Starfield SSL Install Manual

for

Multi-Domain & Wildcard

on

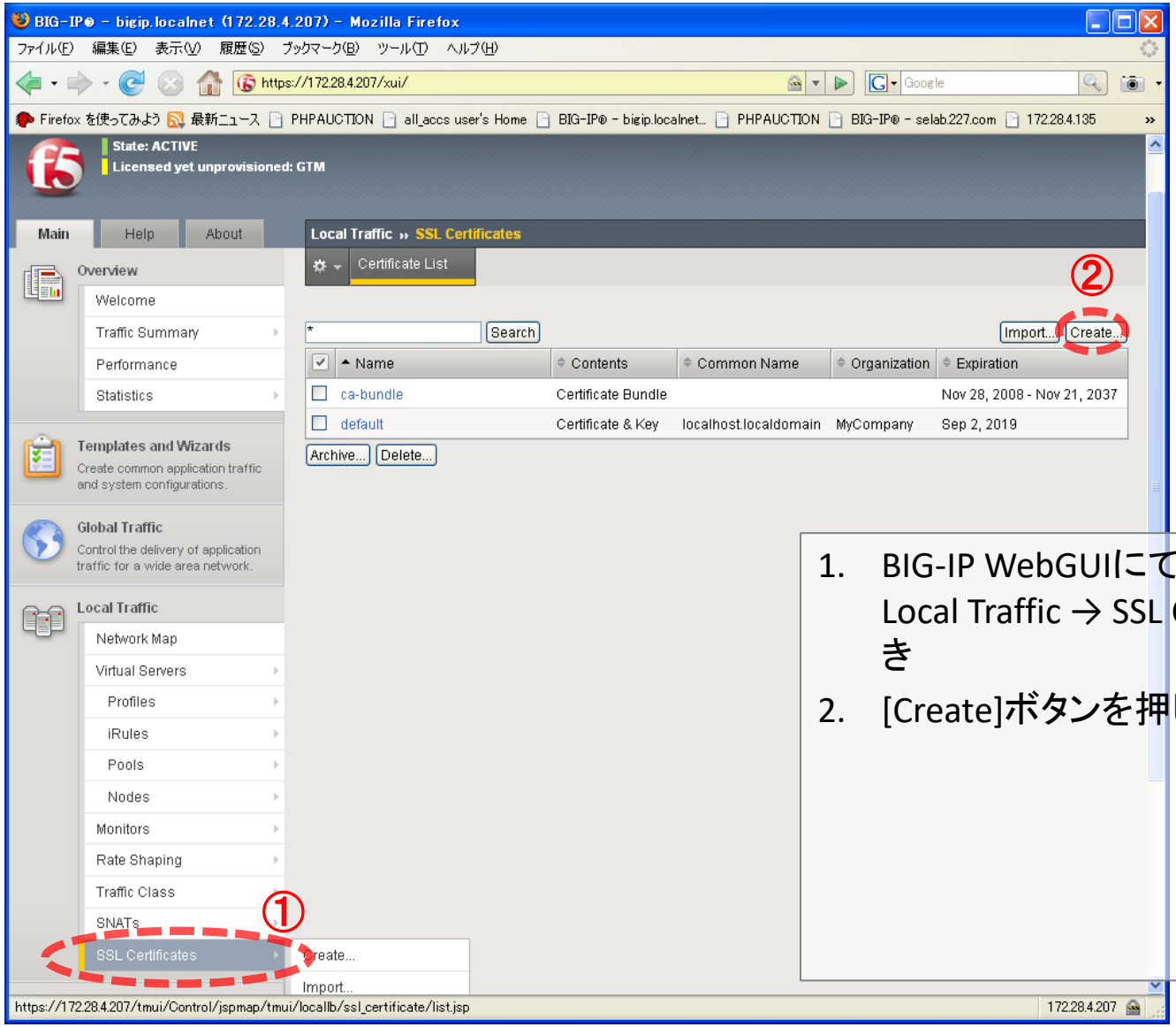
Big- IP/F5

ジェイサート株式会社

CSRファイル作成手順

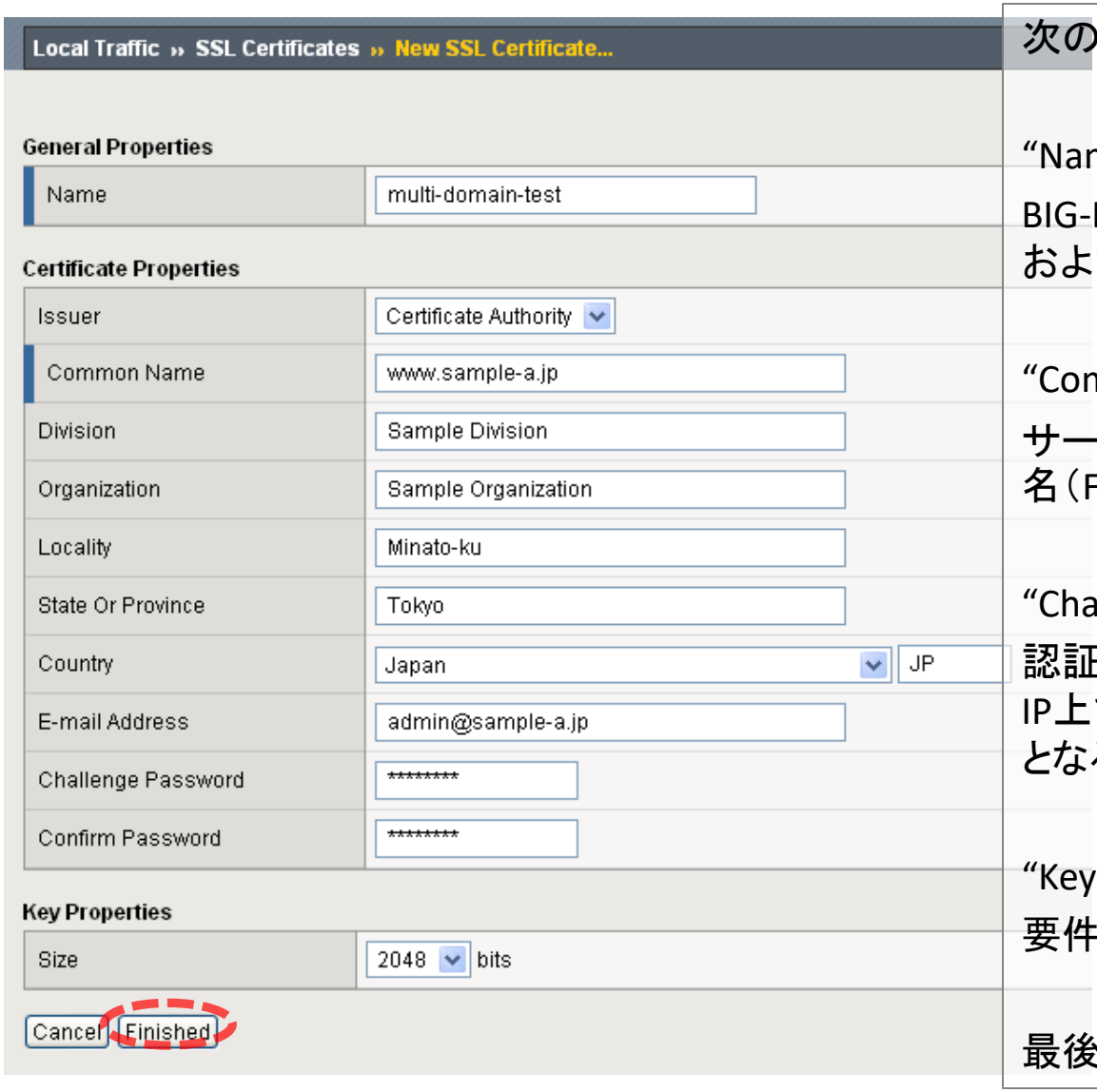
CSRをBIG-IP上で作成する場合は、以下の手順にて行います。
他のシステムにて作成されたサーバ秘密鍵（key）, 証明書（Certificate）をインポートする場合はこの項目の手順は不要です。

