cybertrust

Riverbed®
Stingray Traffic Manager
CSR作成/証明書インストール手順書

はじめに

【！】本手順書をご利用の前に必ずお読みください

1. 本ドキュメントは、「Riverbed ® /Stingray Traffic Manager」の環境下でサイバートラストのサーバー証明書をご利用いただく際の CSR 作成とサーバー証明書のインストールについて解説するドキュメントです。
2. 本ドキュメントは、図研ネットウエイブ株式会社のご協力の元、作成しております。
3. 実際の手順はお客様の環境により異なる場合があり、「Stingray Traffic Manager」の動作を保証するものではございません。あらかじめご了承ください。
4. このドキュメントは予告なく変更される場合があり、サイバートラスト株式会社はその内容に対して責任を負うものではありません。また、このドキュメント内に誤りがあった場合、サイバートラスト株式会社は一切の責任を負いません。
5. このドキュメントの一部または全部を複製することは禁じられており、提供または製造を目的として使用することはできません。ただし、サイバートラスト株式会社との契約または同意文書で定められている場合に限り、この注記の添付を条件として複製することができます。

はじめに

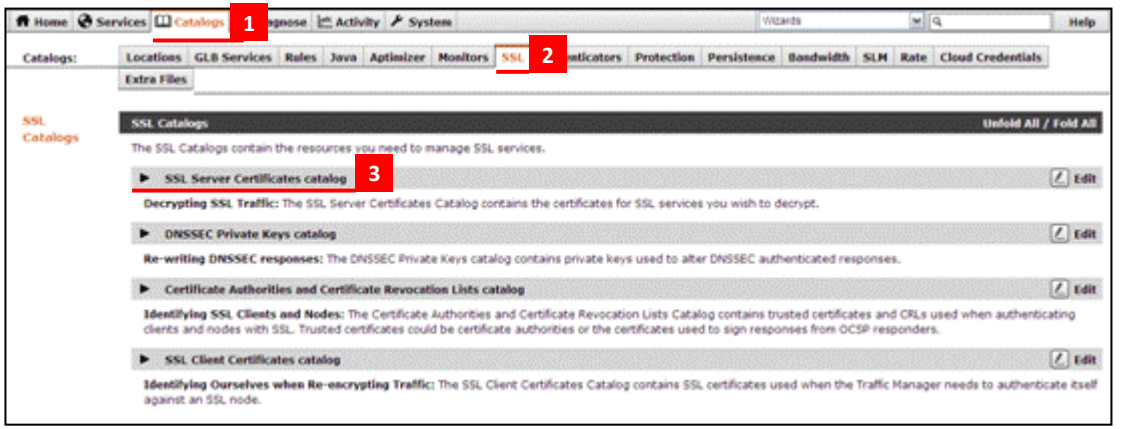
目　次

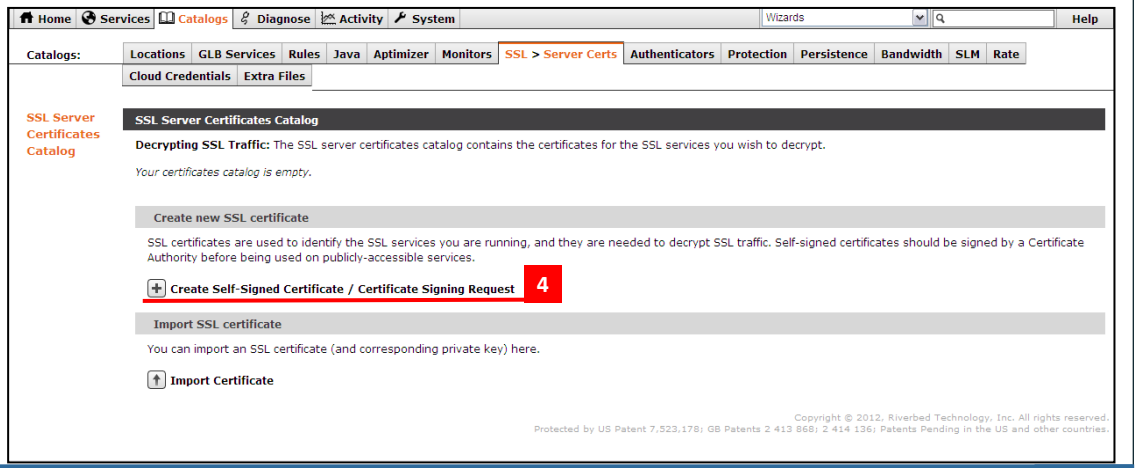
1. CSRの作成

■CSRを作成します。

※CSRの作成方法は、以下のWebページもご参照下さい。
https://www.cybertrust.co.jp/ssl/support/csr.html

1. Administration interface へログイン後、Home画面から[Catalogs]タブをクリックします。
2. [SSL]タブをクリックします。
3. [SSL Server Certificates catalog]をクリックします。
4. [Create new SSL certificate]の「Create Self-Signed Certificate / Certificate Signing Request」をクリックします。





1. CSRの作成

5. [Name:]に任意の登録名を指定します。
この値は、証明書の設定時などに使用します。

※空欄の場合は、【6】の値が使用されます。

6. [Common Name (CN):]に、「実際に接続するURLのFQDN」を指定します。

例）https://www.cybertrust.ne.jp/index.html

⇒ www.cybertrust.ne.jp

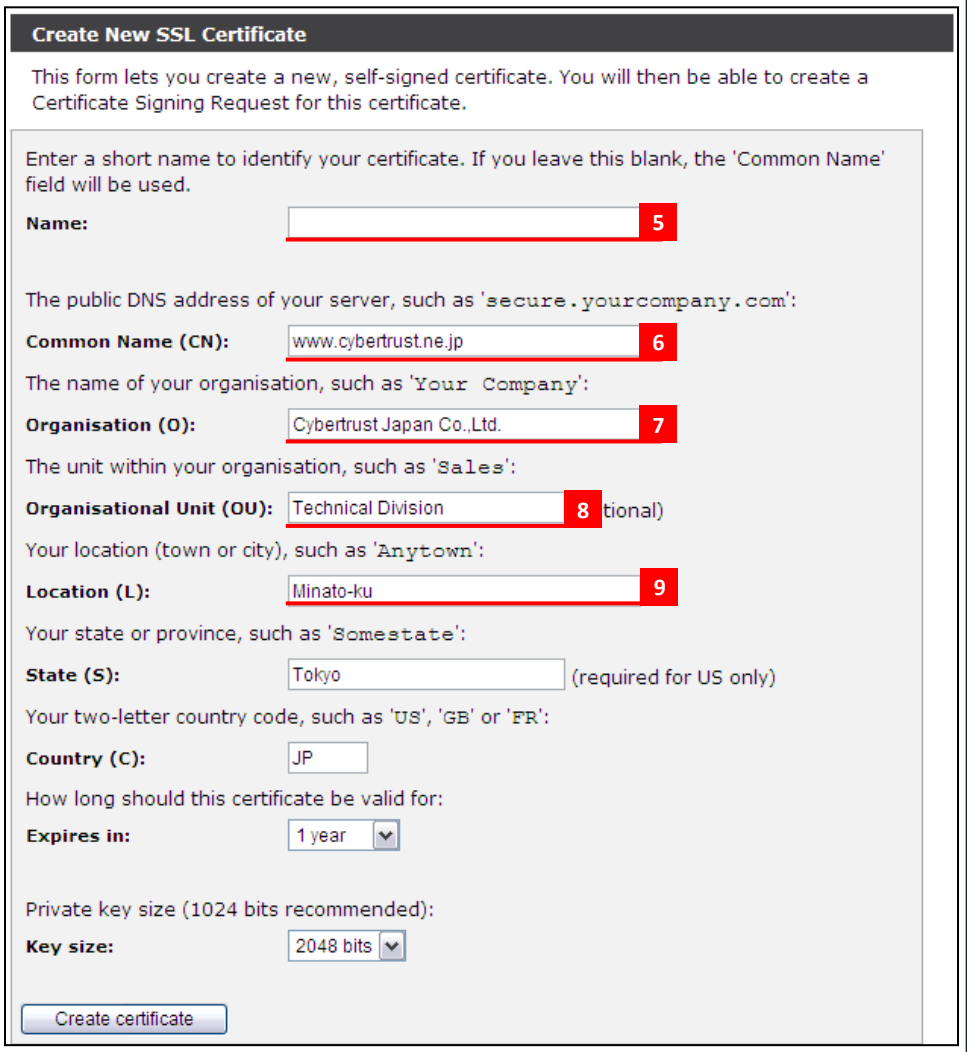
7. [Organisation (O):]に「申請組織の名称（英名）」を指定します。

