Progress®
Kemp® LoadMaster®

Feature Description Lets Encrypt

Generated on: 16 September 2024

Copyright

Visit the following page online to see Progress Software Corporation's current Product Documentation Copyright Notice/Trademark Legend: Product Documentation Copyright Notice & Trademarks | Progress

Table of Contents

Chapter 1: Introduction 4

Chapter 2: Prerequisites 6

Chapter 3: How It Works 7

Chapter 4: Link the LoadMaster with a Let's Encrypt Account 8

Chapter 5: Request a New Certificate. 11

Request a Wildcard Certificate 13

Chapter 6: Convert a Virtual Service with Real Servers to one with SubVSs 15

Chapter 7: Logs Relating to Let's Encrypt. 17

1

Introduction

Introduction

Let's Encrypt is a free, automated, and open Certificate Authority (CA). It is a service provided by the Internet Security Research Group (ISRG).

Digital certificates are issued to enable HTTPS (SSL/TLS) for websites for free in a user-friendly way. The key principles for Let's Encrypt are:

- **Free:** Anyone who owns a domain name can use Let's Encrypt to obtain a trusted certificate at zero cost
- **Automatic:** Software running on a web server can interact with Let's Encrypt to painlessly obtain a certificate, securely configure it for use, and automatically take care of renewal
- **Secure:** Let's Encrypt serves as a platform for advancing TLS security best practices, both on the CA side and by helping site operators to properly secure their servers
- **Transparent:** All certificates issues or revoked are publicly recorded and available for anyone to inspect
- **Open:** The automatic issuance and renewal protocol is published as an open standard that others can adopt
- **Cooperative:** Much like the underlying internet protocols themselves, Let's Encrypt is a joint effort to benefit the community beyond the control of any one organization

As of LoadMaster firmware version 7.2.53, Progress Kemp enables you to leverage the value of Let’s Encrypt certificates by automating the renewal and updating of certificates across your applications.

The main features of the Let's Encrypt support in the LoadMaster are as follows:

- Built-in support for the LoadMaster as an Automated Certificate Management Environment (ACME) protocol client
- Support for obtaining a certificate from the Let's Encrypt servers, in addition to user-driven certificate renewal
- You can create a new Let's Encrypt account using the LoadMaster or use an already-obtained account key
- Support for automated validation of FQDN ownership before a certificate is issued
- Up to 10 Subject Alternative Names (SANs) can be specified per certificate request
- Key generation
- Certificate issuance (create Certificate Signing Request (CSR) and request certificates)
- Automatic/manual certificate renewal and automatic updating of renewed certificates on the LoadMaster

Certificates obtained using the LoadMaster ACME client are available on the **SSL Certificates** page of the LoadMaster User Interface (UI). They can be used for:

- Virtual Service decryption
- Virtual Service re-encryption
- Administrative login

2

Prerequisites

Prerequisites

The following prerequisites must be in place before configuring Let's Encrypt on the LoadMaster:

- A LoadMaster with firmware version 7.2.53 or above
- A HTTP/HTTPS Layer 7 Virtual Service must be already configured with the ability to add a SubVS (so it should not have any Real Servers added)

3

How It Works

How It Works

Let's Encrypt uses a challenge-based protocol. You must prove that you have control over the FQDN for a certificate to be issued successfully. Progress Kemp supports the HTTP-01 method for the challenge. Below is a description of the automatic steps performed by the LoadMaster after you request a new certificate. These steps are all performed automatically by the LoadMaster. This makes the process easy and no server-side modifications are required.

1. The LoadMaster sends a request for the certificate.
2. A token must then be placed in a specific location in the web server. That is what the Virtual Service that is selected when requesting a new certificate is used for. The challenge is served by the HTTP/HTTPS Layer 7 Virtual Service. Let's Encrypt provides a filename.
3. The path of the token file is included in the **Match String** of a content rule that is automatically created.
4. The LoadMaster automatically creates a SubVS in the Virtual Service selected.
5. The content rule is automatically assigned to this SubVS. This content rule will have first precedence. The Virtual Service is served through an error page (**200 OK**).
6. After the certificate issuing process is complete, the content rule and SubVS that were automatically created to perform the challenge are automatically deleted.

