



証明書の検証設定

- [クラウド展開の証明書検証, 1 ページ](#)

クラウド展開の証明書検証

Cisco WebEx Messenger と Cisco WebEx Meeting Center は、デフォルトで次の証明書をクライアントに提示します。

- CAS
- WAPI



(注) Cisco WebEx 証明書はパブリック認証局 (CA) によって署名されます。Cisco Jabber はこれらの証明書を検証し、クラウドベース サービスとのセキュアな接続を確立します。

Cisco Jabber は、Cisco WebEx Messenger から受信した次の XMPP 証明書を検証します。これらの証明書がオペレーティング システムに付属していない場合は、ユーザが入力する必要があります。

- VeriSign Class 3 Public Primary Certification Authority - G5 : この証明書は信頼できるルート認証局に保存されます。
- VeriSign Class 3 Secure Server CA - G3 : この証明書は WebEx Messenger サーバ ID の検証に使用され、中間認証局に保存されます。
- AddTrust 外部 CA ルート
- GoDaddy Class 2 Certification Authority Root Certificate

Cisco Jabber for Windows のルート証明書の詳細については、<https://www.identrust.co.uk/certificates/trustid/install-nes36.html>を参照してください。

Cisco Jabber for Mac のルート証明書の詳細については、<https://support.apple.com>を参照してください。

プロフィール写真の URL の更新

クラウドベース展開では、ユーザを追加またはインポートすると、Cisco WebEx がプロフィール写真に一意の URL を割り当てます。Cisco Jabber は、連絡先情報を解決するときに、写真がホストされている URL の Cisco WebEx からプロフィール写真を取得します。

プロフィール写真の URL は、HTTP セキュア (`https://server_name/`) を使用して、クライアントに証明書を提示します。URL のサーバ名が次の場合：

- Cisco WebEx ドメインを含む完全修飾ドメイン名 (FQDN) : クライアントは、Cisco WebEx 証明書に照らして、プロフィール写真をホストしている Web サーバを検証できます。
- IP アドレス : クライアントは、Cisco WebEx 証明書に照らして、プロフィール写真をホストしている Web サーバを検証できません。この場合、プロフィール写真の URL の IP アドレスで連絡先をルックアップする場合は常に、証明書を受け入れるようクライアントがユーザに指示します。



重要

- サーバ名として IP アドレスを含むすべてのプロフィール写真の URL を更新することをお勧めします。クライアントがユーザに証明書の受け入れを要求しないようにするには、Cisco WebEx ドメインを含む FQDN で IP アドレスを置き換えます。
- 写真を更新すると、クライアントで写真が更新されるまで最大 24 時間かかります。

次の手順では、プロフィール写真の URL の更新方法について説明します。詳細については、該当する Cisco WebEx のマニュアルを参照してください。

手順

- ステップ 1 Cisco WebEx 管理ツールを使用して、ユーザ連絡先データを CSV ファイル形式でエクスポートします。
- ステップ 2 [userProfilePhotoURL] フィールドで、Cisco WebEx ドメインで IP アドレスを置き換えます。
- ステップ 3 CSV ファイルを保存します。
- ステップ 4 Cisco WebEx 管理ツールを使用して、CSV ファイルをインポートします。