[illegible]

[illegible] [illegible]
[illegible]

[illegible]

[illegible]
[illegible] (CA) [illegible]

[illegible]

[illegible]
[illegible]

- [illegible]: [illegible]
- [illegible]: [illegible]
- [illegible] **(CA)**: CA [illegible]
- [illegible]:
  [illegible]
  [illegible] [illegible]
- [illegible]: [illegible]

[illegible]

- [illegible]
- [illegible]
- [illegible]
- [illegible] [illegible]
- [illegible]
- [illegible]

[illegible]

- [illegible]: [illegible]

- 証明書の削除　　：
  証明書がユーザーやポリシーに関連付けられておらず、デバイスで使用されていない場合のみ実行可能です。また、ライセンスの期限が切れている場合、このアクションは無効になることがあります。
- 複数行の選択　　：
  複数行の選択を有効にすることで、複数の証明書を一括で削除できます。削除可能な証明書のみを選択できます。
- 更新　：証明書リストを再読み込みします。

証明書のインポート

証明書をインポートするには、　　証明書のインポート　　をクリックし、　　1 つ以上のファイルを選択します。サポートされている形式は、インポートボタンのツールチップに表示されます。

クライアント

サポートされている形式　　：Base64エンコードされた　　PKCS#12 (.p12 / .pfx)

クライアント証明書は、企業ネットワーク上のユーザーまたはデバイスを識別するためのものです。クライアント証明書は、特定のユーザーに関連付けることができます。

各クライアント証明書は、オプションで特定のユーザーに割り当てることができます。これにより、同じ Wi-Fi EAP設定を多数のデバイスに展開することが可能になります。これは、ポリシーの　　ネットワーク設定　　セクションにて、　　ユーザーの　　**EAP**資格情報　　オプションを使用することで設定できます。

> 　　または、　　ユーザー　　ページからユーザーに証明書を割り当てることもできます。

認証局　　(CA)

サポートされている形式　　：Base64エンコードされた　　X.509 (.crt / .pem / .cer / .der)

CA 証明書は認証局を識別し、その　　CA から発行されたすべての証明書を信頼すべきであることをデバイスに示します。ダッシュボードは、インポートされた　　X.509 証明書が　　CA であることを検証します。

証明書エディター