4

Link the LoadMaster with a Let's Encrypt Account

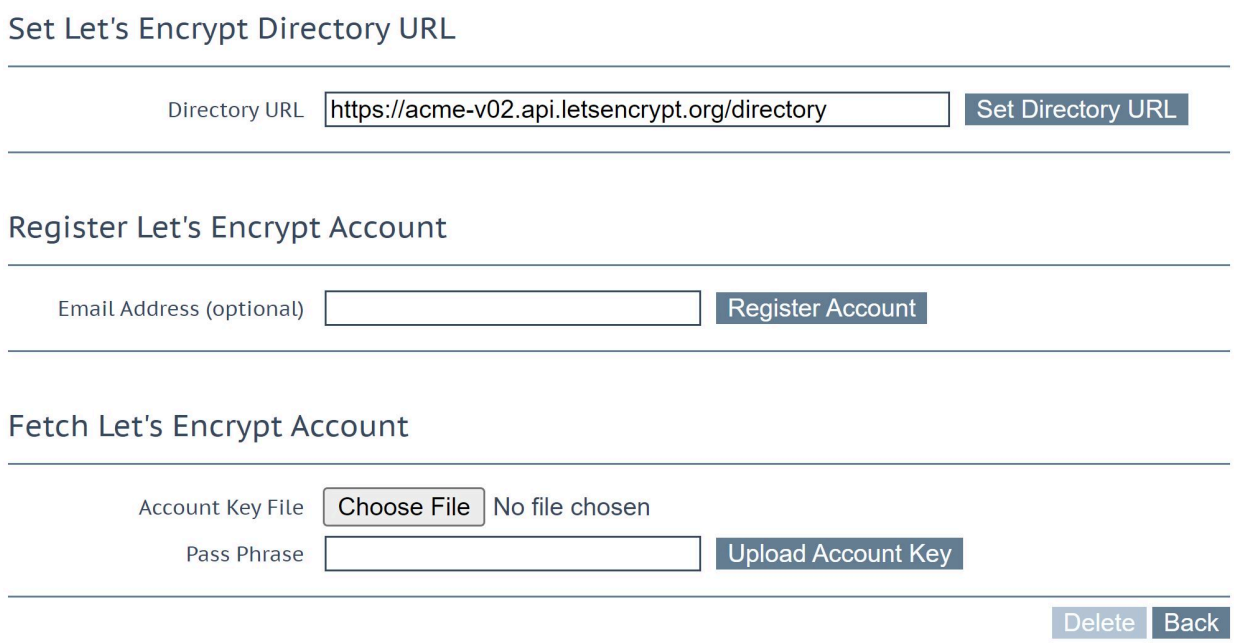
Link the LoadMaster with a Let's Encrypt Account

When initially configuring Let's Encrypt functionality on the LoadMaster, you must either create a new Let's Encrypt account or link to an existing account. To do this, follow the steps below in the LoadMaster User Interface (UI):

1. In the main menu, go to **Certificates & Security > ACME Certificates**.



2. Select **Let's Encrypt**.



3. Enter the URL of the Automated Certificate Management Environment (ACME) server in the **Directory URL** field and click **Set Directory URL**.

   Note: The default URL is the Let's Encrypt production ACME server: **https://acme-v02.api.letsencrypt.org/directory**. This can be changed as needed.The LoadMaster supports API version 2 of the ACME protocol.

4. If you do not already have a Let's Encrypt account, you can register for one by optionally entering your **Email Address** and clicking **Register Account**.

   When you register a Let's Encrypt account through the LoadMaster, a private key (account key) is generated. To reuse the same Let's Encrypt account key on another LoadMaster, take a backup of the LoadMaster (**System Configuration > System Administration > Backup/Restore**) and its related Certificates (**Certificates & Security > Backup/Restore Certs**), if available.To restore the backup on the other LoadMaster with account information only, follow the below steps:

   - Go to **System Configuration > System Administration > Backup/Restore**.
   - Click **Choose File**, browse to and select the created backup file.
   - Select the **LoadMaster Base Configuration** checkbox and then click **Restore Configuration** to restore the backup.