CSRファイル作成手順(1)



1. BIG-IP WebGUIにて、
   Local Traffic → SSL Certificateの画面を開き
2. [Create]ボタンを押します。

CSRファイル作成手順(2)



次の画面で適宜値を入力します。

“Name”

BIG-IP上で作成されるファイルおよびCSRおよびKeyにつけられる名前です。

“Common Name”

サーバ証明書の証明対象となるサーバ名（FQDN）です。

“Challenge Password”

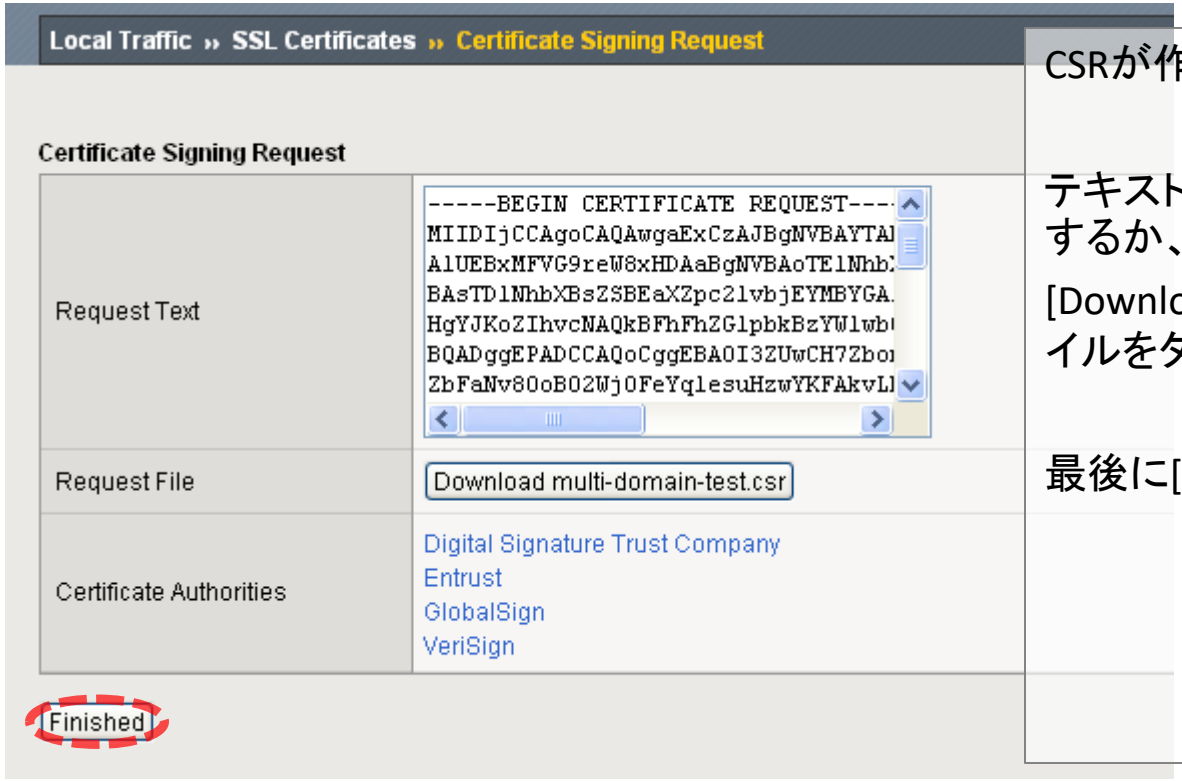
認証局に署名を依頼する際、およびBIG-IP上で当該の証明書を利用する際に必要となるパスワードです。

“Key Properties”

要件に応じて鍵長を設定してください。

最後に[Finished]を押します。

CSRファイル作成手順(3)



