

Let's Encrypt

Feature Description

UPDATED: 28 July 2023

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

These materials and all Progress® software products are copyrighted and all rights are reserved by Progress Software Corporation. The information in these materials is subject to change without notice, and Progress Software Corporation assumes no responsibility for any errors that may appear therein. The references in these materials to specific platforms supported are subject to change.

#1 Load Balancer in Price/Performance, 360 Central, 360 Vision, Chef, Chef (and design), Chef Habitat, Chef Infra, Code Can (and design), Compliance at Velocity, Corticon, Corticon.js, DataDirect (and design), DataDirect Cloud, DataDirect Connect, DataDirect Connect64, DataDirect XML Converters, DataDirect XQuery, DataRPM, Defrag This, Deliver More Than Expected, DevReach (and design), Driving Network Visibility, Flowmon, Inspec, Ipswitch, iMacros, K (stylized), Kemp, Kemp (and design), Kendo UI, Kinvey, LoadMaster, MessageWay, MOVEit, NativeChat, OpenEdge, Powered by Chef, Powered by Progress, Progress, Progress Software Developers Network, SequeLink, Sitefinity (and Design), Sitefinity, Sitefinity (and design), Sitefinity Insight, SpeedScript, Stylized Design (Arrow/3D Box logo), Stylized Design (C Chef logo), Stylized Design of Samurai, TeamPulse, Telerik, Telerik (and design), Test Studio, WebSpeed, WhatsConfigured, WhatsConnected, WhatsUp, and WS_FTP are registered trademarks of Progress Software Corporation or one of its affiliates or subsidiaries in the U.S. and/or other countries.

Analytics360, AppServer, BusinessEdge, Chef Automate, Chef Compliance, Chef Desktop, Chef Workstation, Corticon Rules, Data Access, DataDirect Autonomous REST Connector, DataDirect Spy, DevCraft, Fiddler, Fiddler Classic, Fiddler Everywhere, Fiddler Jam, FiddlerCap, FiddlerCore, FiddlerScript, Hybrid Data Pipeline, iMail, InstaRelinker, JustAssembly, JustDecompile, JustMock, KendoReact, OpenAccess, PASOE, Pro2, ProDataSet, Progress Results, Progress Software, ProVision, PSE Pro, Push Jobs, SafeSpaceVR, Sitefinity Cloud, Sitefinity CMS, Sitefinity Digital Experience Cloud, Sitefinity Feather, Sitefinity Thunder, SmartBrowser, SmartComponent, SmartDataBrowser, SmartDataObjects, SmartDataView, SmartDialog, SmartFolder, SmartFrame, SmartObjects, SmartPanel, SmartQuery, SmartViewer, SmartWindow, Supermarket, SupportLink, Unite UX, and WebClient are trademarks or service marks of Progress Software Corporation and/or its subsidiaries or affiliates in the U.S. and other countries. Java is a registered trademark of Oracle and/or its affiliates. Any other marks contained herein may be trademarks of their respective owners.

Please refer to the NOTICE.txt or Release Notes – Third-Party Acknowledgements file applicable to a particular Progress product/hosted service offering release for any related required third-party acknowledgements.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Table of Contents

1 Introduction **4**

2 Prerequisites **6**

3 How It Works **7**

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

5 Request a New Certificate **11**

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

7 Logs Relating to Let's Encrypt **17**

8 RESTful API Updates **18**

8.1 Register a Let's Encrypt Account 18

8.2 Get an existing Let's Encrypt account 18

8.3 Let's Encrypt global parameters 18

8.4 Request a New Certificate from Let's Encrypt 19

8.5 Renew a Let's Encrypt certificate 19

8.6 Delete a Let's Encrypt certificate 20

8.7 List the Let's Encrypt certificate 20

8.8 Get the Let's Encrypt account information 20

8.9 Get the details of the Let's Encrypt specific certificate 20

Last Updated Date **21**

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

1 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, Kemp enables you to leverage the value of Let’s Encrypt certificates by automating the renewal and updating of certificates across your applications.

This includes:

- Support for HTTP-01 domain validation method
- 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

> As of LoadMaster firmware version 7.2.53 the LoadMaster Let's Encrypt functionality is in beta. There are currently no

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Application Programming Interface (API) commands.
API commands will be added in a future release.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

2 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)

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

3 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. 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.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

4 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 > Let's Encrypt Certs**.

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

   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.

3. 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:

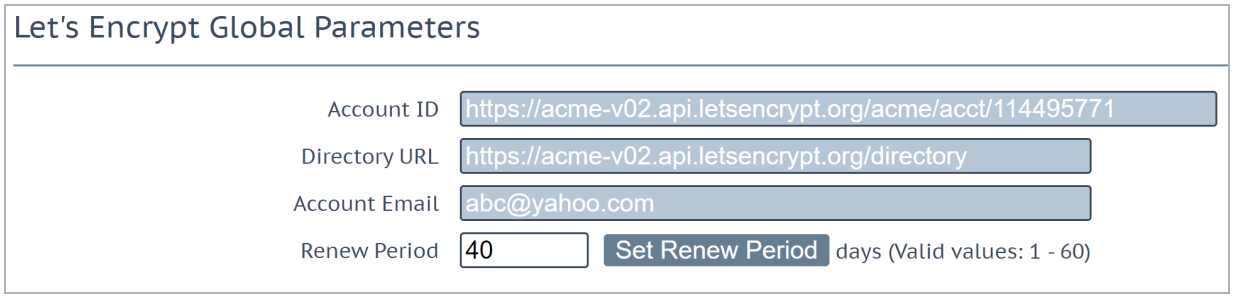
© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

- 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**.

