



SOFTWARE VERSION
1.0.0

Edgenexus SSL Certificate Manager

AN EDGENEXUS EDGEADC APP

Document Properties

Document Number: 2.0.9.9.21.09.09

Document Creation Date: 5 August 2021

Document Last Edited: 9 September 2021

Document Author: Jay Savoor

Document Last Edited by:

Document Disclaimer

This manual's screenshots and graphics may differ slightly from your product due to differences in product release. Edgenexus ensures that they make every reasonable effort to ensure that the information in this document is complete and accurate. Edgenexus assumes no liability for any errors. Edgenexus makes changes and corrections to the information in this document in future releases when the need arises.

Copyrights

© 2021 All rights reserved.

Information in this document is subject to change without prior notice and does not represent a commitment on the manufacturer's part. No part of this guide may be reproduced or transmitted in any form or means, electronic or mechanical, including photocopying and recording, for any purpose, without the express written permission of the manufacturer. Registered trademarks are properties of their respective owners. Every effort is made to make this guide as complete and accurate as possible, but no warranty of fitness is implied. The authors and the publisher shall have neither responsibility nor liability to any person or entity for loss or damages arising from using the information contained in this guide.

Trademarks

Edgenexus logo, Edgenexus, EdgeADC, EdgeWAF, EdgeGSLB, EdgeDNS are all Edgenexus Limited's trademarks. All other trademarks are the properties of their respective owners and are acknowledged.

Edgenexus Support

If you have any technical questions regarding this product, please raise a support ticket at: support@edgenexus.io

Table of Contents

Document Properties	1
Document Disclaimer	1
Copyrights.....	1
Trademarks.....	1
Edgenexus Support	1
What is the Edgenexus SSL Certificate Manager?	3
Get and install the Edgenexus SSL Certificate Manager?.....	4
Downloading and importing the App using the EdgeADC	6
Download and importing the App using direct download.....	7
Making the App Operational in EdgeADC v4.2.x and below	8
Making the App Operational in EdgeADC v4.3.x and above	8
Prerequisites	11
Issuing Certificates with Edgenexus SSL Certificate Manager	12
FlightPATH and how its used	14
Bulk Certificate Import	15

What is the Edgenexus SSL Certificate Manager?

All organizations that use servers delivering applications are required to be secure need SSL certificates to be installed.

To accommodate this requirement, IT managers use domain certificates for internal, domain-joined servers and approach SSL providers for globally trusted certificates when the servers host web-based solutions for private or public access.

The process of obtaining certificates from authorities can be time-consuming and have a cost.

To alleviate this, Edgenexus has introduced Edgenexus SSL Certificate Manager, which allows the IT admin to generate needed certificates using the Let's Encrypt service technology.

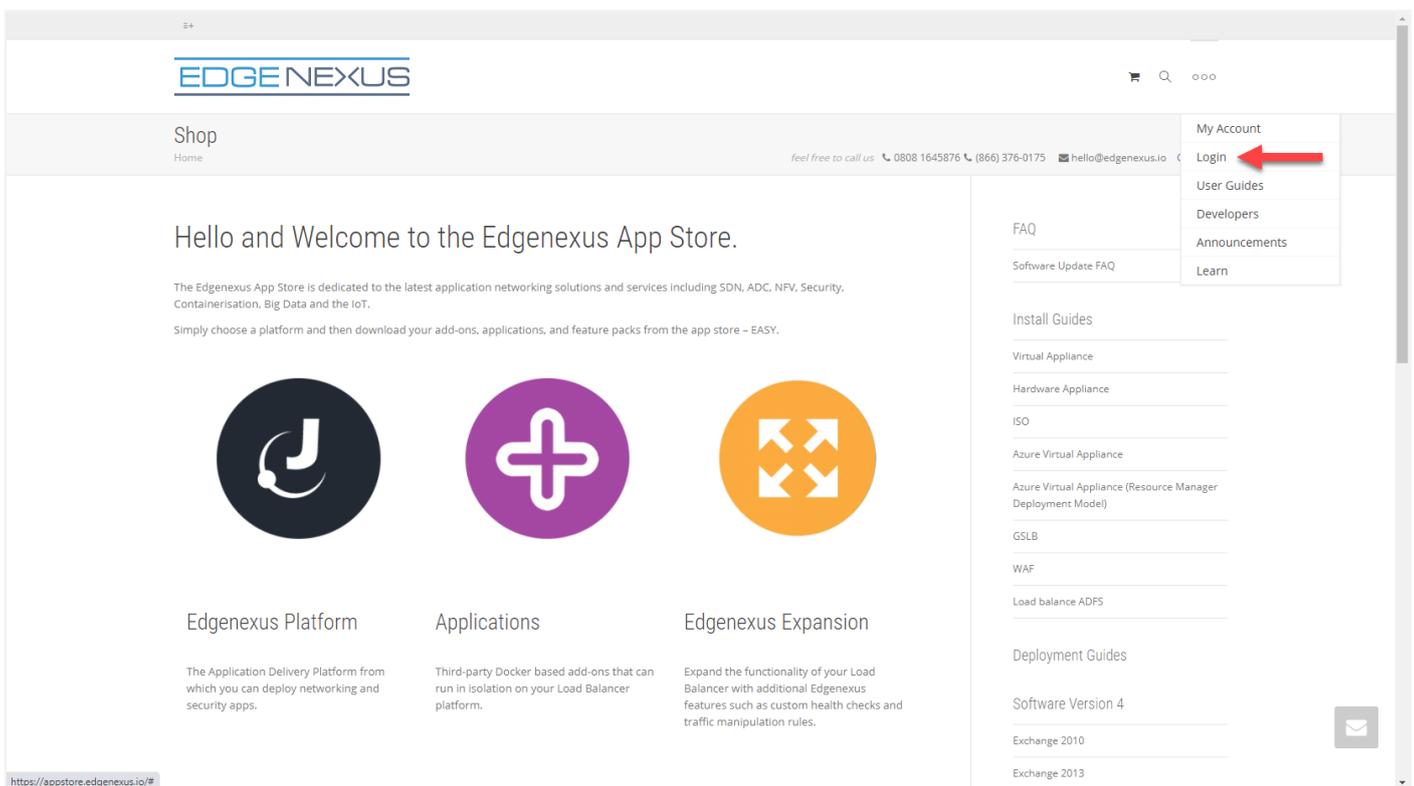
The process of using the Edgenexus SSL Certificate Manager is simple and easy.

Get and install the Edgenexus SSL Certificate Manager?