CSRが作成されました。

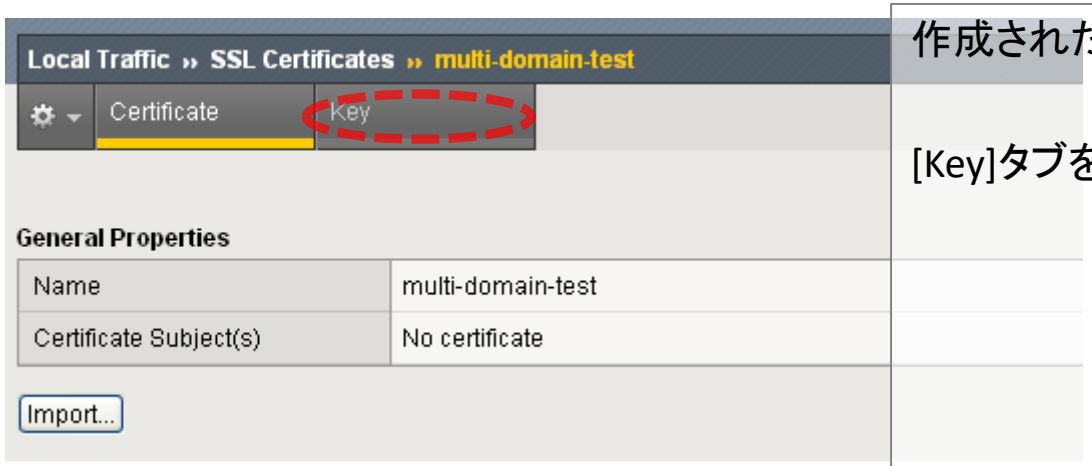
テキストウィンドウ内のテキストをコピーするか、

[Download xxxx.csr]ボタンを押してCSRファイルをダウンロードします。

最後に[Finished]を押します。

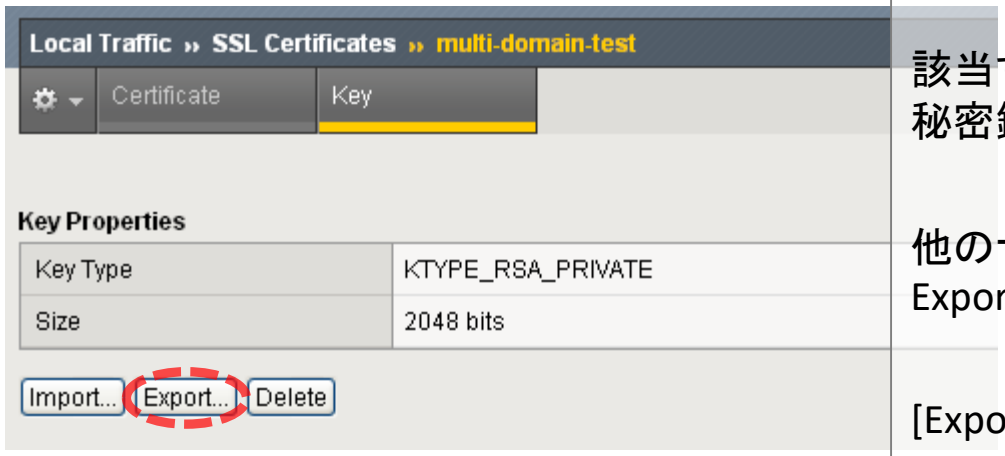
サーバ秘密鍵の保存(バックアップ)

サーバ秘密鍵の保存(1)



作成されたCSRに関する概要が表示されます。

[Key]タブを押します。

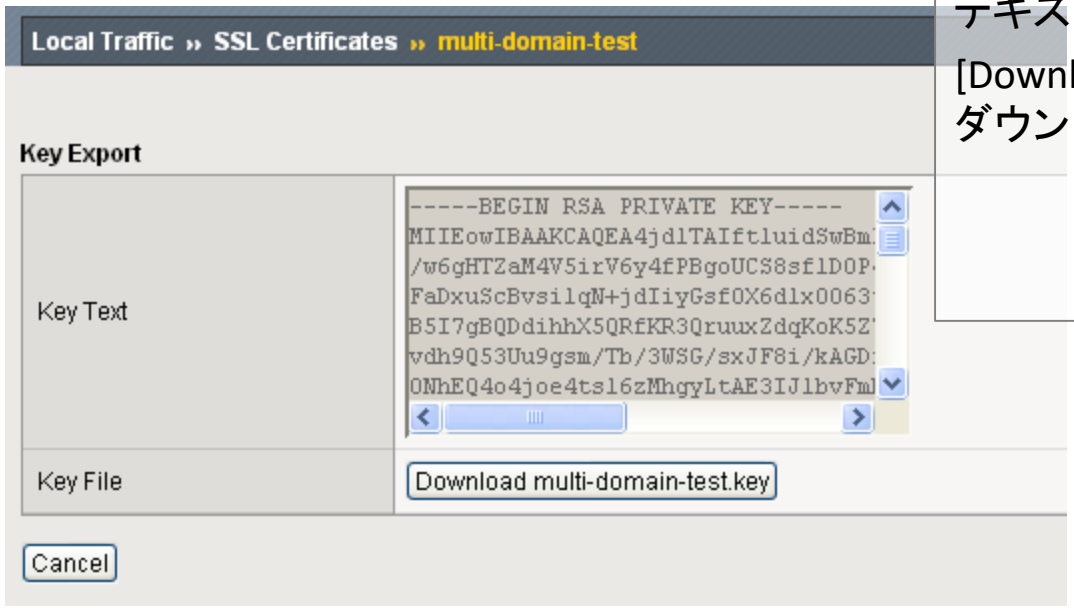


該当するCSRのために生成されたKey(サーバ秘密鍵)に関する概要が表示されます。

他のサーバでの利用やバックアップのためにExportすることができます。

[Export]タブを押します。

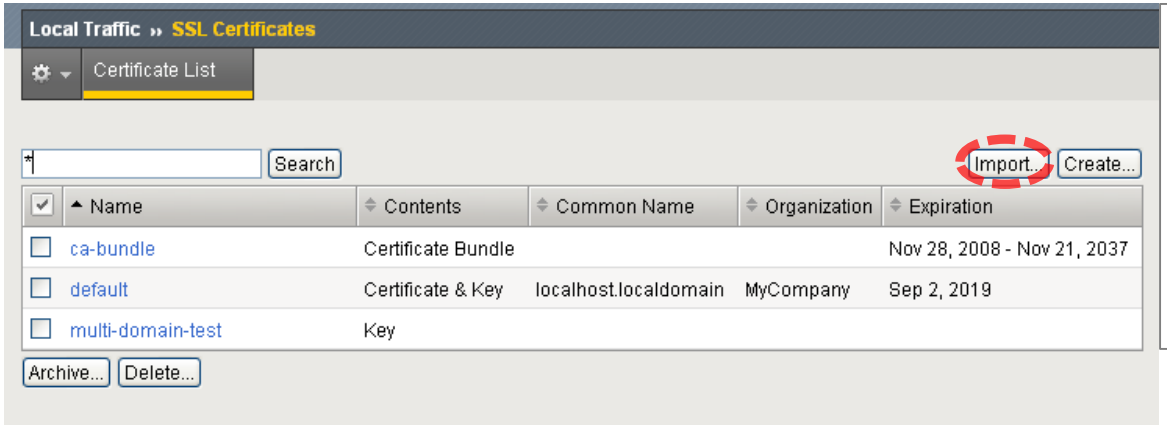
サーバ秘密鍵の保存(2)



テキストウィドウの中身をコピー、または
[Download xxxx.key]ボタンを押してファイルをダウンロードします。

中間証明書インストール手順

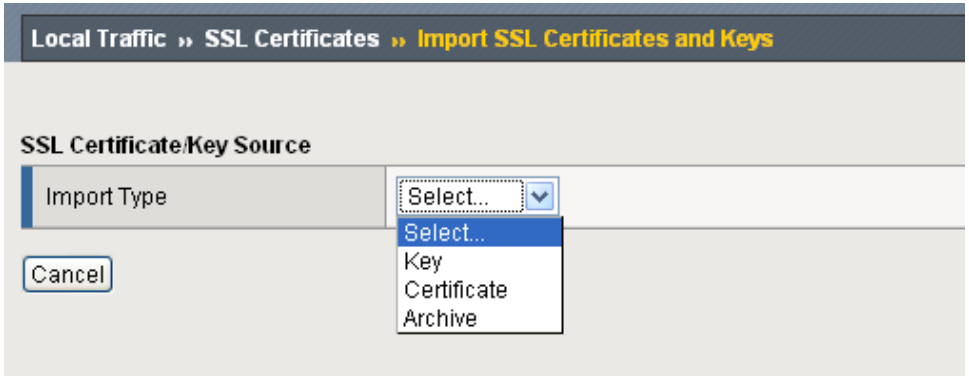
中間証明書インストール手順(1)



