



ソフトウェアバージョン
1.0.0

Edgenexus SSL Certificate Manager

AN EDGENEXUS EDGEADC APP

ドキュメントのプロパティ

ドキュメント番号 : 2.0.9.13.21.14.09

ドキュメント作成日 2021年8月5日

ドキュメントの最終更新日 13 September 2021

ドキュメント作成者 ジェイ・サヴォア

ドキュメント 最後に編集されたのは

ドキュメント免責事項

このマニュアルのスクリーンショットやグラフィックは、製品リリースの違いにより、お使いの製品とは若干異なる場合があります。Edgenexus社は、本書の情報が完全かつ正確であることを保証するために、あらゆる合理的な努力をしています。Edgenexusは、いかなる誤りに対しても責任を負いません。

Edgenexus は、必要に応じて、将来のリリースでこの文書の情報を変更および修正します。

著作権について

© 2021 All rights reserved.

本資料に記載された情報は、予告なしに変更されることがあり、メーカーの確約を示すものではありません。本ガイドのいかなる部分も、メーカーの書面による許可なしに、電子的または機械的（コピーや記録を含む）に、いかなる目的のためにも複製または送信することはできません。登録商標はそれぞれの所有者に帰属します。本ガイドは、可能な限り完全かつ正確なものとなるよう努力していますが、適合性の保証はありません。本ガイドに掲載されている情報を使用したことにより生じた損失や損害について、著者および出版社はいかなる人や組織に対しても責任を負いません。

Edgenexusのロゴ、Edgenexus、EdgeADC、EdgeWAF、EdgeGSLB、EdgeDNSは、すべてEdgenexus Limitedの商標です。その他のすべての商標は、それぞれの所有者の所有物であり、承認されています。

Edgenexusサポート

本製品に関する技術的なご質問は、support@edgenexus.io までサポートチケットをご提出ください。

目次を見る

ドキュメントのプロパティ	1
ドキュメント免責事項	1
著作権について	1
商標について	1
エドジェネクススのサポート	1
Edgenexus SSL Certificate Managerとは何ですか?	3
Edgenexus SSL Certificate Managerを入手してインストールしますか?	4
EdgeADCを使ったアプリのダウンロードとインポート	6
ダイレクトダウンロードによるアプリのダウンロードとインポート	7
EdgeADC v4.2.x以降でのアプリの動作について	8
EdgeADC v4.3.x以降でアプリを動作させるには	9
前提条件	12
Edgenexus SSL Certificate Managerによる証明書の発行	13
FlightPATHとその使用方法	15
証明書の一括インポート	16

Edgenexus SSL Certificate Managerとは何ですか？

アプリケーションの安全性が求められるサーバーを使用するすべての組織では、**SSL証明書**をインストールする必要があります。

この要件に対応するために、IT管理者は、内部のドメインに接続されたサーバにはドメイン証明書を使用し、サーバがプライベートまたはパブリックアクセス用の**Web**ベースのソリューションをホストする場合には、グローバルに信頼できる証明書のために**SSLプロバイダ**にアプローチします。

当局から証明書を入手するプロセスには、時間とコストがかかります。

これを軽減するために、EdgenexusはEdgenexus SSL Certificate Managerを導入し、IT管理者が**Let's Encrypt**サービスの技術を使って必要な証明書を生成できるようにしました。

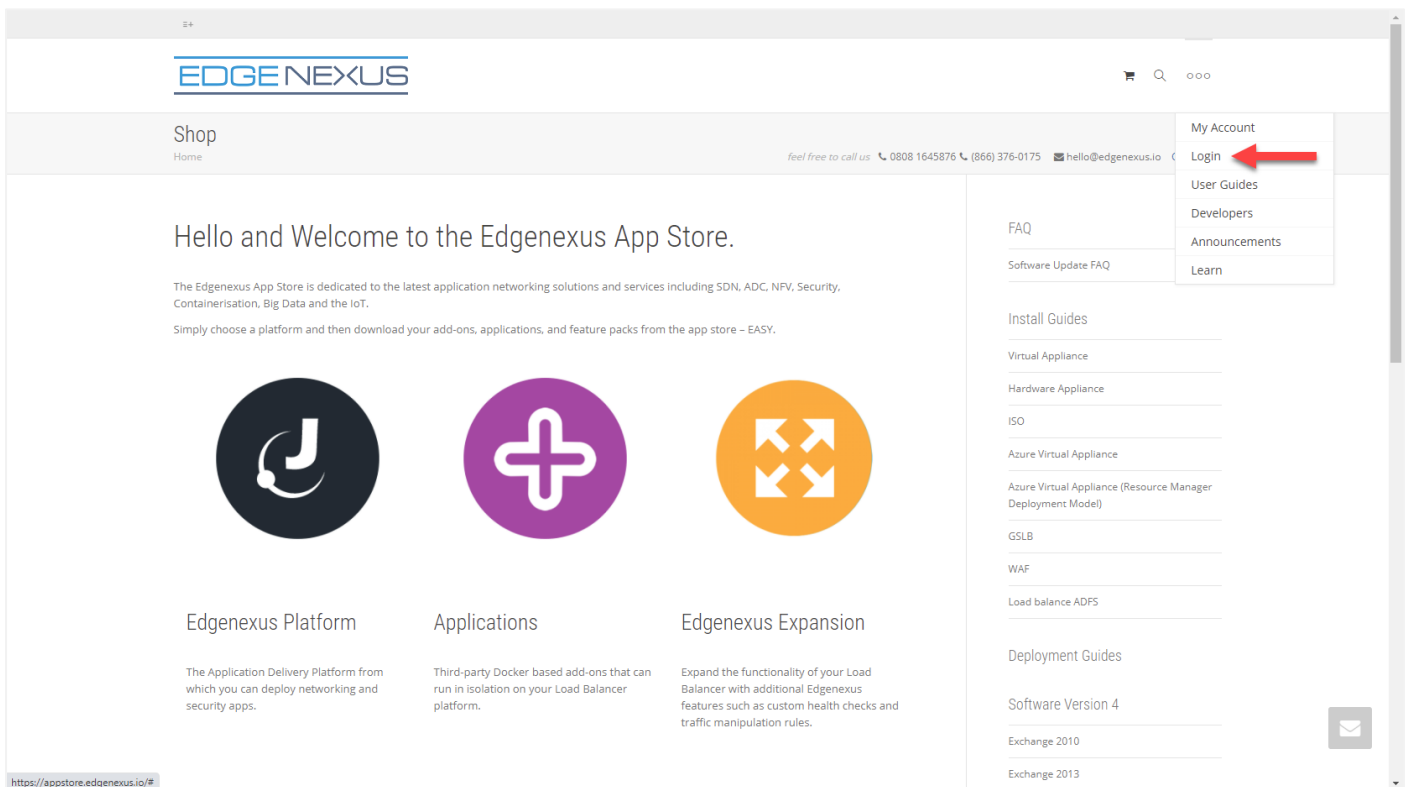
Edgenexus SSL Certificate Managerの使用方法はシンプルで簡単です。