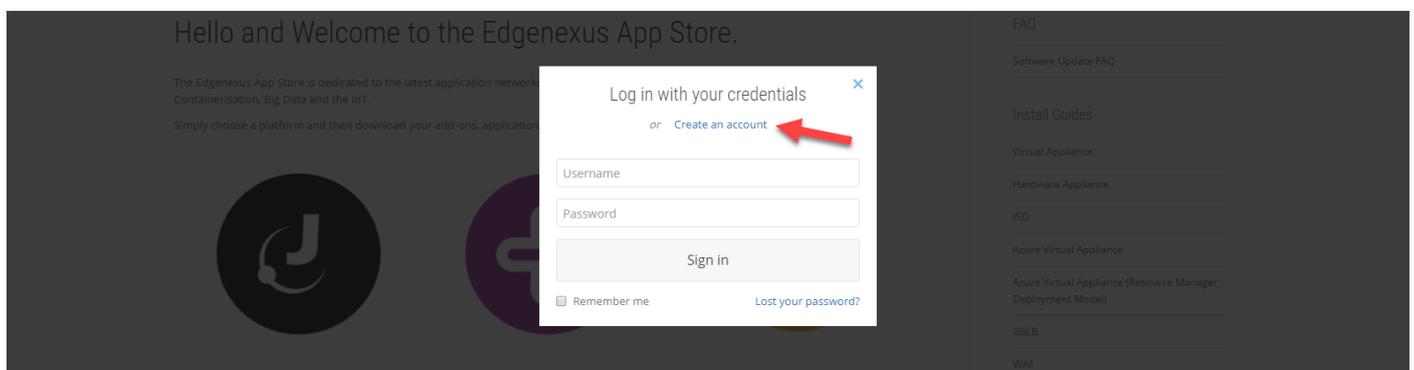
Obtaining the Edgenexus SSL Certificate Manager is very easy.

As with every Edgenexus App, the Edgenexus SSL Certificate Manager is available through the App Store and is free of cost to download, and some are even free to use.

- The first thing to do is to register for access to the Edgenexus App Store. This process is done by using a browser and navigating to <https://appstore.edgenexus.io>.



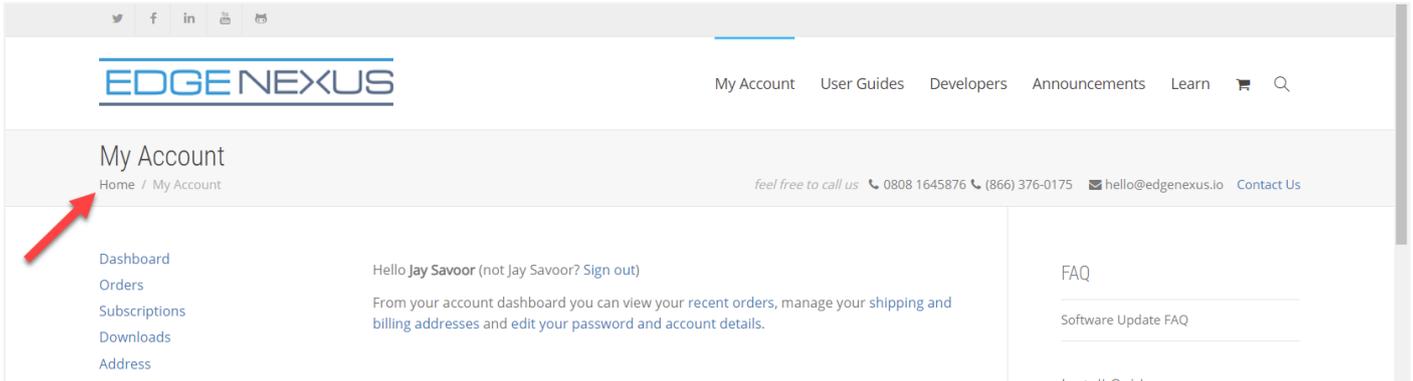
- Click on the login link located in the hamburger icon at the top right.
- Click on the Create an Account, or log in using your account credentials.



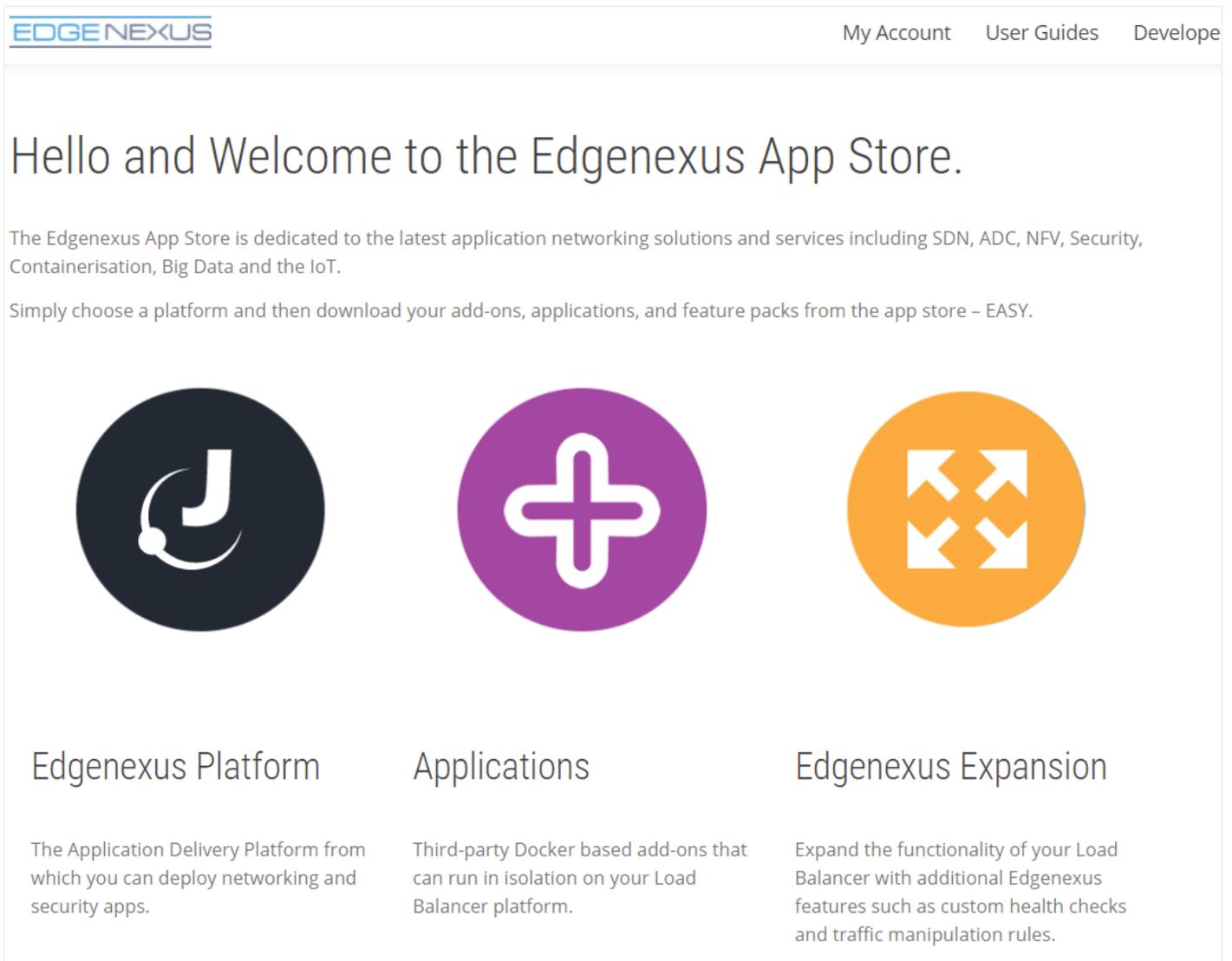
- Once you have logged in, please click on the Home link located under the logo.

