



SOFTWARE VERSION
1.0.0

Edgenexus SSL Certificate Manager

AN EDGENEXUS EDGEADC APP

Dokument-Eigenschaften

Dokumentnummer: 2.0.9.13.21.14.09

Erstellungsdatum des Dokuments: 5. August 2021

Dieses Dokument wurde zuletzt bearbeitet: 13 September 2021

Autor des Dokuments: Jay Savoor

Dokument Zuletzt bearbeitet von:

Dokument Haftungsausschluss

Die Screenshots und Grafiken in diesem Handbuch können aufgrund von Unterschieden in der Produktversion leicht von Ihrem Produkt abweichen. Edgenexus versichert, dass sie alle angemessenen Anstrengungen unternehmen, um sicherzustellen, dass die Informationen in diesem Dokument vollständig und korrekt sind. Edgenexus übernimmt keine Haftung für etwaige Fehler. Edgenexus nimmt Änderungen und Korrekturen an den Informationen in diesem Dokument in zukünftigen Versionen vor, wenn dies erforderlich ist.

Urheberrechte

© 2021 Alle Rechte vorbehalten.

Die Informationen in diesem Dokument können ohne vorherige Ankündigung geändert werden und stellen keine Verpflichtung seitens des Herstellers dar. Kein Teil dieses Handbuchs darf ohne ausdrückliche schriftliche Genehmigung des Herstellers in irgendeiner Form oder mit irgendwelchen Mitteln, elektronisch oder mechanisch, einschließlich Fotokopien und Aufzeichnungen, für irgendeinen Zweck vervielfältigt oder übertragen werden. Eingetragene Marken sind Eigentum ihrer jeweiligen Inhaber. Es wurden alle Anstrengungen unternommen, um diesen Leitfaden so vollständig und genau wie möglich zu gestalten, aber es wird keine Garantie für die Eignung übernommen. Die Autoren und der Herausgeber übernehmen keine Verantwortung oder Haftung für Verluste oder Schäden, die durch die Verwendung der in diesem Leitfaden enthaltenen Informationen entstehen.

Markenzeichen

Das Edgenexus-Logo, Edgenexus, EdgeADC, EdgeWAF, EdgeGSLB, EdgeDNS sind alles Marken von Edgenexus Limited. Alle anderen Marken sind das Eigentum ihrer jeweiligen Inhaber und werden anerkannt.

Edgenexus Unterstützung

Wenn Sie technische Fragen zu diesem Produkt haben, senden Sie bitte ein Support-Ticket an: support@edgenexus.io

Inhaltsverzeichnis

Dokument-Eigenschaften	1
Dokument Haftungsausschluss	1
Copyrights.....	1
Markenzeichen.....	1
Edgenexus Unterstützung	1
Was ist der Edgenexus SSL Certificate Manager?	3
Holen und installieren Sie den Edgenexus SSL Certificate Manager?	4
Herunterladen und Importieren der App mit dem EdgeADC	6
Herunterladen und Importieren der App über den direkten Download.....	7
Die App in EdgeADC v4.2.x und darunter betriebsbereit machen.....	8
Die App in EdgeADC v4.3.x und höher betriebsbereit machen	9
Voraussetzungen.....	11
Ausstellen von Zertifikaten mit Edgenexus SSL Certificate Manager	12
FlightPATH und seine Verwendung	14
Massenimport von Zertifikaten.....	15

Was ist der Edgenexus SSL Certificate Manager?

Alle Unternehmen, die Server verwenden, die sichere Anwendungen bereitstellen, müssen SSL-Zertifikate installieren.

Um dieser Anforderung gerecht zu werden, verwenden IT-Manager Domänenzertifikate für interne, domänenverbundene Server und wenden sich an SSL-Anbieter für global vertrauenswürdige Zertifikate, wenn die Server webbasierte Lösungen für den privaten oder öffentlichen Zugang hosten.

Die Beschaffung von Zertifikaten bei Behörden kann zeitaufwendig sein und Kosten verursachen.

Um dieses Problem zu lösen, hat Edgenexus den Edgenexus SSL Certificate Manager eingeführt, der es dem IT-Administrator ermöglicht, die benötigten Zertifikate mit Hilfe der Let's Encrypt Service-Technologie zu generieren.

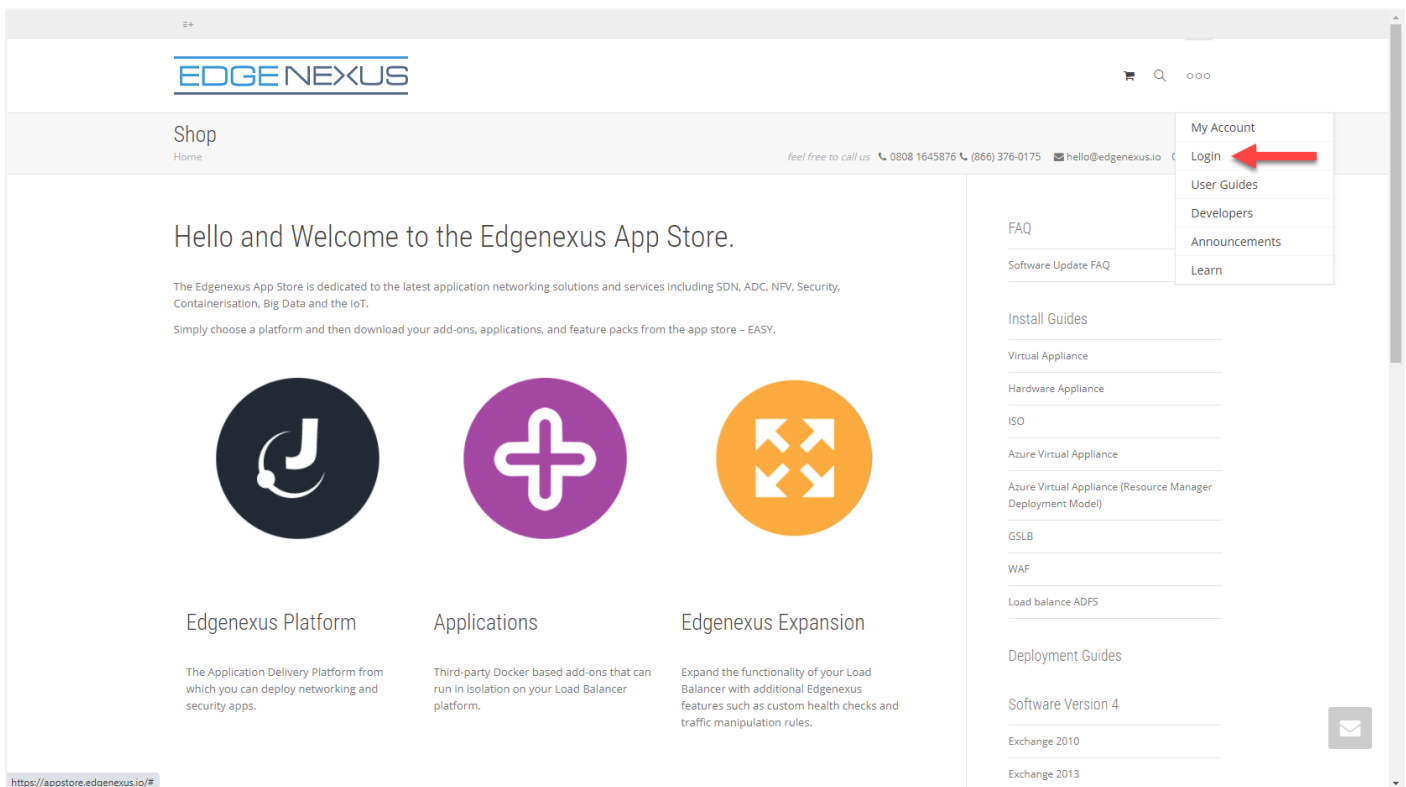
Die Verwendung des Edgenexus SSL Certificate Manager ist einfach und unkompliziert.