8. [Organisational Unit (OU):]に任意の値（部署名など）を指定します。

※2022年6月23日以降に発行されるサーバー証明書には含まれません。

※この値は空欄でも構いません。

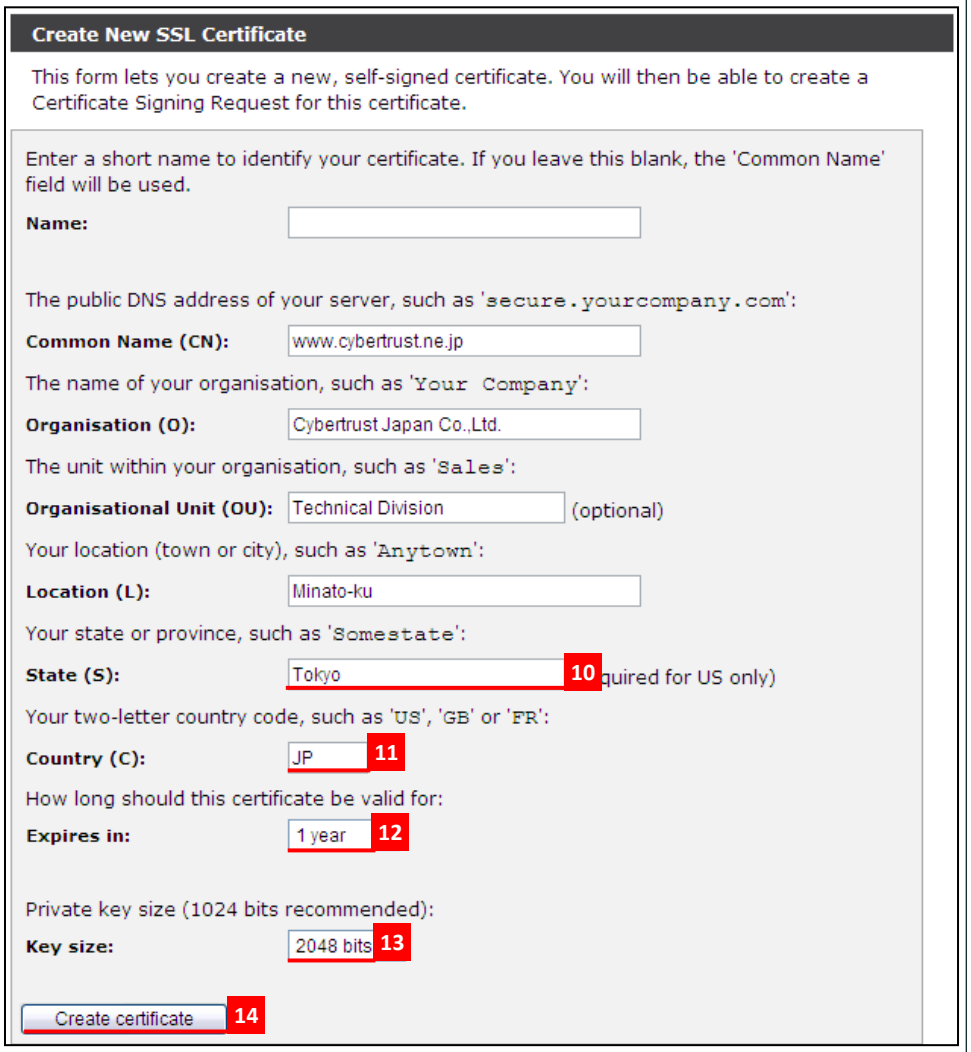
9. [Location (L):]に申請組織の事業所住所の「市町村名（英名）※」を指定します。
※東京 23 区は区名を指定します。



1. CSRの作成

10. [State (S):]に申請組織の事業所住所の「都道府県名（英名）」を指定します。
11. [Country (C):]に申請組織の「国名（JP固定）」を指定します。
12. [Expires in:]はCSRと同時に作成される自己署名用の証明書の有効期限を設定します。