Edgenexus SSL Certificate Manager

User Guide



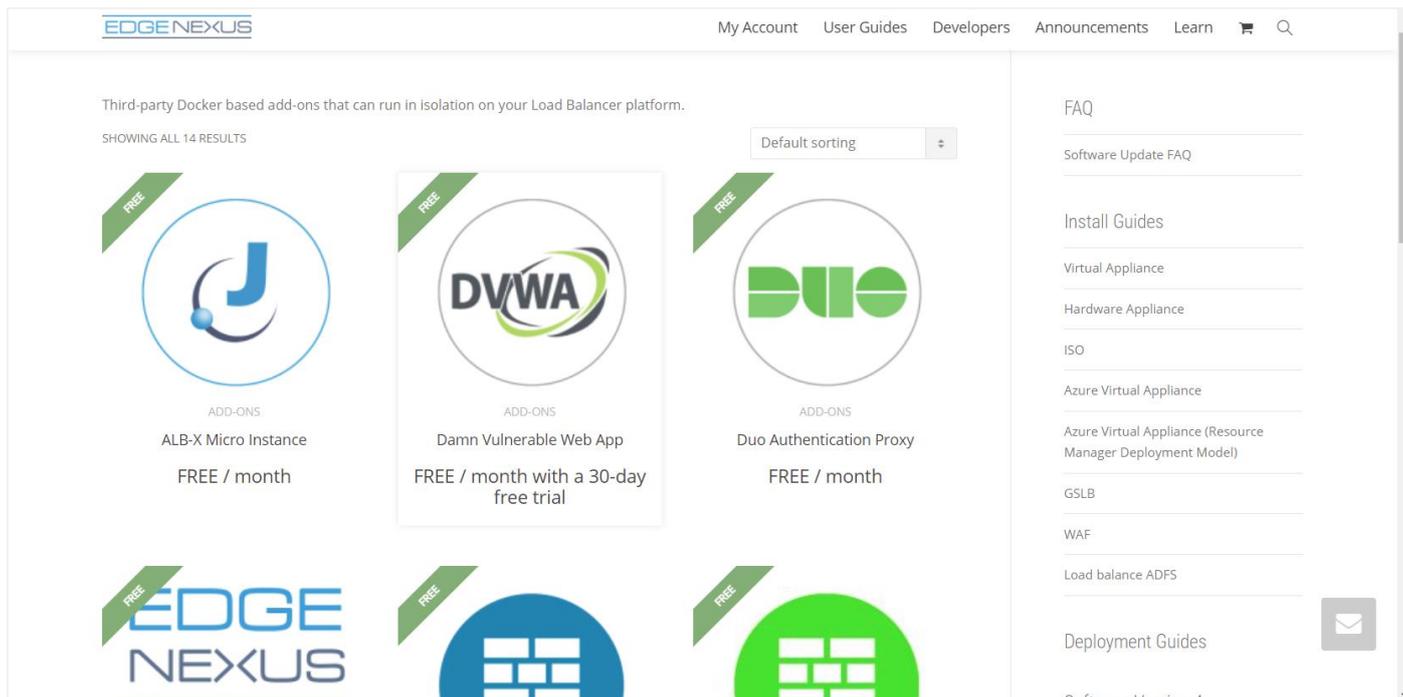
- Next, click on Applications.



- This action will take you to the Applications page, from where you will be able to download the Edgenexus SSL Certificate Manager.

