



Installing an SSL Certificate

ScienceLogic Version 8.7.0

Table of Contents

Introduction	3
What is an SSL Certificate?	4
SSL on ScienceLogic Servers	4
Installing an SSL Certificate	5
Requesting a Commercial SSL Certificate	6
Creating Your Own Certificate	7
Installing the Certificate on an SL1 Appliance	8



Chapter 1

Introduction

Overview

This section provides an overview of SSL certificates and how they are used on SL1 appliances.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon (.
- To view a page containing all of the menu options, click the Advanced menu icon ().

This chapter includes the following topics:

What is an SSL Certificate?	4
SSL on ScienceLogic Servers	4

What is an SSL Certificate?

SSL is an acronym for Secure Sockets Layer. SSL is a protocol for securely transmitting data via the internet. SSL uses a private key to encrypt data to be transferred over the Internet connection. Usually, URLs that include "HTTPS" are using SSL for security.

To implement SSL, an SSL certificate resides on the web server and is used to encrypt the data and to identify the website. The SSL certificate contains information about the certificate holder, the domain for which the certificate was issued, the name of the Certificate Authority who issued the certificate, and the root and the country in which the certificate was issued.

There are two ways to acquire an SSL certificate:

- You can purchase a certificate from a vendor (called a "certificate authority"), such as VeriSign or GeoTrust.
- You can "self-sign" your own certificate. Using available tools (both open source and proprietary), you can create and sign your own SSL certificate instead of purchasing from a certificate authority.

SL1 includes a self-signed certificate from ScienceLogic. Self-signed certificates can trigger a warning message in some browsers. For this reason, some customers might prefer to purchase an SSL certificate from a certificate authority and install the certificate on one or more servers.

SSL on ScienceLogic Servers

Each SL1 appliance includes a self-signed certificate from ScienceLogic.

Each SL1 appliance uses the Nginx web server and OpenSSL.

If you want to use commercial SSL certificates with SL1, you must purchase certificates for the following SL1 appliances:

- For each Administration Portal, Database Server, or All-In-One Appliance you must purchase **two** certificates, one for the standard user interface and one for the Configuration Utility.
- For each Data Collector, you must purchase one certificate, for use with the Configuration Utility.
- For each Message Collector, you must purchase one certificate, for use with the Configuration Utility.



Chapter 2

Installing an SSL Certificate

Overview

This chapter describes how to install SSL certificates on SL1 appliances.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon (.
- To view a page containing all of the menu options, click the Advanced menu icon ().

This chapter includes the following topics:

<i>Requesting a Commercial SSL Certificate</i>	6
<i>Creating Your Own Certificate</i>	7
<i>Installing the Certificate on an SL1 Appliance</i>	8

Requesting a Commercial SSL Certificate

To purchase a commercial SSL certificate, you must first create a private key and then use the private key to create a Certificate Signing Request (CSR). You must then send the CSR to a Certificate Authority (CA). Some well-known CAs are VeriSign, GeoTrust, Thawte, GoDaddy, and Comodo. The CA will charge you a fee and send you a certificate for use with your private key.

To create a CSR, perform the following on each SL1 appliance.

1. Either go to the console of the SL1 appliance or use SSH to access the server. Open a shell session on the SL1 appliance. Log in as "em7admin".
2. First, you must generate a private key for the server. To do this, enter the following at the shell prompt:

```
sudo openssl genrsa -aes256 -out [keyname].key 4096
```

where:

- *[keyname]* is a name for the private key. For example, you might want to name the private key for an administration portal *adminport.key*.

NOTE: Make sure the file is **not** named ***siloss.key***. This is the name of the pre-existing ScienceLogic, self-signed certificate file.

3. You will be prompted to enter a pass phrase for the key.
4. Best practice is to make a backup copy of the key file and the pass phrase and store both in a secure location.
5. You must remove the pass phrase from the key before generating a Certificate Signing Request (CSR). To do this, enter the following at the shell prompt, inserting the keyname you used where indicated:

```
sudo openssl rsa -in [keyname].key -out [keyname].key.insecure
```

6. Next, you must create a Certificate Signing Request (CSR) for the private key you created in the previous steps. To do this, enter the following at the shell prompt:

```
sudo openssl req -new -key [keyname].key.insecure -out [keyname].csr
```

where:

- *[keyname]* is a name for the CSR for the specific server. For example, you might want to name the private key for an administration portal *adminport.key* and name the CSR for that key *adminport.csr*.