Holen und installieren Sie den Edgenexus SSL Certificate Manager?

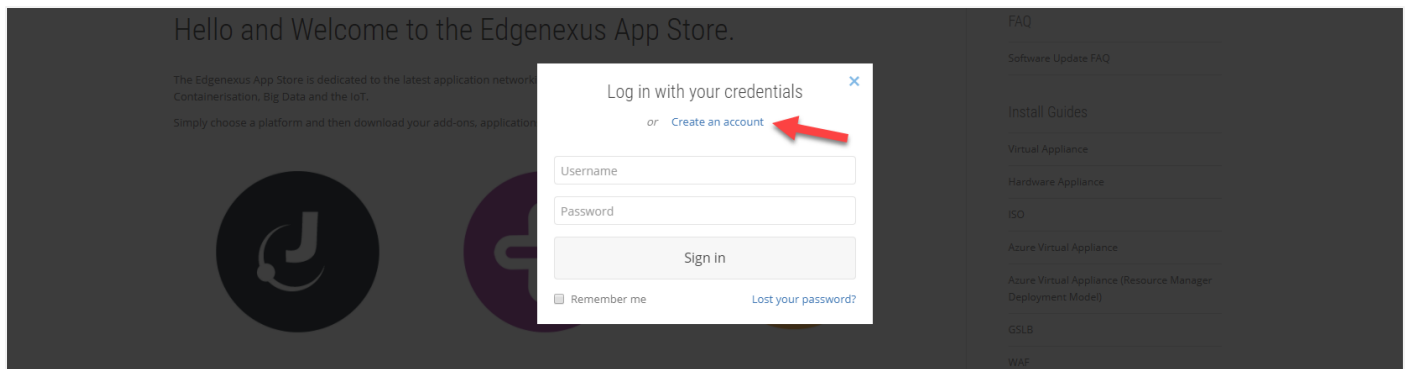
Der Bezug des Edgenexus SSL Certificate Manager ist sehr einfach.

Wie jede Edgenexus App ist auch der Edgenexus SSL Certificate Manager über den App Store erhältlich und kann kostenlos heruntergeladen werden, einige davon sogar kostenlos.

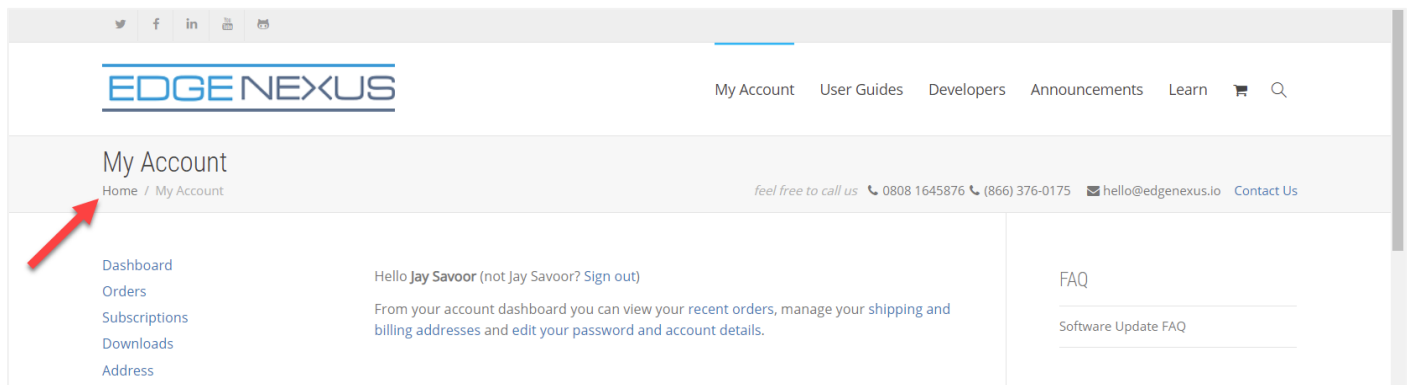
- Als erstes müssen Sie sich für den Zugang zum Edgenexus App Store registrieren. Verwenden Sie dazu einen Browser und navigieren Sie zu <https://appstore.edgenexus.io>.



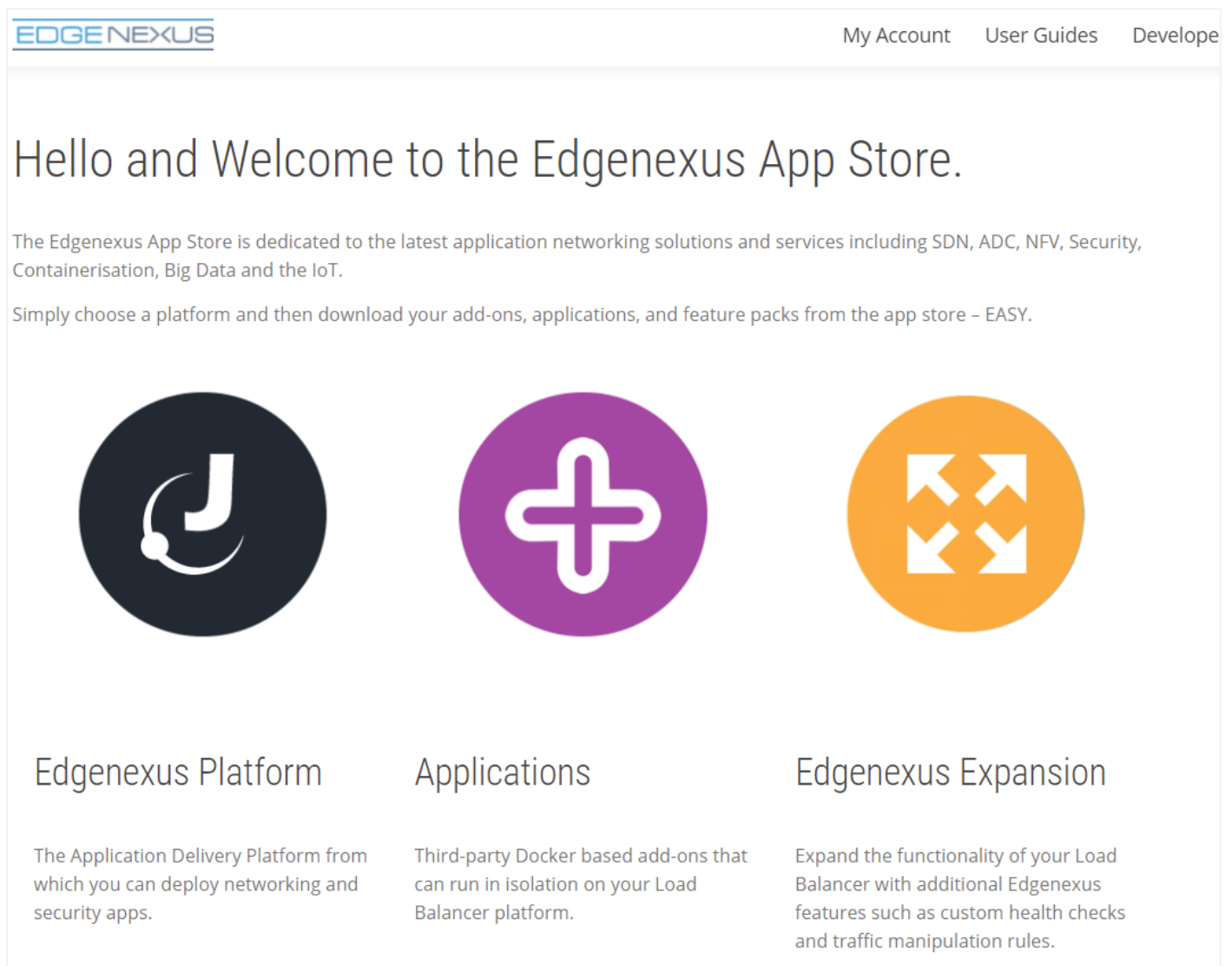
- Klicken Sie auf den Login-Link, der sich im Hamburger-Symbol oben rechts befindet.
- Klicken Sie auf Konto erstellen, oder melden Sie sich mit Ihren Zugangsdaten an.