Edgenexus SSL Certificate Manager

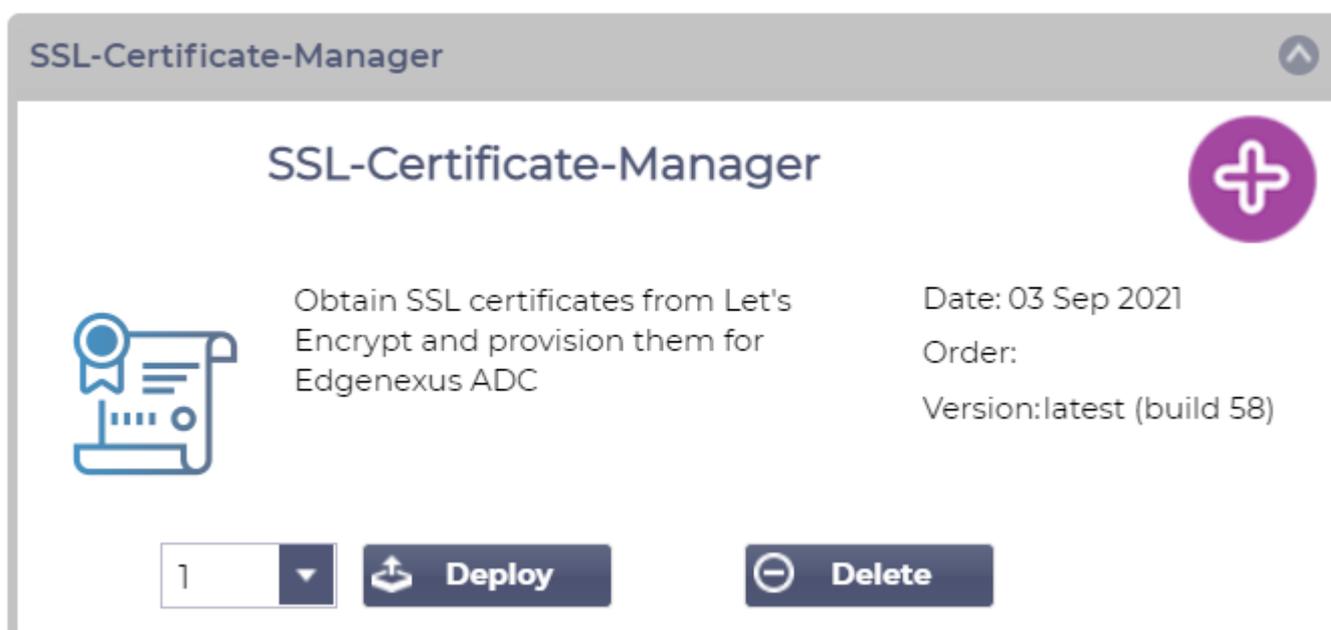
User Guide



- Within the applications page, you can browse for and order the App.
- The Edgenexus SSL Certificate Manager app is free of cost, but you will still need to follow the route of making a purchase.
- At this point, you have two options: Using the App Store from within the EdgeADC or directly downloading the App from the App Store and then uploading it to the EdgeADC

Downloading and importing the App using the EdgeADC

- The first option is to log in using your App Store credentials from inside the EdgeADC. The integrated App Store interface is available using Services > App Store.
- This method will allow you to make the purchase, and then you will find it available within the Purchased Apps section located in Library > Apps.
- The Edgenexus SSL Certificate Manager App looks something like the one shown below.



Edgenexus SSL Certificate Manager

User Guide

- You can choose to download the App then, and it will then appear in the Downloaded Apps section.
- From the Library > Apps > Downloaded Apps section, locate the Dell-ECS Load Balancing App and then deploy it to the EdgeADC containers by clicking the Deploy button.
- If you wish to deploy more than one copy, you can select the number of copies of the App using the dropdown.
- Once deployed, it will be available in the Library > Add-Ons tab

Download and importing the App using direct download

- The secondary method uses your App Store login and directly downloads it to your desktop using a browser.
- Once downloaded, please make sure you save it without altering the filename.
- Please also ensure that there is no (1) or something similar in the filename, possibly indicating a second download, etc.
- With the file downloaded, navigate to Advanced > Software of the EdgeADC GUI using your browser.

The screenshot shows the Edgenexus Software page. The 'Upload Software' section is highlighted with a red box. It contains the following elements:

- Software Version: 4.3.0 (Build 1950) 712100
- A 'Browse' button for selecting a software file.
- An 'Upload Apps And Software' button.
- An 'Upload And Apply Software' button.

Below the 'Upload Software' section, there is an 'Apply Software' section with a table of software updates:

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

- There are several sections within the Software page, but we need the Upload Software section.
- First, click the Browse button and find the Dell ECS Load Balancing App you download.
- Next, click the Upload Apps and Software button.
- The App will be shown in the Downloaded Apps section of Library > Apps.
- From the Library > Apps > Downloaded Apps section, locate the Dell-ECS Load Balancing App and then deploy it to the EdgeADC by clicking the Deploy button.
- If you wish to deploy more than one copy, you can select the number of copies of the App using the dropdown.

Edgenexus SSL Certificate Manager

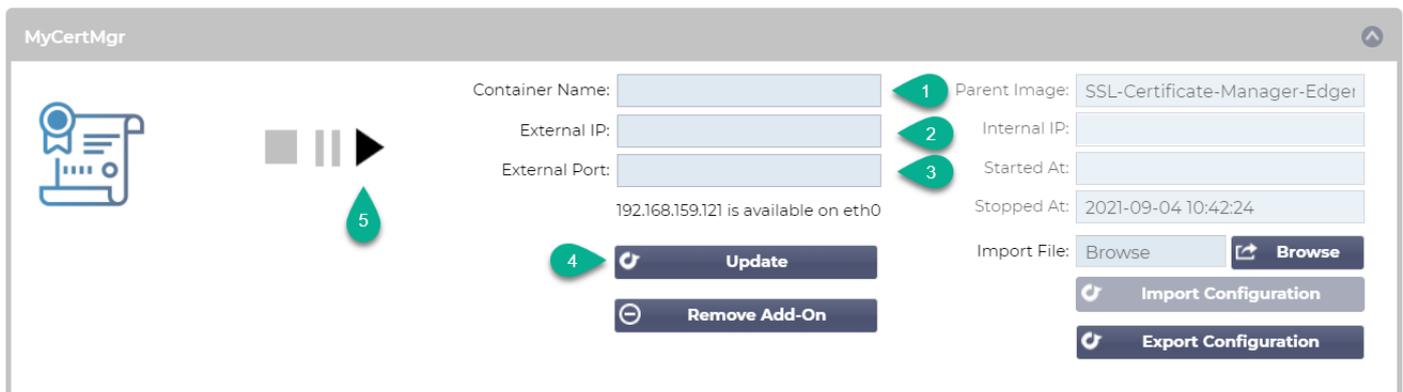
User Guide

- Once deployed, it will be available in the Library > Add-Ons tab

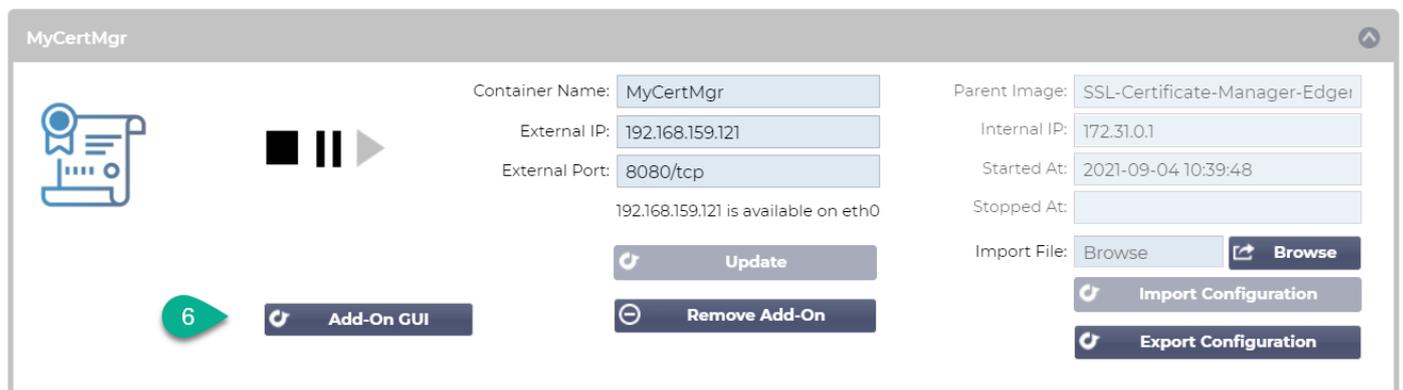
Making the App Operational in EdgeADC v4.2.x and below

When an App is downloaded and deployed, it is yet to be made operational. It has to be given an IP address in the same subnet as the EdgeADC and ports through which it needs to be accessible.