必要な中間証明書をインポートします。

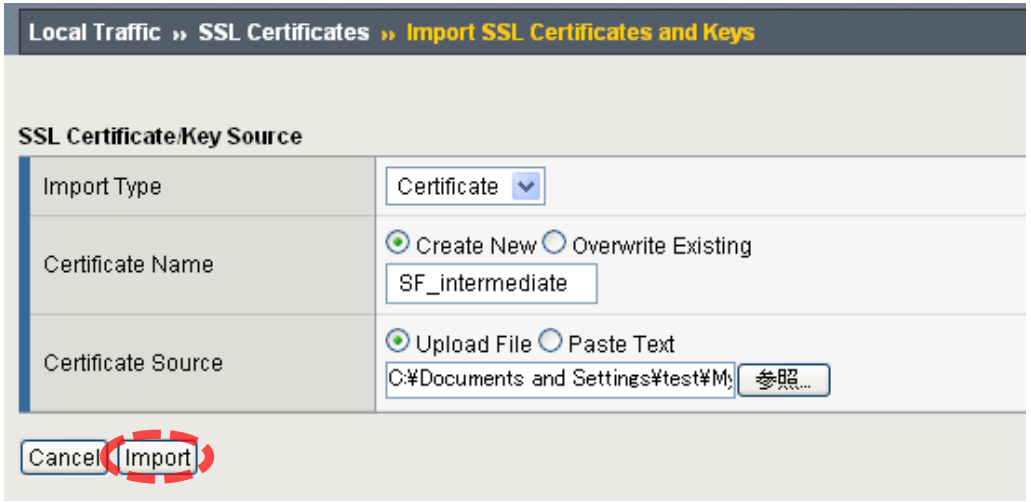
- https://www.jcert.co.jp/support/certificate/ から、
- **“bundle.crt”形式ファイル**を取得。

[Import]ボタンを押してファイルをアップロードします。

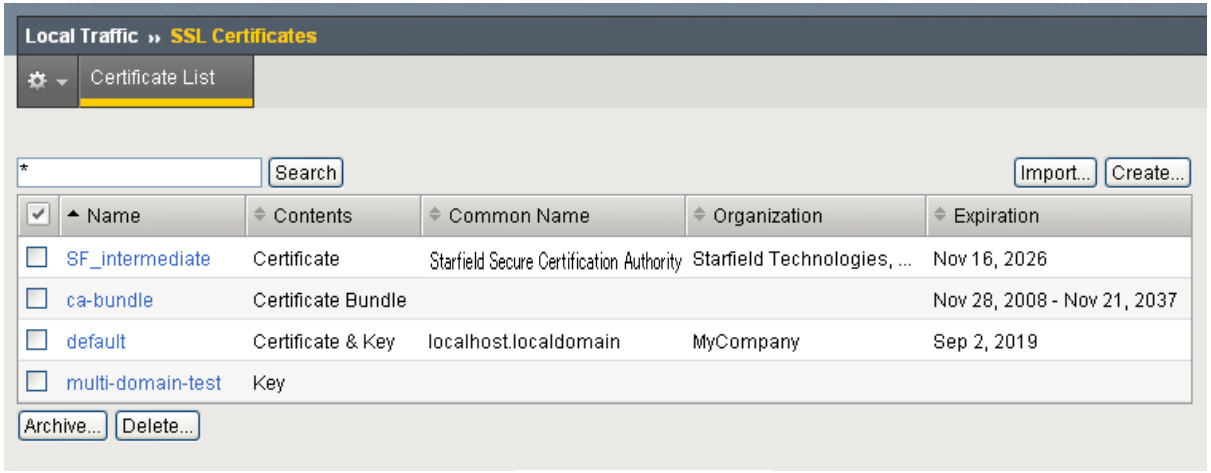


次のページにて、“Import Type”に”Certificate”を選択します。

中間証明書インストール手順(2)



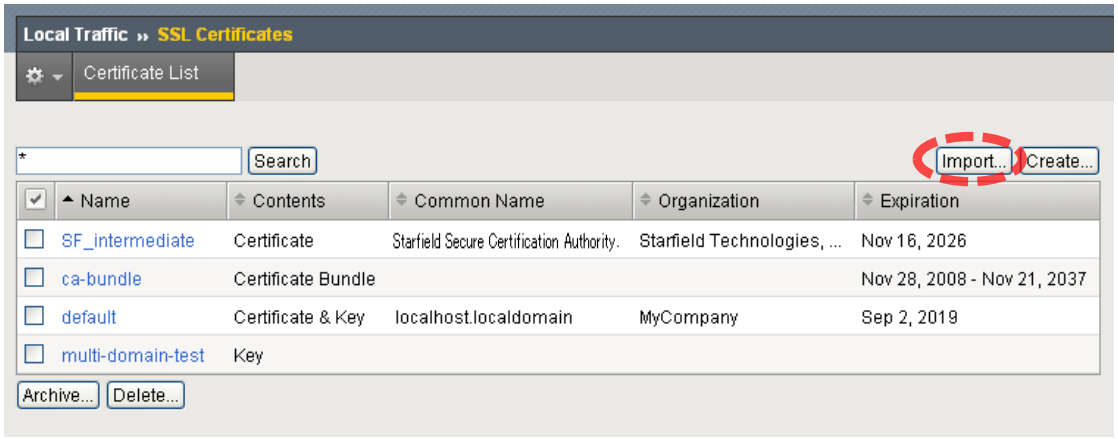
任意の”Certificate Name”を設定し、該当する中間証明書を選択。
[Import]ボタンを押してファイルをアップロードします。



