



软件版本
1.0.0

Edgenexus SSL Certificate Manager

AN EDGENEXUS EDGEADC APP

文件属性

文件编号：2.0.9.13.21.14.09

文件创建日期。2021年8月5日

文件最后编辑。13 September 2021

文件作者。杰伊-萨沃尔

文件最后编辑者。

文件免责声明

由于产品发布的差异，本手册的屏幕截图和图形可能与您的产品略有不同。Edgenexus公司确保他们作出一切合理的努力，以确保本文件中的信息是完整和准确的。Edgenexus公司对任何错误不承担任何责任。

Edgenexus公司会在未来的版本中，在需要时对本文件中的信息进行修改和更正。

版权

© 2021保留所有权利。

本文件中的信息如有变化，恕不另行通知，也不代表制造商的承诺。未经制造商明确的书面许可，本指南的任何部分都不得以任何形式或手段、电子或机械，包括影印和录音，为任何目的进行复制或传播。注册商标是其各自所有者的财产。我们尽一切努力使本指南尽可能地完整和准确，但并不意味着保证其适用性。作者和出版商对任何个人或实体因使用本指南中的信息而产生的损失或损害不承担任何责任。

商标

Edgenexus标志、Edgenexus、EdgeADC、EdgeWAF、EdgeGSLB、EdgeDNS都是Edgenexus有限公司的商标。所有其他商标都是其各自所有者的财产，并得到承认。

埃德纳克斯支持

如果你有关于本产品的任何技术问题，请提出支持票：support@edgenexus.io

目录

| | |
|------------------------------------|----|
| 文件属性 | 1 |
| 文件免责声明 | 1 |
| 版权 | 1 |
| 商标 | 1 |
| 埃德纳克斯支持 | 1 |
| 什么是Edgenexus SSL证书管理器？ | 3 |
| 获取并安装Edgenexus SSL证书管理器？ | 4 |
| 使用EdgeADC下载和导入应用程序 | 6 |
| 使用直接下载的方式下载并导入App | 7 |
| 让应用程序在EdgeADC v4.2.x及以下版本中运行 | 8 |
| 使应用程序在EdgeADC v4.3.x及以上版本中运行 | 9 |
| 先决条件 | 12 |
| 使用Edgenexus SSL证书管理器颁发证书 | 13 |
| FlightPATH和它的使用方法 | 15 |
| 批量导入证书 | 16 |

什么是Edgenexus SSL证书管理器？

所有使用服务器交付应用程序的组织都需要安装**SSL**证书，以确保安全。

为了适应这一要求，IT经理们对内部的、与域相连的服务器使用域证书，而当服务器承载基于网络的私人或公共访问解决方案时，则与**SSL**供应商联系以获得全球信任的证书。