- Navigate to Library > Add-Ons and locate the Edgenexus SSL Certificate Manager App.
- It should look something like the image below.



- Give the Add-On a name ❶ – the EdgeADC's internal DNS system uses this to refer to the App when needed.
- Add an appropriate static IP address ❷. This entry is optional for EdgeADC v4.3.x and above but is mandatory for any version lower than 4.3.x.
- Enter a value for the Port(s) using a port address value of **8080/tcp**.
- Once you have done this, click the Update button ❹ to initialize the App.
- Click the PLAY icon ❺ above to activate the App into an operational state.
- Once operational, it will look like the following image and be listed in the Services section as an embedded App.



- Note the Add-On GUI ❻ button to launch the App GUI and the Pause App and Stop App buttons.
- Once the App is launched, it will open in a new browser tab.

Making the App Operational in EdgeADC v4.3.x and above

When an App is downloaded and deployed, it is yet to be made operational. It has to be given an IP address in the same subnet as the EdgeADC and ports through which it needs to be accessible.

- Navigate to Library > Add-Ons and locate the Dell-ECS Load Balancing App.
- It should look something like the image below.

Edgenexus SSL Certificate Manager

User Guide

MyCertMgr

Add-On Name: 1

External IP: 2

External Ports: 8080/tcp

192.168.159.236 is available on eth0

Update

Remove Add-On

View Log

Add-on: edgenexus/cert-manage

Internal IP:

Started At:

Stopped At: 2021-09-04 09:54:25

Import File: Browse

Import Configuration

Export Configuration

3

- Give the Add-On a name ① – the EdgeADC's internal DNS system uses this to refer to the App when needed.
- Add an appropriate static IP address ②. This entry is optional for EdgeADC v4.3.x and above but is mandatory for any version lower than 4.3.x.
- If you have EdgeADC v4.3.x and above, you do not need to enter a value for the Port(s) as this has already been provided. With earlier editions of EdgeADC (4.2.x and below), you will need to provide a port address value of **8080/tcp**.
- Once you have done this, click the Update button to initialize the App.
- It should look something like the one below.

MyCertMgr

Add-On Name: MyCertMgr

External IP: 192.168.159.236

External Ports: 8080/tcp

192.168.159.236 is available on eth0

Update

Remove Add-On

View Log

Add-on: edgenexus/cert-manage

Internal IP:

Started At:

Stopped At: 2021-09-04 09:56:48

Import File: Browse

Import Configuration

Export Configuration

3

- Click the PLAY icon ③ above to activate the App into an operational state.
- Once operational, it will look like the following image and be listed in the Services section as an embedded App.

MyCertMgr

Add-On Name: MyCertMgr

External IP: 192.168.159.236

External Ports: 8080/tcp

192.168.159.236 is available on eth0

Update

Remove Add-On

View Log

Add-on: edgenexus/cert-manage

Internal IP: 172.31.0.6

Started At: 2021-09-04 09:55:01

Stopped At:

Import File: Browse

Import Configuration

Export Configuration

4 View app

3

- Note the View App ④ button to launch the App GUI and the Pause App and Stop App buttons.

- On EdgeADC versions 4.3 and above, You can also launch by clicking the App Name you provided in the Services section within the Navigation panel.
- Once the App is launched, it will open in a new browser tab for EdgeADC versions below 4.3. On EdgeADC version 4.3 and above, the App will open in the right-side panel.

Prerequisites

To use the Edgenexus SSL Certificate Manager, you must ensure that you have the following prerequisites in place. Failure to have these will lead to a failure to produce useable certificates.

1. You will need to ensure that you have an EdgeADC with a licence installed. The license can be for an evaluation or one that has been purchased.
2. A VIP configured on HTTP Port 80 the ADC for the purposes shown below.
3. You must have a public IP address available that is redirected to the VIP using HTTP Port 80. This measure ensures that the Let's Encrypt systems can connect and validate the DNS ownership for the SSL you will generate.

Mode	VIP	VS	Enabled	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type
Active			<input checked="" type="checkbox"/>	192.168.159.110	255.255.255.0	80		HTTP

4. An entry must be made in your DNS for the FQDN (fully qualified domain name). This entry will point to the public IP address. This measure ensures that the FQDN for which you are generating the SSL certificate is valid in terms of IP addressing.

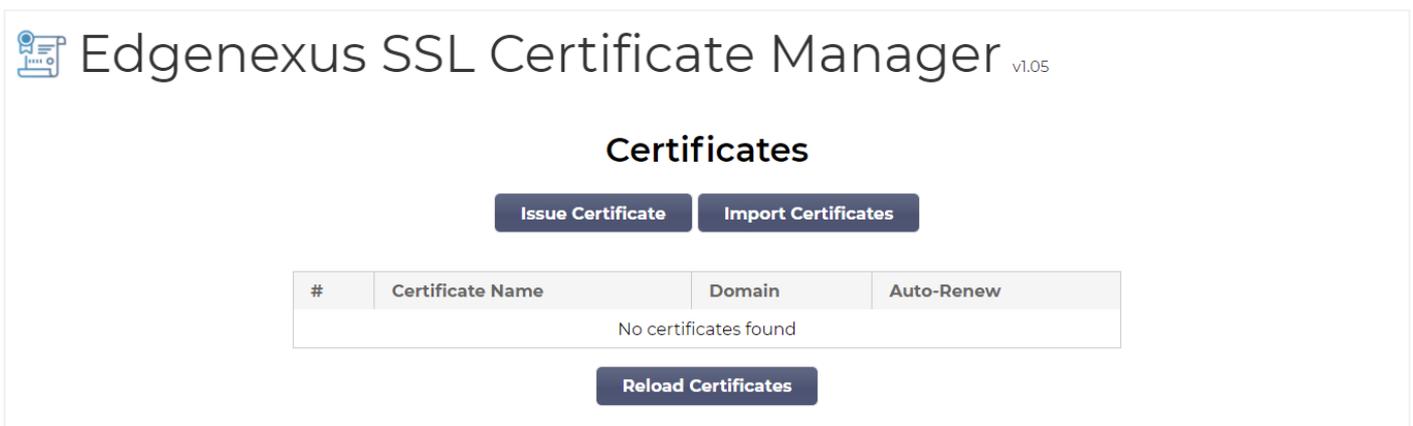
Once you have done this, you are all good to go.