Edgenexus SSL Certificate Managerを入手してインストールしますか？

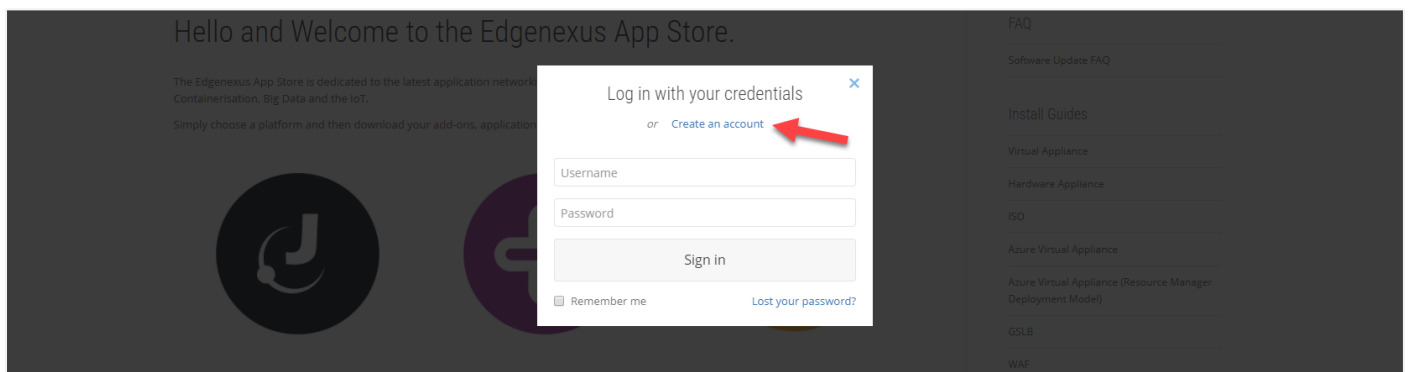
Edgenexus SSL Certificate Managerの取得は非常に簡単です。

すべてのEdgenexus Appと同様に、Edgenexus SSL Certificate ManagerはApp Storeを通じて入手可能で、ダウンロードにはコストがかからず、一部は無料で使用することができます。

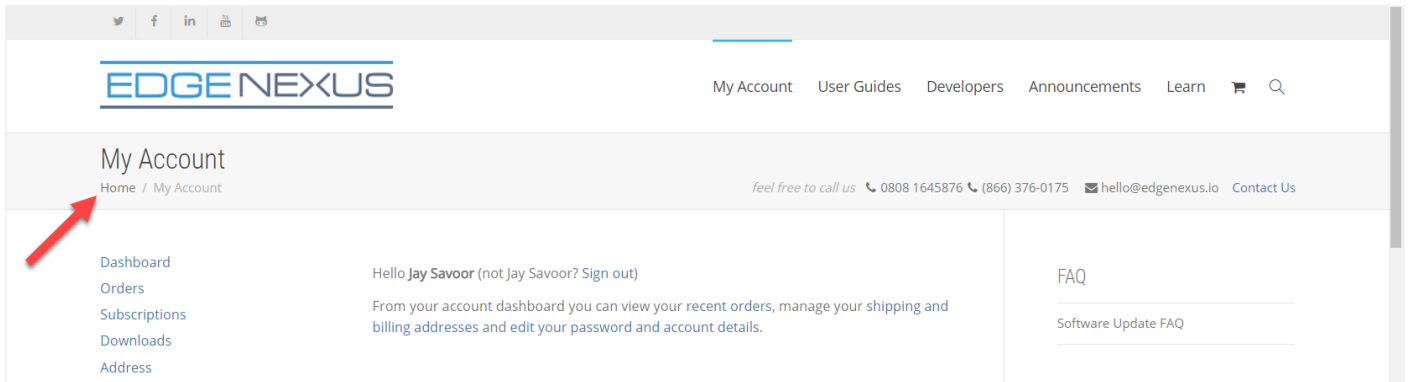
- まず最初に、Edgenexus App Storeへのアクセスを登録する必要があります。この作業は、ブラウザを使用して、<https://appstore.edgenexus.io> にナビゲートして行います。