从权威机构获得证书的过程可能很费时，而且有一定的成本。

为了缓解这种情况，Edgenexus公司推出了Edgenexus SSL证书管理器，它允许IT管理员使用Let's Encrypt服务技术生成所需的证书。

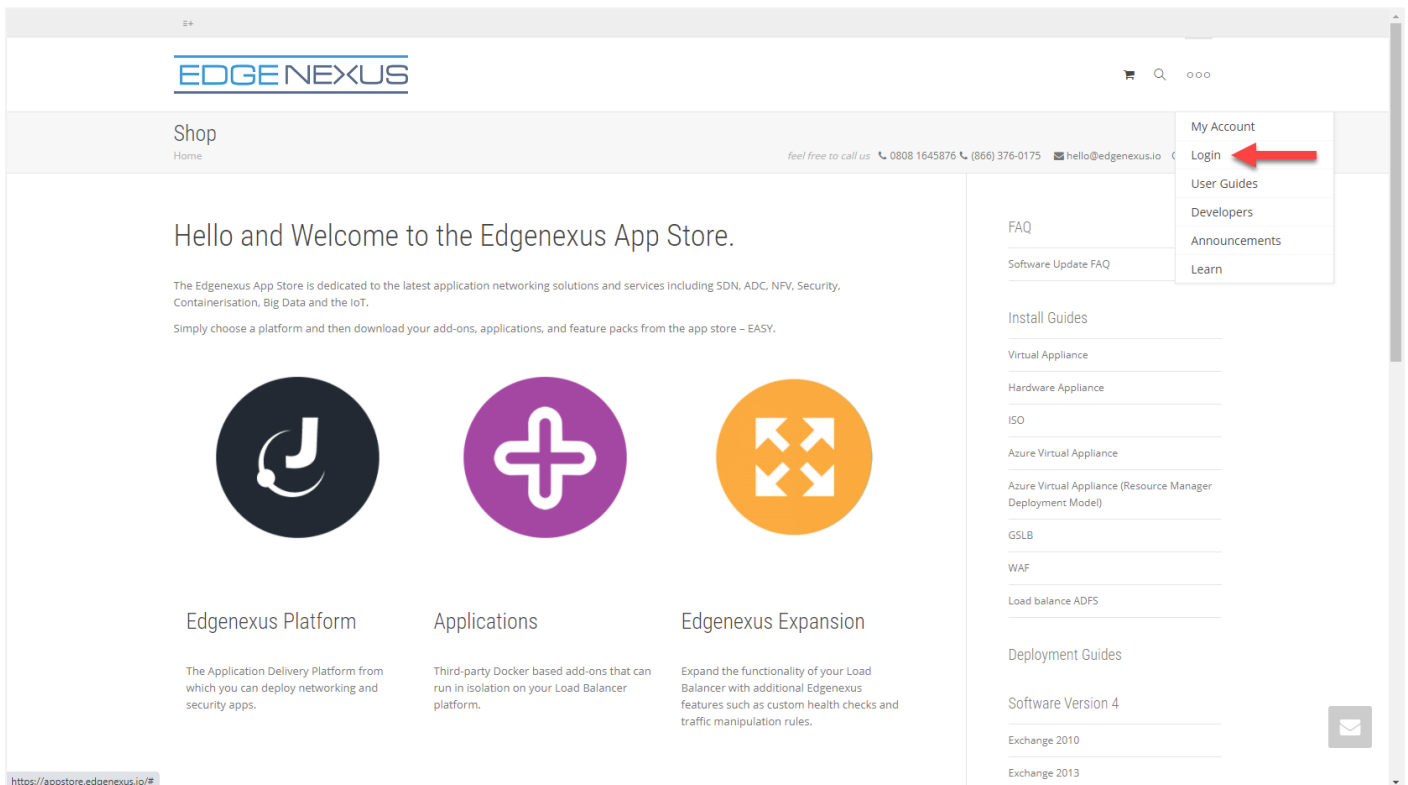
使用Edgenexus SSL证书管理器的过程简单而容易。

获取并安装Edgenexus SSL证书管理器？

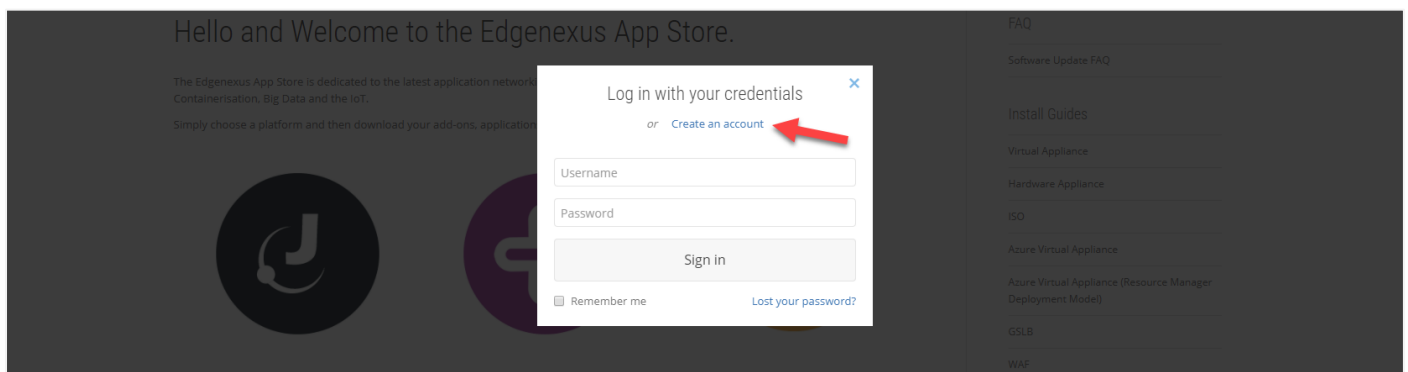
获得Edgenexus SSL证书管理器是非常容易的。

与每一个Edgenexus应用程序一样，Edgenexus SSL证书管理器可以通过应用程序商店获得，并且可以免费下载，有些甚至可以免费使用。

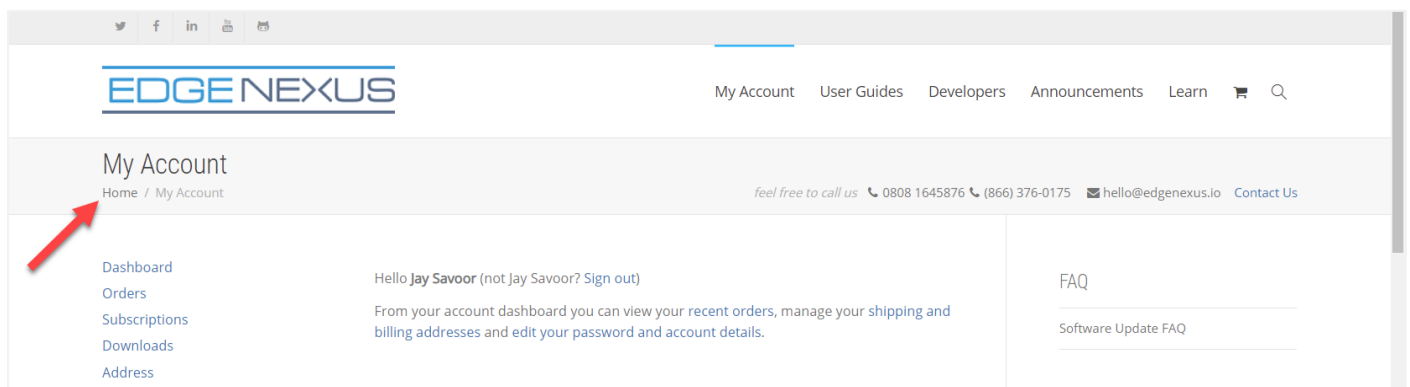
- 首先要做的是注册访问Edgenexus应用程序商店。这一过程是通过使用浏览器和导航到<https://appstore.edgenexus.io>。



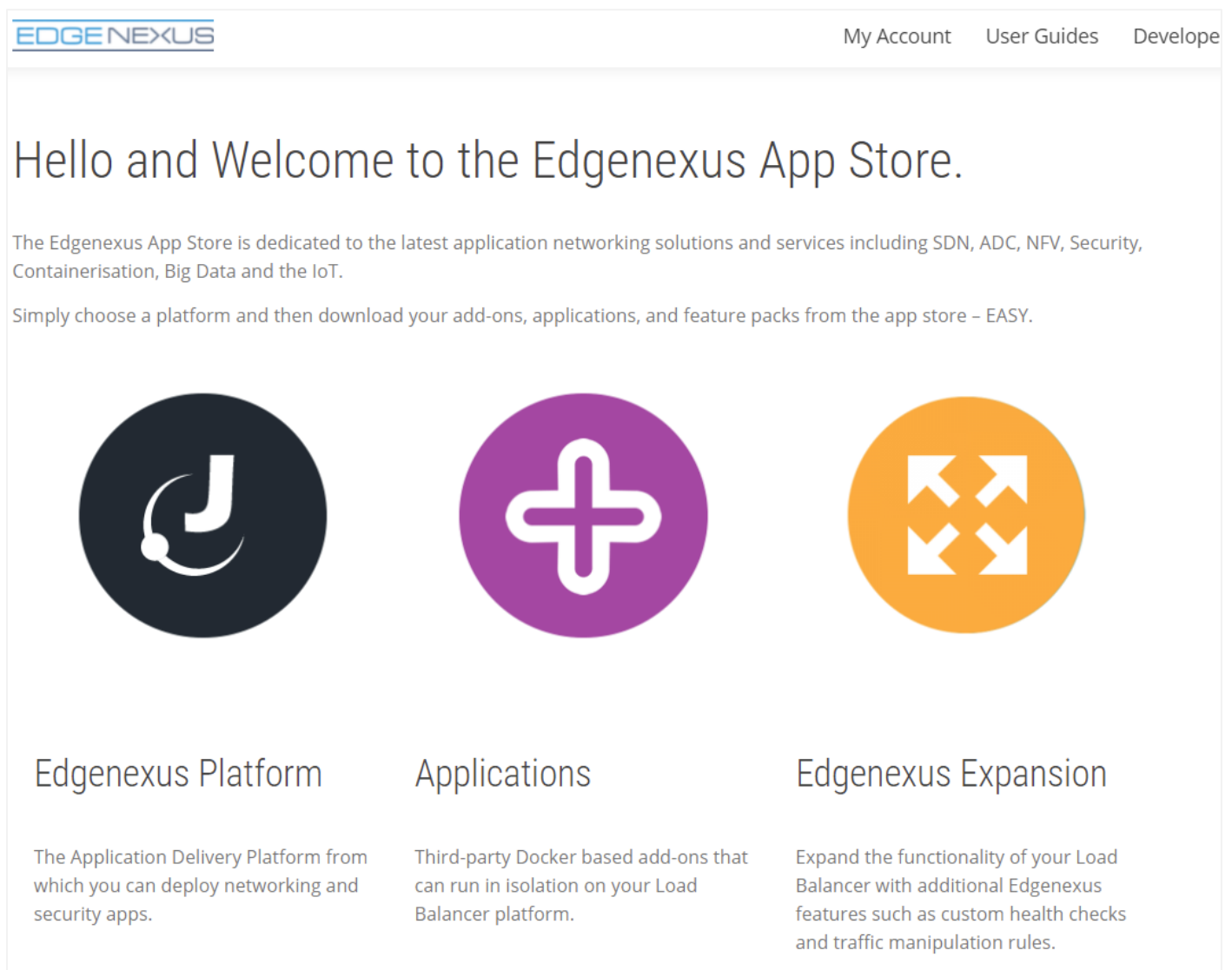
- 点击位于右上方汉堡包图标中的登录链接。
- 点击 "创建账户"，或使用您的账户凭证登录。



