デバイスへのアップロード

このメニューのオプションを使用して、新しいファームウェアまたはOSDロゴをデバイスにアップロードしたり、証明書を管理したりできます。 これらのオプションは、OSD から使用できません。

ファームウェアのアップロード

[Firmware] Web ページでは、新しいファームウェア ビルドをクライアントにアップロードできます。

図 *1*：*[Firmware Upload] Web* ページ

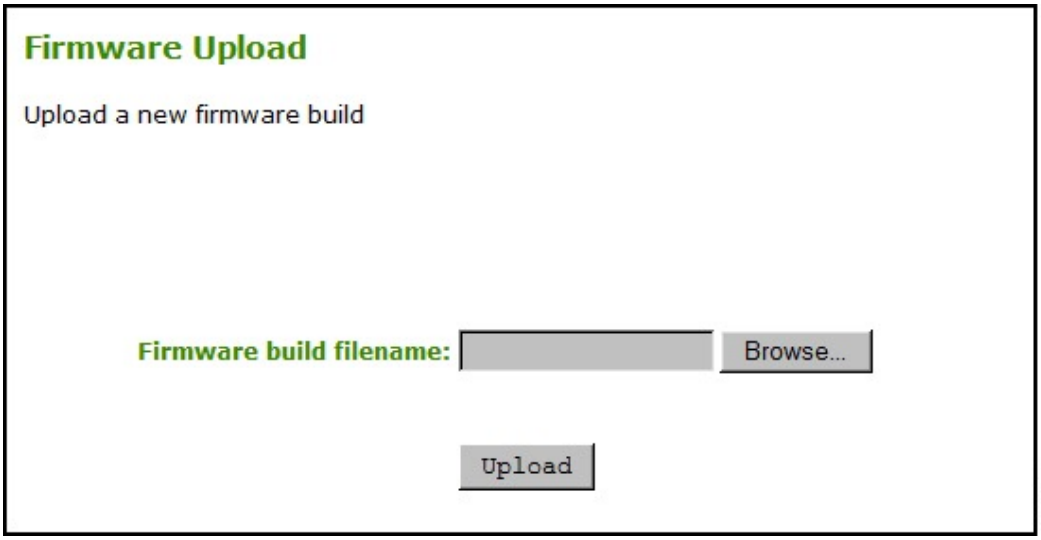

表 *1*：*[Firmware Upload]* のパラメータ

パラメータ	説明
Firmware build filename	アップロードされるファームウェアイメージのファイル名。[Browse] ボタンを使用してファイルを参照できます。 ファイルは、Web ブラウザ（ローカル ドライブ上またはアクセス可能なネットワーク ドライブ上）にアクセス可能である必要があります。 ファームウェア イメージは、`.all` ファイルになっている必要があります。
Upload	[Upload] ボタンをクリックして、指定したファイルをデバイスに転送します。 誤ったアップロードを防止するため、Webインターフェイスからこのアクションの確認を求められます。

ファームウェア アップロード プロセスの例

手順

1. クライアントが仮想マシンから切断されていることを確認します。
2. クライアントの管理用 Web インターフェイスにログインします（パスワードが有効になっている場合は、パスワードを使用）。
3. [Firmware Upload] Web ページから、ファームウェアの .all ファイルを参照します（たとえば、`tera1x00_rel1-9-v175.all`）。
4. [Open] をクリックします。
5. [Upload] をクリックします。
6. [OK] をクリックして、アップロードを続行することを確定します。 ファームウェアのアップロードが完了すると、「Success Flash successfully programmed! You must reset the device for the changes to take effect」というメッセージが表示されます。
7. [Reset] をクリックします。 「The PCoIP processor will reset on the next host system restart; your changes will take effect then. Are you sure you want to proceed?」というメッセージが表示されます。
8. [OK] をクリックします。
9. クライアントが自動的にリセットを行わない場合は、手動でリセットします。
10. PCoIP セッションを通常どおり開始します。

ロゴのアップロード

[OSD Logo]ページでは、イメージをデバイスにアップロードできます。 このイメージは、ローカル GUI オン スクリーン ディスプレイ（OSD）ロゴの [Connect] ウィンドウに表示されます。

[VMware View Advanced] ページには、[Use OSD Logo for View Banner] オプションがあり、View バナーの代わりに OSD ロゴが View ログイン画面に表示されるかどうかを設定できます。 詳細については、VMware View 接続の設定を参照してください。