   If the created backup includes the account details, certificates and connected virtual services information, then follow the below steps to restore the backup:

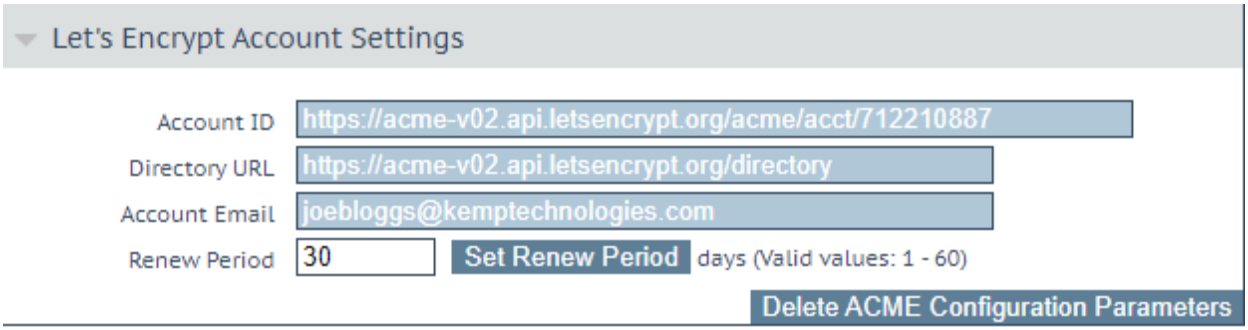
   - Go to **System Configuration > System Administration > Backup/Restore**.
   - Click **Choose File**, browse to and select the created backup file.
   - Select the **LoadMaster Base Configuration** and **VS Configuration** checkbox and then click **Restore Configuration** to restore the backup.
   - Then, go to **Certificates & Security > Backup/Restore Certs**.

- Click **Choose File**, browse to and select the certificate backup file.
- Select the type of certificates from drop-down list provided.
- Enter the passphrase associated with the certificate backup file and click **Restore Certificates**.

5. If you have an existing Let's Encrypt account, you can upload the **Account Key File**, enter the **Pass Phrase**, and click **Upload Account Key** to link to your existing account.

Note: You can retrieve the account key file from other ACME clients that you registered the account with (like Certbot).

6. Once you have successfully registered or linked to your existing Let's Encrypt account, the **Manage ACME Certificates** screen appears.



7. You can set the **Renew Period** for the Let's Encrypt certificates.

Note: Let's Encrypt certificates are valid for 90 days. The **Renew Period** value specifies how many days in advance of certificate expiry you would like the certificate to be renewed. The **Renew Period** is an account-wide setting. Per-certificate renewal periods are not supported at this time.The **Renew Period** is set to **30** days by default. Let's Encrypt recommends renewing certificates 30 days before expiry. Valid values for the **Renew Period** field range from 1 to 60 (days). The old certificates are replaced and assigned to the HTTPS Virtual Service when the renewal is successful.

The next step is to request a new certificate. Refer to the section below for instructions on how to do this.

You can click **Delete ACME Configuration Parameters** to remove the ACME account settings (which allows you to configure the ACME account settings from the start).

Note: You can only delete the configuration if there are no ACME certificates.

Note: If you downgrade the LoadMaster from version 7.2.53 (or above) to 7.2.52 (or below), any Let's Encrypt certificates that exist at the time of downgrade are preserved in the downgraded system so that Virtual Service connectivity is not inadvertently affected by the downgrade. However, the automatic certificate management functionality is not available in earlier versions. These certificates are listed on the **SSL Certificates** page and can be deleted after the downgrade, if needed.

5

Request a New Certificate

To request a new certificate, follow the steps below in the LoadMaster UI:

1. In the main menu, go to **Certificates & Security > ACME Certificates**.
2. Click **Request New Certificate** to request a new certificate from the Let's Encrypt CA.

   Note: All fields on the **Request a New Certificate** screen are optional except for **Certificate Identifier** and **Common Name** (and you must select a Virtual Service next to the **Common Name** field). Wildcard certificates are also supported. For further details, refer to the following section: Request a Wildcard Certificate.