4. 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.

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

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



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

> 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

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

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.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

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 > Let's Encrypt Certs**.
2. Click **Request New Certificate** to request a new certificate from the Let's Encrypt CA.

   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).

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

   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.

   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.

   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.
   An HTTP Redirect VS must be configured to redirect all port 80 requests to 443 as Let's Encrypt communicates on port 80 to perform the HTTP-01 challenge.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

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.

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

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

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

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.

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.

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.

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

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

15. Optional: Select the relevant Virtual Service.

> 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.

> When manually assigning a new certificate to a Virtual Service for the first time, the Virtual Service will restart so Kemp recommends 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.

> 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**.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

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.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

6 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**.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

If needed, contact Kemp Support for assistance.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

7 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**.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

8 RESTful API Updates

This section contains details about the Let's Encrypt API commands and parameters. You can retrieve or configure each of these parameters using the **get** or **set** RESTful API commands.

8.1 Register a Let's Encrypt Account

To register a Let's Encrypt account to the LoadMaster, run the **registerleaccount** command. For example:

/access/registerleaccount

Users can also register a Let's Encrypt account using an email address as an optional parameter, run the **registerleaccount?email=abc@yahoo.com** command. For example:

/access/registerleaccount?email=abc@yahoo.com

8.2 Get an existing Let's Encrypt account

To get an existing Let's Encrypt account registered with other ACME clients such as Certbot, run the **fetchleaccount?password=<password>** command. For example:

curl -X POST --data-binary "@account.key" -k "https://<Username>:<Password>@<LoadMasterIPAddress>/access/fetchleaccount?password=<password>"

8.3 Let's Encrypt global parameters

The Let's Encrypt global parameters can be configured using the **get** or **set** commands.

To set the **Renew Period** for the Let's Encrypt certificate, run the **set?param=renewperiod&value=<value>** command. For example:

/access/set?param=renewperiod&value=<value>

> Valid values for the **Renew Period** field range from 1 to 60 (days).

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

To get the details of the **Renew Period** for the Let's Encrypt certificate, run the **get?param=renewperiod** command. For example:

/access/get?param=renewperiod

To set the Let's Encrypt directory URL information, run the **set?param=directoryurl&value=<value>** command. For example:

/access/set?param=directoryurl&value=<value>

To get the Let's Encrypt directory URL information, run the **get?param=directoryurl** command. For example:

/access/get?param=directoryurl>

8.4 Request a New Certificate from Let's Encrypt

To request a new certificate from Let's Encrypt, run the **addlecert?cert=<cert_identifier>&cn=<FQDN>&vid=<value>** command using **cert**, **cn** and **vid** as a mandatory parameters. For example:

/access/addlecert?cert=<cert_identifier>&cn=<FQDN>&vid=<value>

Other optional parameters are also available, such as:

san1,san2,..,san10, vid1,vid2,...vid10 are for SAN and it's respective VID, country, state, city, company, organization, email, key_size, etc.

Below are some examples of commands that contains optional parameters:

/access/addlecert?cert=<cert_identifier>&cn=<FQDN>&vid=<value>&ec=no&key_size=4096

/access/addlecert?cert=<cert_identifier>&cn=<FQDN>&vid=<value>&ec=no&key_size=2048

/access/addlecert?cert=<cert_identifier>&cn=<FQDN>&vid=<value>&ec=yes

/access/addlecert?cert=<cert_identifier>&cn=<FQDN>&vid=<value>&san1=<FQDN>&vid1=<value>&san2=<FQDN>&vid2=<value>

8.5 Renew a Let's Encrypt certificate

To renew a Let's Encrypt certificate, run the **renewlecert?cert=<cert_identifier>** command. For example:

/access/renewlecert?cert=<cert_identifier>

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

8.6 Delete a Let's Encrypt certificate

To delete a Let's Encrypt certificate from the LoadMaster, run the **dellecert?cert=<cert_identifier>** command. For example:

/access/dellecert?cert=<cert_identifier>

8.7 List the Let's Encrypt certificate

To list the Let's Encrypt certificates that are installed on the LoadMaster, run the **listlecert** command. For example:

/access/listlecert

8.8 Get the Let's Encrypt account information

To get the Let's Encrypt account information from the LoadMaster, run the **leaccountinfo** command. For example:

/access/leaccountinfo

8.9 Get the details of the Let's Encrypt specific certificate

To get the details of the Let's Encrypt specific certificate from the LoadMaster, run the **getlecert?cert=<cert_identifier>** command. For example:

/access/getlecert?cert=<cert_identifier>

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Last Updated Date

This document was last updated on 28 July 2023.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.