図 *2*：*[OSD Logo Upload] Web* ページ

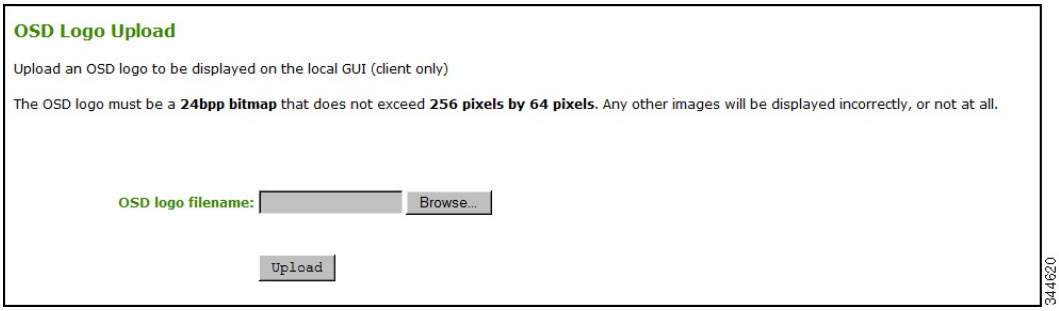

表 *2*：*[OSD Logo]* のパラメータ

パラメータ	説明
OSD logo filename	アップロードするロゴイメージのファイル名を指定します。 [Browse] ボタンを使用して対象ファイルを参照できます。 ファイルは、Web ブラウザ（ローカル ドライブ上またはアクセス可能なネットワーク ドライブ上）にアクセス可能である必要があります。 24 ビット/ピクセルのイメージは BMP 形式にする必要があり、その寸法が幅 256 ピクセル、高さ 64 ピクセルを超えてはいけません。 ファイル拡張子が正しくない場合、エラー メッセージが表示されます。
Upload	[Upload] をクリックして、指定したイメージ ファイルをクライアントに転送します。アップロードを確認するメッセージが表示されます。

OSD ロゴのアップロード プロセスの例

手順

1. [OSD Logo] Web ページで [Browse] をクリックし、対象のロゴ ファイルを検索します。
2. [Open] をクリックします。
3. [Upload] をクリックします。 「Are you sure? This will upload a new logo for the local GUI. This operation may take a few minutes」というメッセージが表示されます。
4. [OK] をクリックします。

5 OSD ロゴのアップロードが完了するまで待ちます。 正常にアップロードされると、そのことを示すメッセージが表示されます。
6 クライアントをリセットします。

証明書のアップロード

[Certificate Upload] ページでは、CA ルート証明書とクライアント証明書をアップロードして、管理できます。 証明書は 16 件までアップロードできます。 ファームウェア リリース 3.5 では、PCoIP プロトコルは 802.1X 対応ネットワークの 802.1X クライアント証明書を 1 つだけ読み取ります。 そのクライアント証明書に PCoIP デバイスのすべてのセキュリティ情報が含まれていることを確認します。

図 *3*：*[Certificate Upload]* ページ

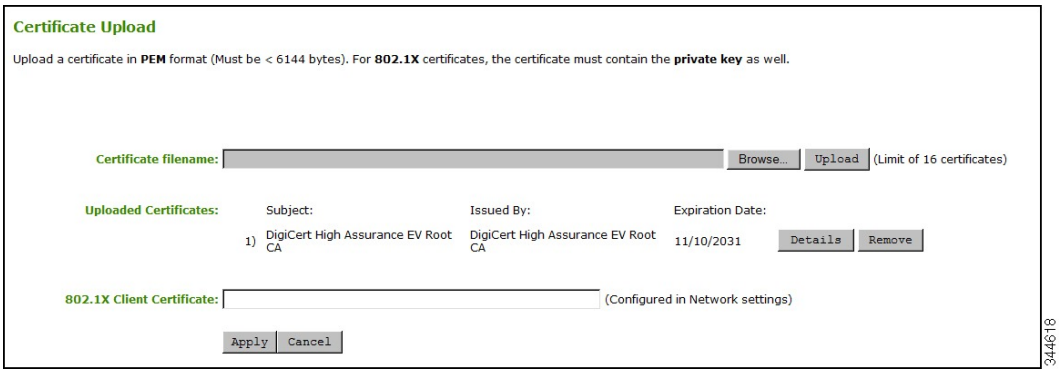

表 *3*：*[Certificate Upload]* のパラメータ

パラメータ	説明
Certificate filename	最大 16 件のルート証明書とクライアント証明書をアップロードします。
Uploaded Certificates	これにより、アップロードされた証明書が表示されます。 アップロードされた証明書を削除するには、[Remove] ボタンをクリックします。 デバイスをリブートした後に削除が行われます。 証明書の詳細を表示するには、[Detail] ボタンをクリックします。 これらの証明書は、[Network] ページの [Client Certificate] ドロップダウンメニューでオプションとして表示されます。
802.1X Client Certificate	これは、読み取り専用フィールドです。 [Network] ページの [Client Certificate] フィールドにリンクされています。