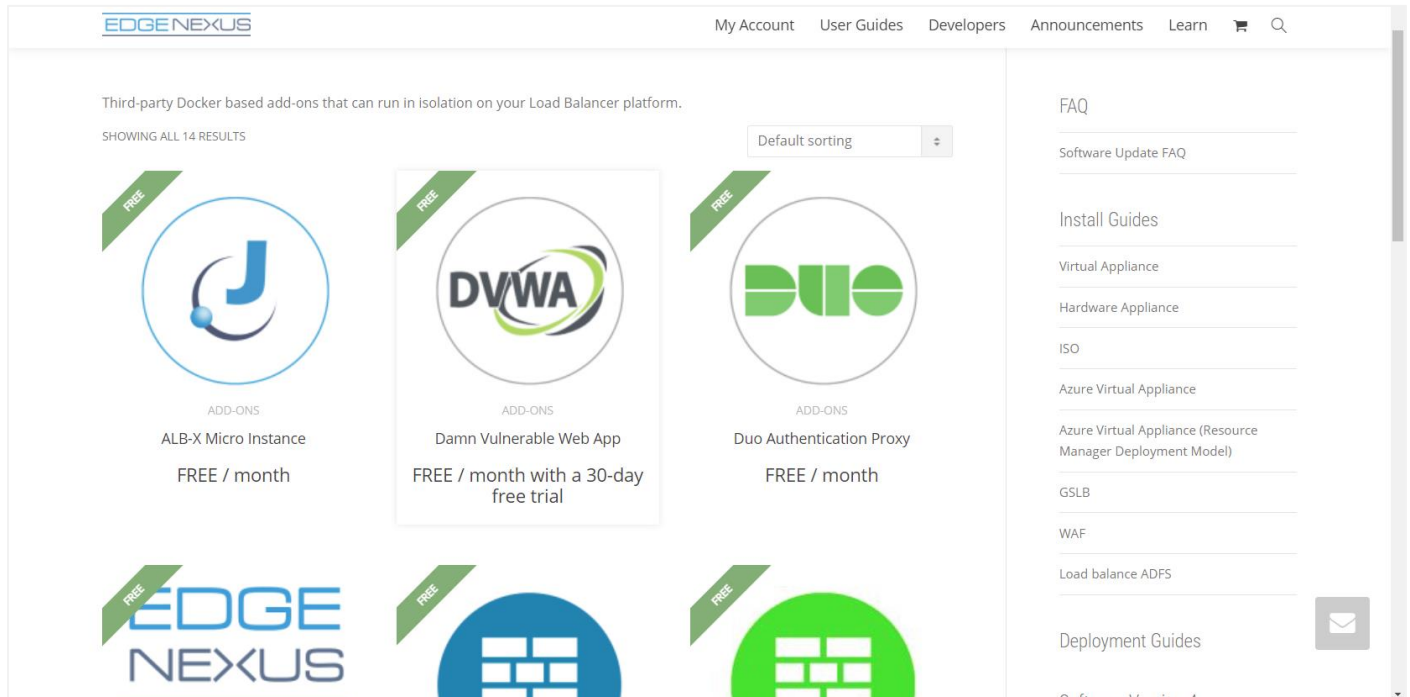
- Sobald Sie sich eingeloggt haben, klicken Sie bitte auf den Link Home unter dem Logo.



- Klicken Sie anschließend auf Anwendungen.



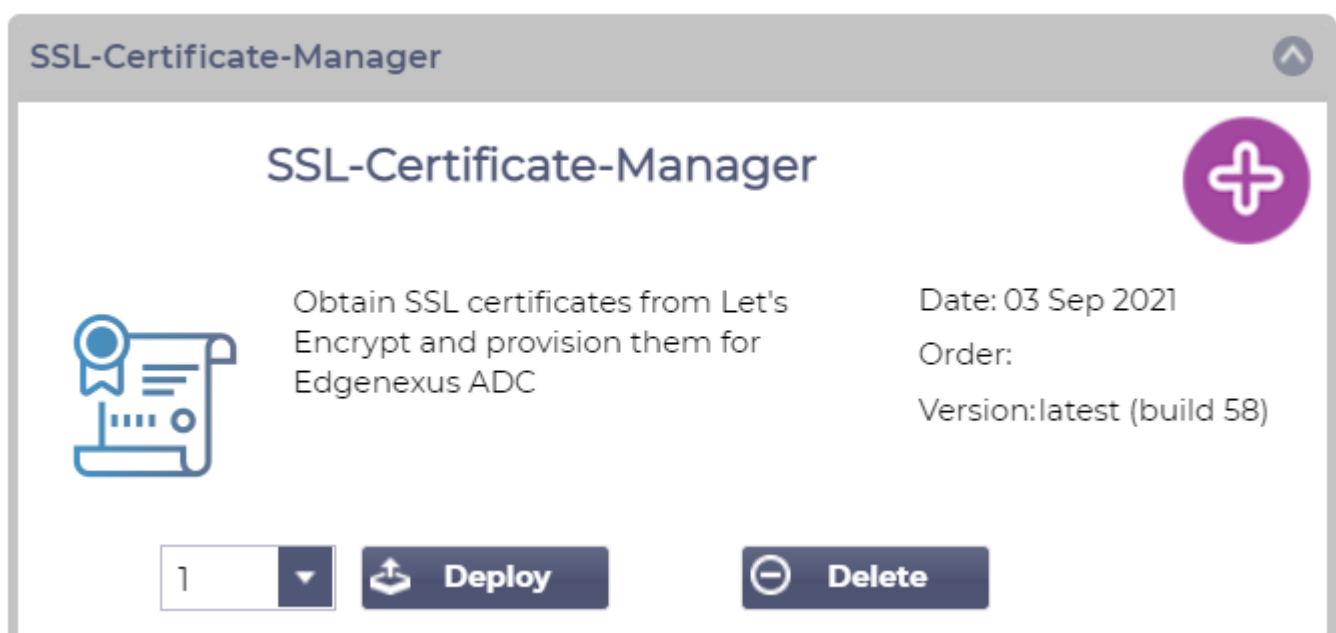
- Diese Aktion führt Sie zur Seite Anwendungen, von wo aus Sie den Edgenexus SSL Certificate Manager herunterladen können.