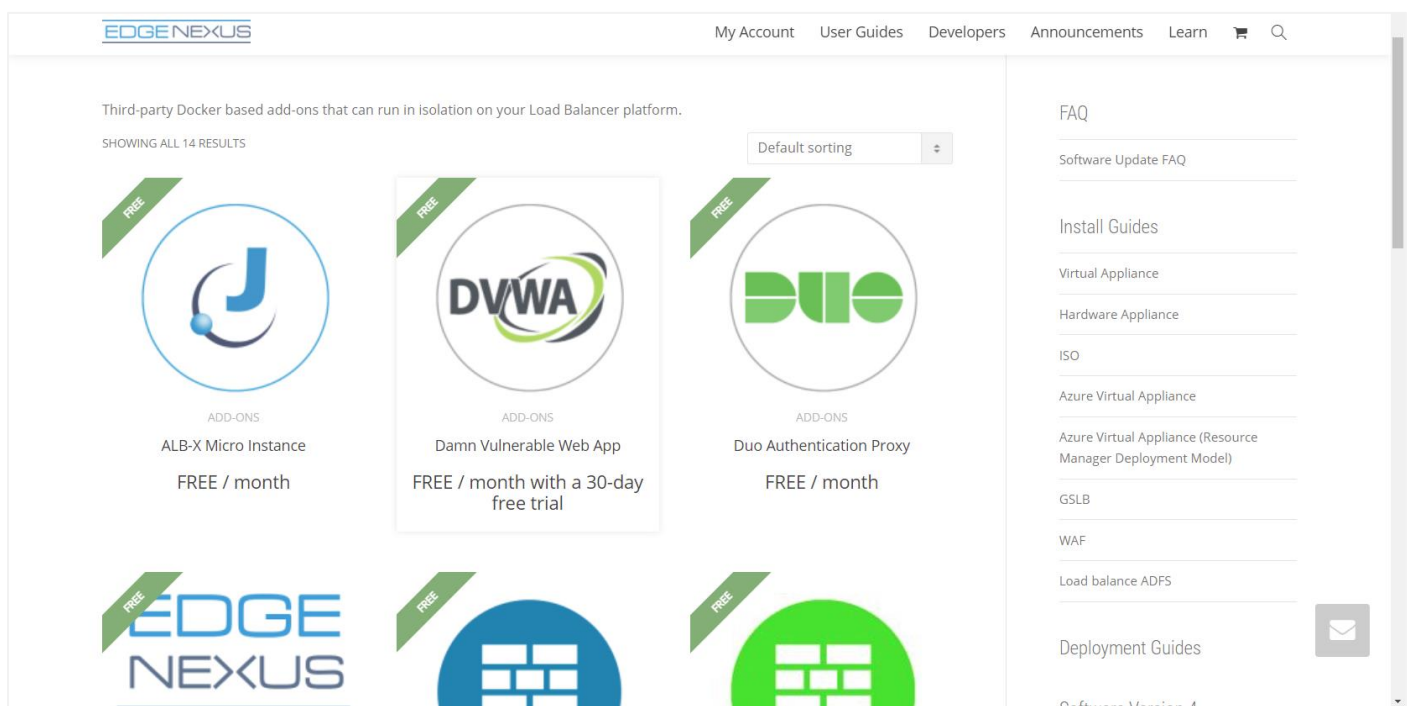
- 一旦你登录，请点击位于标志下的主页链接。



- 接下来，点击 "应用程序"。



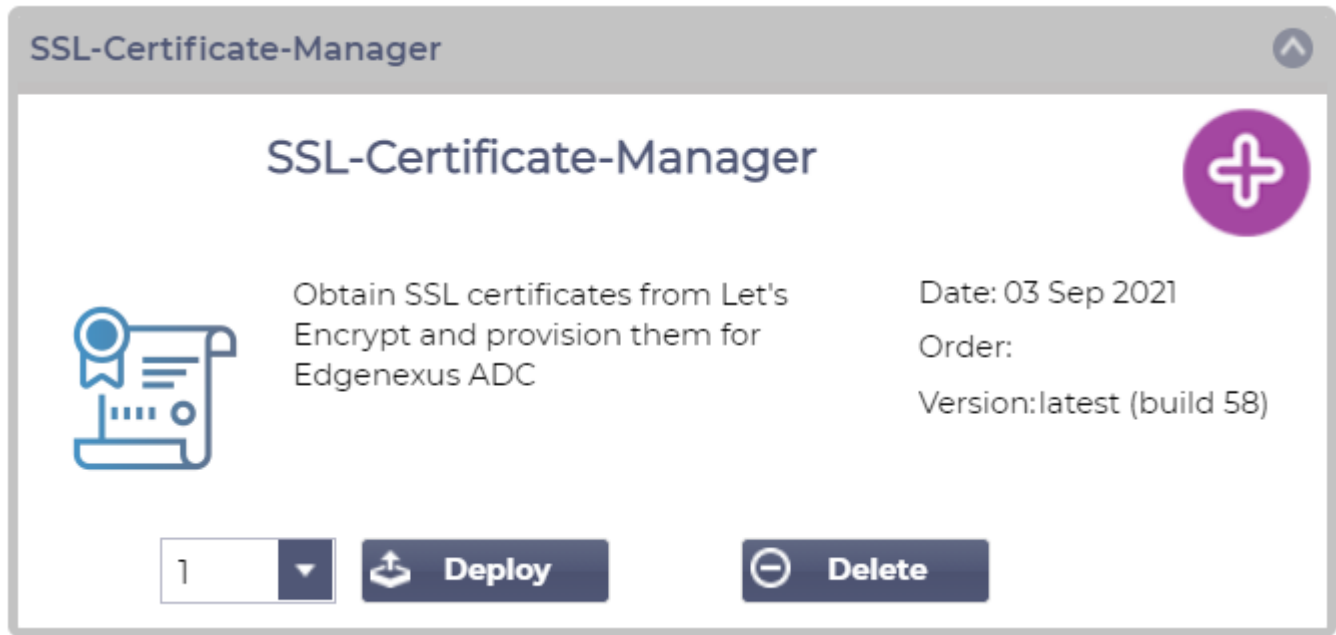
- 这个动作将带你到应用程序页面，在那里你将能够下载Edgenexus SSL证书管理器。



- 在应用程序页面内，你可以浏览和订购应用程序。
- Edgenexus SSL证书管理器应用程序是免费的，但你仍然需要遵循购买的途径。
- 在这一点上，您有两个选择。从EdgeADC内部使用App Store，或者直接从App Store下载App，然后上传到EdgeADC。

使用EdgeADC下载和导入应用程序

- 第一个选择是在EdgeADC内部使用您的App Store凭证登录。使用 "服务">"应用程序商店"可以获得集成的应用程序商店界面。
- 这种方法将允许你进行购买，然后你会发现它在位于图书馆>应用程序中的已购买的应用程序部分可用。
- Edgenexus的SSL证书管理器应用程序看起来就像下图所示。