3. Enter the unique identifier for your certificate in the **Certificate Identifier** field.

   Note: The **Certificate Identifier** value must be unique for all certificates on the LoadMaster.

4. Enter the Fully Qualified Domain Name (FQDN) of your web server in the **Common Name** field. The FDQN name is case-insensitive.

   Note: Certificates are only issued to valid hosting domains that you have control over.

5. Select the Virtual Service that is used for this domain. This will be used for the validation challenge to prove ownership of the domain.

   Note: A HTTP/HTTPS Layer 7 Virtual Service must be already configured with the ability to add a SubVS (so it should not have any Real Servers added to the parent Virtual Service - but if there are existing SubVSs they can have Real Servers attached). For instructions on how to convert an existing Virtual Service with Real Servers attached to one with SubVSs with Real Servers attached, refer to the Convert a Virtual Service with Real Servers to one with SubVSs section.A HTTP Redirect VS must be

configured to redirect all port 80 requests to 443 because Let's Encrypt communicates on port 80 to perform the HTTP-01 challenge.All valid Virtual Services that meet the criteria are listed in the drop-down list.

6. Optional: Enter the **2 Letter Country Code** that should be included in the certificate.

   Note: If using Let's Encrypt, the **2 Letter Country Code** to **Email Address** fields are truncated.

   Note: For a list of valid country codes, refer to the following page: SSL Certificate Country Codes.

7. Optional: Enter the **State/Province** that should be included in the certificate.

   Note: Enter the full name, for example **New York** (not NY).

8. Optional: Enter the **City** that should be included in the certificate.
9. Optional: Enter the name of the **Company** that should be included in the certificate.
10. Optional: Enter the department or organizational unit that should be included in the certificate in the **Organization** field.
11. Optional: Enter the **Email Address** of the person or organization that should be contacted regarding this certificate.
12. Optional: Enable or disable the **Generate Elliptic Curve Request** check box.

    Note: If this is enabled, an Elliptic Curve request is generated instead of an RSA request.

13. Optional: Select the key algorithm size from the **Key Size** drop-down list.

    Note: If you are generating an Elliptic Curve (EC) request, the **Key Size** drop-down is grayed out. The default size of 256 Bits is used for EC requests.If you are generating an RSA request, you can specify the **Key Size**.

14. Optional: Enter the Subject Alternate Name (SAN) in the **SAN/UCC Names** field.

    Note: This must be a valid domain.Up to 10 SANs can be specified.

15. Optional: Select the relevant Virtual Service.

    Note: For every SAN you must select a HTTP/HTTPS Layer 7 Virtual Service (you can use the same Virtual Service). For each SAN you must prove your authority to the Let's Encrypt server. A HTTP/HTTPS Virtual Service must be already configured with the ability to add a SubVS (so it should not have any Real Servers added to the parent Virtual Service - but if there are existing SubVSs they can have Real Servers attached). For instructions on how to convert an existing Virtual Service with Real Servers attached to one with SubVSs with Real Servers attached, refer to the Convert a Virtual Service with Real Servers to one with SubVSs section.All valid Virtual Services that meet the criteria are listed in the drop-down list.

16. Click **Request Certificate**.

A list of issued certificates and related details are displayed at the bottom of the **Let's Encrypt Certs** screen. The **HTTP Challenge VS(s)** column lists the Virtual Service (or Services) that were used for the HTTP challenge. These are not the Virtual Services that the certificates are assigned to.

Once the certificate is issued successfully, it will be listed in **Certificates & Security > SSL Certificates**. You can then assign it to any HTTPS Virtual Service or use it as an administrative certificate.

Note: When manually assigning a new certificate to a Virtual Service for the first time, the Virtual Service will restart so we recommend doing this outside of working hours.

When Let's Encrypt certificates are renewed, the Virtual Services that have the certificate assigned will be automatically updated with the renewed certificate.

Note: Automatic renewal and updating of certificates is seamless and does not affect Virtual Service traffic.

Certificates are automatically renewed at the number of days specified in the **Renew Period** before the expiry date of each certificate. You can manually renew the certificate by clicking **Renew Certificate**.

You can also delete a certificate associated with the domain by clicking **Delete Certificate**.