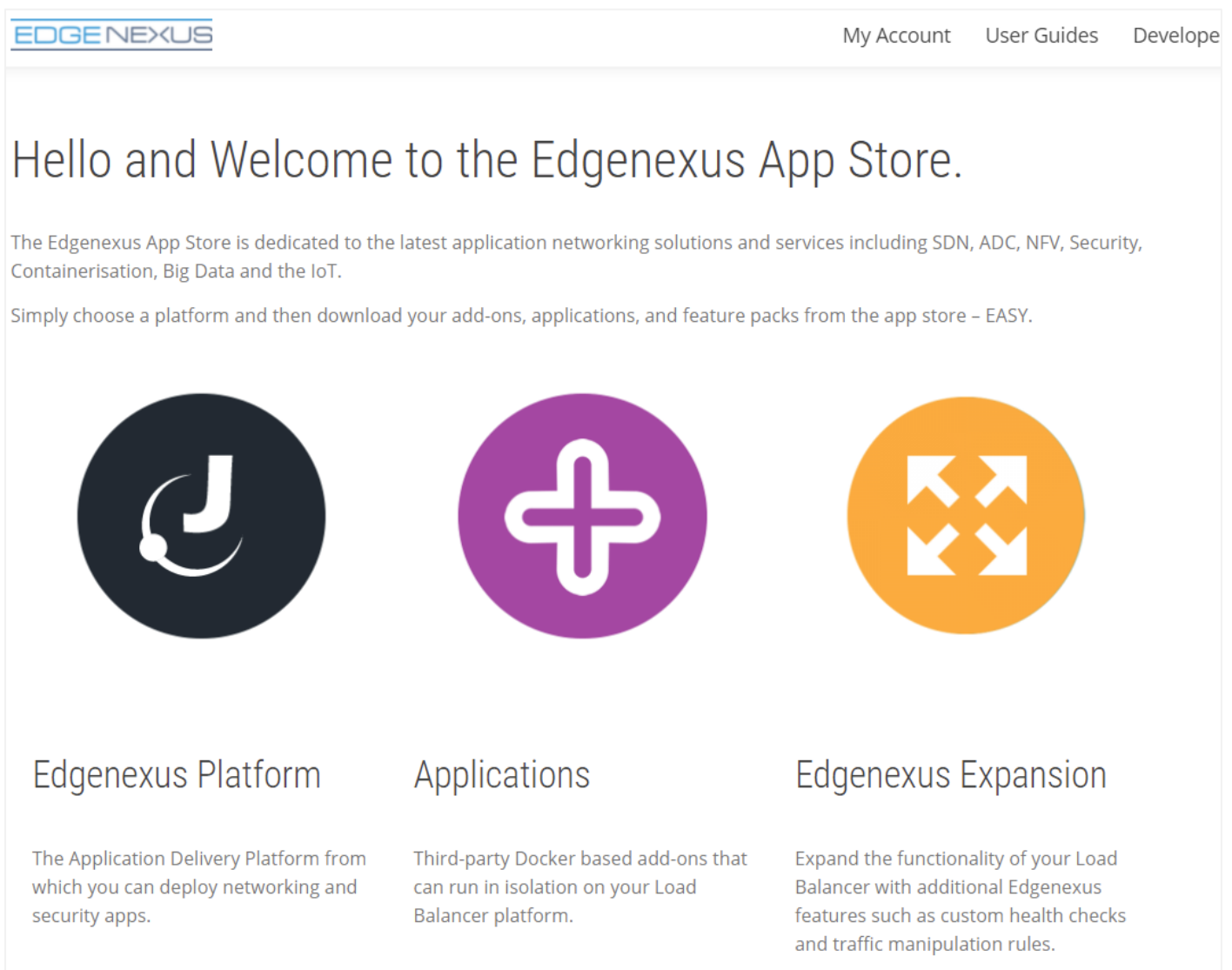
- 右上のハンバーガーアイコンにあるログインリンクをクリックしてください。
- Create an Account** (アカウントの作成) をクリックするか、アカウントの認証情報を使ってログインしてください。