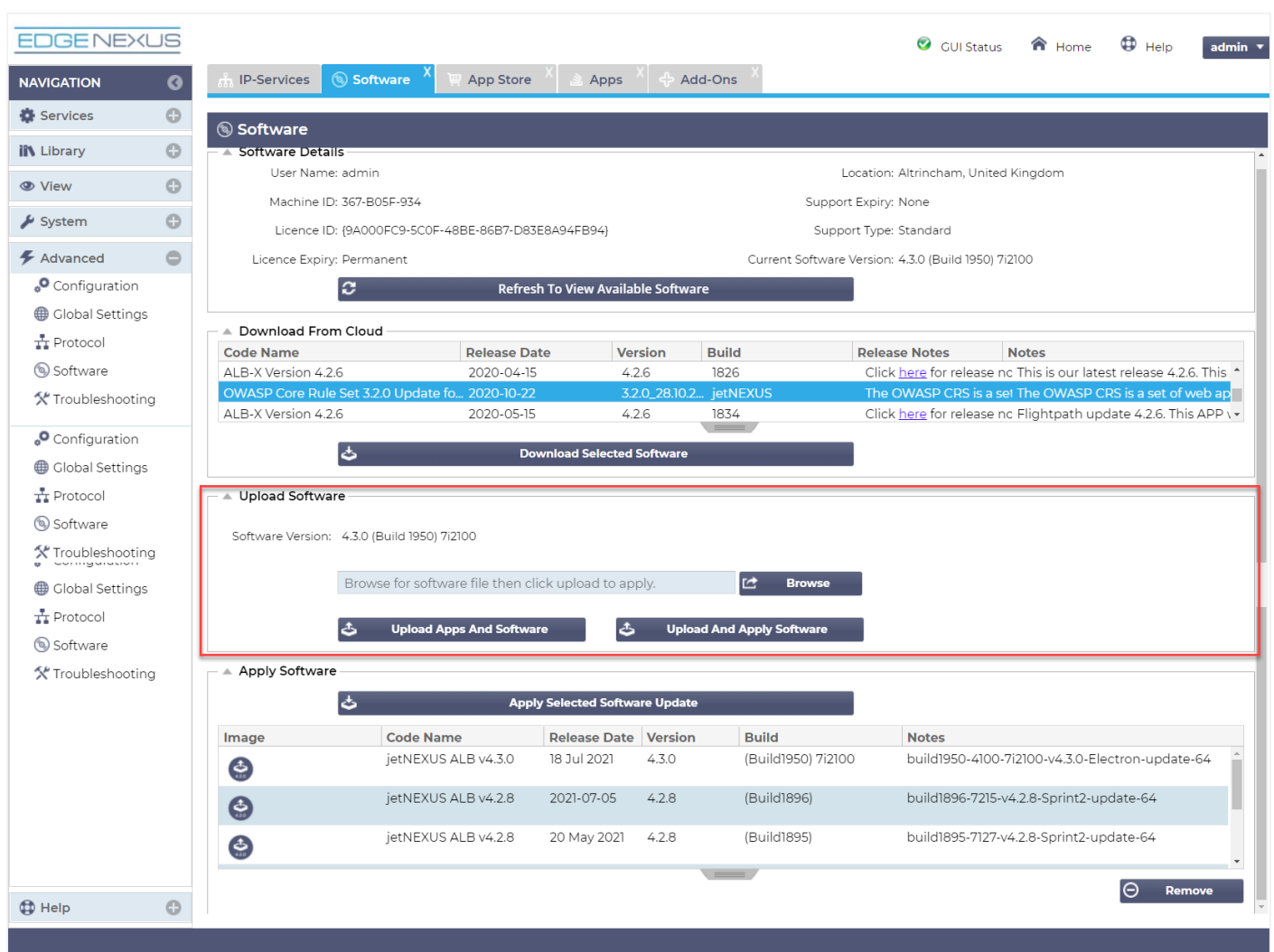
- 你可以选择下载该应用程序，然后它就会出现在已下载的应用程序部分。
- 从图书馆>应用程序>下载的应用程序部分，找到Dell-ECS负载平衡应用程序，然后通过单击部署按钮将其部署到EdgeADC容器。
- 如果你希望部署一个以上的副本，你可以使用下拉菜单选择应用程序的副本数量。
- 一旦部署，它将在图书馆>附加组件标签中可用。

使用直接下载的方式下载并导入App

- 第二种方法是使用你的App Store登录，用浏览器直接下载到你的桌面。
- 一旦下载，请确保在不改变文件名的情况下保存它。
- 也请确保文件名中没有(1)或类似的东西，可能表明是第二次下载等。
- 下载文件后，用浏览器导航到EdgeADC GUI的高级>软件。

Edgenexus SSL Certificate Manager

用户指南



- 在软件页面内有几个部分，但我们需要上传软件部分。
- 首先，点击浏览按钮，找到您下载的Dell ECS负载均衡应用程序。
- 接下来，点击上传应用程序和软件按钮。
- 该应用程序将显示在图书馆>应用程序的已下载应用程序部分。
- 从图书馆>应用程序>下载的应用程序部分，找到Dell-ECS负载均衡应用程序，然后通过点击部署按钮将其部署到EdgeADC。
- 如果你希望部署一个以上的副本，你可以使用下拉菜单选择应用程序的副本数量。
- 一旦部署，它将在图书馆>附加组件标签中可用。