SSL Certificatesの画面にて、該当する中間証明書がインポートされていることと確認できます。

サーバ証明書インストール手順

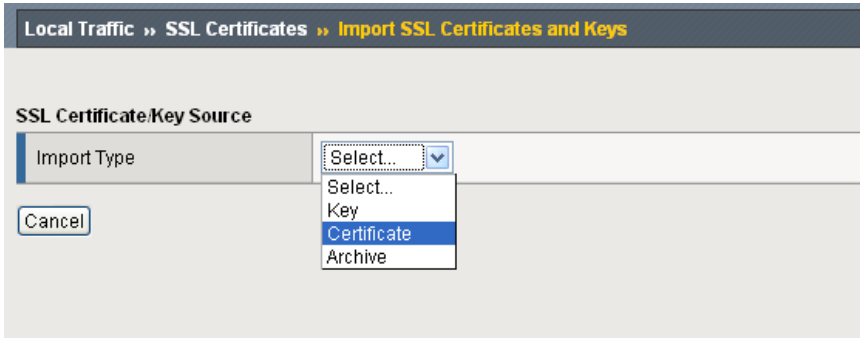
サーバ証明書インストール手順(1)



認証局より署名されたサーバ証明書をインポートします。

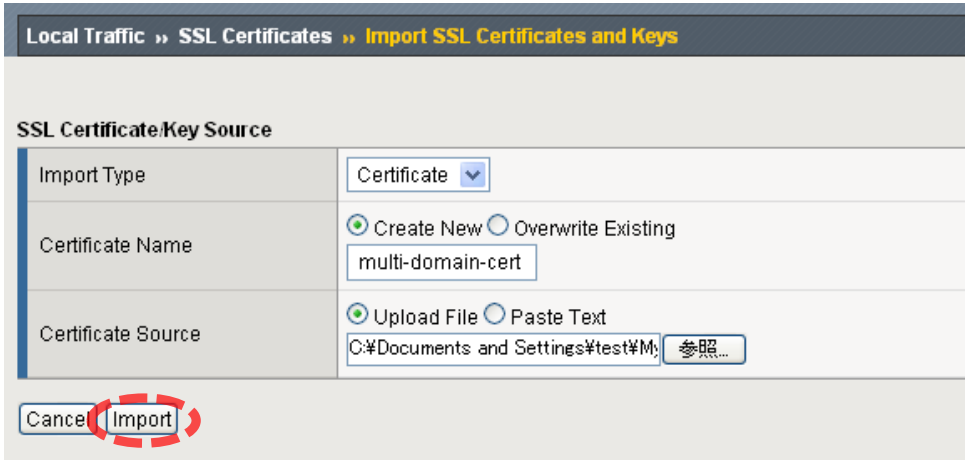
Local Traffic →SSL Certificatesの画面にて、

[Import]ボタンを押します。



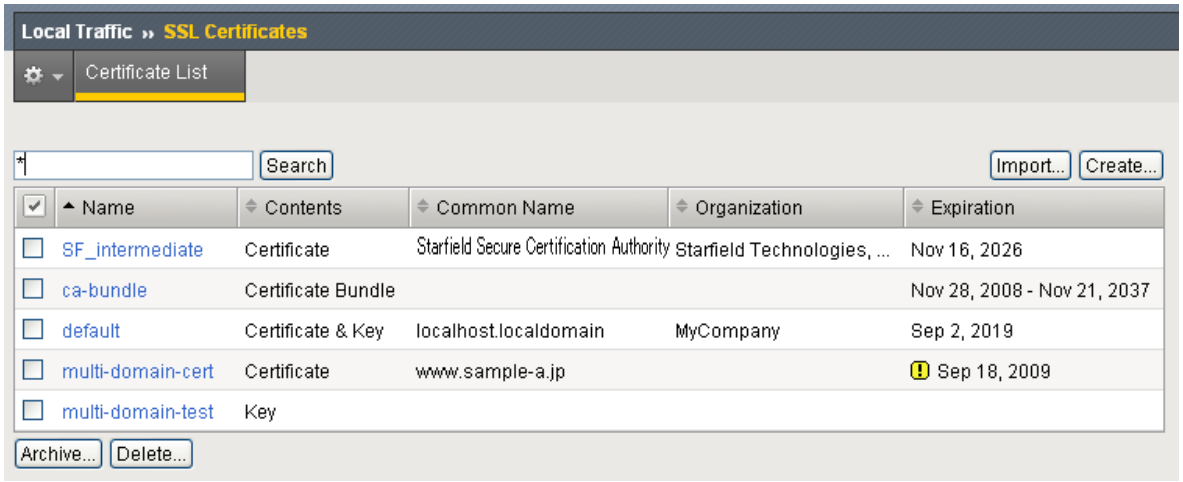
次のページにて、“Import Type”に”Certificate”を選択します。

サーバ証明書インストール手順(2)