- Auf der Anwendungsseite können Sie nach der App suchen und sie bestellen.
- Die Edgenexus SSL Certificate Manager App ist kostenlos, aber Sie müssen trotzdem den Weg des Kaufs gehen.
- An diesem Punkt haben Sie zwei Möglichkeiten: Sie können den App Store vom EdgeADC aus nutzen oder die App direkt aus dem App Store herunterladen und sie dann auf den EdgeADC hochladen.

Herunterladen und Importieren der App mit dem EdgeADC

- Die erste Möglichkeit besteht darin, sich mit Ihren App Store-Zugangsdaten vom EdgeADC aus anzumelden. Die integrierte App Store-Schnittstelle finden Sie unter Dienste > App Store.
- Auf diese Weise können Sie den Kauf tätigen. Anschließend finden Sie die App im Abschnitt Gekaufte Apps unter Bibliothek > Apps.
- Die Edgenexus SSL Certificate Manager App sieht in etwa so aus wie die unten abgebildete.



- Sie können dann wählen, ob Sie die App herunterladen möchten. Sie wird dann im Bereich Heruntergeladene Apps angezeigt.
- Suchen Sie im Bereich Bibliothek > Apps > Heruntergeladene Apps die Dell-ECS Load Balancing App und stellen Sie sie dann in den EdgeADC-Containern bereit, indem Sie auf die Schaltfläche Bereitstellen klicken.
- Wenn Sie mehr als eine Kopie bereitstellen möchten, können Sie über das Dropdown-Menü die Anzahl der Kopien der App auswählen.
- Nach der Bereitstellung ist es auf der Registerkarte Bibliothek > Add-Ons verfügbar.

Herunterladen und Importieren der App über den direkten Download

- Die sekundäre Methode verwendet Ihr App Store-Login und lädt es direkt über einen Browser auf Ihren Desktop.
- Wenn Sie die Datei heruntergeladen haben, stellen Sie bitte sicher, dass Sie sie speichern, ohne den Dateinamen zu ändern.
- Vergewissern Sie sich auch, dass im Dateinamen keine (1) oder etwas Ähnliches enthalten ist, was auf einen zweiten Download hinweisen könnte usw.
- Wenn Sie die Datei heruntergeladen haben, navigieren Sie mit Ihrem Browser zu Erweitert > Software der EdgeADC-Benutzeroberfläche.

Software Details

User Name: admin Location: Altrincham, United Kingdom
Machine ID: 367-B05F-934 Support Expiry: None
Licence ID: {9A000FC9-5C0F-48BE-86B7-D83E8A94FB94} Support Type: Standard
Licence Expiry: Permanent Current Software Version: 4.3.0 (Build 1950) 712100

[Refresh To View Available Software](#)

Download From Cloud

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	

[Download Selected Software](#)

Upload Software

Software Version: 4.3.0 (Build 1950) 712100

Browse for software file then click upload to apply. [Browse](#)

[Upload Apps And Software](#) [Upload And Apply Software](#)

Apply Software

[Apply Selected Software Update](#)

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

[Remove](#)

- Es gibt mehrere Bereiche auf der Seite Software, aber wir brauchen den Bereich Software hochladen.
- Klicken Sie zunächst auf die Schaltfläche Durchsuchen und suchen Sie die Dell ECS Load Balancing App, die Sie heruntergeladen haben.
- Klicken Sie anschließend auf die Schaltfläche Apps und Software hochladen.

- Die App wird im Abschnitt Heruntergeladene Apps unter Bibliothek > Apps angezeigt.
- Suchen Sie im Bereich Bibliothek > Apps > Heruntergeladene Apps die Dell-ECS Load Balancing App und stellen Sie sie auf dem EdgeADC bereit, indem Sie auf die Schaltfläche Bereitstellen klicken.
- Wenn Sie mehr als eine Kopie bereitstellen möchten, können Sie über das Dropdown-Menü die Anzahl der Kopien der App auswählen.
- Nach der Bereitstellung ist es auf der Registerkarte Bibliothek > Add-Ons verfügbar.

Herstellung der Betriebsbereitschaft der Appin EdgeADC v4.2.x und darunter

Wenn eine App heruntergeladen und bereitgestellt wurde, muss sie noch in Betrieb genommen werden. Sie muss eine IP-Adresse im gleichen Subnetz wie der EdgeADC und Ports erhalten, über die sie erreichbar sein muss.

- Navigieren Sie zu Bibliothek > Add-Ons und suchen Sie die Edgenexus SSL Certificate Manager App.
- Es sollte in etwa so aussehen wie das Bild unten.

MyCertMgr

Container Name:

External IP:

External Port:

192.168.159.121 is available on eth0

1

2

3

4

5

Parent Image: SSL-Certificate-Manager-Edge

Internal IP:

Started At:

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

Import File:

- Geben Sie dem Add-On einen Namen ①- das interne DNS-System des EdgeADC verwendet diesen, um bei Bedarf auf die App zu verweisen.
- Fügen Sie eine geeignete statische IP-Adresse hinzu ②. Dieser Eintrag ist optional für EdgeADC v4.3.x und höher, aber obligatorisch für alle Versionen unter 4.3.x.
- Geben Sie einen Wert für den/die Port(s) ein und verwenden Sie als Portadresse den Wert **8080/tcp**.
- Wenn Sie dies getan haben, klicken Sie auf die Schaltfläche Aktualisieren, um die App zu initialisieren. ④
- Klicken Sie auf das PLAY-Symbol ⑤ oben, um die App zu aktivieren und in den Betriebszustand zu versetzen.
- Sobald sie betriebsbereit ist, sieht sie wie das folgende Bild aus und wird im Abschnitt Dienste als eingebettete App aufgeführt.