Issuing Certificates with Edgenexus SSL Certificate Manager

The Edgenexus SSL Certificate Manager configuration is performed using a wizard-based system and so is very easy to use.

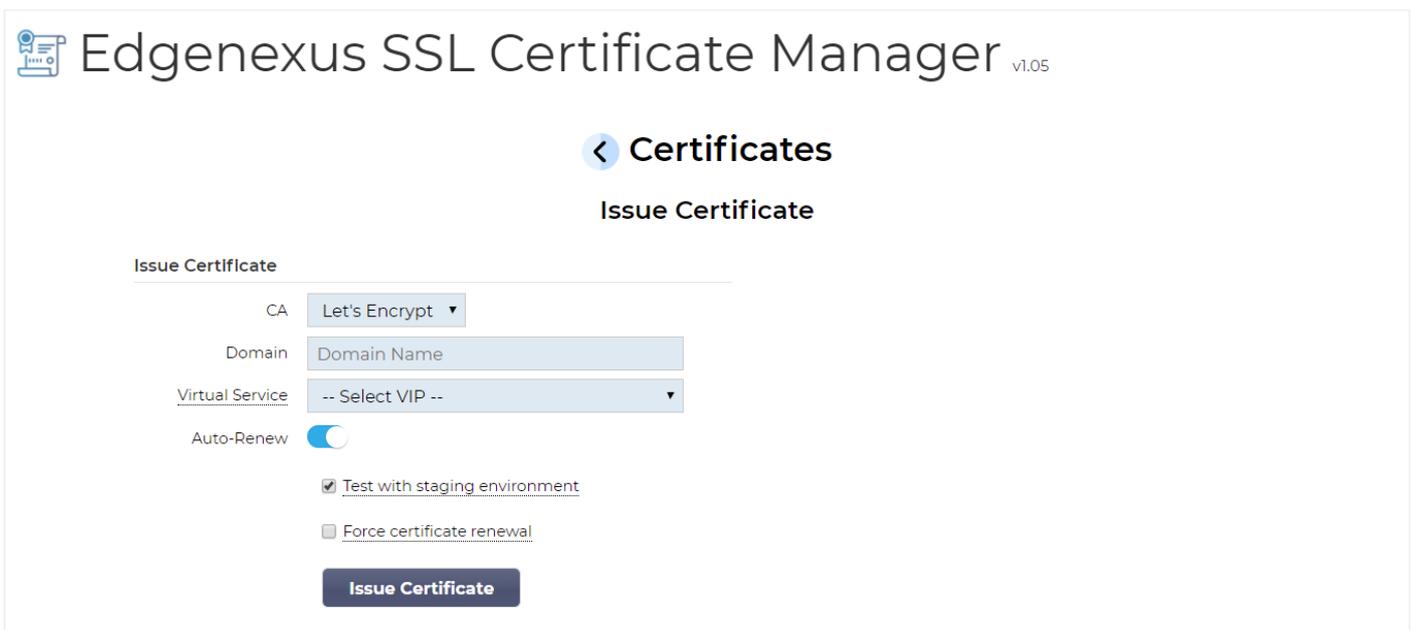
When you launch the user interface, you will see a page similar to the image below. You can see that you can perform two tasks with the Edgenexus SSL Certificate Manager: Issue Certificates and Import Certificates.

The import certificates function is used to migrate from another platform such as F5 and import SSL certificates in bulk.



The Edgenexus SSL Certificate Manager work in conjunction with Let's Encrypt to allow the generation and issuance of Let's Encrypt SSL certificates in real-time, including automatic renewal of the SSL certificate.

- Click the Issue Certificate button to begin the issuance process.
- The page will change to the one you see below.



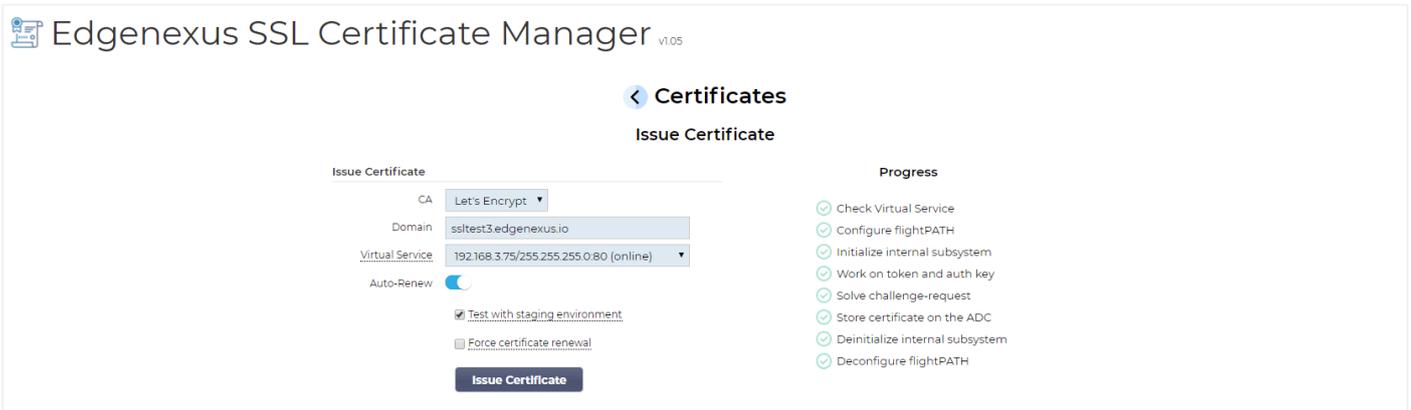
- As you can see, various items are need configuration so that you can issue an SSL certificate.