- ログイン後、ロゴの下にある「ホーム」をクリックしてください。



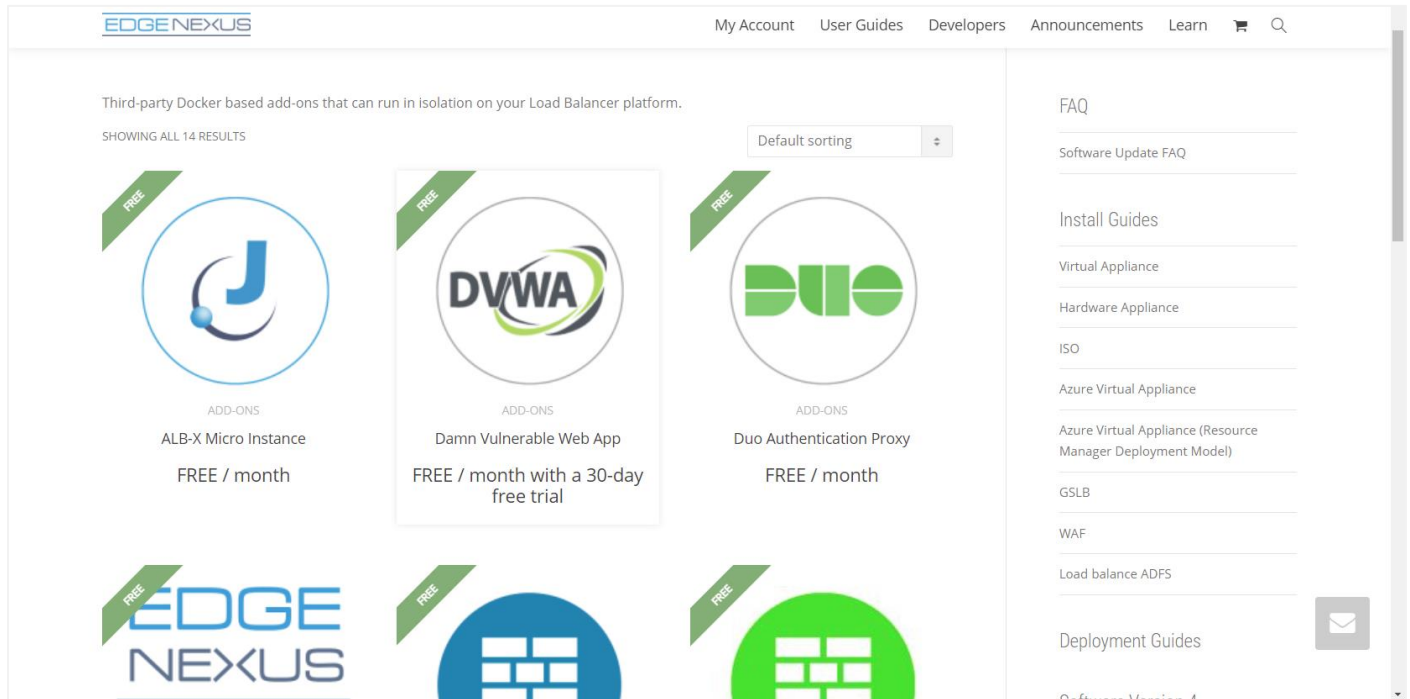
- 次に「アプリケーション」をクリックします。



- この操作で「アプリケーション」ページに移動し、そこからEdgenexus SSL Certificate Managerをダウンロードすることができます。

Edgenexus SSL Certificate Manager

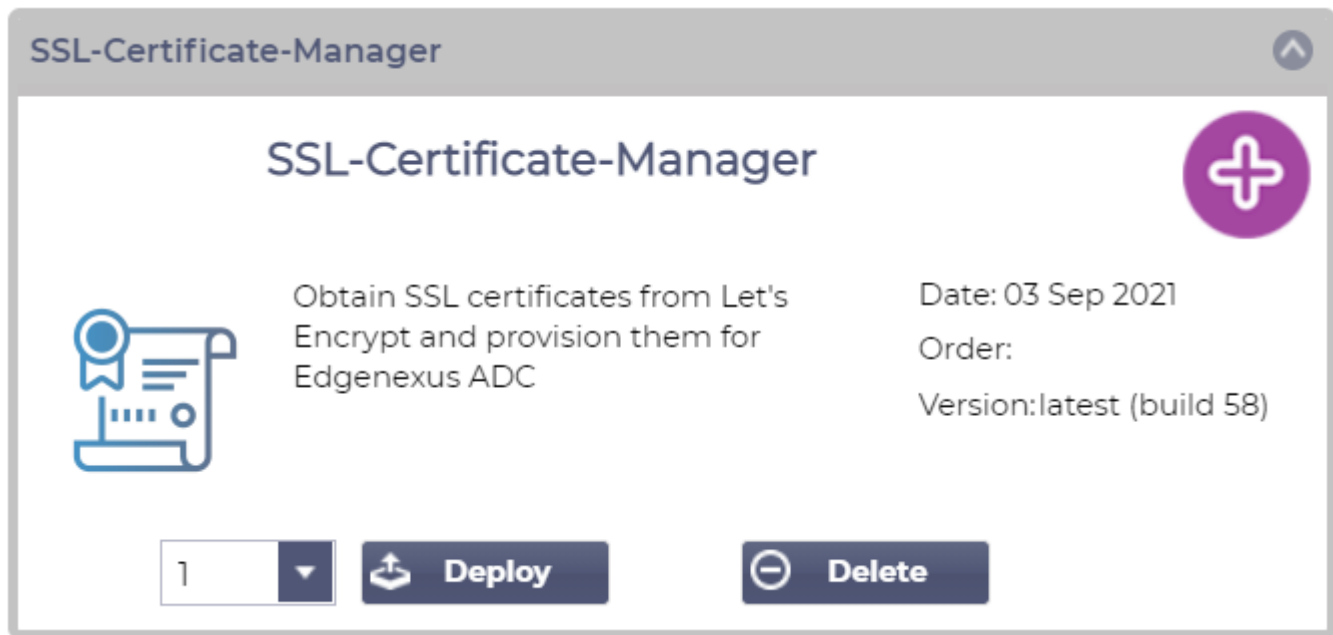
ユーザーガイド



- アプリケーションページ内では、アプリの閲覧や注文ができます。
- 「Edgenexus SSL Certificate Manager」アプリは無償で提供されていますが、購入するというルートをとる必要があります。
- この時点では、2つの選択肢があります。EdgeADC内でApp Storeを利用する方法と、App Storeから直接アプリをダウンロードしてEdgeADCにアップロードする方法です。

EdgeADCを使ったアプリのダウンロードとインポート

- 最初のオプションは、EdgeADC の内部から App Store のクレデンシャルを使用してログインすることです。統合されたApp Storeインターフェースは、「サービス」→「App Store」で利用できます。
- この方法で購入すると、「ライブラリ」→「アプリ」の中にある「購入済みアプリ」のセクションで利用できるようになります。
- Edgenexus SSL Certificate Manager Appの外観は以下のようになっています。



- その際、アプリのダウンロードを選択すると、「ダウンロードしたアプリ」セクションに表示されます。
- **Library > Apps > Downloaded Apps**セクションから**Dell-ECS Load Balancing App**を探し、**Deploy**ボタンをクリックして**EdgeADC**コンテナにデプロイします。
- 複数のコピーを配置したい場合は、ドロップダウンでアプリのコピー数を選択できます。
- デプロイされると、「ライブラリ」>「アドオン」タブで利用可能になります。

ダイレクトダウンロードによる本アプリのダウンロードとインポート

- 2つ目の方法は、**App Store**のログインを利用し、ブラウザを使って直接デスクトップにダウンロードする方法です。
- ダウンロード後は、必ずファイル名を変更せずに保存してください。
- また、ファイル名に**(1)**などが含まれていないことを確認してください。これは2回目のダウンロードである可能性があります。
- ファイルをダウンロードした状態で、ブラウザを使って**EdgeADC GUI**の**Advanced > Software**に移動します。

Edgenexus SSL Certificate Manager

ユーザーガイド

The screenshot shows the Edgenexus web interface. The top navigation bar includes 'IP-Services', 'Software' (selected), 'App Store', 'Apps', and 'Add-Ons'. The left sidebar contains 'NAVIGATION' with options like 'Services', 'Library', 'View', 'System', 'Advanced', 'Configuration', 'Global Settings', 'Protocol', 'Software', and 'Troubleshooting'. The main content area is titled 'Software' and includes 'Software Details' (User Name: admin, Machine ID: 367-B05F-934, Licence ID: {9A000FC9-5C0F-48BE-86B7-D83E8A94FB94}, Licence Expiry: Permanent, Location: Altrincham, United Kingdom, Support Expiry: None, Support Type: Standard, Current Software Version: 4.3.0 (Build 1950) 712100) and a 'Refresh To View Available Software' button. Below this is the 'Download From Cloud' section with a table of available software updates. The 'Upload Software' section is highlighted with a red box and contains a 'Browse' button and 'Upload Apps And Software' and 'Upload And Apply Software' buttons. The 'Apply Software' section shows a table of installed software updates.

Code Name	Release Date	Version	Build	Release Notes	Notes
ALB-X Version 4.2.6	2020-04-15	4.2.6	1826	Click here for release nc This is our latest release 4.2.6. This	
OWASP Core Rule Set 3.2.0 Update fo...	2020-10-22	3.2.0_28.10.2...	jetNEXUS	The OWASP CRS is a set The OWASP CRS is a set of web ap	
ALB-X Version 4.2.6	2020-05-15	4.2.6	1834	Click here for release nc Flightpath update 4.2.6. This APP	

Image	Code Name	Release Date	Version	Build	Notes
	jetNEXUS ALB v4.3.0	18 Jul 2021	4.3.0	(Build1950) 712100	build1950-4100-712100-v4.3.0-Electron-update-64
	jetNEXUS ALB v4.2.8	2021-07-05	4.2.8	(Build1896)	build1896-7215-v4.2.8-Sprint2-update-64
	jetNEXUS ALB v4.2.8	20 May 2021	4.2.8	(Build1895)	build1895-7127-v4.2.8-Sprint2-update-64

- ソフトウェア」ページにはいくつかのセクションがありますが、「ソフトウェアのアップロード」セクションが必要です。
- まず、「Browse」ボタンをクリックして、ダウンロードした「Dell ECS Load Balancing App」を探します。
- 次に、「Apps and Softwareのアップロード」ボタンをクリックします。
- そのアプリは、「ライブラリ」→「アプリ」の「ダウンロードしたアプリ」に表示されます。
- Library > Apps > Downloaded AppsセクションからDell-ECS Load Balancing Appを探し、DeployボタンをクリックしてEdgeADCにデプロイします。
- 複数のコピーを配置したい場合は、ドロップダウンでアプリのコピー数を選択できます。
- デプロイされると、「ライブラリ」>「アドオン」タブで利用可能になります。