Note: If the certificate is used (for example if it is assigned in a Virtual Service or used as an administrative certificate) the **Delete Certificate** button is grayed out.

You cannot delete or replace Let's Encrypt certificates from the **SSL Certificates** screen. You can only delete or replace Let's Encrypt certificates from the **Let's Encrypt Certs** screen. The **Replace Certificate** and **Delete Certificate** buttons are grayed out on the **SSL Certificates** screen for Let's Encrypt certificates.

Related Links

- Request a Wildcard Certificate

Request a Wildcard Certificate

To request a wildcard certificate, follow the steps below in the LoadMaster User Interface (UI):

1. Go to **Certificates & Security > ACME Certificates**.
2. Click **Request New Certificate** to request a wildcard certificate from the Let's Encrypt Certificate Authority (CA).

   Note: All fields on the **Request New Certificate** screen are optional except for **Certificate Identifier** and **Common Name**. You must select a Virtual Service and DNS provider (including related credential parameters) next to the **Common Name** field.

3. Enter the unique identifier for your certificate in the **Certificate Identifier** field.

   Note: The **Certificate Identifier** value must be unique for all certificates on the LoadMaster.

4. Enter the Fully Qualified Domain Name (FQDN) of your web server in the **Common Name (The FQDN of your web server)** field. For example, ***.example1.com** matches anything that ends in **.example1.com**.
5. Select the Virtual Service that is used for this domain. This will be used for the validation challenge to prove ownership of the domain.
6. Select the DNS provider API from **Select DNS API** drop-down.

   For wildcard certificate validation, the DNS-01 challenge type is used. This requires the addition and removal of temporary DNS records. For automatic DNS record updates during wildcard name validation,

you must select your DNS provider from the **Select DNS API** drop-down list.

7. Set the access credential parameters for the selected DNS provider. The fields to fill out vary depending on the selected DNS provider.
   A list of DNS providers is as follows:
   - Progress-LM-GEO
   - CloudFlare
   - GoDaddy.com
   - Azure-DNS
   - DNSMadeEasy
   - DigitalOcean
   - NS1.com
   - Amazom-Route53

When you are finished setting the relevant fields, click **Request Certificate** to create a new certificate request using the specified data. It can take approximately 25 seconds to generate the certificate request. If the request fails, you must fill out the form again. A list of issued certificates and related details are displayed at the bottom of the **Manage ACME Certificates** screen.

6

Convert a Virtual Service with Real Servers to one with SubVSs

Convert a Virtual Service with Real Servers to one with SubVSs

When requesting a new certificate, you must select an existing Virtual Service that has the ability to have a SubVS. As a result, the parent Virtual Service cannot have Real Servers attached, but it can have SubVSs with Real Servers attached. If you have an existing Virtual Service with a Real Server attached and you would like to convert it to one with SubVSs so that you can use this Virtual Service for the certificate validation challenge, follow the steps below:

1. Go to **Virtual Services > View/Modify Services**.
2. Click **Modify** on the relevant Virtual Service.
3. Expand the **Real Servers** section.
4. Take note of the existing Real Server details.
5. Delete any existing Real Servers.
6. In the **Real Servers** section, click **Add SubVS**.
7. Click **Modify** on the SubVS.
8. Expand the **Real Servers** section.
9. Configure any settings as needed.
10. Click **Add New**.
11. Configure any settings as needed and click **Add This Real Server**.

12. Click **Back** to return to the SubVS modify screen.
13. Expand the **Advanced Properties** section.
14. Click **Enable** for **Content Switching**.
15. In the **Real Servers** section, click **None** in the **Rules** column.
16. Select the **default** rule and click **Add**.

If needed, contact Progress Kemp Support for assistance.

7

Logs Relating to Let's Encrypt

Logs Relating to Let's Encrypt

You can check the logs for detailed information about any errors that may occur, for example when linking to the Let's Encrypt account or requesting a new certificate. Logs relating to Let's Encrypt are available in both the **System Message File** and **Audit LogFile**. The audit log file contains logs relating to if the account was successfully registered or if a certificate is issued/renewed successfully. You can view both of these log files by going to **System Configuration > Logging Options > System Log Files**.