MyCertMgr

Container Name: MyCertMgr

External IP: 192.168.159.121

External Port: 8080/tcp

192.168.159.121 is available on eth0

6

Parent Image: SSL-Certificate-Manager-Edge

Internal IP: 172.31.0.1

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

Stopped At:

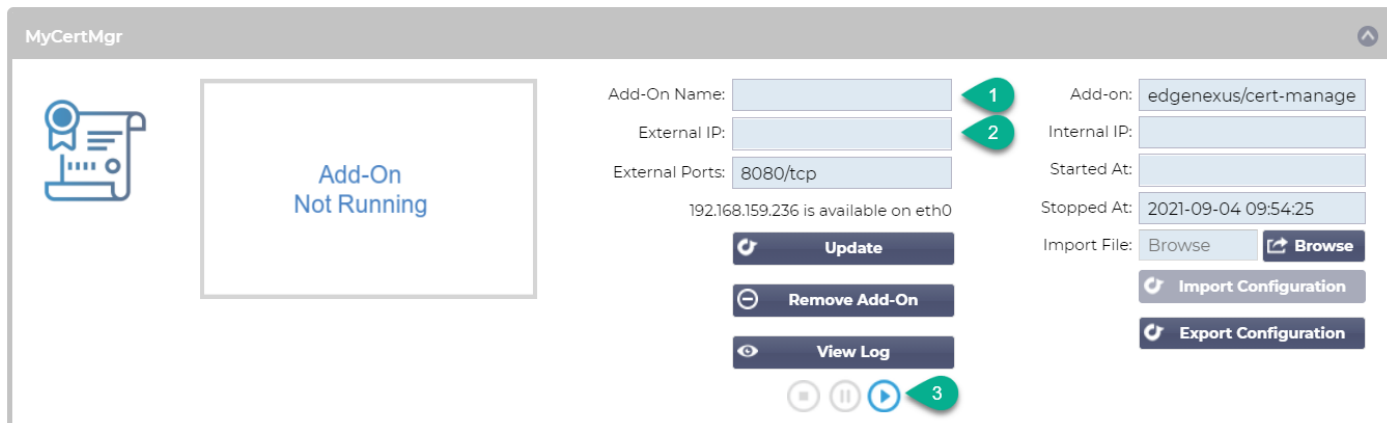
Import File:

- Beachten Sie die Schaltfläche ⑥ Add-On GUI zum Starten der App-GUI sowie die Schaltflächen App anhalten und App stoppen.
- Sobald die App gestartet ist, wird sie in einem neuen Browser-Tab geöffnet.

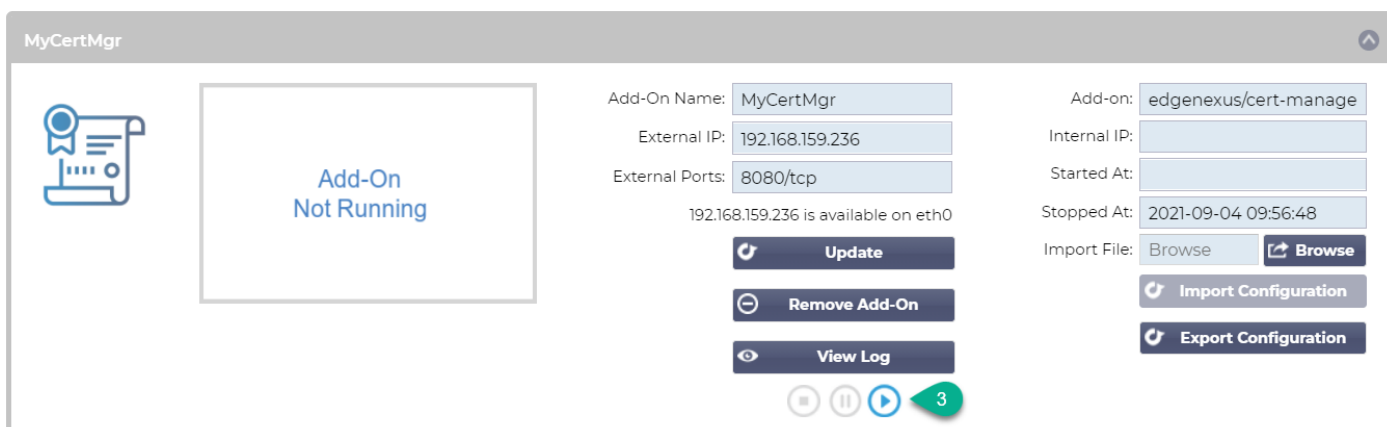
Die App in EdgeADC v4.3.x und höher betriebsbereit machen

Wenn eine App heruntergeladen und bereitgestellt wurde, muss sie noch in Betrieb genommen werden. Sie muss eine IP-Adresse im gleichen Subnetz wie der EdgeADC und Ports erhalten, über die sie erreichbar sein muss.

- Navigieren Sie zu Bibliothek > Add-Ons und suchen Sie die Dell-ECS Load Balancing App.
- Es sollte in etwa so aussehen wie das Bild unten.



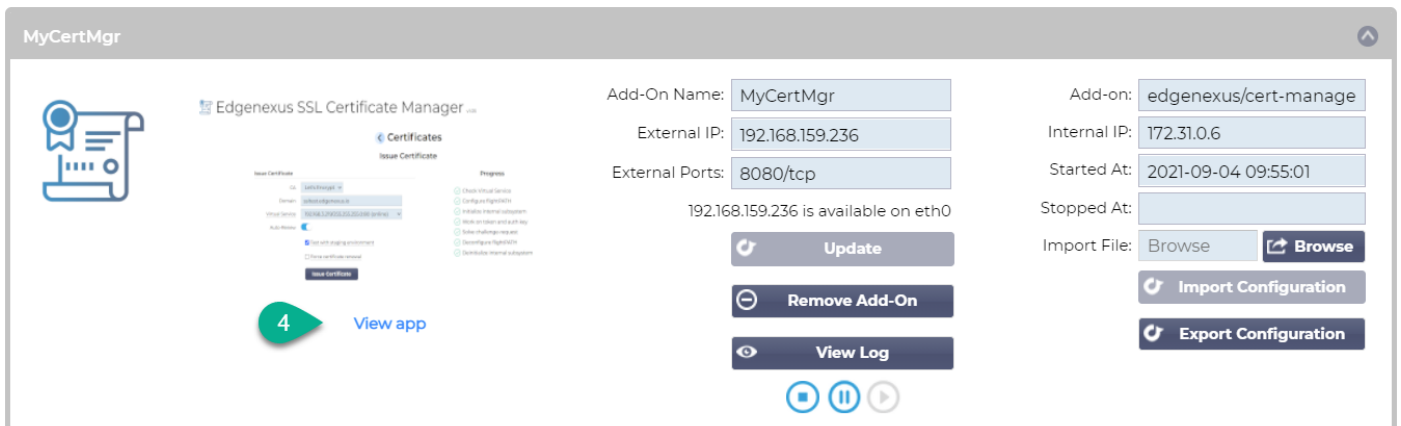
- Geben Sie dem Add-On einen Namen ①- das interne DNS-System des EdgeADC verwendet diesen, um bei Bedarf auf die App zu verweisen.
- Fügen Sie eine geeignete statische IP-Adresse hinzu ②. Dieser Eintrag ist optional für EdgeADC v4.3.x und höher, aber obligatorisch für alle Versionen unter 4.3.x.
- Wenn Sie EdgeADC v4.3.x und höher haben, brauchen Sie keinen Wert für den/die Port(s) einzugeben, da dieser bereits vorgegeben ist. Bei früheren Versionen von EdgeADC (4.2.x und darunter) müssen Sie einen Wert für die Portadresse **8080/tcp** angeben.
- Wenn Sie dies getan haben, klicken Sie auf die Schaltfläche Aktualisieren, um die App zu initialisieren.
- Es sollte in etwa so aussehen wie das untenstehende Bild.