Edgenexus SSL Certificate Manager

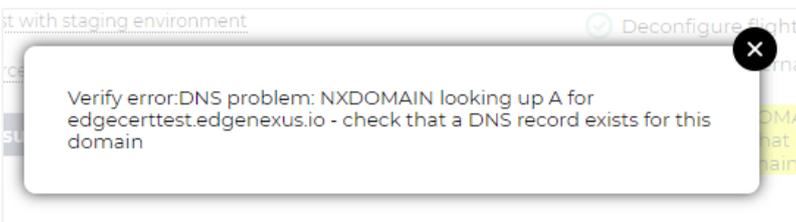
User Guide

Field	Description
CA	Currently, only the Let's Encrypt option is available. In the future, as more providers become available, we will include them here.
Domain	The domain field is used to specify the FQDN for which the certificate is required. For example, www.acme.com , or *.acme.com in the case of a wildcard. NOTE: The FQDN you place here must be reachable via DNS query.
Virtual Service	A virtual service must be online and work on HTTP port 80 to answer a challenge request by the Let's Encrypt system. This virtual service must follow the guidance provided in the chapter on prerequisites.
Auto-Renew	When enabled at the time of issuance, the certificate will be set to auto-renew.
Test with staging environment	Use the Let's Encrypt staging server to issue a new certificate (for testing).
Force certificate renewal	If your Let's Encrypt certificate is already issued and not expired, you won't be able to issue a new certificate without enabling this option.

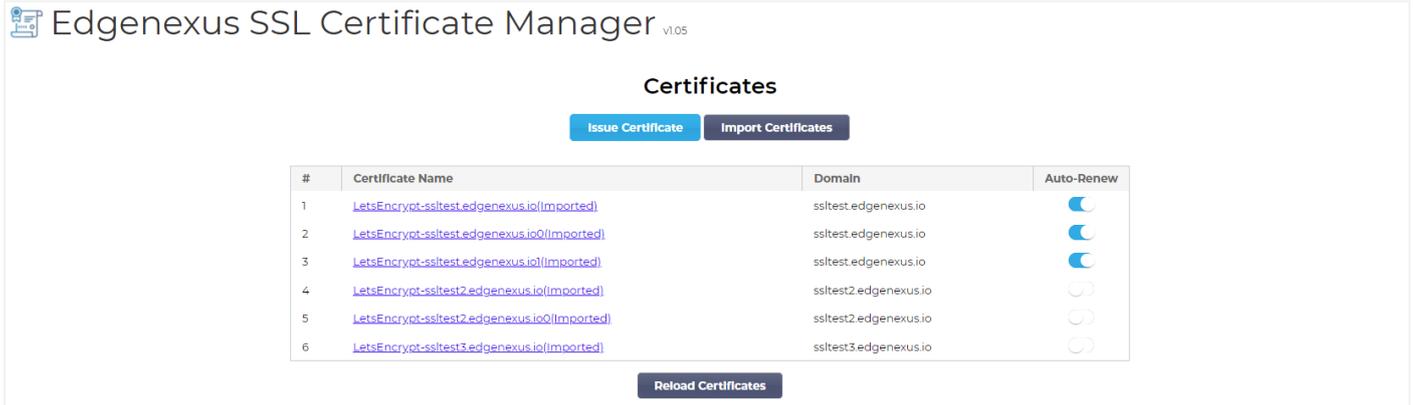
- Once you have completed the form, click the Issue Certificate button to proceed to the verification stage.
- Once you click the Issue Certificate button, the Edgenexus SSL Certificate Manager begins the process of verification with the Let's Encrypt or other ACME certificate system supported within the Edgenexus SSL Certificate Manager.
- You will see a screen similar to the one below as the process finishes.



- The Edgenexus SSL Certificate Manager will store the SSL certificate you created in the EdgeADC's SSL Store if the process is successful.
- The Edgenexus SSL Certificate Manager will display the following error if the process encounters any problem.



The certificates you have issued will be listed on the launch page of the App.



The screenshot shows the Edgenexus SSL Certificate Manager interface. At the top, there is a header with the logo and the text "Edgenexus SSL Certificate Manager v1.05". Below the header, the word "Certificates" is centered. Underneath, there are two buttons: "Issue Certificate" and "Import Certificates". A table lists six certificates with columns for "#", "Certificate Name", "Domain", and "Auto-Renew". The "Auto-Renew" column contains toggle switches, some of which are turned on. Below the table is a "Reload Certificates" button.

#	Certificate Name	Domain	Auto-Renew
1	LetsEncrypt-ssltest.edgenexus.io(Imported)	ssltest.edgenexus.io	<input checked="" type="checkbox"/>
2	LetsEncrypt-ssltest.edgenexus.io0(Imported)	ssltest.edgenexus.io	<input checked="" type="checkbox"/>
3	LetsEncrypt-ssltest.edgenexus.io1(Imported)	ssltest.edgenexus.io	<input checked="" type="checkbox"/>
4	LetsEncrypt-ssltest2.edgenexus.io(Imported)	ssltest2.edgenexus.io	<input type="checkbox"/>
5	LetsEncrypt-ssltest2.edgenexus.io0(Imported)	ssltest2.edgenexus.io	<input type="checkbox"/>
6	LetsEncrypt-ssltest3.edgenexus.io(Imported)	ssltest3.edgenexus.io	<input type="checkbox"/>

FlightPATH and how its used

As part of the certificate creation process, the Let's Encrypt needs to validate the domain name you have provided using a challenge request.

The Edgenexus SSL Certificate Manager does this by using flightPATH, meaning that you can create SSL certificates as needed without doing this on the actual servers.

When you click on the Issue Certificate button, the EdgeADC creates a flightPATH rule that intercepts the challenge request from the certificate-issuing authority, Let's Encrypt, or any supported ACME system.

The flightPATH rule then initiates a request redirect to the Edgenexus SSL Certificate Manager rather than the real server for which it is intended. The Edgenexus SSL Certificate Manager then acknowledges the challenge request and validates it for certificate issuance.

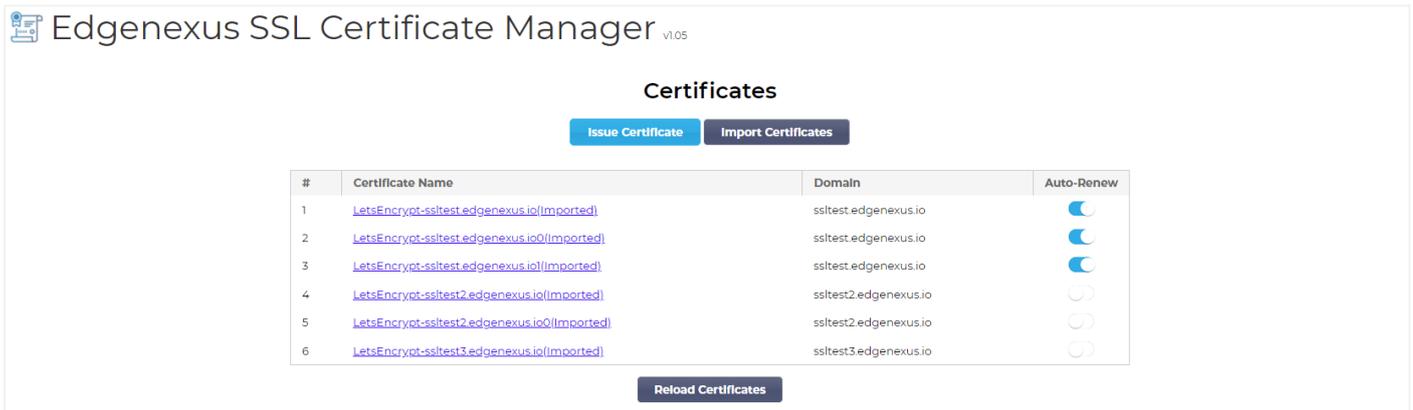
Everything is done automatically from within the EdgeADC itself, without any intervention required from the administrator.