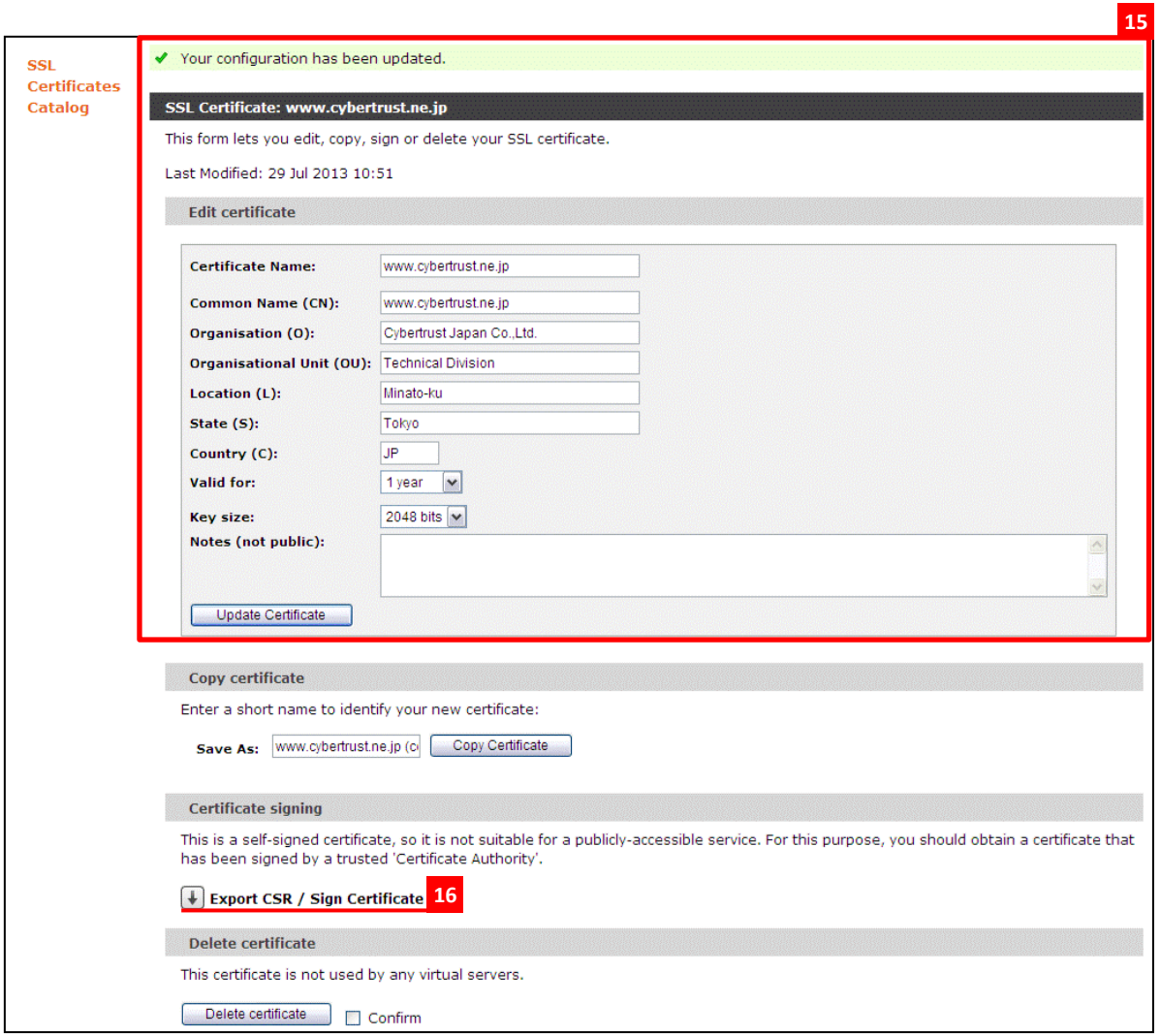
    CSRや弊社から発行される証明書には影響がないため、デフォルトで構いません。
13. [Key size:]は「2048 bits」を指定します。
14. すべての入力が終わったら、「Create certificate」ボタンをクリックします。



1. CSRの作成

15. 「Your configuration has been updated.」と表示され、指定した値が表示されます。
ご指定の値にお間違いがないか、確認してください。

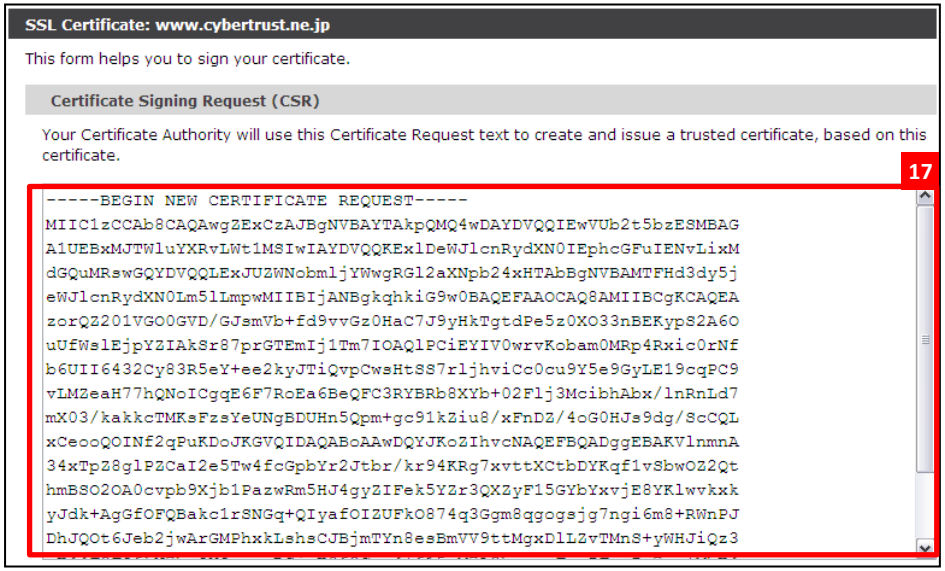
16. 「Export CSR / Sign Certificate」をクリックします。



1. CSRの作成

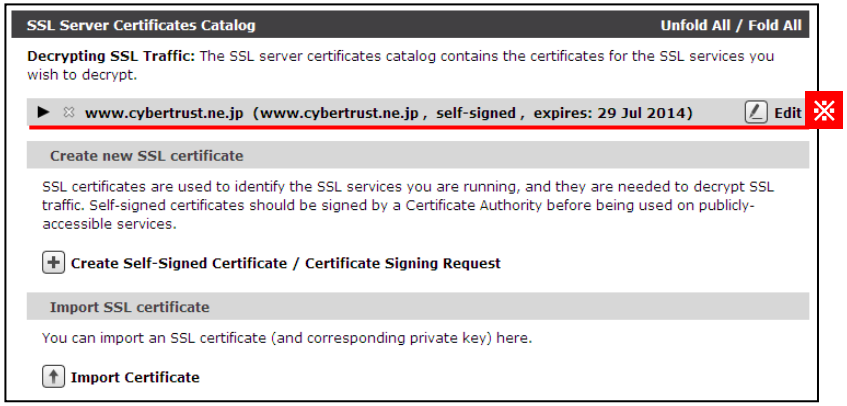
17. [Certificate Signing Request (CSR)]にCSRの内容が表示されますので、「-----BEGIN NEW CERTIFICATE REQUEST-----」から「-----END NEW CERTIFICATE REQUEST-----」の部分までを全てコピーし、テキストファイルへ貼り付けて任意の名前で保存してください。

※右記のCSRはサンプルです。ご申請にはご利用いただけません。



以上で、CSRの作成は完了です。

※サーバー証明書のインストールができなくなるため、[SSL Server Certificates Catalog]に表示されている右記を削除しないよう、ご注意ください。



2.証明書のお申し込み

■証明書のお申し込みを行います。

作成したCSRをテキストエディタで開いて「-----BEGIN NEW CERTIFICATE REQUEST-----」から、「-----END NEW CERTIFICATE REQUEST-----」までをハイフンを含めすべてコピーし、WEBの申請サイト(※)の申請フォームへ貼り付けて、弊社へお申し込みください。なお、1文字でも欠けると正しく解析できませんのでご注意ください。

※WEBの申請サイトは以下よりご利用いただけます。

▼SureBoard

https://sstra.cybertrust.ne.jp/IRA/loginSb/

▼SureHandsOn

https://sstra.cybertrust.ne.jp/IRA/loginSho/

＜CSRサンプル＞ ※お申し込みにはご利用いただけません。

```
-----BEGIN NEW CERTIFICATE REQUEST-----
.....
MIIEhDCCA2wCAQAwgYkxCzAJBgNVBAYTAkpQMQ4wDAYDVQQIDAVUb2t5bzESMBAG
A1UEBwwJTWluYXRvLWt1MSIwIAYDVQQKDBlDeWJlcnRydXN0IEphcGFuIENvLixM
dGQuMRIwEAYDVQQLDAlUZXN0IFVuaXQxHjAcBgNVBAMMFXRlc3QuY3liZXJ0cnVz
2t/rD9fTPgo7u4aYzw4BpnAqLmGgy3XpsvCo6f4ROcFsgrk05FgeUCaeDFyllEST
.....
-----END NEW CERTIFICATE REQUEST-----
```