- Klicken Sie auf das PLAY-Symbol ③ oben, um die App zu aktivieren und in den Betriebszustand zu versetzen.
- Sobald sie betriebsbereit ist, sieht sie wie das folgende Bild aus und wird im Bereich Dienste als eingebettete App aufgeführt.

Edgenexus SSL Certificate Manager

Benutzerhandbuch



- Beachten Sie die Schaltfläche 4 App anzeigen, um die App-GUI zu starten, sowie die Schaltflächen App anhalten und App stoppen.
- Bei EdgeADC Versionen 4.3 und höher können Sie die App auch starten, indem Sie auf den Namen der App klicken, den Sie im Abschnitt Dienste im Navigationsbereich angegeben haben.
- Sobald die App gestartet ist, wird sie bei EdgeADC-Versionen unter 4.3 in einer neuen Browser-Registerkarte geöffnet. Bei EdgeADC Version 4.3 und höher öffnet sich die App im rechten Seitenbereich.

Voraussetzungen

Um den Edgenexus SSL Certificate Manager verwenden zu können, müssen Sie sicherstellen, dass Sie über die folgenden Voraussetzungen verfügen. Wenn Sie diese nicht haben, können Sie keine brauchbaren Zertifikate erstellen.

1. Sie müssen sicherstellen, dass Sie einen EdgeADC mit einer Lizenz installiert haben. Dabei kann es sich um eine Testlizenz oder eine gekaufte Lizenz handeln.
2. Ein VIP, das auf HTTP Port 80 des ADC für die unten aufgeführten Zwecke konfiguriert ist.
3. Sie müssen über eine öffentliche IP-Adresse verfügen, die über den HTTP-Port 80 an das VIP weitergeleitet wird. Diese Maßnahme stellt sicher, dass die Let's Encrypt-Systeme eine Verbindung herstellen und die DNS-Eigentümerschaft für das von Ihnen generierte SSL validieren können.

Virtual Services									
<input type="text" value="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. In Ihrem DNS muss ein Eintrag für den FQDN (fully qualified domain name) vorgenommen werden. Dieser Eintrag wird auf die öffentliche IP-Adresse verweisen. Diese Maßnahme stellt sicher, dass der FQDN, für den Sie das SSL-Zertifikat erstellen, in Bezug auf die IP-Adressierung gültig ist.

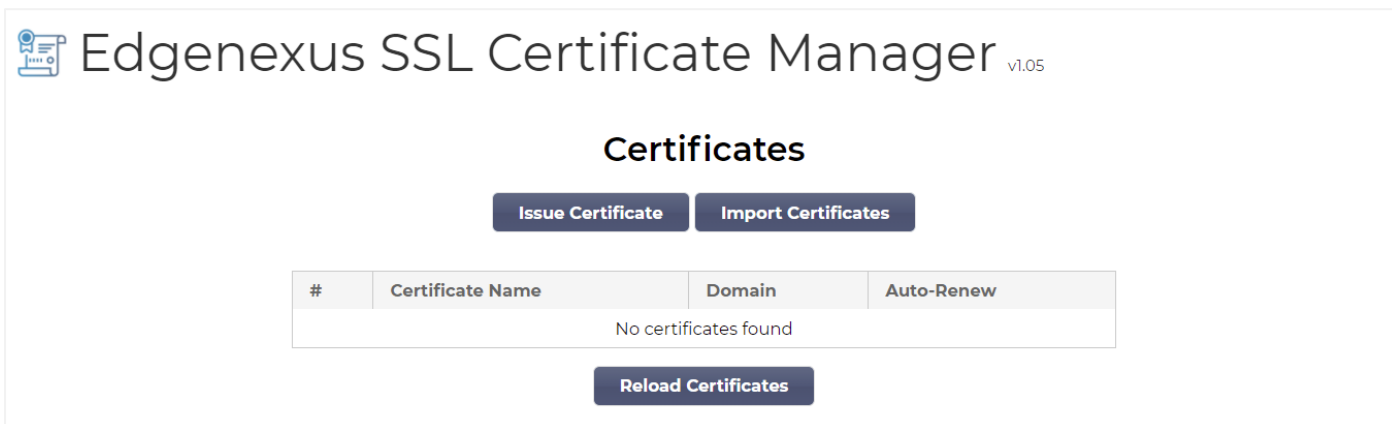
Wenn Sie dies getan haben, sind Sie startklar.

Ausstellen von Zertifikaten mit Edgenexus SSL Certificate Manager

Die Konfiguration des Edgenexus SSL Certificate Managers erfolgt über einen Assistenten und ist daher sehr einfach zu bedienen.

Wenn Sie die Benutzeroberfläche starten, sehen Sie eine Seite ähnlich der untenstehenden Abbildung. Sie sehen, dass Sie mit dem Edgenexus SSL Certificate Manager zwei Aufgaben durchführen können: Ausstellen von Zertifikaten und Importieren von Zertifikaten.

Die Funktion Zertifikate importieren wird verwendet, um von einer anderen Plattform wie F5 zu migrieren und SSL-Zertifikate in großen Mengen zu importieren.