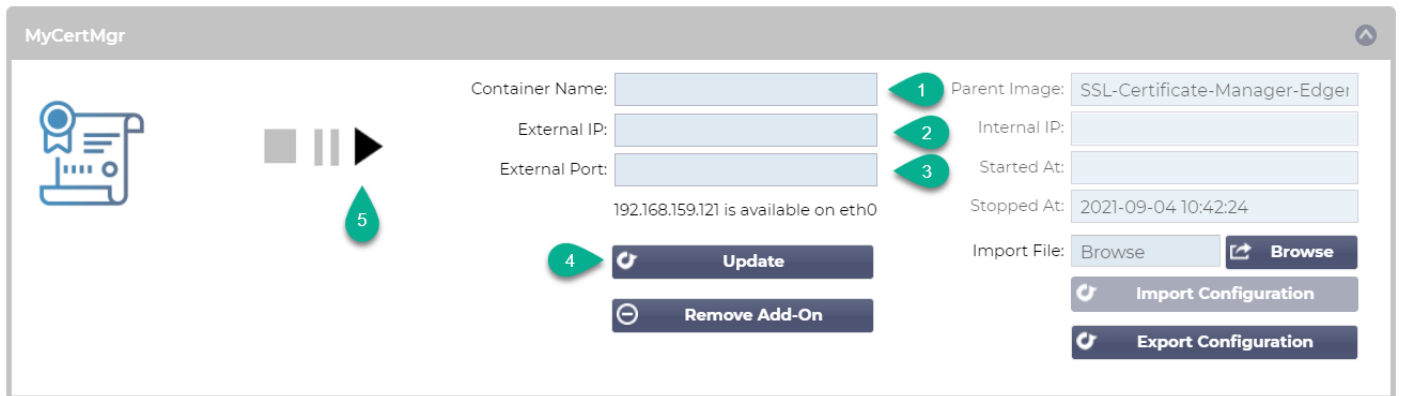
使应用程序在EdgeADC v4.2.x及以下版本中运行

当一个应用程序被下载和部署后，它还需要被操作。它必须与EdgeADC相同的子网中获得一个IP地址，并且需要通过该端口进行访问。

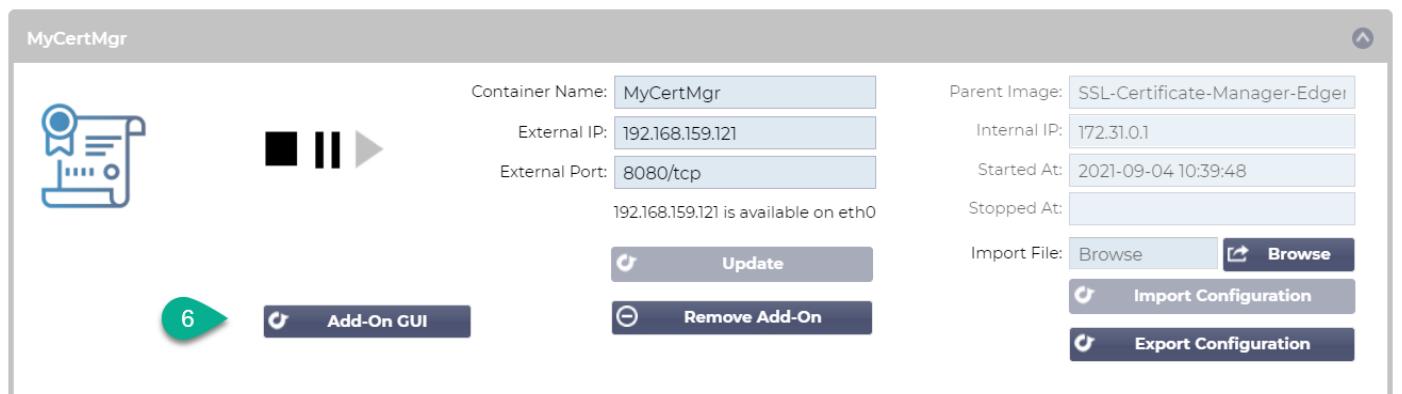
- 导航至图书馆>插件，找到Edgenexus SSL证书管理器应用程序。
- 它应该看起来像下面的图片。

Edgenexus SSL Certificate Manager

用户指南



- 给Add-On一个名字 ❶- EdgeADC的内部DNS系统在使用这个名字来参考App。
- 添加一个适当的静态 IP 地址 ❷。这个条目对于EdgeADC v4.3.x及以上版本是可选的，但对于任何低于4.3.x的版本是必须的。
- 使用8080/tcp的端口地址值，为端口输入一个值。
- 一旦你完成了这些，点击更新按钮 ❹来初始化该应用程序。
- 点击 ❺ 上面的PLAY图标，激活应用程序进入运行状态。
- 一旦运行，它将看起来像下面的图片，并作为一个嵌入式应用程序列在服务部分。



- 注意启动App GUI的Add-On GUI ❹按钮，以及暂停App和停止App按钮。
- 一旦启动该应用程序，它将在一个新的浏览器标签中打开。

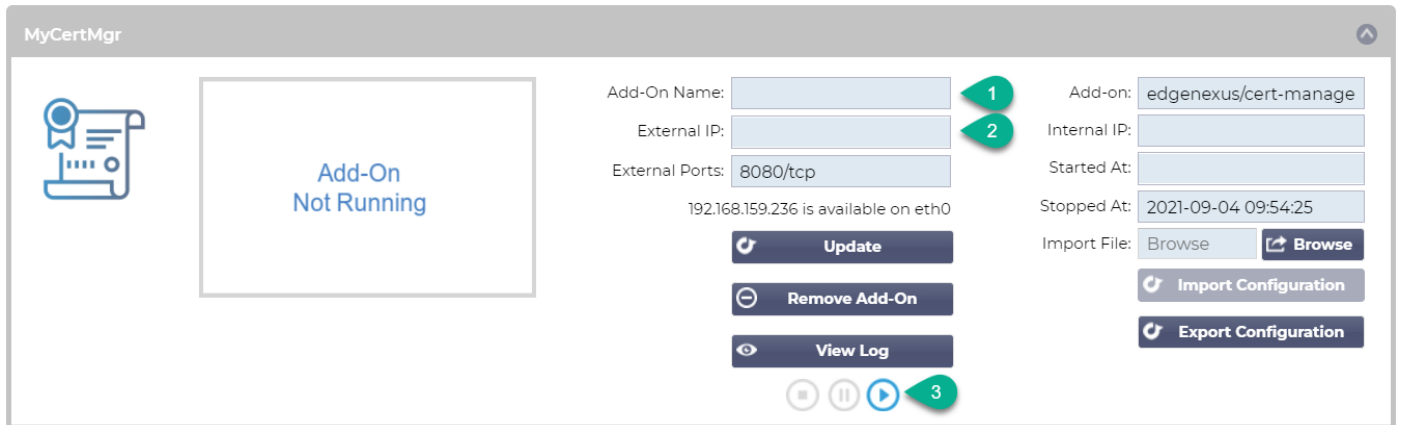
使应用程序在EdgeADC v4.3.x及以上版本中运行

当一个应用程序被下载和部署后，它还需要被操作。它必须与EdgeADC相同的子网中获得一个IP地址，并且需要通过该端口进行访问。

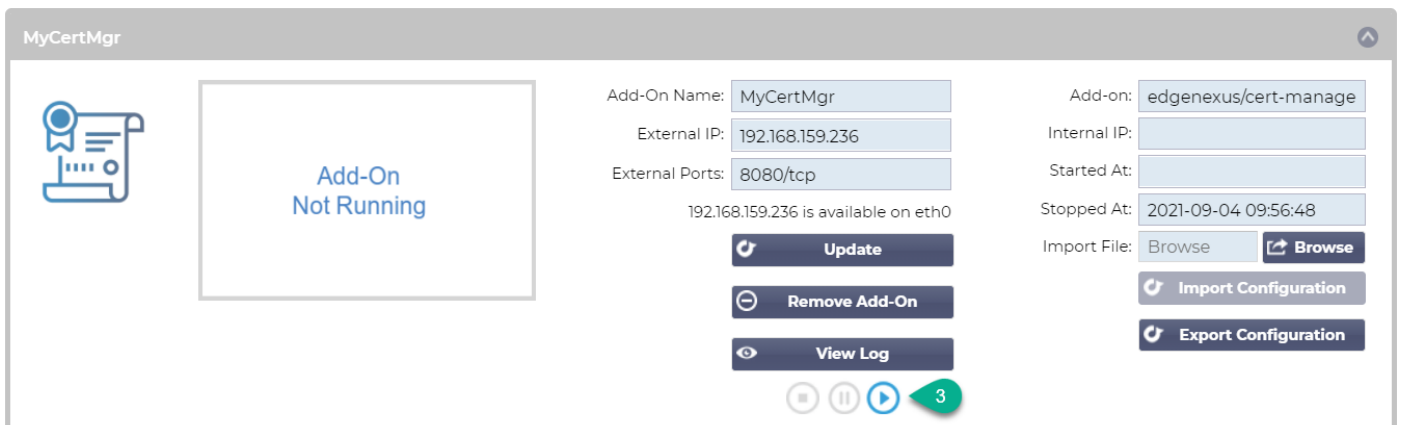
- 导航到图书馆>插件，找到Dell-ECS负载平衡应用程序。
- 它应该看起来像下面的图片。