EdgeADC v4.2.x以降でのアプリの動作について

アプリがダウンロードされ、デプロイされても、そのアプリはまだ運用されていません。アプリには、EdgeADCと同じサブネットにあるIPアドレスと、アクセスするためのポートが与えられなければなりません。

- Library > Add-Ons」に移動し、「Edgenexus SSL Certificate Manager App」を探します。
- 下の画像のように表示されるはずですが。

Edgenexus SSL Certificate Manager

ユーザーガイド

MyCertMgr

Container Name:

External IP:

External Port:

192.168.159.121 is available on eth0

Parent Image: SSL-Certificate-Manager-Edge

Internal IP:

Started At:

Stopped At: 2021-09-04 10:42:24

Import File:

- Add-Onに名前を付け①ます。EdgeADCの内部DNSシステムは、必要に応じてこの名前を使ってAppを参照します。
- 適切な静的 IP アドレスを追加します②。このエントリは、EdgeADC v4.3.x以上ではオプションですが、4.3.x以下のバージョンでは必須です。
- ポートアドレスの値として**8080/tcp**を使用して、Port(s)の値を入力します。
- これができたら、「Update」ボタンをクリックしてAppを初期化します。④
- 上のPLAYアイコンをクリックする⑤と、アプリが動作状態になります。
- 運用が開始されると、以下の画像のように表示され、埋め込みアプリとして「サービス」セクションに表示されます。

MyCertMgr

Container Name: MyCertMgr

External IP: 192.168.159.121

External Port: 8080/tcp

192.168.159.121 is available on eth0

Parent Image: SSL-Certificate-Manager-Edge

Internal IP: 172.31.0.1

Started At: 2021-09-04 10:39:48

Stopped At:

Import File:

- AppのGUIを起動する「Add-On GUI」⑥ボタンと、「Pause App」「Stop App」ボタンに注目してください。
- アプリを起動すると、新しいブラウザタブで表示されます。

EdgeADC v4.3.x以降でのアプリの動作確認

アプリがダウンロードされ、デプロイされても、そのアプリはまだ運用されていません。アプリには、EdgeADCと同じサブネットにあるIPアドレスと、アクセスするためのポートが与えられなければなりません。

- Library > Add-Ons」に移動し、「Dell-ECS Load Balancing App」を見つけます。
- 下の画像のように表示されるはずですが。

Edgenexus SSL Certificate Manager

ユーザーガイド

MyCertMgr

Add-On Name:

External IP:

External Ports:

192.168.159.236 is available on eth0

Update

Remove Add-On

View Log

Add-on:

Internal IP:

Started At:

Stopped At:

Import File:

Import Configuration

Export Configuration

3

- Add-Onに名前を付け①ます。EdgeADCの内部DNSシステムは、必要に応じてこの名前を使ってAppを参照します。
- 適切な静的 IP アドレスを追加します②。このエントリは、EdgeADC v4.3.x以上ではオプションですが、4.3.x以下のバージョンでは必須です。
- EdgeADC v4.3.x以上をお使いの場合、Port(s)の値はすでに提供されているので、入力する必要はありません。EdgeADCの以前のバージョン（4.2.x以下）では、ポートアドレスの値として8080/tcpを入力する必要があります。
- これができたら、「Update」ボタンをクリックしてAppを初期化します。
- 以下のように表示されます。

MyCertMgr

Add-On Name:

External IP:

External Ports:

192.168.159.236 is available on eth0

Update

Remove Add-On

View Log

Add-on:

Internal IP:

Started At:

Stopped At:

Import File:

Import Configuration

Export Configuration

3

- 上のPLAYアイコンをクリックする③と、アプリが動作状態になります。
- 運用が開始されると、以下の画像のように表示され、埋め込みアプリとして「サービス」セクションに表示されます。

MyCertMgr

Add-On Name:

External IP:

External Ports:

192.168.159.236 is available on eth0

Update

Remove Add-On

View Log

Add-on:

Internal IP:

Started At:

Stopped At:

Import File:

Import Configuration

Export Configuration

4

View app

- アプリのGUIを起動する「View App④」ボタンと、「Pause App」「Stop App」ボタンに注目してください。
- EdgeADCバージョン4.3以上では、ナビゲーションパネル内の「サービス」セクションで指定したアプリ名をクリックして起動することもできます。
- アプリを起動すると、EdgeADCのバージョン4.3以下では、新しいブラウザタブで開きます。EdgeADCのバージョン4.3以上では、アプリは右側のパネルで開きます。

前提条件

Edgenexus SSL Certificate Managerを使用するには、以下の前提条件が整っている必要があります。これらが揃っていないと、使用可能な証明書を作成することができません。

1. ライセンスがインストールされたEdgeADCがあることを確認する必要があります。ライセンスは、評価版でも購入済みのものでも構いません。
2. 以下の目的のために、ADCのHTTPポート80にVIPを設定しています。
3. HTTPポート80を使用してVIPにリダイレクトされるパブリックIPアドレスを用意する必要があります。この対策により、Let's Encryptのシステムが接続し、生成するSSLのDNSオーナーシップを検証することができます。

Virtual Services									
Search					Copy Service		Add Service		Remove Service
Mode	VIP	VS	Enabled	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type	
Active			☒	192.168.159.110	255.255.255.0	80		HTTP	