弊社にてお申し込み内容の審査を行い、すべてのお手続き完了後にサーバー証明書を発行いたします。(発行はメールにてお知らせいたします。)

サーバー証明書が発行されましたら、次のステップへお進みください。

3.証明書のダウンロード

■インストールが必要となるサーバー証明書と中間CA証明書を事前にダウンロードします。

【1】サーバー証明書のダウンロード

サーバー証明書が発行されましたら、証明書発行のお知らせのメール内リンクより事前にダウンロードし、【.cer】や【.txt】などの拡張子で保存してください。

※サーバー証明書のダウンロードについては、以下をご参考ください。

https://www.cybertrust.co.jp/ssl/support/download.html

【2】中間CA証明書のダウンロード

サーバー証明書をご利用の際、お使いの機器へ中間CA証明書のインストールが必要となります。

ご選択いただいた商品により必要な証明書が異なりますので、証明書の種類をご確認のうえ、以下弊社ホームページからダウンロードしてください。

▼ルート・中間CA証明書のダウンロード

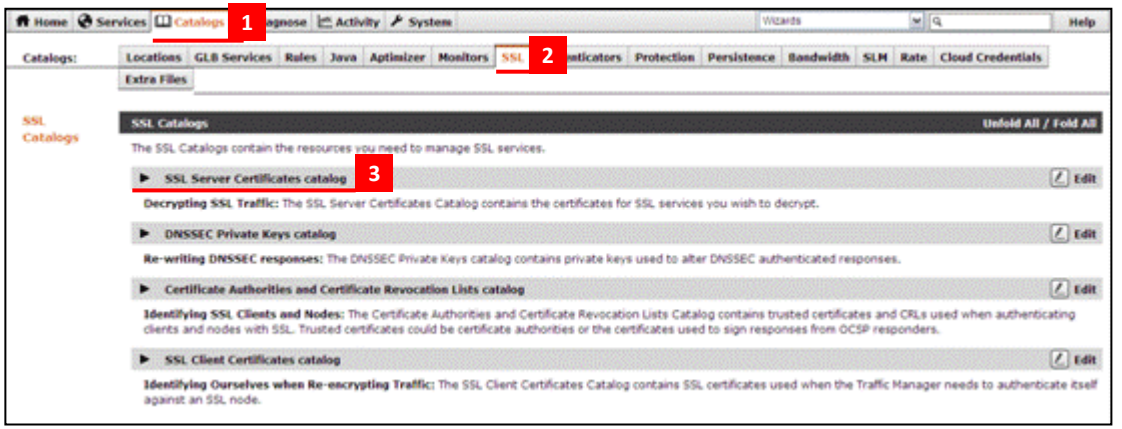
https://www.cybertrust.ne.jp/ssl/download-ca/

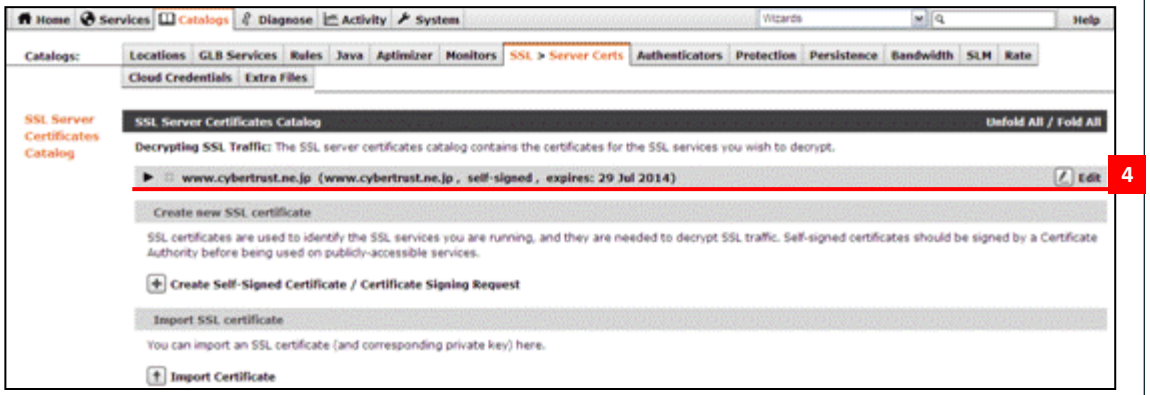
4.証明書のインストール

■サーバー証明書と中間CA証明書をインストールします

【1】サーバー証明書のインストール

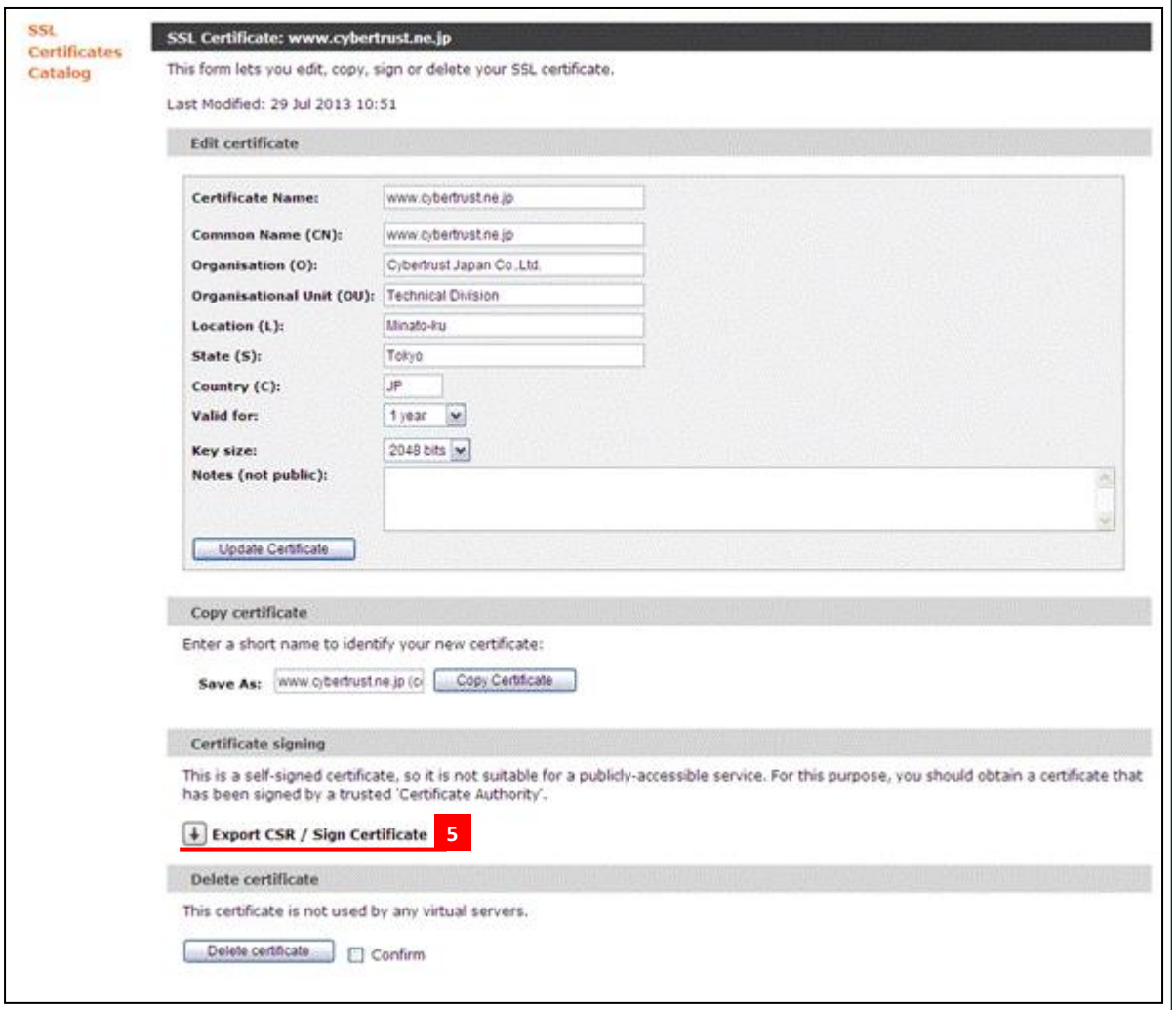
1. Administration interface へログイン後、Home画面から[Catalogs]タブをクリックします。
2. [SSL]タブをクリックします。
3. [SSL Server Certificates Catalog]をクリックします。
4. CSR作成時に[Name] で指定した値をクリックします。





