関連トピック

[Cisco Webex Shareへの接続とアクティベーション](#)

認証機関またはルート証明書を追加する

始める前に

wifiまたは802.1xでアップロードする認証機関(CA)またはルート証明書があります。

デバイスのIPアドレスを取得します。

手順

ステップ1 Webブラウザを開いて、次のURLを入力します。*IP address*はデバイスのIPアドレスです。

http://IP address

ステップ2 設定 > をナビゲートして証明書を追加します。

ステップ3 認証機関またはルート証明書を追加します。

ステップ4 以下から少なくとも1つは選択してください。

802.1x

EAP-TLS

デジタル サイネージ

ステップ5 [証明書のアップロード] をクリックします。

関連トピック

[Cisco Webex Shareへの接続とアクティベーション](#)

証明書をサポートするようにWi-Fi設定を構成する

署名された証明書をアップロードした後、Wi-Fi 設定を設定し、証明書を選択します。

始める前に

デバイスのIPアドレスを取得します。

手順

- ステップ 1 Webブラウザを開いて、次のURLを入力します。 *IP address*はデバイスのIPアドレスです。
`http://IP address`
- ステップ 2 設定 > をナビゲートして証明書を追加します。
- ステップ 3 ネットワークの > **Wi-Fi**にいきます。
- ステップ 4 SSIDを選択します。
- ステップ 5 最初のドロップダウンリストボックスをクリックして、サポートされているプロトコルを表示します。
- ステップ 6 **EAP-TLS**を選択してください。
- ステップ 7 [クライアント証明書の選択]で証明書を選択します。
- ステップ 8 [CA 証明書の選択]で証明書を選択します。
- ステップ 9 (任意) ユーザ名を入力してください。
- ステップ 10 [参加 (Join)]をクリックします。

関連トピック

[Cisco Webex Shareへの接続とアクティベーション](#)

イーサネット802.1X証明書を登録する

Wi-Fiを使用するデバイスにはイーサネット802.1x証明書が必要です。

デバイスのIPアドレスを取得します。

始める前に

802.1xプロトコルで証明書を生成して署名します。

手順

- ステップ 1 Webブラウザを開いて、次のURLを入力します。 *IP address*はデバイスのIPアドレスです。

`http://IP address`

- ステップ2 設定 > をナビゲートして証明書を追加します。
- ステップ3 Ethernet 802.1X 証明書を選択します。
- ステップ4 ドロップダウンリストから証明書を選択します。
- ステップ5 [選択 (Select)]をクリックします。

関連トピック

[Cisco Webex Shareへの接続とアクティベーション](#)

利用可能な証明書を表示する

証明書をアップロードすると、証明書の情報を表示できます。これは問題をトラブルシューティングするときに役立ちます。

始める前に

デバイスのIPアドレスを取得します。

手順

-
- ステップ1 Webブラウザを開いて、次のURLを入力します。*IP address*はデバイスのIPアドレスです。

`http://IP address`

- ステップ2 設定 > をナビゲートして証明書を追加します。
- ステップ3 証明書の登録を選択します。
- ステップ4 情報をクリックして証明書に関する情報を表示します。
各証明書は以下を示します。
 - 共通名: 完全修飾ドメイン名
 - Cert Type - 値は CSR 証明書、ローカル、CA /ルートです。
 - Cert Usage - 証明書がサポートするプロトコルを一覧表示します (802.1x、EAP / TLS) 。
- ステップ5 (任意) 必要に応じて、[削除]をクリックして証明書を削除します。

関連トピック

[Cisco Webex Shareへの接続とアクティベーション](#)