Bulk Certificate Import

One of the requirements of specific customers is the need to import certificates in bulk. The need to import certificates in bulk could be because they have many certificates or want to migrate from other load balancers such as F5.

The Edgenexus SSL Certificate Manager can import PFX certificates in bulk using a zip file. The proviso here is that the password for the PFX must be the same for all certificates. A common password is normally the case when you perform a bulk export from another vendor's load balancer.

- To import SSL certificates in bulk, click the Import Certificates button on the App's page.

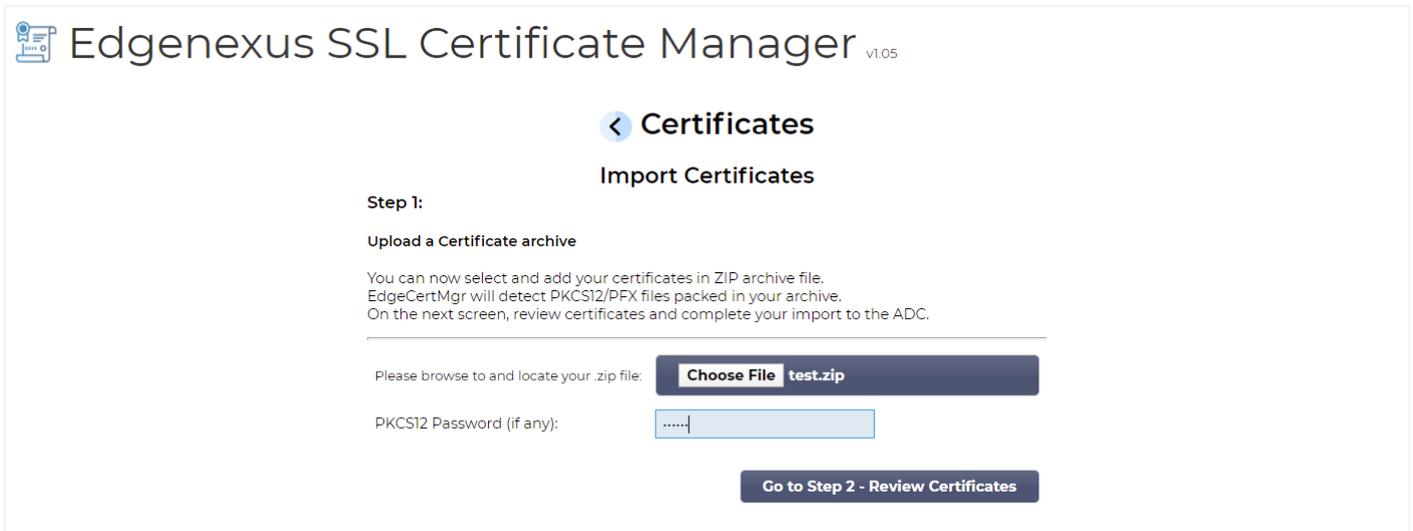


The screenshot shows the 'Certificates' page in the Edgenexus SSL Certificate Manager. At the top, there are two buttons: 'Issue Certificate' and 'Import Certificates'. Below these is a table with the following data:

#	Certificate Name	Domain	Auto-Renew
1	LetsEncrypt-ssltest.edgenexus.io(Imported)	ssltest.edgenexus.io	<input checked="" type="checkbox"/>
2	LetsEncrypt-ssltest.edgenexus.io0(Imported)	ssltest.edgenexus.io	<input checked="" type="checkbox"/>
3	LetsEncrypt-ssltest.edgenexus.io1(Imported)	ssltest.edgenexus.io	<input checked="" type="checkbox"/>
4	LetsEncrypt-ssltest2.edgenexus.io(Imported)	ssltest2.edgenexus.io	<input type="checkbox"/>
5	LetsEncrypt-ssltest2.edgenexus.io0(Imported)	ssltest2.edgenexus.io	<input type="checkbox"/>
6	LetsEncrypt-ssltest3.edgenexus.io(Imported)	ssltest3.edgenexus.io	<input type="checkbox"/>

At the bottom of the table is a 'Reload Certificates' button.

- The next step is to select the ZIP file you have created, either manually or using a bulk export.



The screenshot shows the 'Import Certificates' step in the Edgenexus SSL Certificate Manager. The page title is 'Certificates' with a back arrow. Below it is the heading 'Import Certificates'. The instructions are:

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: test.zip

PKCS12 Password (if any):

- Enter the PFX password.
- Click on Goto Step 2 – Review Certificates button.
- The next page will allow you to review what certificates you are going to import.

Edgenexus SSL Certificate Manager

User Guide

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.

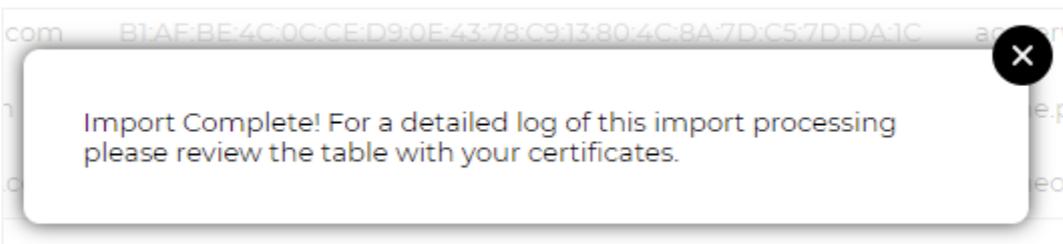
Import Certificates

#	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

- If everything is correct, you can click the Import Certificates button.
- You should see a confirmatory message if the import succeeds.



- Closing this pop-up will show the final screen as below, indicating that the import was successful.

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

You can review the SSL certificates imported using Library > SSL Certificates.