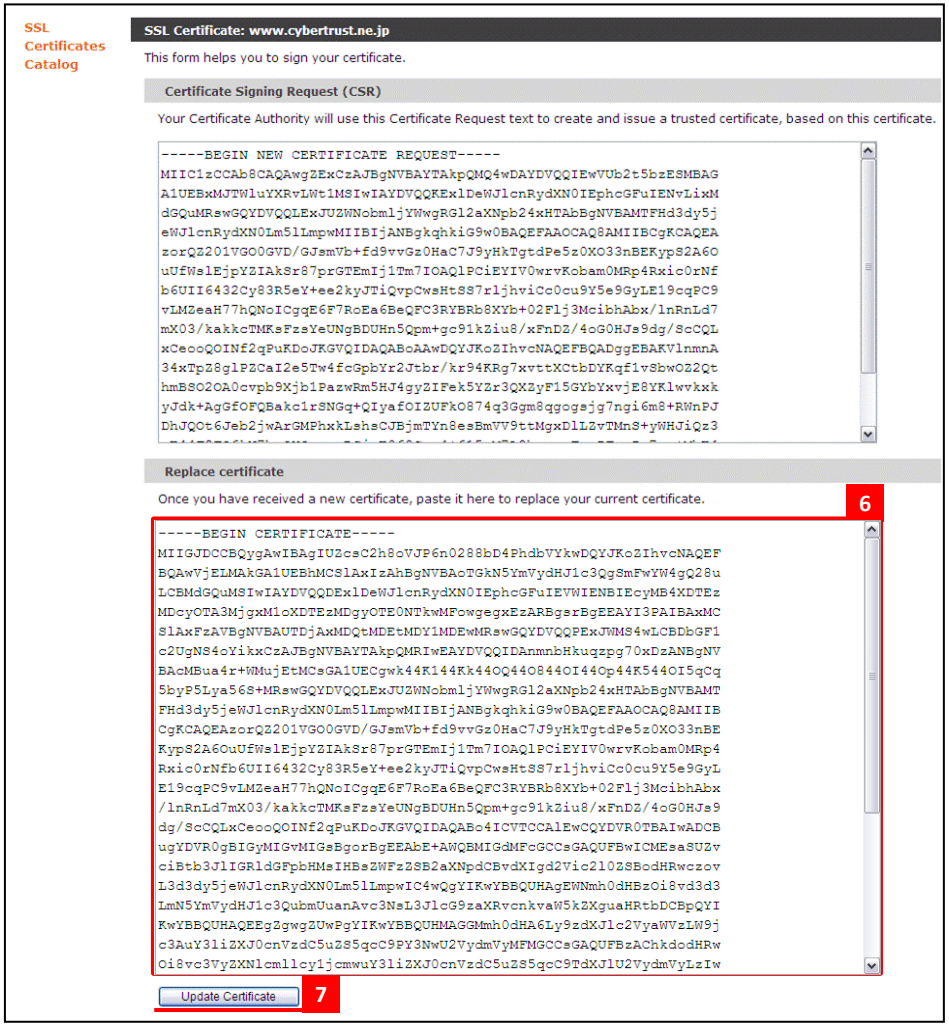
4.証明書のインストール

5. 「Export CSR / Sign Certificate」をクリックします。



4.証明書のインストール

6. サーバー証明書をテキストエディタなどで開き、「-----BEGIN CERTIFICATE-----」から「-----END CERTIFICATE-----」まで、ハイフンを含めてすべてコピーして貼り付けます。
7. 「Update Certificate」ボタンをクリックします。