802.1X 認証に向けた証明書のアップロード

802.1X 認証を使用する場合の一般的なガイドラインを次に示します。 詳細は、Teradici サポートサイトの PCoIP ゼロ クライアントの証明書管理情報を参照してください。

- 802.1X 認証では、802.1X クライアント証明書と 802.1X サーバ CA ルート証明書の 2 つの証明書が必要です。
- 802.1X クライアント証明書の形式は .pem で、RSA 暗号化を使用する秘密キーが含まれている必要があります。 証明書が別の形式になっている場合、秘密キーを含め最初に証明書を .pem 形式に変換してからアップロードします。
- 802.1X クライアント証明書を [Certificate Upload] ページからアップロードしたら、[Network] ページで 802.1X 認証を設定する必要があります。 このためには 802.1X 認証を有効にし、ゼロ デバイスの ID 文字列を入力し、ドロップダウン リストから正しい 802.1X クライアント証明書を選択して、設定を適用します。 詳細については、ネットワーク設定を参照してください。
- 802.1X サーバ CA ルート証明書の形式は .pem でなければなりませんが、秘密キーを含める必要はありません。 証明書が別の形式になっている場合、証明書を .pem 形式に変換してからアップロードします。 この証明書は [Network] ページで設定する必要はありません。
- 802.1X クライアント証明書と 802.1X サーバ CA ルート証明書は両方とも、6 KB 未満でなければなりません。そうしないと、アップロードできなくなります。 複数の証明書を含んだ証明書ファイルもあります。 証明書ファイルのサイズが大きすぎて、複数の証明書が中に入っている場合、ファイルをテキストエディタで開き、証明書をそれぞれコピーして自分のファイルに保存できます。

View 5.1 セキュリティ設定

ゼロ クライアントを VMware View 5.1 に接続する場合、SSL はデフォルトで View Connection Server（VCS）で有効になっています。 ゼロ クライアントからの接続がセキュアでない場合、ゼロ クライアントの [VCS Certificate Check Mode] 設定に応じて、VCS はユーザを許可、警告、またはブロックできます（デフォルト設定：[Warn if the connection may be insecure]）。

デフォルトでは、ゼロ クライアントの証明書信頼ストアは空です（管理用 PCoIP ルート CA 証明書は除く）。

注意 ゼロ クライアントをファームウェア リリース 3.5.x からファームウェア リリース 4.0.0 にアップグレードしたら、ユーザは警告を受け入れ、通常どおりログインしてデスクトップに接続できます。 ただし、IEEE 802.1x 証明書がゼロ クライアントにアップロードされているものの、VCS によって信頼されたルート証明書がアップロードされていない場合、View Connection Server は接続をブロックします。

ゼロ クライアントでの警告またはブロックされた接続を回避するには、次のいずれかを実行する必要があります。

- （推奨）VCS によって信頼された SSL ルート証明書をゼロ クライアントにアップロードします。 管理 Web インターフェイスからアップロードできます。 この場合、ゼロ クライアントは警告を出さずに接続できます（[connection] ダイアログの [VCS address] フィールドに [HTTPS] が緑色で表示されます）。
- （非セキュア）[VCS Certificate Check Mode] を [Allow the unverifiable connection] に設定します。 OSD または管理 Web インターフェイスを使用して、このパラメータをゼロ クライアントの [Session] ページで設定できます。 この場合、すべての接続が許可されます（[connection] ダイアログの [VCS address] フィールドに [HTTPS] が赤の取り消し線で表示されます）。

Cisco VXC 2111/2211 からの証明書の削除

以前にロードした証明書を Cisco VXC 2111/2211 から削除し、[Trusted View Connection Server] リストをクリアするには、次の手順を実行します。

1. 管理 Web インターフェイスで、[Upload] > [Certificates] をクリックします。
2. [Uploaded Certificates] リストで、証明書を選択し、[Remove] をクリックします。（複数の証明書を削除するには、必要に応じてこの手順を繰り返します）。
3. [Apply] をクリックします。
4. [Continue] をクリックします。
5. 管理 Web インターフェイスで、[Configuration] > [Session] をクリックします。
6. [Advanced Options] の [Trusted View Connection Servers] フィールドで、[Clear] をクリックします。
7. [Apply] をクリックします。
8. [Continue] をクリックします。