NOTE: Make sure the keyname is **not** ***siloss.key***. This is the name of the pre-existing ScienceLogic, self-signed certificate file.

7. You will be prompted to enter the Common Name. Enter the fully qualified domain name of the server where the certificate will be used and SSL and https will be run.

For example, if the SL1 appliance is accessed at `https://company.adminportal.com`, you would enter "company.adminportal.com" as the Common Name.

8. You can now send the .csr file to a Certificate Authority. The Certificate Authority will provide details on how to send the .csr file. The Certificate Authority will send you a .crt file. The .crt file is the public key that matches your private key for the SL1 appliance. Some Certificate Authorities, e.g. GoDaddy, might use an intermediate certificate to sign the provided certificate. If an intermediate certificate is used, the Certificate Authority will provide a bundle of chained certificates in a second .crt file.

Creating Your Own Certificate

There are two ways to create your own SSL certificate:

- If your organization is a root Certificate Authority (for example, some departments of the US government), you can create your own private key and public key for each ScienceLogic server.
- If your security requirements allow a self-signed certificate, you can create your own private key and public key for each SL1 appliance.

Remember to create key pairs for all for each SL1 appliance in your SL1 system and also remember to create two key pairs for each Administration Portal in your SL1 system.

If your organization is a Certificate Authority, see your organization's internal documentation on creating a certificate for Nginx.

If you want to create a self-signed certificate, perform the following:

1. Either go to the console of the SL1 appliance or use SSH to access the server. Open a shell session on the SL1 appliance. Log in as "em7admin".
2. First, you must generate a private key for the server. To do this, enter the following at the shell prompt:

```
sudo openssl genrsa -aes256 -out [keyname].key 4096
```

where [keyname] is a name for the private key. For example, you might want to name the private key for an administration portal `adminport.key`.

NOTE: Make sure the file is **not** named **siloss.key**. This is the name of the pre-existing ScienceLogic, self-signed certificate file.

3. You will be prompted to enter a pass phrase for the key. Best practice is to make a backup copy of the key file and the pass phrase and store both in a secure location.

5. Next, you must create a self-signed certificate based on the private key you generated in the previous steps.

To do this, enter the following at the shell prompt:

```
sudo openssl req -new -x509 -nodes -sha1 -days 365 -key [keyname].key -out [keyname].crt
```

where:

- `[keyname].key` is the private key for the SL1 appliance .
- `[keyname].crt` is the public key (certificate) for the SL1 appliance.

For example, you might want to name the private key for an administration portal `adminport.key` and name the certificate file for that key `adminport.crt`. The resulting `.crt` file is the public key that matches your private key for the SL1 appliance.

NOTE: Make sure the files are **not** named `silossl.crt` and `silossl.key`. These are the names of the pre-existing ScienceLogic, self-signed certificate files.

6. Remove the private key pass phrase. To do this, enter the following at the shell prompt:

```
sudo openssl rsa -in [keyname].key -out [keyname].key.insecure
```

7. Copy your private key and certificate files to `/etc/nginx`.
8. **On Collectors.** Add the private key and certificate file to each Collector for the Configuration Utility. To do this, add the names of the new `.key` and `.crt` files to the following files:

```
/etc/nginx/conf.d/em7ngx_web_ui.conf  
/etc/nginx/conf.d/em7ngx_em7proxy_web_ui.conf
```

9. **On the Administration Portal, Database Server, or All-in-One Appliance.** Add the private key and certificate file for the user interface. To do this, add the names of the new `.key` and `.crt` files to the following files:

```
/etc/nginx/conf.d/em7ngx_web_ui.conf  
/etc/nginx/conf.d/em7ngx_em7proxy_web_ui.conf
```

10. Restart the Web Configuration Utility and web server by entering the following command:

```
sudo systemctl restart nginx
```

Installing the Certificate on an SL1 Appliance

ScienceLogic does not provide support for third party certificates. Be advised that installing a new SSL certificate can affect the operation of SSL services.

Most certificate authorities provide support and resources on installing and enabling their certificates in Nginx web servers. If you have questions, please refer to your Certificate Authority.

WARNING: The following steps will stop and restart the SL1 appliance and temporarily make the Administration Portal site unavailable. Confirm with your System Administrator that you are permitted to restart the ScienceLogic Web Service.

NOTE: These instructions assume that you are familiar with the Linux shell and the "vi" editor.