任意の”Certificate Name”を設定し、該当するサーバ証明書を選択。

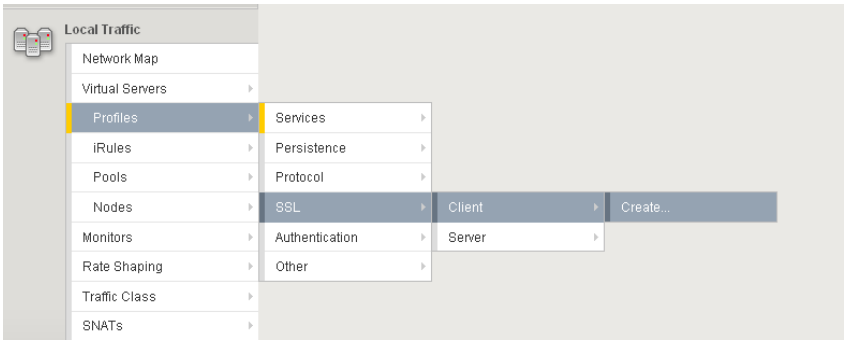
[Import]ボタンを押してファイルをアップロードします。



SSL Certificatesの画面にて、該当する証明書がインポートされていることと確認できます。

サーバ証明書適用手順（例）

サーバ証明書適用手順(1)　SSLプロファイル



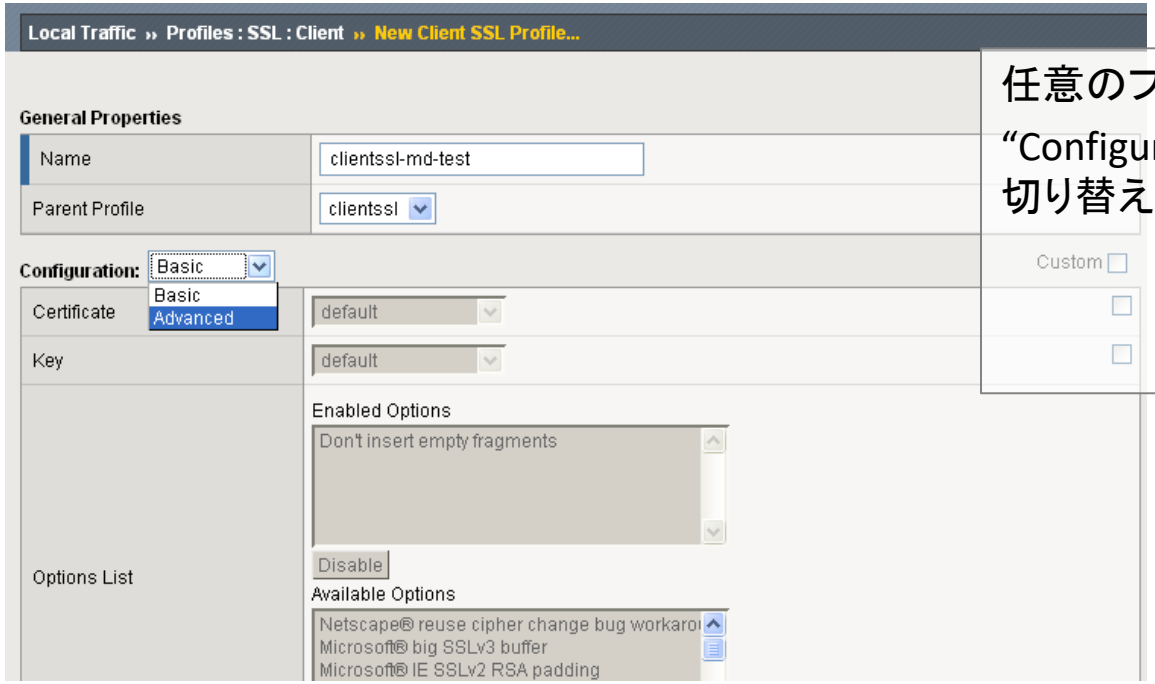
インポートしたサーバ証明書を適用するためのClientSSLプロファイルを作成します。

左図のようにFly-outメニュー(v10以降の機能)から
Profiles → SSL → Client → Create

または

または、
Profiles → SSLタブ → Client → [Create]ボタン
と進みます。

サーバ証明書適用手順(2)　SSLプロファイル



任意のプロファイル名を設定し、
“Configuration”を”Advanced”メニューに切り替えます。

サーバ証明書適用手順(3)　SSLプロファイル

必要な設定項目は以下の通りです。

各項目の右側のチェックボックスにチェックを入れることで、値の編集が可能になります。

“Certificate”

認証局によって署名され、先の手順でインポートしたサーバ証明書です。

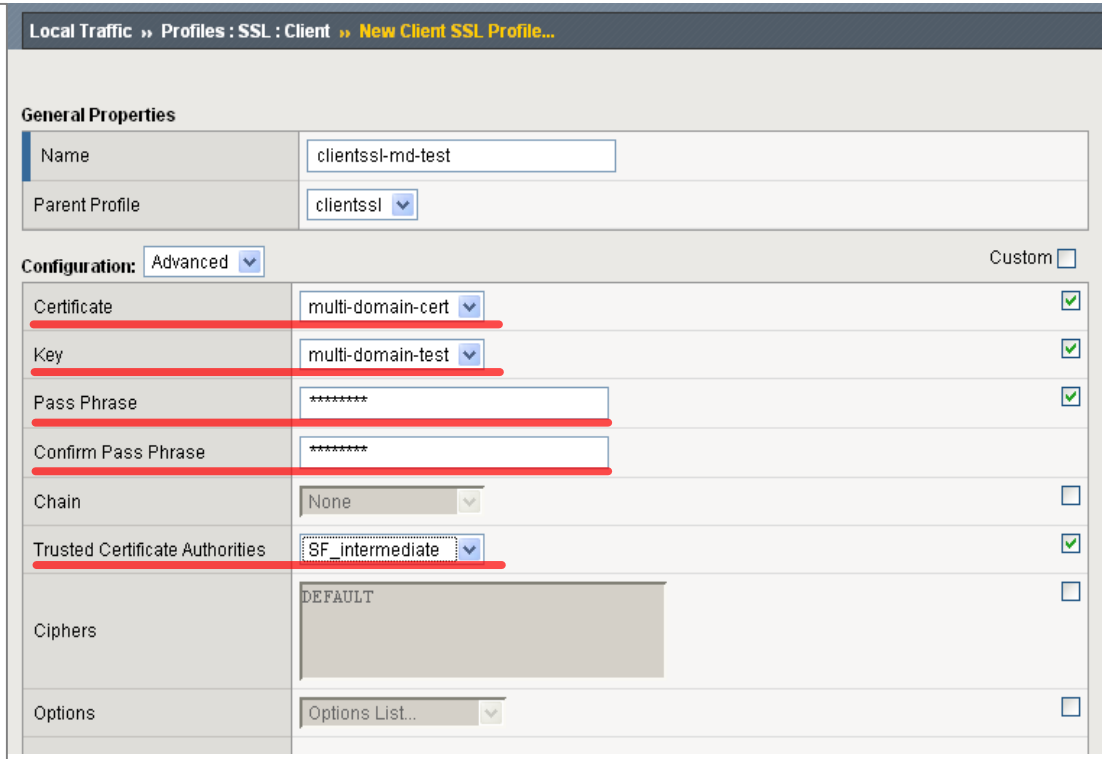
BIG-IPにインポートした際につけた名称をプルダウンメニューから選択します。

“Key”

BIG-IP上でCSRを作成した場合にはCSRと同じ名称のKey（サーバ秘密鍵）を、外部からインポートしたKeyを使う場合はインポート時につけた名前を選択します。

“Pass Phrase”