4.証明書のインストール

8. 「Your configuration has been updated.」と表示され、設定したサーバー証明書の内容が表示されます。

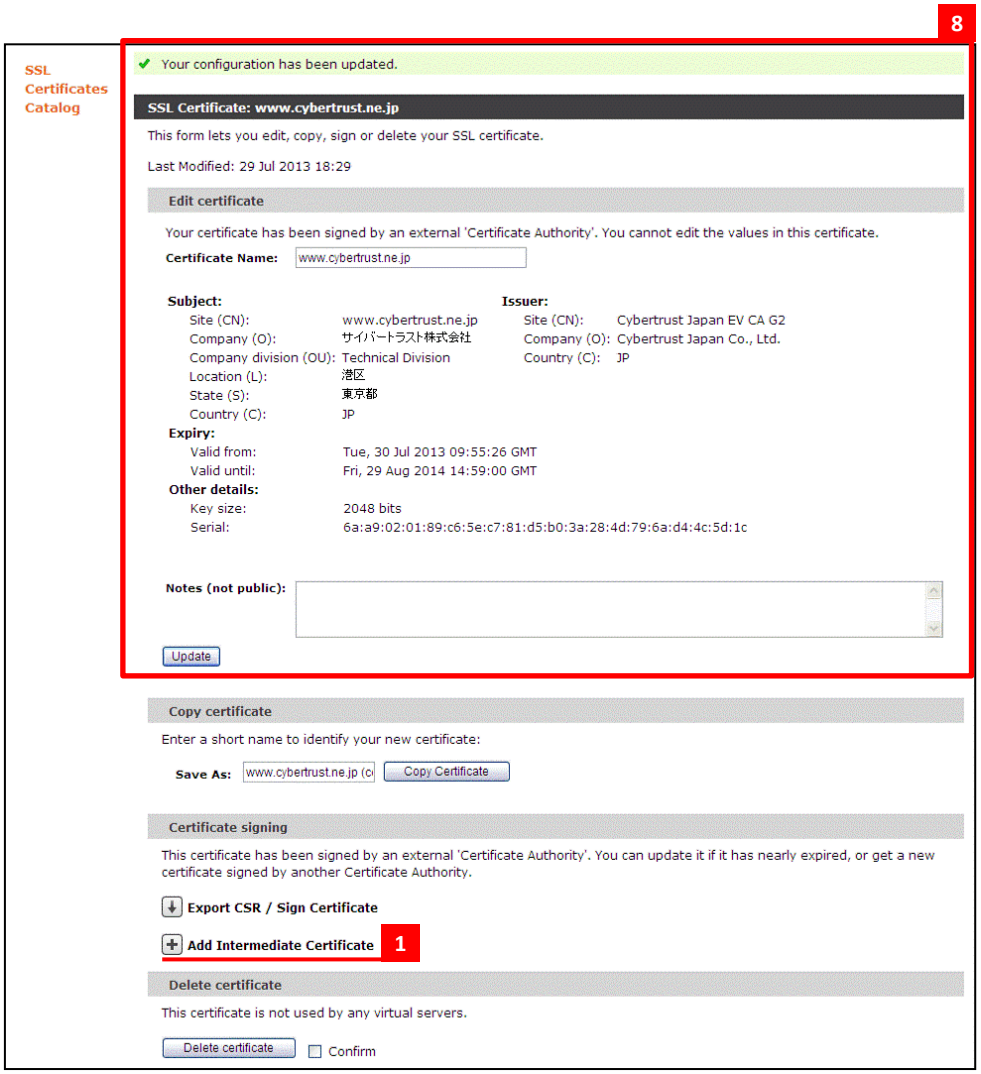
以上でサーバー証明書のインストールは完了です。

続いて、中間CA証明書のインストールを行います。

【2】中間CA証明書のインストール

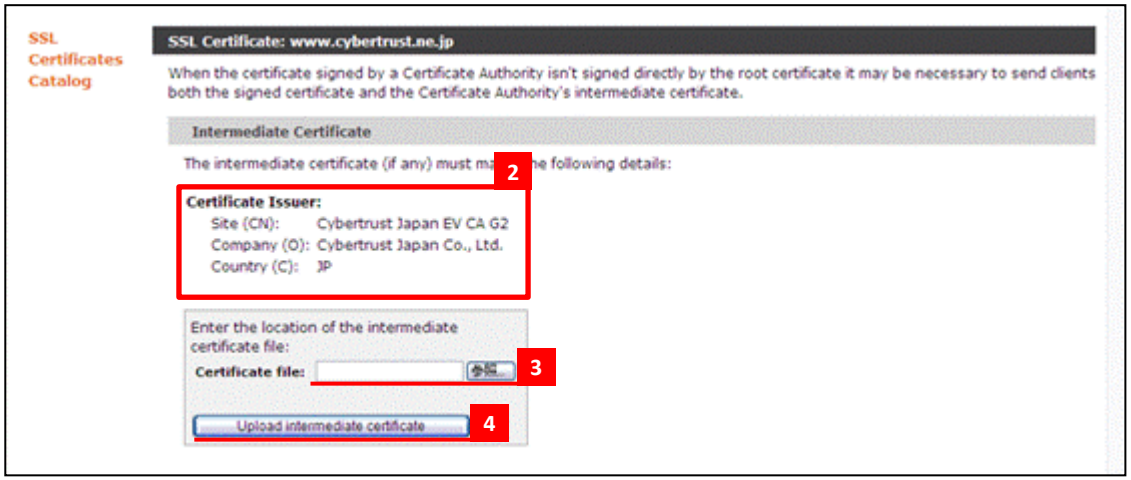
※必要な中間CA証明書をすでにインストール済みの場合は、設定不要です。

1. 「Add Intermediate Certificate」をクリックします。



4.証明書のインストール

2. [Certificate Issuer:]としてインストールが必要な中間CA証明書の情報が表示されますので、事前にダウンロードした中間CA証明書と一致していることを確認します。
3. 「参照」ボタンをクリックして、設定する中間CA証明書を指定します。
4. 「Upload Intermediate certificate」をクリックします。



4.証明書のインストール

5. 「Your configuration has been updated.」と表示されます。
6. [Intermediate Certificate 1 Issuer:]として、インストールした中間CA証明書の情報が表示されます。