To install a commercial SSL certificate on a SL1 appliance, perform the following:

1. Purchase a certificate from a certificate authority.
2. Copy the certificate files (*.key and all *.crt files) to a server that can access the SL1 appliance via SFTP.

NOTE: Make sure the files are **not** named **silossl.crt** and **silossl.key**. These are the names of the pre-existing ScienceLogic, self-signed certificate files.

3. Use SFTP or SCP to copy the .crt file(s) and the .key file to the SL1 appliance in the /etc/nginx directory.
4. Either go to the console of the SL1 appliance or use SSH to access the server. Open a shell session on the SL1 appliance. Log in as "em7admin".
5. If an intermediate certificate has been used to sign the certificate file, execute the following commands to combine the server certificate and the bundle of chained certificates provided by the Certificate Authority, entering the server certificate name, bundle name, and combined certificate name where indicated:

```
cd /etc/nginx
cat [server certificate name].crt [bundle name].crt > [combined certificate name].crt
```

Use the combined .crt file name when updating the nginx configuration.

6. For each appliance, edit the following files to configure the certificate for the Configuration Utility:
 - /etc/nginx/conf.d/em7webconfig.conf
 - /etc/nginx/conf.d/em7_sladmin.conf
 - Edit the following lines, removing references to silossl.crt and silossl.key and replacing with the names of the new .key and .crtfiles:

```
ssl_certificate /etc/nginx/[name of .crt file];
ssl_certificate_key /etc/nginx/[name of .key file];
```

7. In addition, for each Administration Portal, Database Server, and All-In-One Appliance, you must also edit the following files to configure the certificate for the user interface:

- `/etc/nginx/conf.d/em7ngx_web_ui.conf`
- `/etc/nginx/conf.d/em7ngx_em7proxy_web_ui.conf`
- Edit the following lines, removing references to `silossl.pem` and `silossl.key` and replacing with the names of the new key files:


```
ssl_certificate /etc/nginx/[name of .crt file];  
  
ssl_certificate_key /etc/nginx/[name of .key file];
```

8. Next, you will need to restart the webconfig and webserver. To do this, execute the following command:

- For all appliances, enter:

```
sudo systemctl restart nginx
```

9. To test the SSL certificate, open a browser session and connect to the Administration Portal, Database Server, or All-In-One Appliance using https.

- From the Administration Portal, go to System > Settings > Appliances.
- In the **Appliance Manager** page, select the toolbox icon () for each server. Notice that the URL for the Configuration Utility includes https.

© 2003 - 2020, ScienceLogic, Inc.

All rights reserved.

LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

ALL INFORMATION AVAILABLE IN THIS GUIDE IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED. SCIENCELOGIC™ AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT.

Although ScienceLogic™ has attempted to provide accurate information on this Site, information on this Site may contain inadvertent technical inaccuracies or typographical errors, and ScienceLogic™ assumes no responsibility for the accuracy of the information. Information may be changed or updated without notice. ScienceLogic™ may also make improvements and / or changes in the products or services described in this Site at any time without notice.

Copyrights and Trademarks

ScienceLogic, the ScienceLogic logo, and EM7 are trademarks of ScienceLogic, Inc. in the United States, other countries, or both.

Below is a list of trademarks and service marks that should be credited to ScienceLogic, Inc. The ® and ™ symbols reflect the trademark registration status in the U.S. Patent and Trademark Office and may not be appropriate for materials to be distributed outside the United States.

- ScienceLogic™
- EM7™ and em7™
- Simplify IT™
- Dynamic Application™
- Relational Infrastructure Management™

The absence of a product or service name, slogan or logo from this list does not constitute a waiver of ScienceLogic's trademark or other intellectual property rights concerning that name, slogan, or logo.

Please note that laws concerning use of trademarks or product names vary by country. Always consult a local attorney for additional guidance.

Other

If any provision of this agreement shall be unlawful, void, or for any reason unenforceable, then that provision shall be deemed severable from this agreement and shall not affect the validity and enforceability of any remaining provisions. This is the entire agreement between the parties relating to the matters contained herein.

In the U.S. and other jurisdictions, trademark owners have a duty to police the use of their marks. Therefore, if you become aware of any improper use of ScienceLogic Trademarks, including infringement or counterfeiting by third parties, report them to Science Logic's legal department immediately. Report as much detail as possible about the misuse, including the name of the party, contact information, and copies or photographs of the potential misuse to: legal@sciencelogic.com



800-SCI-LOGIC (1-800-724-5644)

International: +1-703-354-1010