4. DNSにFQDN（完全修飾ドメイン名）のエントリを作成する必要があります。このエントリは、パブリックIPアドレスを指します。この対策により、SSL証明書を生成するFQDNがIPアドレスの観点から有効であることが保証されます。

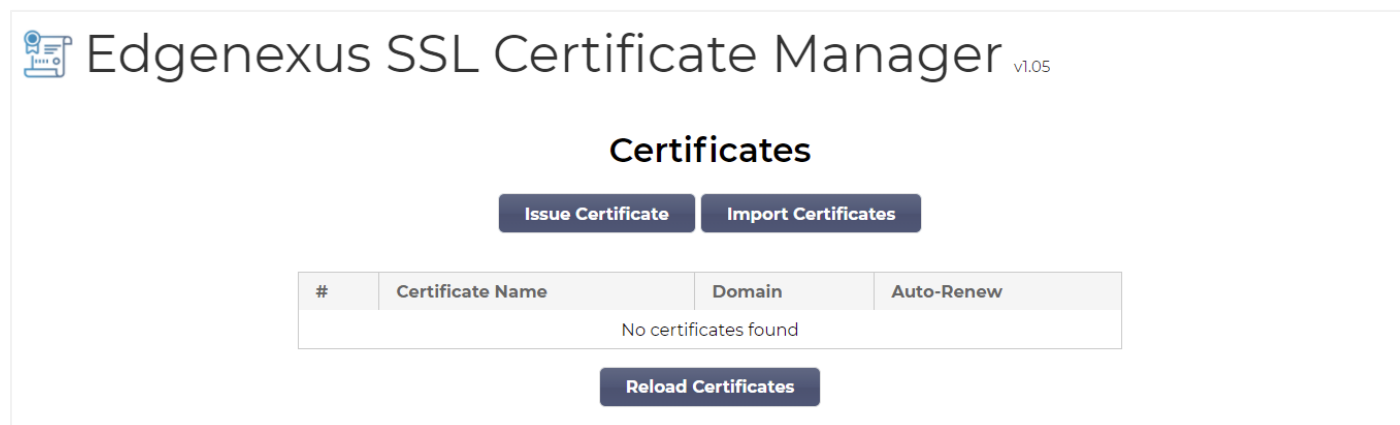
ここまでくればもう大丈夫です。

Edgenexus SSL Certificate Managerによる証明書の発行

Edgenexus SSL Certificate Managerの設定は、ウィザード形式で行われるため、非常に簡単に使用することができます。

ユーザーインターフェースを起動すると、以下の画像のようなページが表示されます。Edgenexus SSL Certificate Managerでは、2つのタスクを実行できることがわかります。証明書の発行」と「証明書のインポート」です。

証明書のインポート機能は、F5などの他のプラットフォームから移行し、SSL証明書を一括してインポートする際に使用します。



Edgenexus SSL Certificate Manager v1.05

Certificates

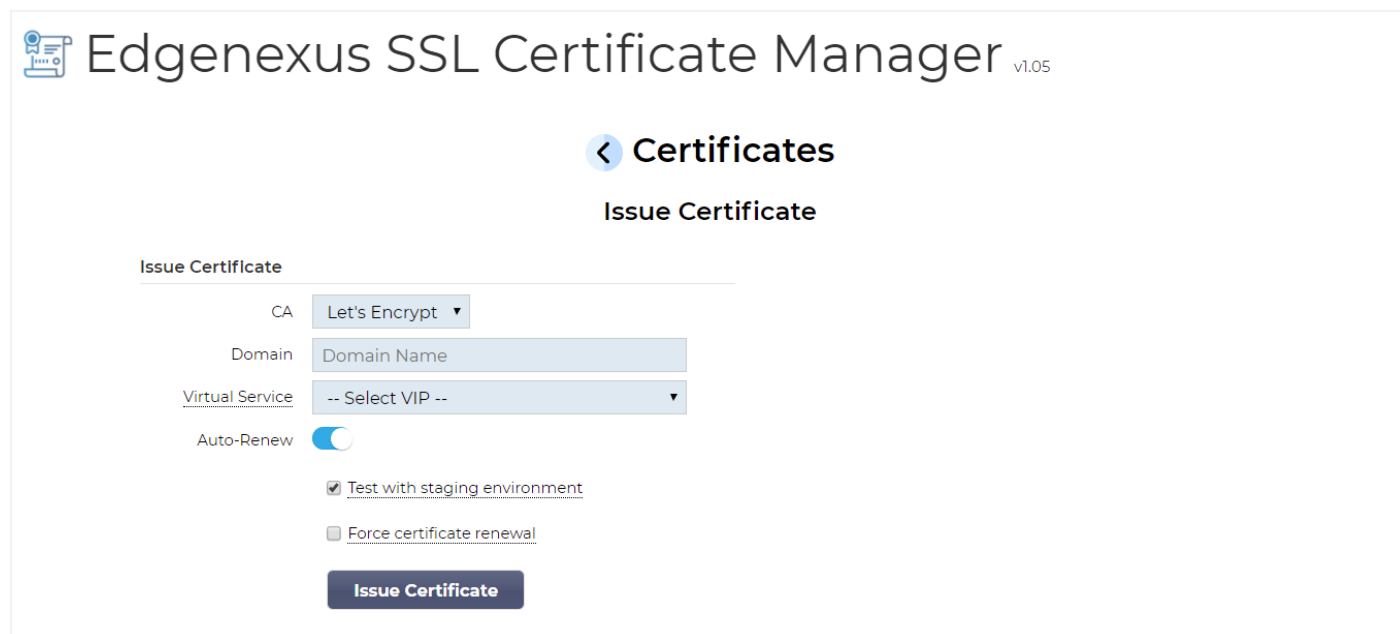
[Issue Certificate](#) [Import Certificates](#)

#	Certificate Name	Domain	Auto-Renew
No certificates found			

[Reload Certificates](#)

Edgenexus SSL Certificate ManagerはLet's Encryptと連携し、Let's EncryptのSSL証明書をリアルタイムで生成・発行し、SSL証明書の自動更新も可能です。

- 証明書の発行ボタンをクリックすると、発行手続きが開始されます。
- 下図のようなページに変わります。



Edgenexus SSL Certificate Manager v1.05

< Certificates

Issue Certificate

Issue Certificate

CA: Let's Encrypt ▼

Domain: Domain Name

Virtual Service: -- Select VIP -- ▼

Auto-Renew: ☒

☒ Test with staging environment

☐ Force certificate renewal

[Issue Certificate](#)