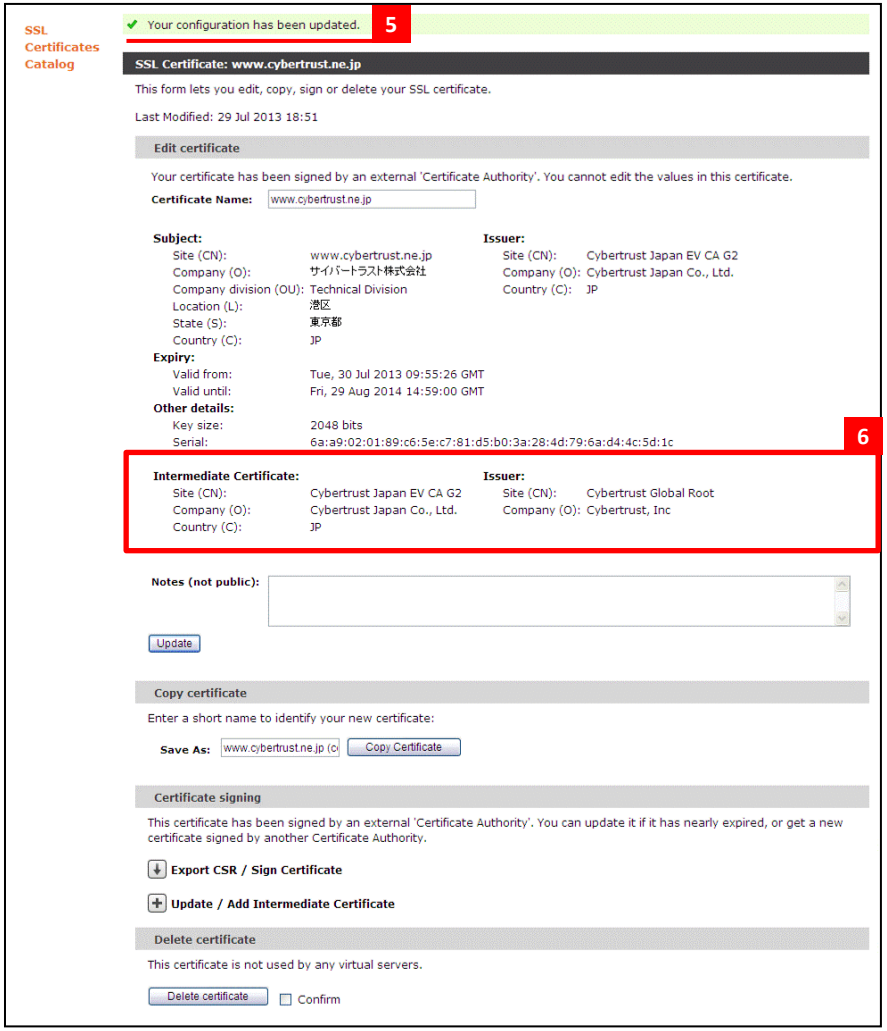
以上で中間CA証明書のインストールは完了です。

【！】クロスルート方式をご設定の場合

クロスルート方式をご設定の場合は、『【2】中間CA証明書のインストール』- 1～6の手順を繰り返し行い、クロスルート用中間CA証明書をインストールします。

▼クロスルート方式の対象商品

2025年6月1日現在、対象商品はありません

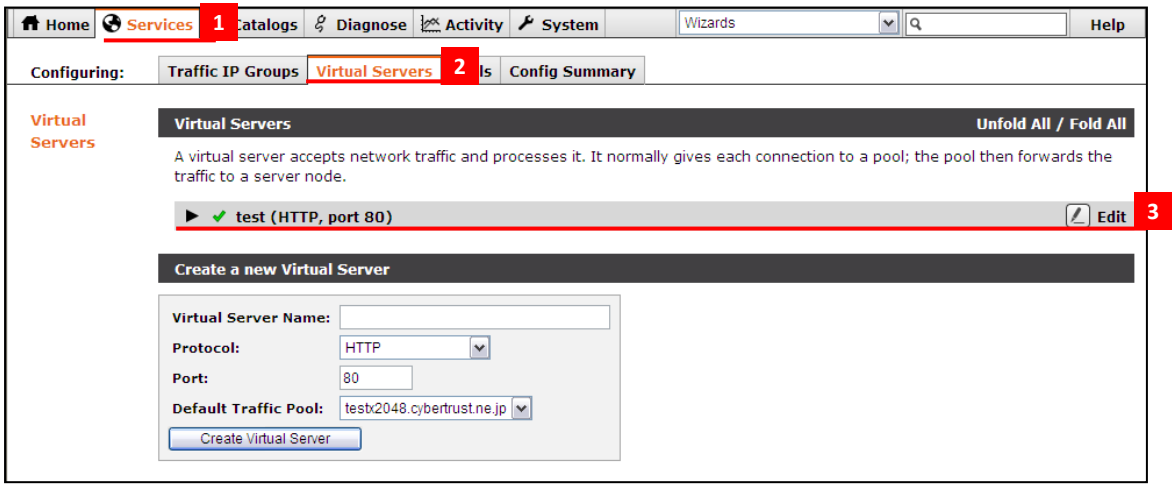


5.証明書インストール後の設定（例）

※本項は、「Virtual server」と「Pool」が作成済みであることを前提としています。

【1】Virtual Serverの設定

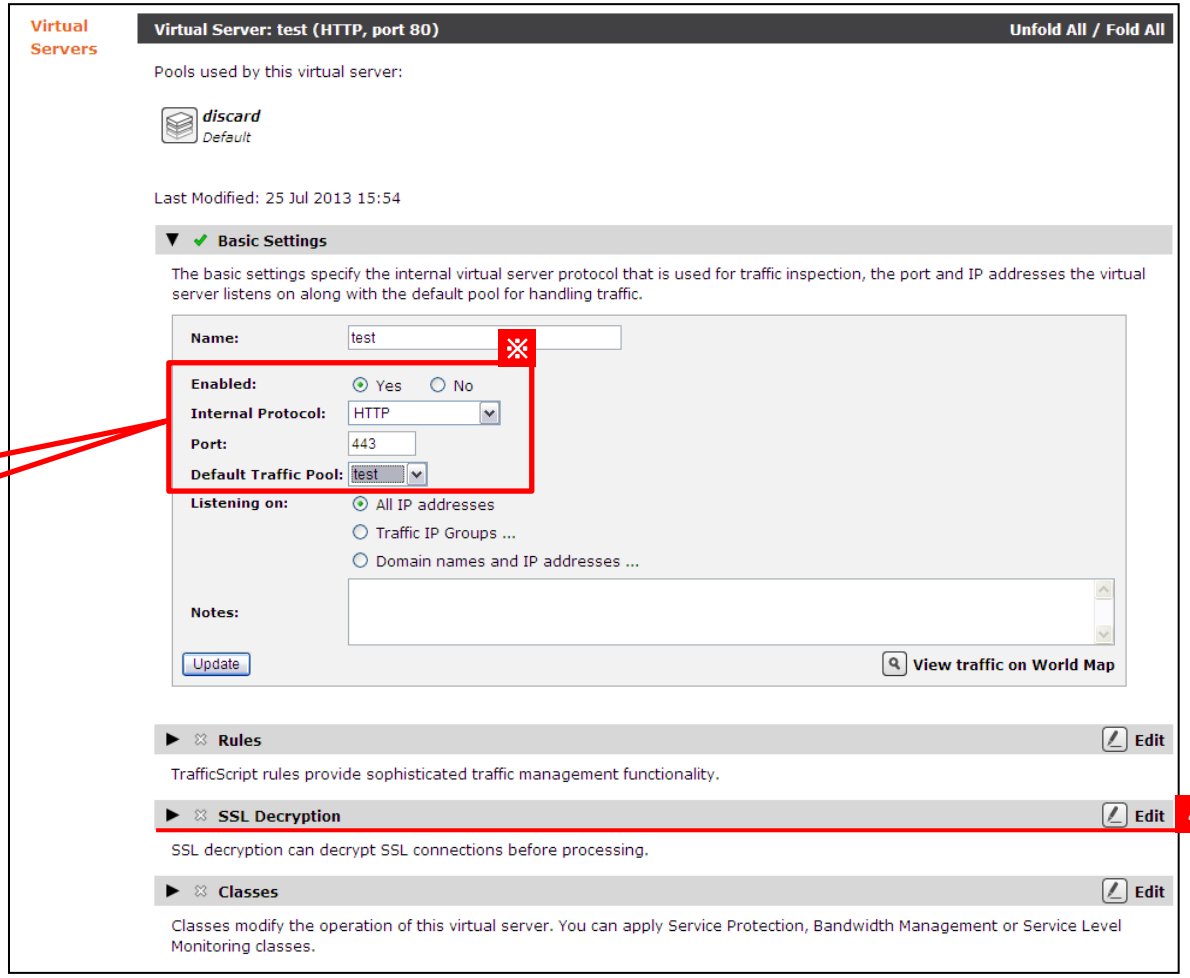
1. Administration interface へログイン後、Home画面から[Services]タブをクリックします。
2. [Virtual Servers]タブをクリックします。
3. 設定を行う仮想サーバーの名称をクリックします。



5.証明書インストール後の設定(例)

※本項は、「Virtual server」と「Pool」が作成済みであることを前提としています。

4. [SSL Decryption]をクリックします。



※以下の設定になっていることを確認してください。

[Enabled:]: Yes

[Internal protocols]: HTTP(Inertnal のプロトコルを指定)