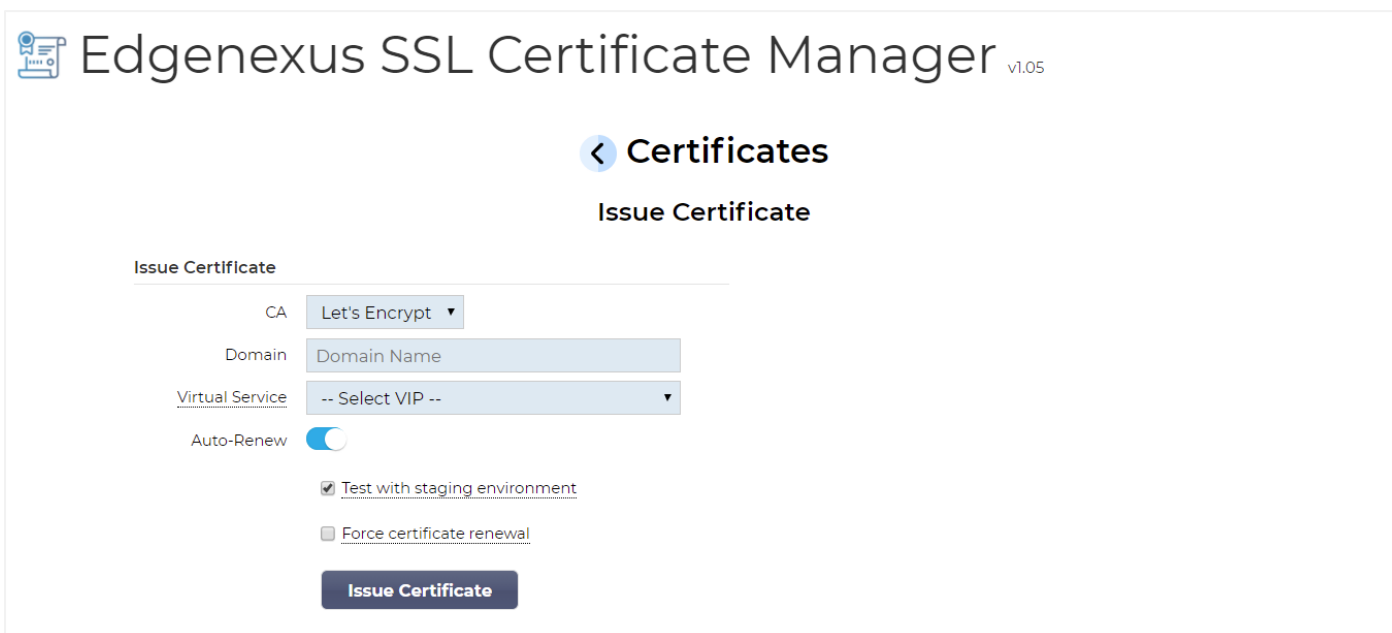


The screenshot shows the 'Certificates' page of the Edgenexus SSL Certificate Manager v1.05. At the top, there is a header with the product name and version. Below the header, the title 'Certificates' is centered. Underneath, there are two buttons: 'Issue Certificate' and 'Import Certificates'. A table with four columns is shown: '#', 'Certificate Name', 'Domain', and 'Auto-Renew'. The table is empty, with the text 'No certificates found' in the center. At the bottom, there is a 'Reload Certificates' button.

#	Certificate Name	Domain	Auto-Renew
No certificates found			

Der Edgenexus SSL Certificate Manager arbeitet mit Let's Encrypt zusammen und ermöglicht die Erstellung und Ausstellung von Let's Encrypt SSL-Zertifikaten in Echtzeit, einschließlich der automatischen Erneuerung des SSL-Zertifikats.

- Klicken Sie auf die Schaltfläche Zertifikat ausstellen, um den Ausstellungsprozess zu starten.
- Die Seite ändert sich zu der Seite, die Sie unten sehen.



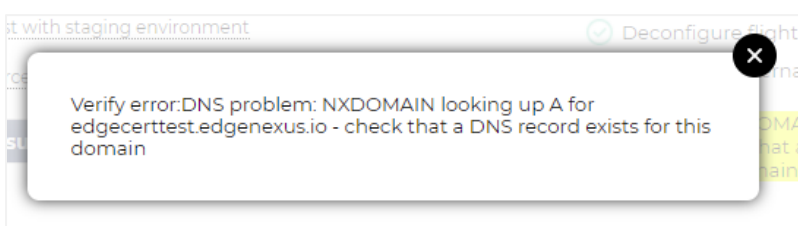
The screenshot shows the 'Issue Certificate' page of the Edgenexus SSL Certificate Manager v1.05. At the top, there is a header with the product name and version. Below the header, the title 'Certificates' is centered, followed by the subtitle 'Issue Certificate'. Underneath, there is a form with the following fields: 'CA' (dropdown menu with 'Let's Encrypt' selected), 'Domain' (text input field with 'Domain Name' placeholder), 'Virtual Service' (dropdown menu with '-- Select VIP --' selected), and 'Auto-Renew' (checkbox). There are also two checkboxes: 'Test with staging environment' (checked) and 'Force certificate renewal' (unchecked). At the bottom, there is an 'Issue Certificate' button.

- Wie Sie sehen können, müssen verschiedene Elemente konfiguriert werden, damit Sie ein SSL-Zertifikat ausstellen können.

Feld	Beschreibung
CA	Derzeit ist nur die Option Let's Encrypt verfügbar. Sobald weitere Anbieter verfügbar sind, werden wir sie hier aufnehmen.
Domain	Im Feld Domain geben Sie den FQDN an, für den das Zertifikat benötigt wird. Zum Beispiel www.acme.com oder *.acme.com im Falle eines Platzhalters. HINWEIS: Der FQDN, den Sie hier eingeben, muss per DNS-Abfrage erreichbar sein.
Virtueller Dienst	Ein virtueller Dienst muss online sein und am HTTP-Port 80 arbeiten, um eine Challenge-Anfrage des Let's Encrypt Systems zu beantworten. Dieser virtuelle Dienst muss den Anweisungen im Kapitel über die Voraussetzungen folgen.
Auto-Renew	Wenn diese Option zum Zeitpunkt der Ausstellung aktiviert ist, wird das Zertifikat auf automatische Erneuerung eingestellt.
Test mit Staging-Umgebung	Verwenden Sie den Let's Encrypt Staging-Server, um ein neues Zertifikat (zum Testen) auszustellen.
Erneuerung des Zertifikats erzwingen	Wenn Ihr Let's Encrypt-Zertifikat bereits ausgestellt und noch nicht abgelaufen ist, können Sie kein neues Zertifikat ausstellen, ohne diese Option zu aktivieren.

- Sobald Sie das Formular ausgefüllt haben, klicken Sie auf die Schaltfläche Zertifikat ausstellen, um mit der Verifizierung fortzufahren.
- Sobald Sie auf die Schaltfläche Zertifikat ausstellen klicken, beginnt der Edgenexus SSL Certificate Manager mit der Verifizierung durch Let's Encrypt oder ein anderes ACME-Zertifikatssystem, das vom Edgenexus SSL Certificate Manager unterstützt wird.
- Wenn der Vorgang abgeschlossen ist, sehen Sie einen Bildschirm ähnlich dem unten abgebildeten.


- Der Edgenexus SSL Certificate Manager speichert das von Ihnen erstellte SSL-Zertifikat im SSL-Speicher des EdgeADC, wenn der Vorgang erfolgreich war.
- Der Edgenexus SSL Certificate Manager zeigt die folgende Fehlermeldung an, wenn ein Problem auftritt.



Edgenexus SSL Certificate Manager

Benutzerhandbuch

Die von Ihnen ausgestellten Zertifikate werden auf der Startseite der App aufgelistet.

 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	<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"/>

[Reload Certificates](#)

FlightPATH und wie es verwendet wird

Im Rahmen der Zertifikatserstellung muss Let's Encrypt den von Ihnen angegebenen Domännennamen mit einer Sicherheitsabfrage validieren.

Der Edgenexus SSL Certificate Manager macht dies mit flightPATH, d.h. Sie können SSL-Zertifikate nach Bedarf erstellen, ohne dies auf den eigentlichen Servern zu tun.

Wenn Sie auf die Schaltfläche Zertifikat ausstellen klicken, erstellt der EdgeADC eine flightPATH-Regel, die die Abfrage von der zertifikatsausstellenden Behörde, Let's Encrypt oder einem unterstützten ACME-System abfängt.

Die flightPATH-Regel initiiert dann eine Umleitung der Anfrage an den Edgenexus SSL Certificate Manager und nicht an den eigentlichen Server, für den sie bestimmt ist. Der Edgenexus SSL Certificate Manager bestätigt dann die Challenge-Anfrage und validiert sie für die Ausstellung des Zertifikats.