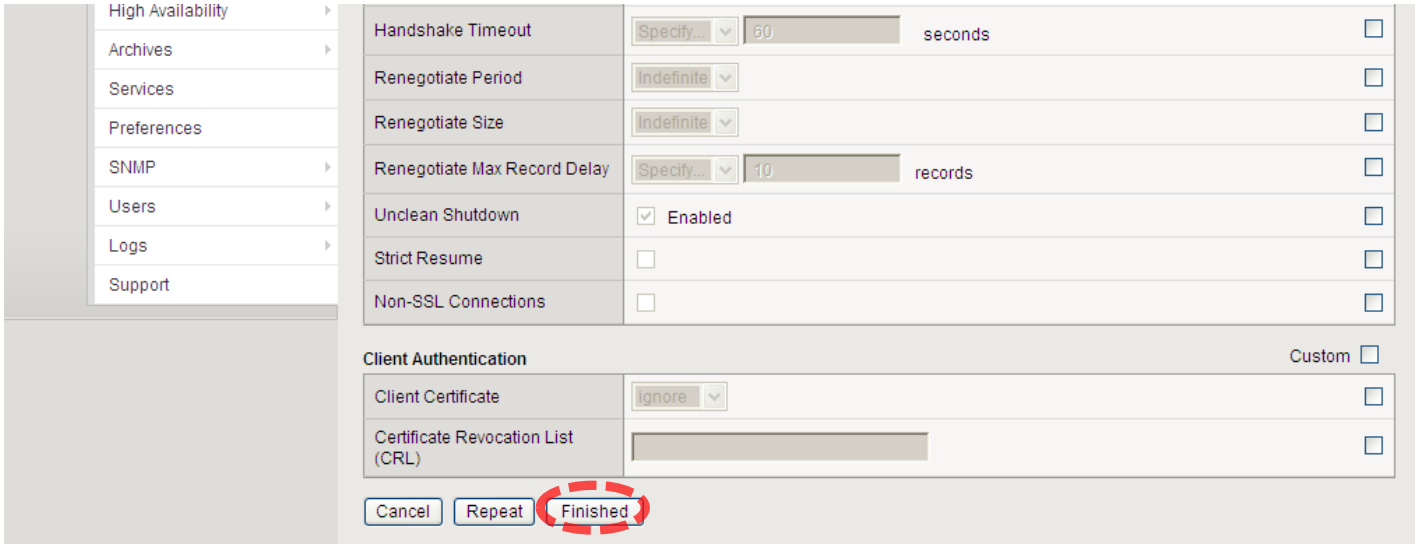
上で選択したKey（サーバ秘密鍵）を作成する際に設定したパスワードです。



“Trusted Certificate Authorities”