- このように、SSL証明書を発行するためには様々な項目を設定する必要があります。

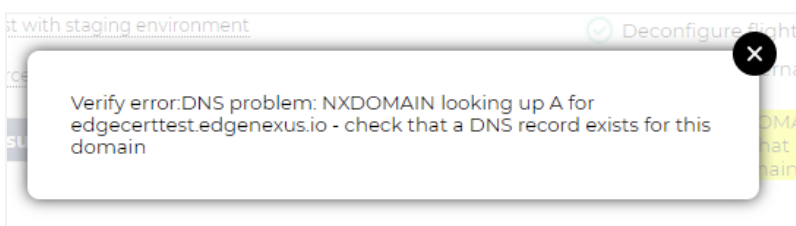
Edgenexus SSL Certificate Manager

ユーザーガイド

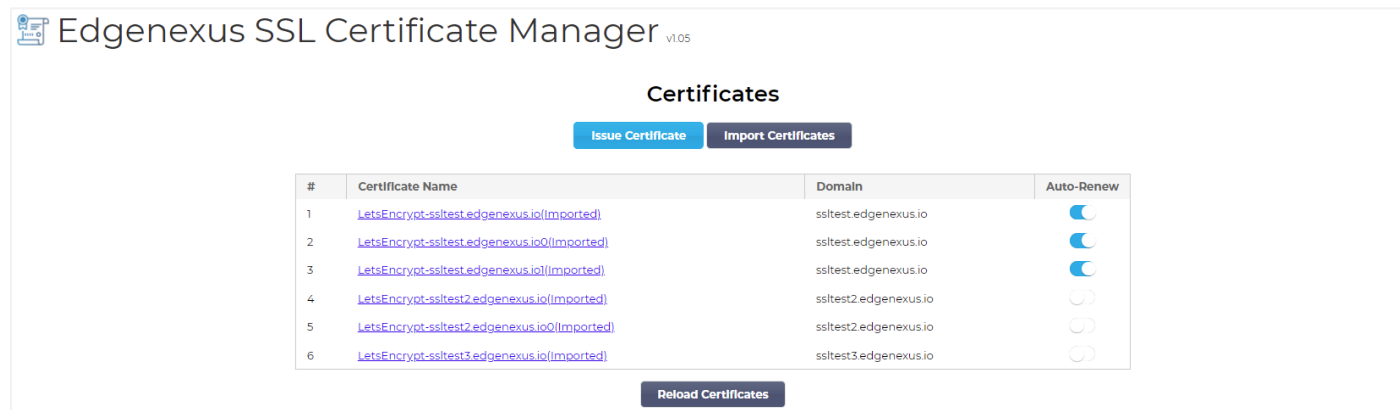
フィールド	説明
CA	現在は、 Let's Encrypt のオプションのみ利用可能です。今後、利用可能なプロバイダーが増えれば、ここに掲載する予定です。
ドメイン	ドメインフィールドは、証明書を必要とするFQDNを指定するために使用します。例えば、 www.acme.com 、ワイルドカードの場合は、 *.acme.com となります。 注：ここで設定するFQDNは、DNSクエリで到達可能である必要があります。
バーチャルサービス	Let's Encrypt システムからのチャレンジリクエストに答えるためには、仮想サービスがオンラインで HTTP ポート 80 で動作する必要があります。この仮想サービスは、「前提条件」の章に記載されているガイダンスに従う必要があります。
オートリニュー	発行時に有効にすると、証明書が自動更新されるように設定されます。
ステージング環境でのテスト	Let's Encrypt のステージングサーバーを使って、新しい証明書を発行する（テスト用）。
証明書の強制更新	Let's Encrypt の証明書がすでに発行されており、有効期限が切れていない場合は、このオプションを有効にしないと新しい証明書を発行することができません。

- フォームの入力が完了したら、[Issue Certificate]ボタンをクリックして、検証段階に進みます。
- 証明書の発行 ボタンをクリックすると、Edgenexus SSL Certificate Managerは、Let's EncryptまたはEdgenexus SSL Certificate Manager内でサポートされている他のACME証明書システムとの検証プロセスを開始します。
- 処理が終了すると、以下のような画面が表示されます。

- Edgenexus SSL Certificate Managerは、処理が成功すると、作成したSSL証明書をEdgeADCのSSLストアに格納します。
- Edgenexus SSL Certificate Managerは、プロセスに何らかの問題が発生した場合、以下のエラーを表示します。



発行した証明書は、アプリの起動画面に表示されます。



FlightPATHとその使用方法

証明書作成プロセスの一環として、Let's Encryptはチャレンジリクエストを使用して提供されたドメイン名を検証する必要があります。

Edgenexus SSL Certificate ManagerはflightPATHを使用してこれを行います。つまり、実際のサーバー上でこれを行うことなく、必要に応じてSSL証明書を作成することができるのです。

証明書の発行」ボタンをクリックすると、EdgeADCは、証明書発行機関、Let's Encrypt、またはサポートされているACMEシステムからのチャレンジ要求を遮断するflightPATHルールを作成します。

flightPATHルールは、意図された実際のサーバではなく、Edgenexus SSL Certificate Managerへのリクエスト・リダイレクトを開始します。Edgenexus SSL Certificate Managerは、チャレンジ・リクエストを確認し、証明書発行のためにそれを検証します。

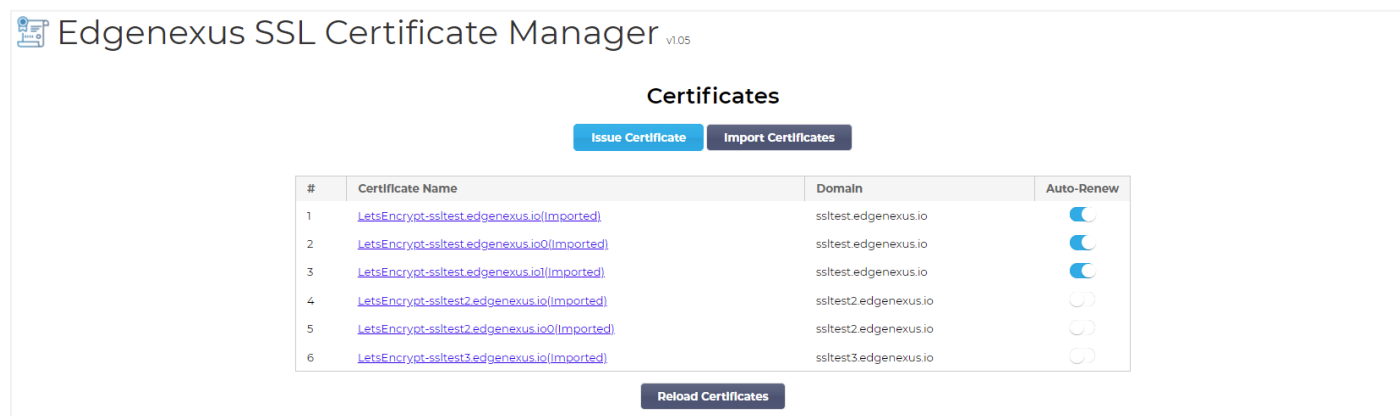
すべての作業はEdgeADC本体から自動的に行われ、管理者は何もする必要がありません。

証明書の一括インポート

特定のお客様の要件の一つに、証明書を一括してインポートする必要があります。証明書を一括してインポートする必要があるのは、証明書の数が多い場合や、F5などの他のロードバランサーから移行したい場合などが考えられます。