Edgenexus SSL Certificate Manager

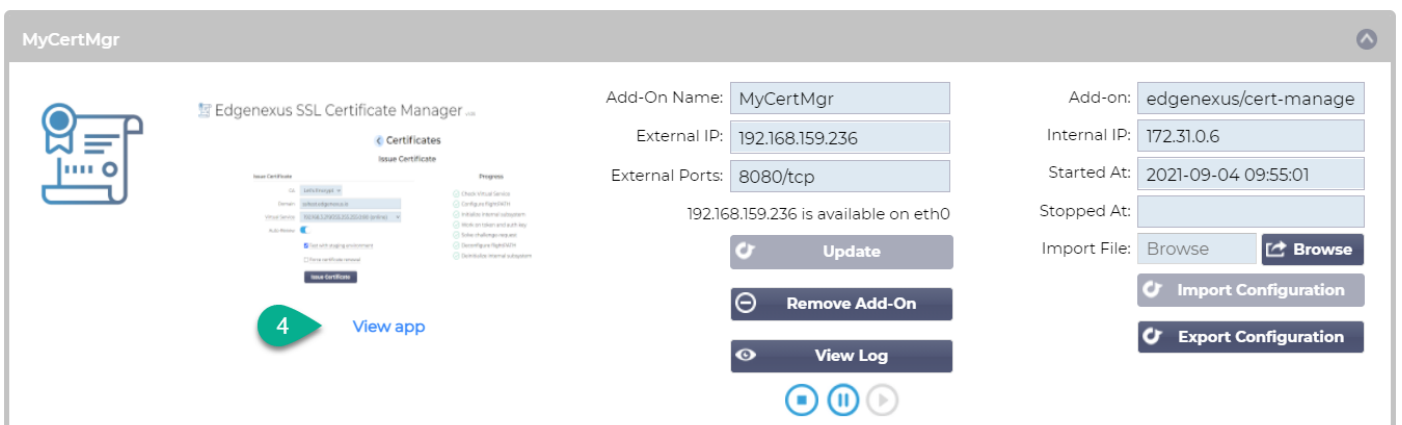
用户指南



- 给Add-On一个名字 ①- EdgeADC的内部DNS系统在需要时使用这个名字来参考App。
- 添加一个适当的静态 IP 地址②。这个条目对于EdgeADC v4.3.x及以上版本是可选的，但对于任何低于4.3.x的版本是必须的。
- 如果你有EdgeADC v4.3.x及以上版本，你不需要输入端口的值，因为已经提供了这个值。对于EdgeADC的早期版本（4.2.x及以下），你需要提供一个8080/tcp的端口地址值。
- 一旦你完成了这些，点击更新按钮来初始化该应用程序。
- 它应该看起来像下面这样。



- 点击③上面的PLAY图标，激活应用程序进入运行状态。
- 一旦运行，它将看起来像下面的图片，并作为一个嵌入式应用程序列在服务部分。



- 注意查看应用程序④按钮，以启动应用程序图形用户界面，以及暂停应用程序和停止应用程序按钮。
- 在EdgeADC 4.3及以上版本，您也可以通过点击您在导航面板内的服务部分提供的应用程序名称来启动。
- 一旦应用程序被启动，对于EdgeADC 4.3以下的版本，它将在一个新的浏览器标签中打开。在EdgeADC 4.3及以上版本中，App将在右侧面板上打开。

先决条件

要使用Edgenexus SSL证书管理器，你必须确保你有以下先决条件。如果不具备这些条件，将导致无法生成可使用的证书。

1. 你需要确保你有一个安装了许可证的EdgeADC。许可证可以是评估版的，也可以是已经购买的。
2. 一个配置在HTTP端口80上的VIP是ADC的目的，如下所示。
3. 你必须有一个可用的公共IP地址，使用HTTP端口80重定向到VIP。这项措施确保Let's Encrypt系统可以连接并验证你将生成的SSL的DNS所有权。

| 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 | | | <input checked="" type="checkbox"/> | 192.168.159.110 | 255.255.255.0 | 80 | | HTTP | |

4. 必须在你的DNS中为FQDN（完全合格的域名）建立一个条目。该条目将指向公共IP地址。这项措施确保你生成SSL证书的FQDN在IP地址方面是有效的。

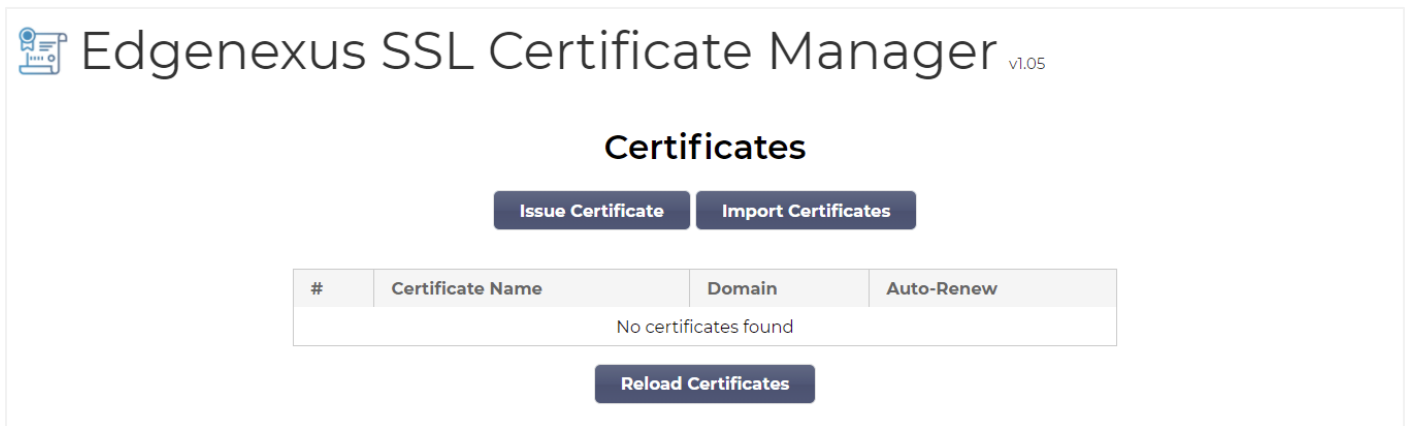
一旦你完成了这些，你就可以开始了。

使用Edgenexus SSL证书管理器颁发证书

Edgenexus SSL证书管理器的配置是通过一个基于向导的系统进行的，因此非常容易使用。

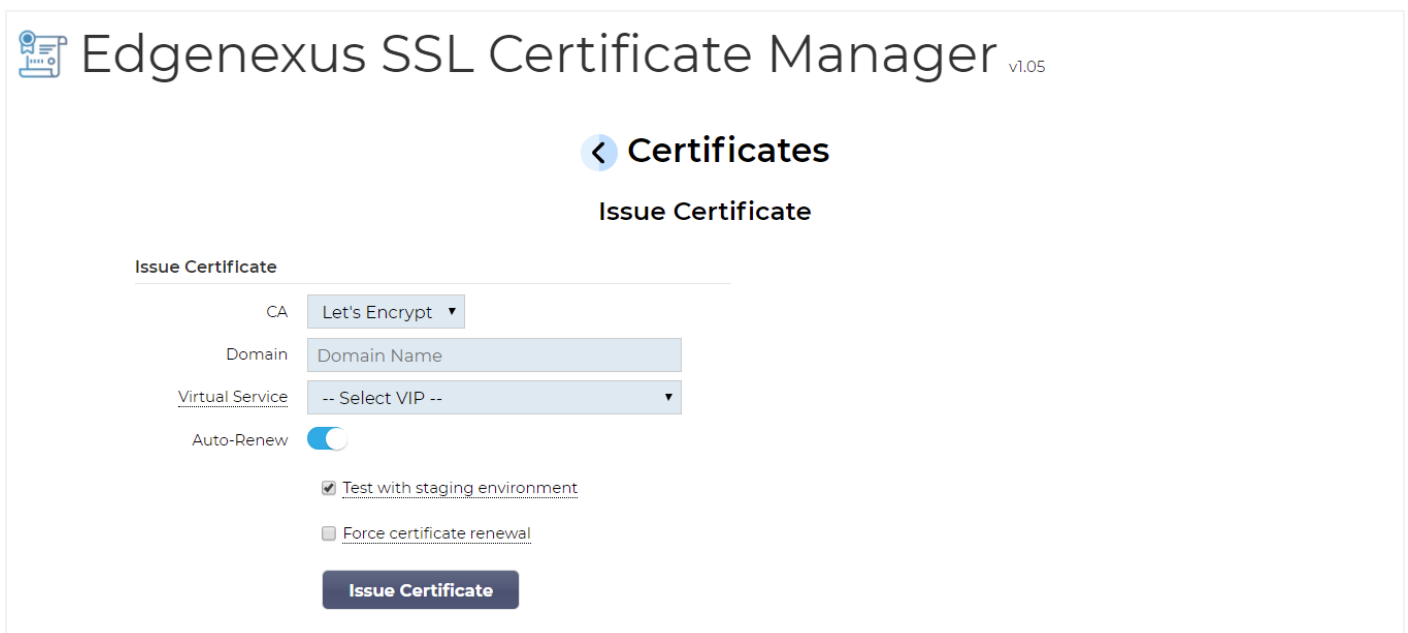
当你启动用户界面时，你会看到一个类似于下图的页面。你可以看到，你可以使用Edgenexus SSL证书管理器执行两项任务。发布证书和导入证书。