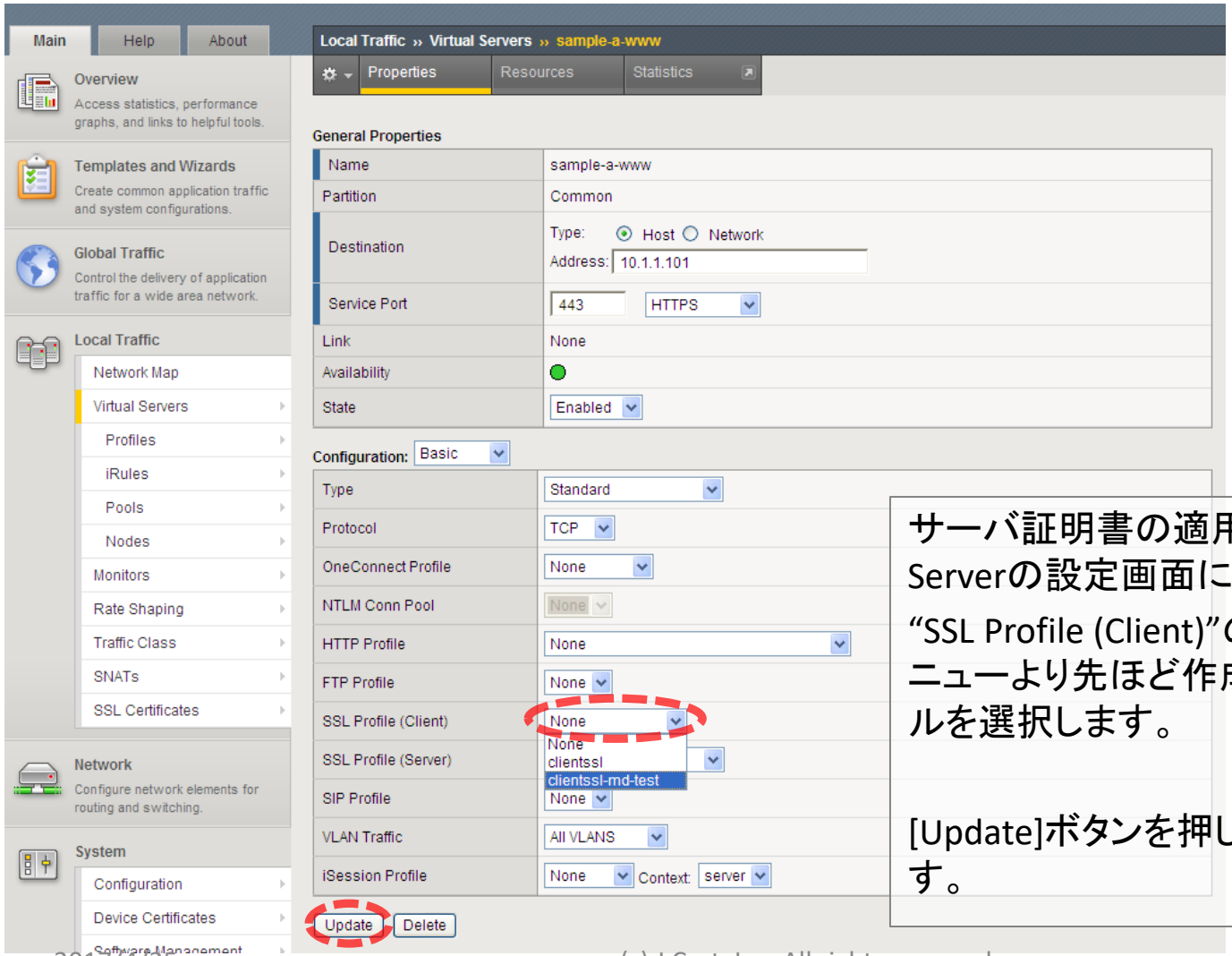
先の手順でインストールした中間証明書をプルダウンメニューから選択します。

サーバ証明書適用手順(3)　SSLプロファイル



[Finished] ボタンを押してSSLプロファイルの作成を完了します。

サーバ証明書適用手順(4) Virtual Server設定

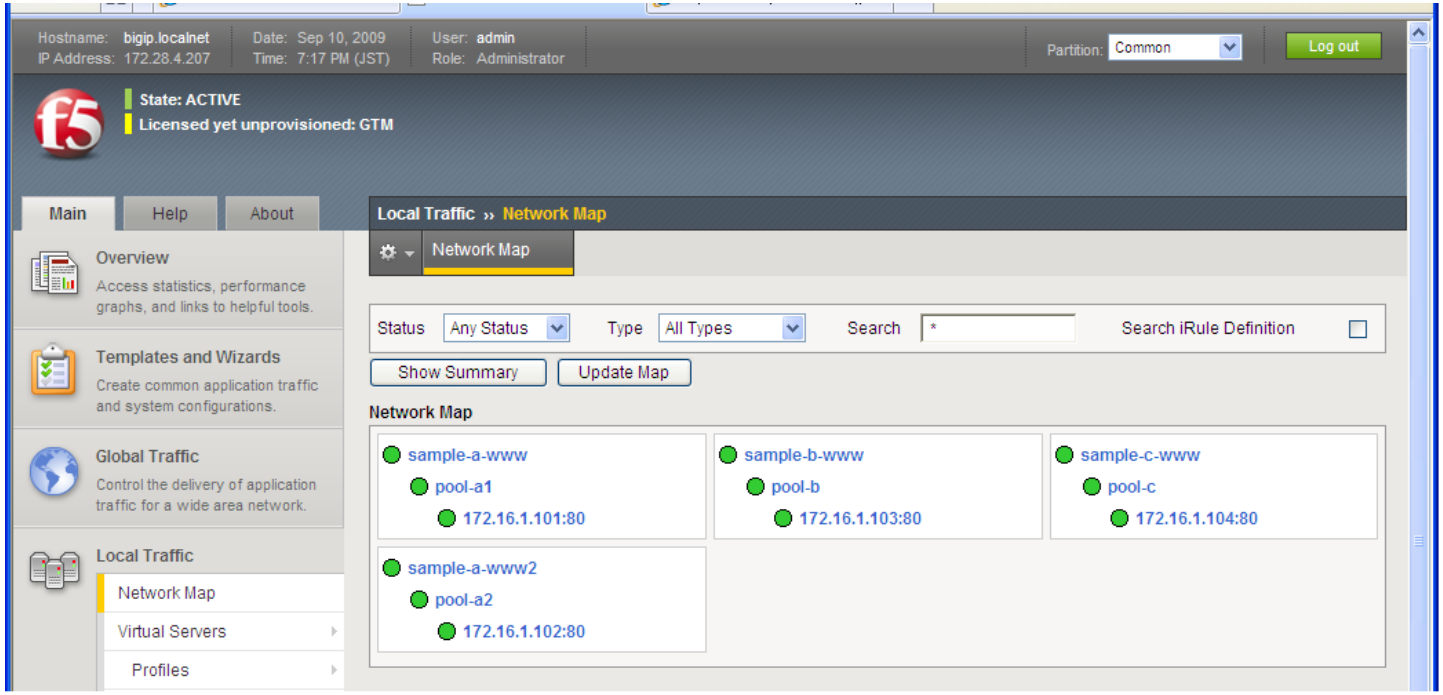


サーバ証明書の適用対象であるVirtual Serverの設定画面にて、

“SSL Profile (Client)”のプルダウンメニューより先ほど作成したSSLプロファイルを選択します。

[Update]ボタンを押して設定を反映します。

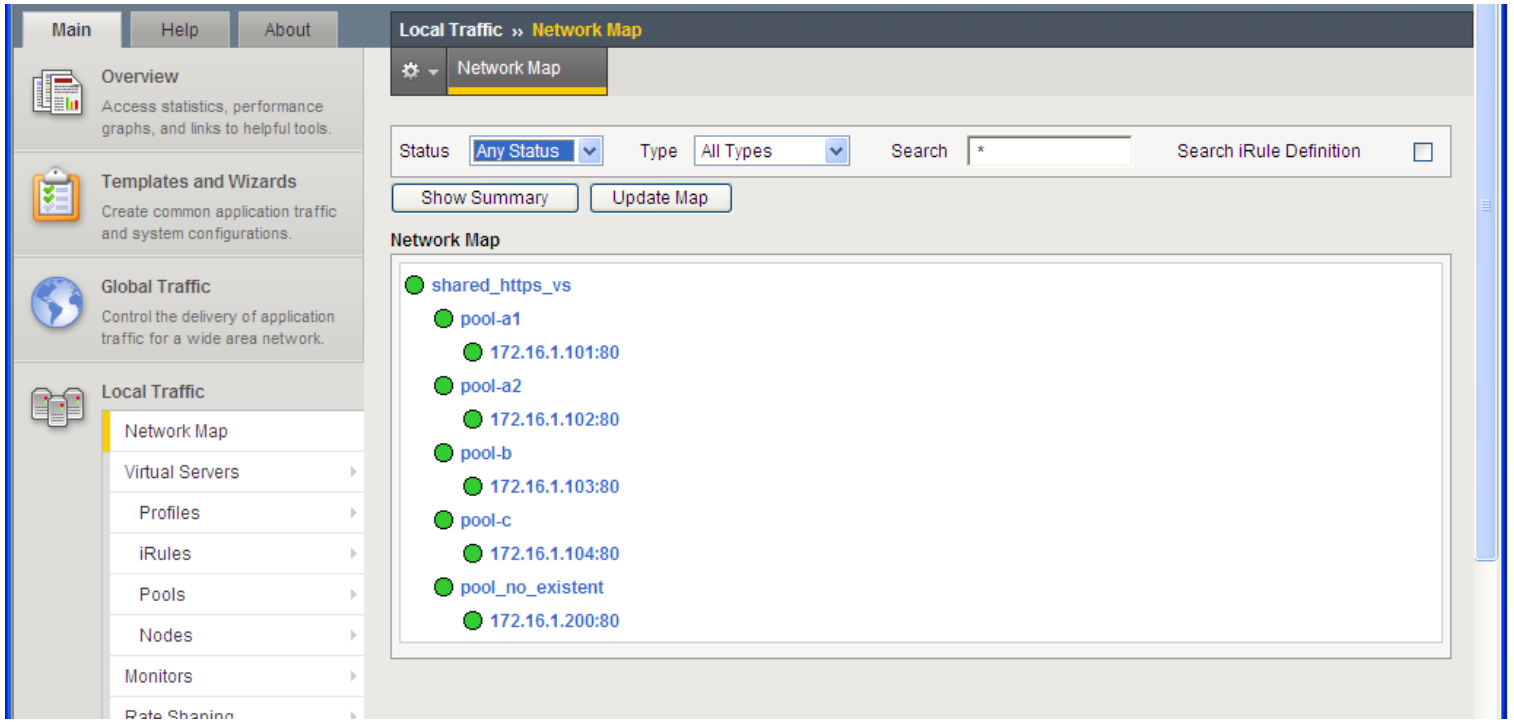
サーバ証明書適用手順(5)



MultiDomain証明書の対象となるWebサーバが個別にIPアドレスを持つ場合は、BIG-IP上でのVirtual ServerはIPアドレス（およびポート）ごとに個別に作成しますが、

- 一つのSSL証明書を複数のSSLプロファイルに割り当てる、または
- 一つのSSL証明書を一つのSSLプロファイルに割り当て、それを複数のVirtual Serverに適用することのどちらも可能です。

サーバ証明書適用手順(6)



MultiDomain証明書の対象となるWebサーバが一つのIPアドレスを共有する場合は、BIG-IP上でのVirtual Serverは一つ作成し、BIG-IPのHTTP Class機能等を用いて、リクエストされたホスト名に応じて適切なWebサーバにトラフィックを振り分けます。

この場合は、MultiDomain証明書を一つのSSLプロファイルに割り当て、それを一つのVirtual Serverに適用して利用します。