Edgenexus SSL Certificate Managerは、ZIPファイルを使ってPFX証明書を一括でインポートすることができます。ここでの但し書きは、PFXのパスワードは全ての証明書で共通でなければならないということです。パスワードを共通にするのは、通常、他のベンダーのロードバランサーから一括エクスポートを行う場合です。

- SSL証明書を一括してインポートするには、アプリのページにある「証明書のインポート」ボタンをクリックします。



Edgenexus SSL Certificate Manager v1.05

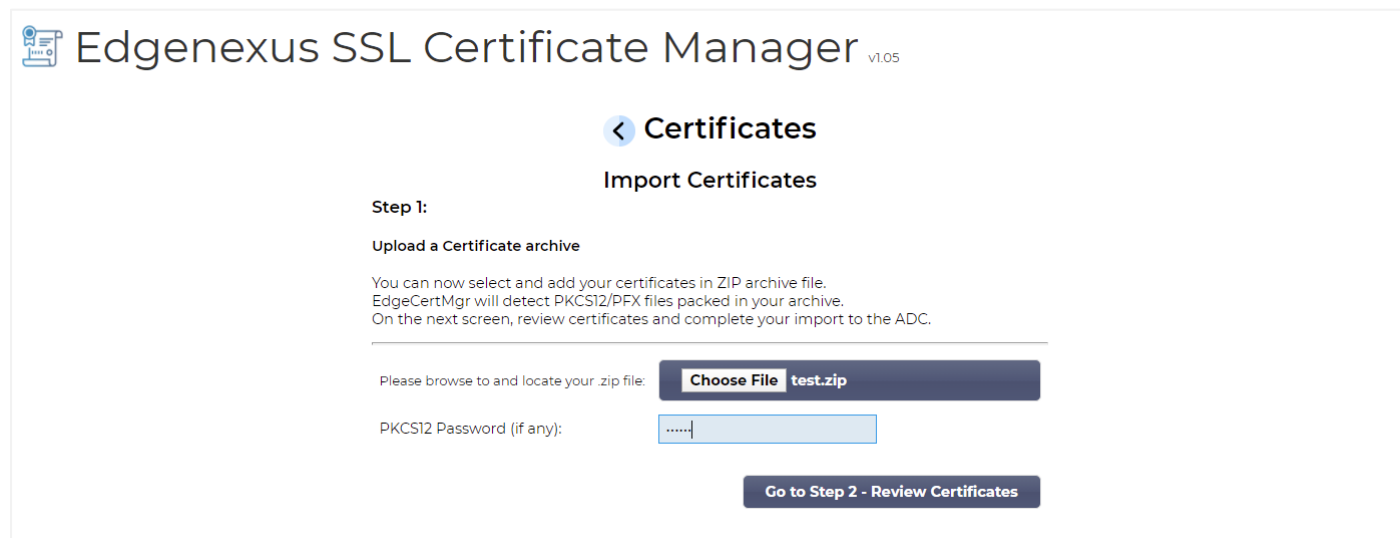
Certificates

Issue Certificate Import Certificates

#	Certificate Name	Domain	Auto-Renew
1	LetsEncrypt-ssltest.edgenexus.io(Imported)	ssltest.edgenexus.io	☒
2	LetsEncrypt-ssltest.edgenexus.io0(Imported)	ssltest.edgenexus.io	☒
3	LetsEncrypt-ssltest.edgenexus.io1(Imported)	ssltest.edgenexus.io	☒
4	LetsEncrypt-ssltest2.edgenexus.io(Imported)	ssltest2.edgenexus.io	☐
5	LetsEncrypt-ssltest2.edgenexus.io0(Imported)	ssltest2.edgenexus.io	☐
6	LetsEncrypt-ssltest3.edgenexus.io(Imported)	ssltest3.edgenexus.io	☐

Reload Certificates

- 次のステップでは、手動または一括エクスポートを使用して作成したZIPファイルを選択します。



Edgenexus SSL Certificate Manager v1.05

< **Certificates**

Import Certificates

Step 1:

Upload a Certificate archive

You can now select and add your certificates in ZIP archive file.
EdgeCertMgr will detect PKCS12/PFX files packed in your archive.
On the next screen, review certificates and complete your import to the ADC.

Please browse to and locate your .zip file: **Choose File** test.zip

PKCS12 Password (if any):

Go to Step 2 - Review Certificates

- PFXのパスワードを入力します。
- Go to Step 2 - Review Certificates** ボタンをクリックします。
- 次のページでは、どのような証明書をインポートするのかを確認できます。

 Edgenexus SSL Certificate Manager v1.05

< Certificates

Import Certificates

Step 2:

Review & Submit

The ZIP file has been analyzed.
Please review SSL certificates below.
Click Import Certificates to complete the import process.

Import Certificates

#	Domain	Certificate Fingerprint	PKCS12 File Name
1	www.acmetwo.com	B1:AF:BE:4C:0C:CE:D9:0E:43:78:C9:13:80:4C:8A:7D:C5:7D:DA:1C	acmerwo.pfx
2	www.acme.com	F3:ED:2E:5C:14:07:51:51:B1:51:BB:C5:C2:97:64:13:5F:EB:13:A2	acme.pfx
3	www.acmeone.com	7F:07:7C:83:4C:E2:F5:1A:8C:42:01:28:76:9A:0F:65:50:28:D9:17	acmeone.pfx

Go Back

Import Certificates

- すべてが正しければ、「証明書のインポート」ボタンをクリックすることができます。
- インポートに成功すると、確認のメッセージが表示されます。

Import Complete! For a detailed log of this import processing
please review the table with your certificates.

- このポップアップを閉じると、以下のような最終画面が表示され、インポートが成功したことを示します。

 Edgenexus SSL Certificate Manager v1.05

< Certificates

Import Certificates

Step 2:

Review & Submit

The ZIP file has been analyzed.
Please review SSL certificates below.
Click Import Certificates to complete the import process.

#	Domain	Certificate Fingerprint	PKCS12 File Name	
1	www.acmetwo.com	B1:AF:BE:4C:0C:CE:D9:0E:43:78:C9:13:80:4C:8A:7D:C5:7D:DA:1C	acmerwo.pfx	✓
2	www.acme.com	F3:ED:2E:5C:14:07:51:51:B1:51:BB:C5:C2:97:64:13:5F:EB:13:A2	acme.pfx	✓
3	www.acmeone.com	7F:07:7C:83:4C:E2:F5:1A:8C:42:01:28:76:9A:0F:65:50:28:D9:17	acmeone.pfx	✓

Go Back

インポートしたSSL証明書は、「ライブラリ」→「SSL証明書」で確認できます。