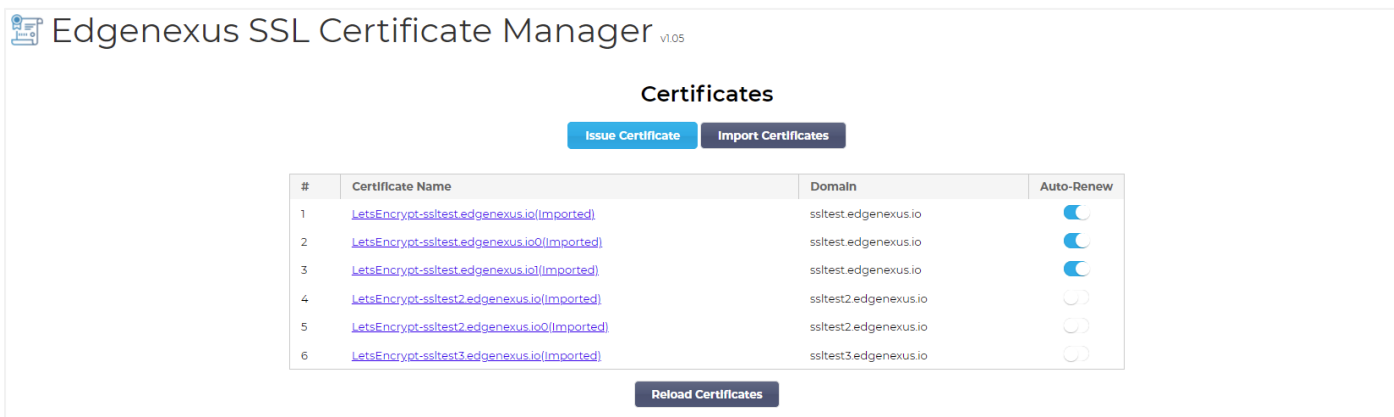
Alles wird automatisch vom EdgeADC selbst erledigt, ohne dass der Administrator eingreifen muss.

Massenimport von Zertifikaten

Eine der Anforderungen bestimmter Kunden ist der Bedarf, Zertifikate in großen Mengen zu importieren. Die Notwendigkeit, Zertifikate in großen Mengen zu importieren, könnte darin bestehen, dass sie viele Zertifikate haben oder von anderen Load Balancern wie F5 migrieren möchten.

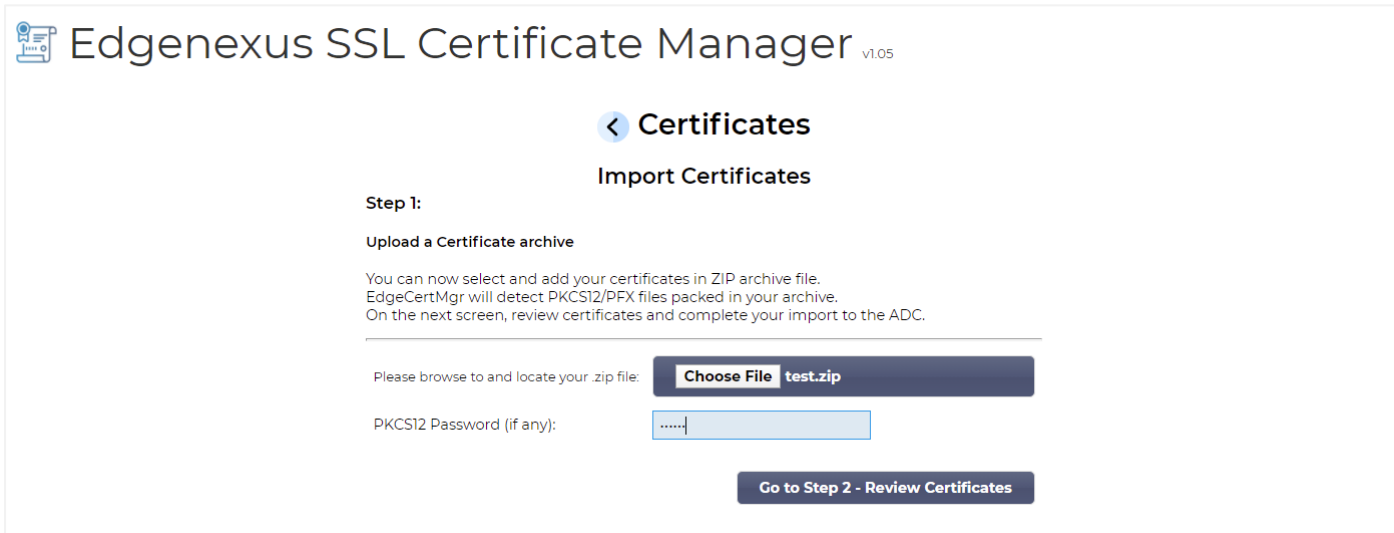
Der Edgenexus SSL Certificate Manager kann PFX-Zertifikate mit Hilfe einer Zip-Datei in großen Mengen importieren. Voraussetzung dafür ist, dass das Passwort für die PFX für alle Zertifikate gleich ist. Ein gemeinsames Passwort ist normalerweise der Fall, wenn Sie einen Massenexport vom Load Balancer eines anderen Anbieters durchführen.

- Um SSL-Zertifikate in großen Mengen zu importieren, klicken Sie auf die Schaltfläche **Zertifikate importieren** auf der Seite der App.



#	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"/>

- Im nächsten Schritt wählen Sie die ZIP-Datei aus, die Sie entweder manuell oder über einen Bulk-Export erstellt haben.



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

- Geben Sie das PFX-Passwort ein.
- Klicken Sie auf die Schaltfläche **Gehe zu Schritt 2 - Zertifikate prüfen**.
- Auf der nächsten Seite können Sie überprüfen, welche Zertifikate Sie importieren möchten.

 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.

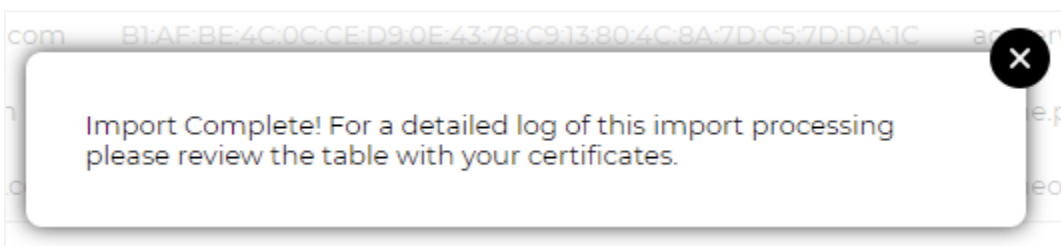
Import Certificates

#	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: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

- Wenn alles korrekt ist, können Sie auf die Schaltfläche Zertifikate importieren klicken.
- Sie sollten eine Bestätigungsmeldung sehen, wenn der Import erfolgreich war.



- Wenn Sie dieses Popup-Fenster schließen, erscheint der unten abgebildete Bildschirm, der anzeigt, dass der Import erfolgreich war.

 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: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

Sie können die importierten SSL-Zertifikate mit Bibliothek > SSL-Zertifikate überprüfen.