导入证书功能用于从其他平台（如F5）迁移并批量导入SSL证书。



Edgenexus SSL证书管理器与Let's Encrypt一起工作，允许实时生成和颁发Let's Encrypt SSL证书，包括自动更新SSL证书。

- 点击 "签发证书" 按钮，开始签发过程。
- 页面将变为你所看到的下图。



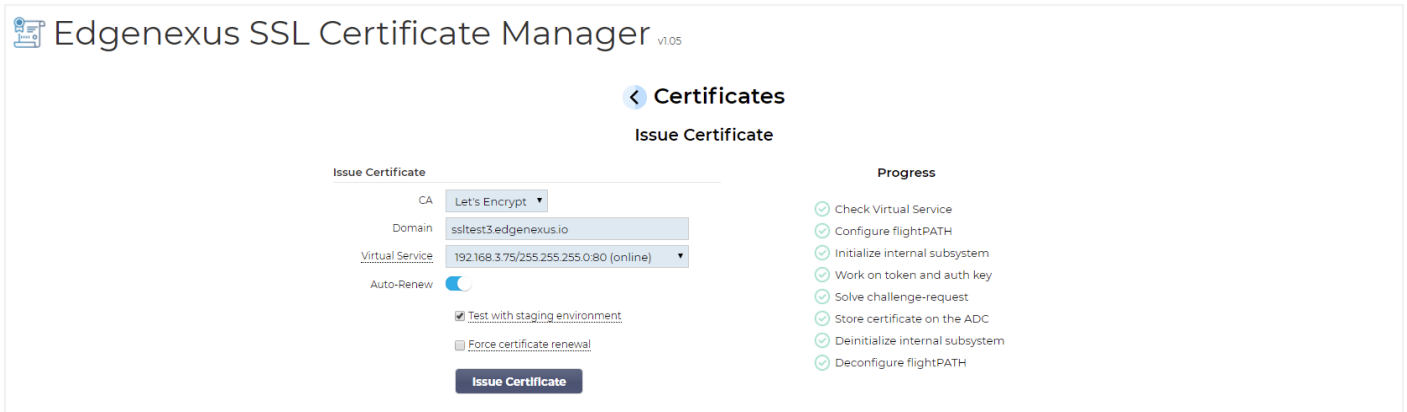
- 正如你所看到的，各种项目都需要配置，以便你可以颁发SSL证书。

Edgenexus SSL Certificate Manager

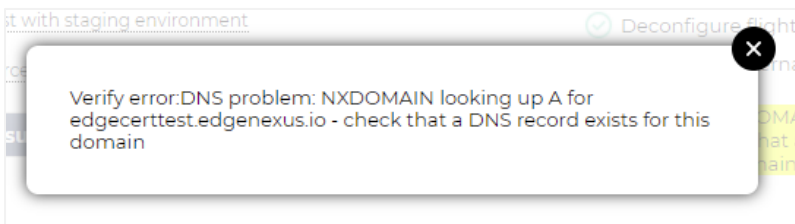
用户指南

| 场地 | 描述 |
|-----------|--|
| CA | 目前，只有Let's Encrypt选项可用。将来，随着更多供应商的出现，我们将把它们纳入这里。 |
| 领域 | 域名字段用于指定需要使用证书的FQDN。例如， www.acme.com ，如果是通配符，则为*.acme.com。 注意：你放在这里的FQDN必须是可以通过DNS查询到达的。 |
| 虚拟服务 | 一个虚拟服务必须在线并在 HTTP 80 端口工作，以回答Let's Encrypt系统的挑战请求。这个虚拟服务必须遵循先决条件一章中提供的指导。 |
| 自动更新 | 如果在签发时启用，证书将被设置为自动更新。 |
| 用暂存环境进行测试 | 使用Let's Encrypt暂存服务器签发一个新的证书（用于测试）。 |
| 强制更新证书 | 如果你的Let's Encrypt证书已经签发并且没有过期，不启用这个选项，你就无法签发新的证书。 |

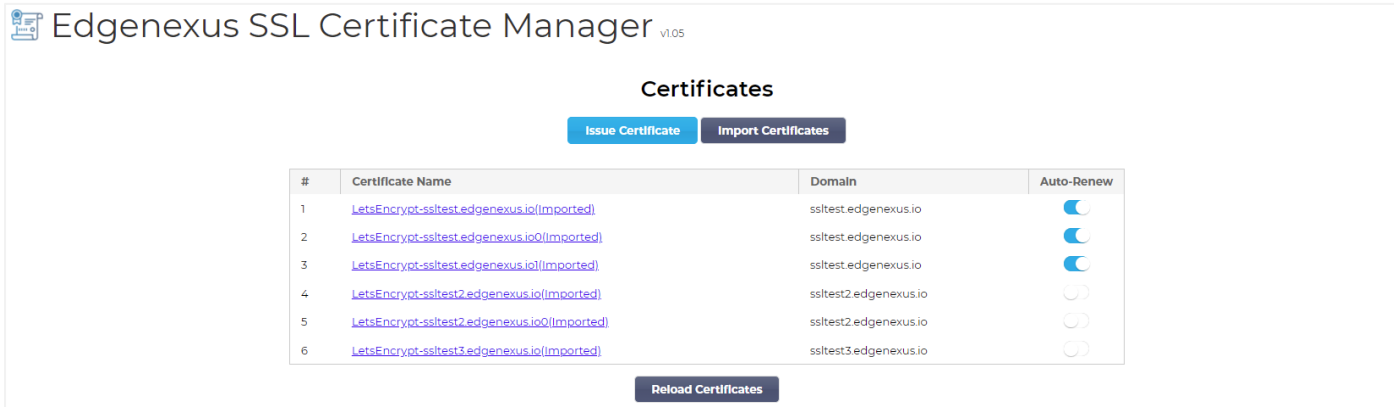
- 一旦你完成了表格，点击 "签发证书" 按钮，进入验证阶段。
- 一旦你点击签发证书按钮，Edgenexus SSL证书管理器就开始与Let's Encrypt或Edgenexus SSL证书管理器支持的其他ACME证书系统进行验证。
- 当这个过程结束时，你会看到一个与下面类似的屏幕。