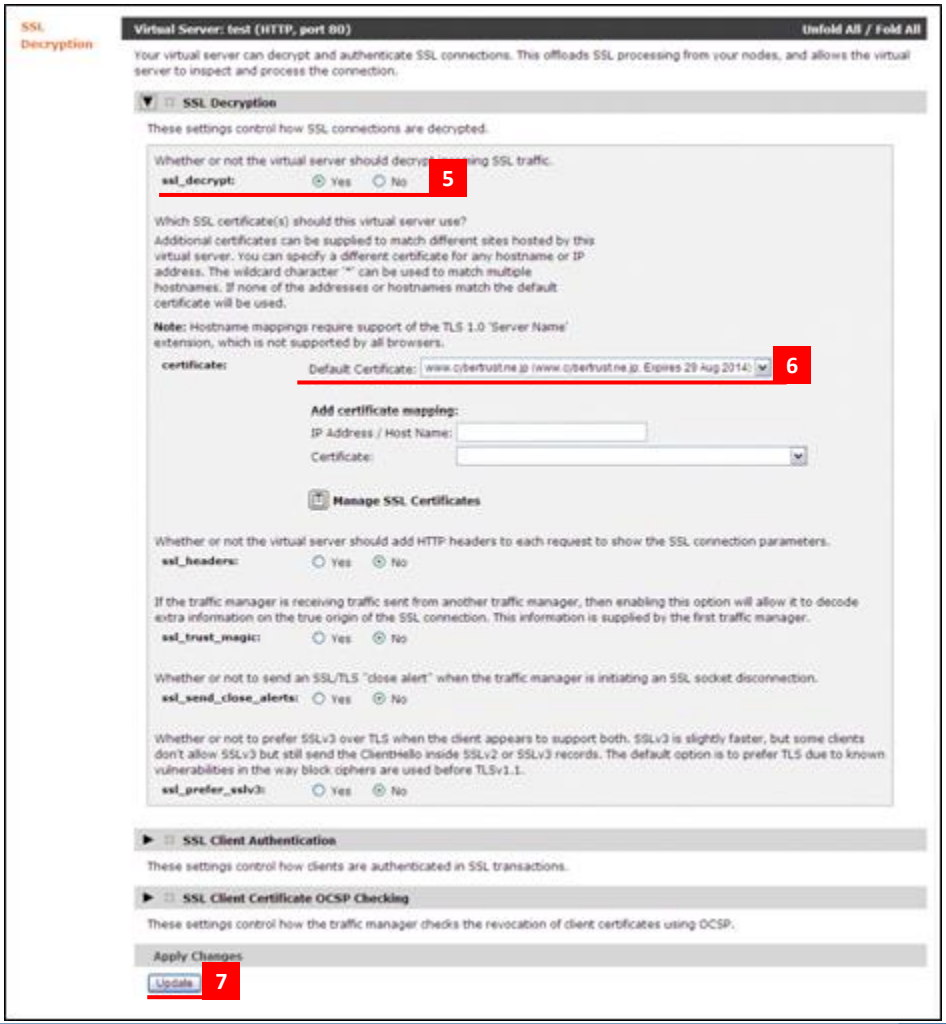
[Port:]: 443

[Default Traffic Pool:] 使用したいPoolを選択

5.証明書インストール後の設定(例)

※本項は、「Virtual server」と「Pool」が作成済みであることを前提としています。

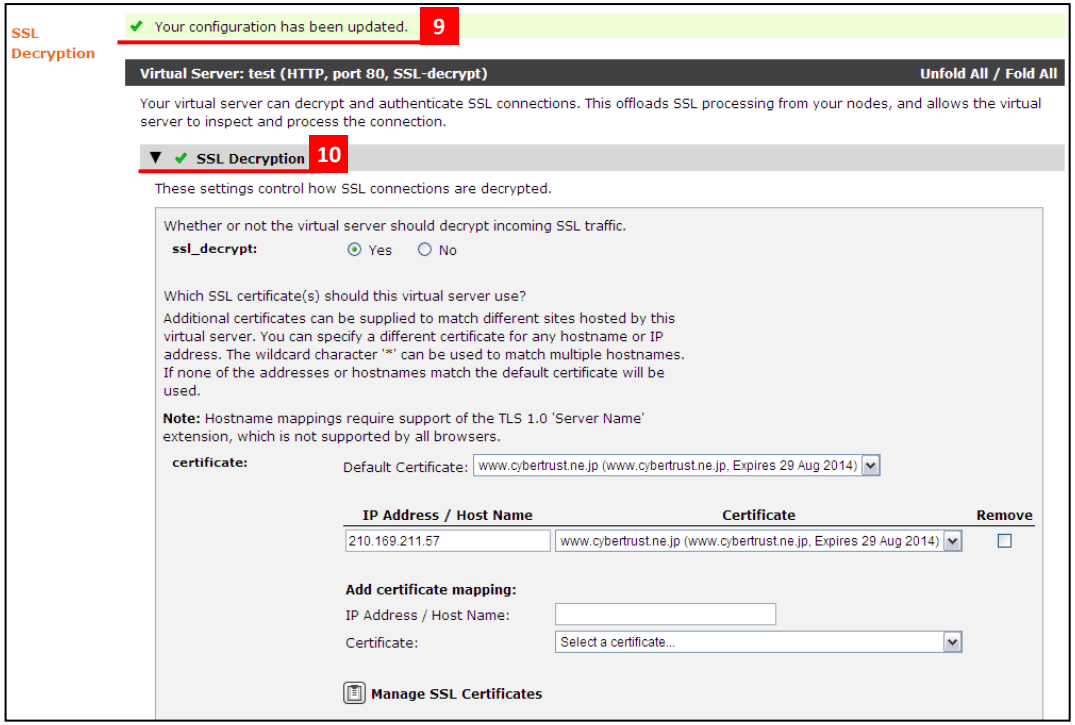
5. [ssl decrypt:] を「Yes」に変更します。
6. [Default Certificate:]に使用するサーバー証明書を選択します。
7. 「Update」ボタンをクリックします。



5.証明書インストール後の設定（例）

※本項は、「Virtual server」と「Pool」が作成済みであることを前提としています。

9. 「Your configuration has been updated.」と表示されます。
10. [SSL Decryption]に有効状態を示す緑色のチェックがつきます。



以上で設定完了です。

サーバー証明書とマッピングしたIPアドレス、またはホスト名にhttps（443）のアクセスがあった場合、設定したサーバー証明書を利用した暗号化通信が行われます。

6.SSL通信の確認

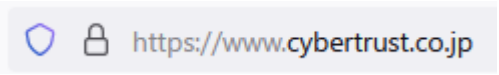
サーバー証明書が正しく設定され、エラーやセキュリティ警告が表示されず、正常にSSL通信が可能であることを確認します。

- SSL通信の確認は設定を行っているサーバー以外のWEBブラウザやスマートフォンなどの携帯端末、弊社「SSLサーバ証明書　導入サポートツール」のサーバ証明書の設定確認から行うことを推奨します。

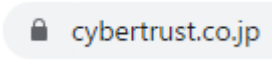
■設定確認例

<Edge>

<Firefox>



<Chrome>



※接続時にセキュリティ警告やエラーが表示される場合は、以下よくある質問の「SSL通信時のセキュリティ警告やエラーについて」をご参照ください。

https://www.cybertrust.co.jp/ssl/support/faq/