- 如果过程成功，Edgenexus SSL证书管理器将把你创建的SSL证书存储在EdgeADC的SSL存储中。
- 如果进程遇到任何问题，Edgenexus SSL证书管理器将显示以下错误。



你所签发的证书将列在应用程序的启动页上。



FlightPATH和它的使用方法

作为证书创建过程的一部分，Let's Encrypt需要使用挑战请求来验证您提供的域名。

Edgenexus SSL证书管理器通过使用flightPATH来做到这一点，这意味着你可以根据需要创建SSL证书，而无需在实际的服务器上这样做。

当你点击签发证书按钮时，EdgeADC创建一个flightPATH规则，拦截来自证书签发机构、Let's Encrypt或任何支持的ACME系统的挑战请求。

然后flightPATH规则启动一个请求重定向到Edgenexus SSL证书管理器，而不是它要使用的真正的服务器。然后Edgenexus SSL证书管理器确认挑战请求并验证它以颁发证书。

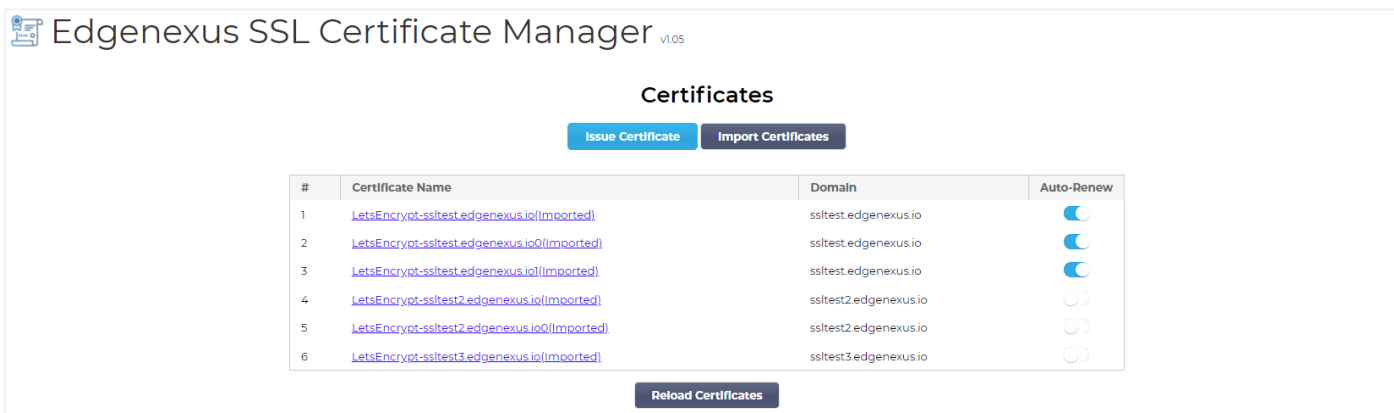
一切都在EdgeADC内部自动完成，不需要管理员的任何干预。

批量导入证书

特定客户的要求之一是需要批量导入证书。需要批量导入证书的原因可能是他们有很多证书，或者想从其他负载均衡器（如F5）迁移过来。

Edgenexus SSL证书管理器可以使用一个压缩文件批量导入PFX证书。这里的限制条件是，所有证书的PFX密码必须是相同的。通常情况下，当你从另一个供应商的负载均衡器进行批量导出时，会有一个共同的密码。

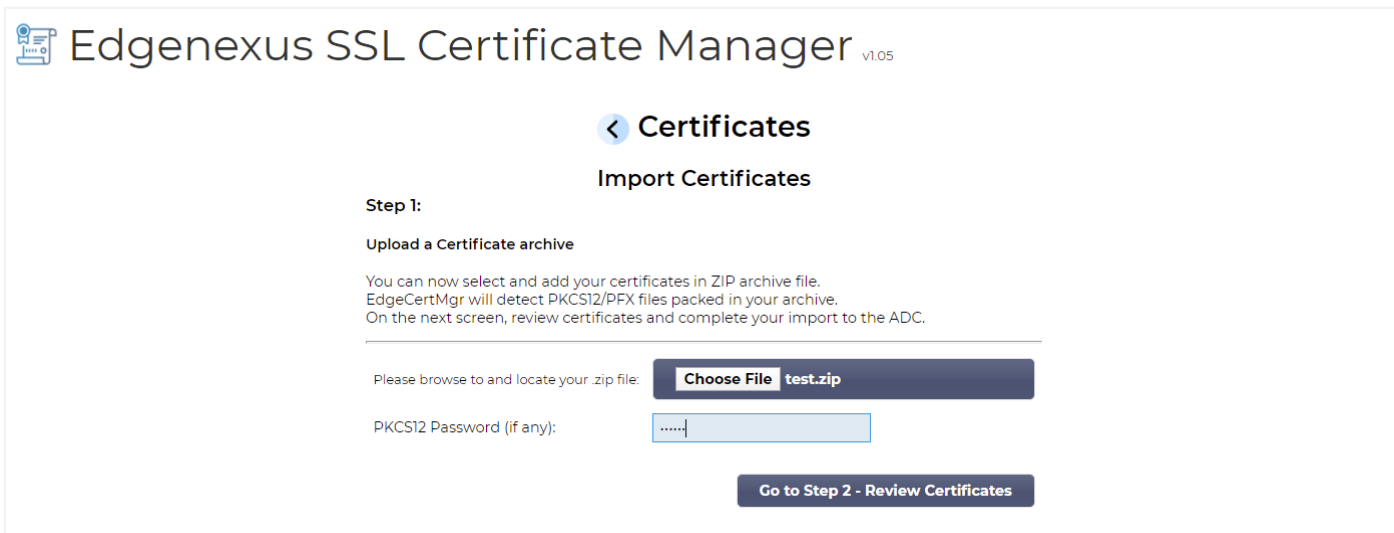
- 要批量导入SSL证书，请点击应用程序页面上的导入证书按钮。



The screenshot shows the 'Certificates' section of the Edgenexus SSL Certificate Manager. It features two buttons: 'Issue Certificate' and 'Import Certificates'. Below these is a table with the following columns: '#', 'Certificate Name', 'Domain', and 'Auto-Renew'. The table lists six certificates, all with names starting with 'LetsEncrypt-ssltest' and domains like 'ssltest.edgenexus.io' or 'ssltest2.edgenexus.io'. The 'Auto-Renew' column shows toggle switches, with the first three turned on and the last three turned off. A 'Reload Certificates' button is located at the bottom of the table.

| # | 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"/> |

- 下一步是选择你已经创建的ZIP文件，无论是手动还是使用批量导出。



The screenshot shows the 'Import Certificates' step in the Edgenexus SSL Certificate Manager. It includes a heading 'Step 1: Upload a Certificate archive' and instructions: '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.' Below this, there is a prompt 'Please browse to and locate your .zip file:' followed by a 'Choose File' button and a file name 'test.zip'. There is also a text input field for 'PKCS12 Password (if any):' with a masked password '.....'. At the bottom, there is a 'Go to Step 2 - Review Certificates' button.

- 输入PFX密码。
- 点击 "转到第2步 - 审查证书" 按钮。
- 下一页将允许你审查你要导入的证书。

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

- 如果一切都正确，你可以点击导入证书按钮。
- 如果导入成功，你应该看到一个确认信息。

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

- 关闭这个弹出窗口将显示如下的最后画面，表明导入成功。

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

你可以使用库>SSL证书查看导入的SSL证书。