Configuring SL1 to Comply with PCI DSS

ScienceLogic version 10.1.5

Table of Contents

Chapter 1

Introduction to PCI Compliance

Overview

This manual describes how to configure SL1 to comply with PCI DSS.

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 the menu options, click the Advanced menu icon ( ).

This chapter includes the following topics:

What is PCI DSS?

PCI DSS (Payment Card Industry Data Security Standard) is a set of security requirements for protecting information from customers' credit cards and debit cards. PCI DSS is a self-imposed industry standard. To do business with Visa, MasterCard, American Express, Discover, and JCB, all organizations that store, process, or transmit cardholder data must comply with PCI DSS requirements.

PCI DSS was created by Visa, MasterCard, American Express, Discover, and JCB. Visa and MasterCard require large and medium-sized merchants and service providers to be validated for compliance by a third-party auditor; small merchants and service providers can perform self-validation.

Visa, MasterCard, American Express, Discovery, and JCB can assess fines for businesses that do not comply with PCI DSS. Although PCI DSS is an industry standard, many states have separate laws that allow states to asses fines against organizations that leak data or have security breaches. Organizations that comply with PCI DSS have a significantly lower risk of data leaks and security breaches.

What is in This Manual?

This manual describes how to configure SL1 to comply with PCI DSS. This manual will walk you through the following configuration tasks:

- Configuring SL1 to use HTTPS instead of HTTP.
- Configuring SL1 to disable the auto-complete feature and disable saving credentials in the browser cache.
- Installing a security certificate.
- Strengthening SSL ciphers to the highest security.
- Disabling phpMyAdmin.
- Applying the latest update and/or patch.

This manual will also describe common issues that arise during a scan for vulnerabilities and how the configuration tasks described in this document address these issues.

Chapter 2

Configuring SL1 to Use Only HTTPS and to Disable Auto-Complete

Overview

This chapter describes how to configure SL1 to use only HTTPS and to disable the auto-complete feature.

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 the menu options, click the Advanced menu icon ( ).

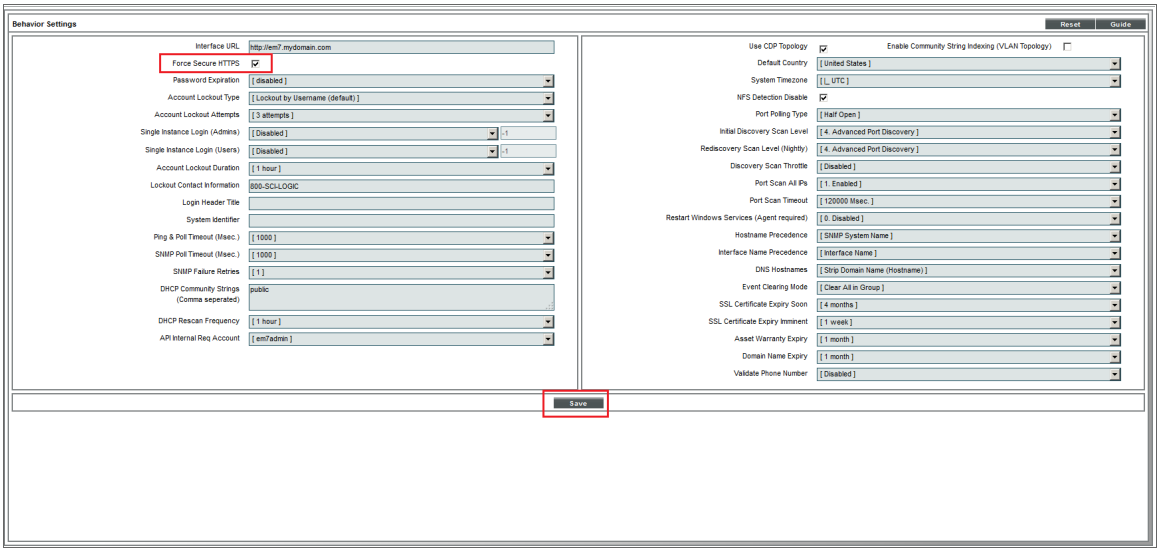
This chapter includes the following topics:

Configuring SL1 to Use Only HTTPS

To comply with PCI DSS, SL1 must use only HTTPS (secure HTTP), both for browser sessions to the Administration Portal and when sending HTTP data to other devices.

To configure SL1 to use only HTTPS:

1. Go to the **Behavior Settings** page (System > Settings > Behavior).
2. Click the checkbox for ***Force Secure HTTPS***.
3. Click the **[Save]** button.

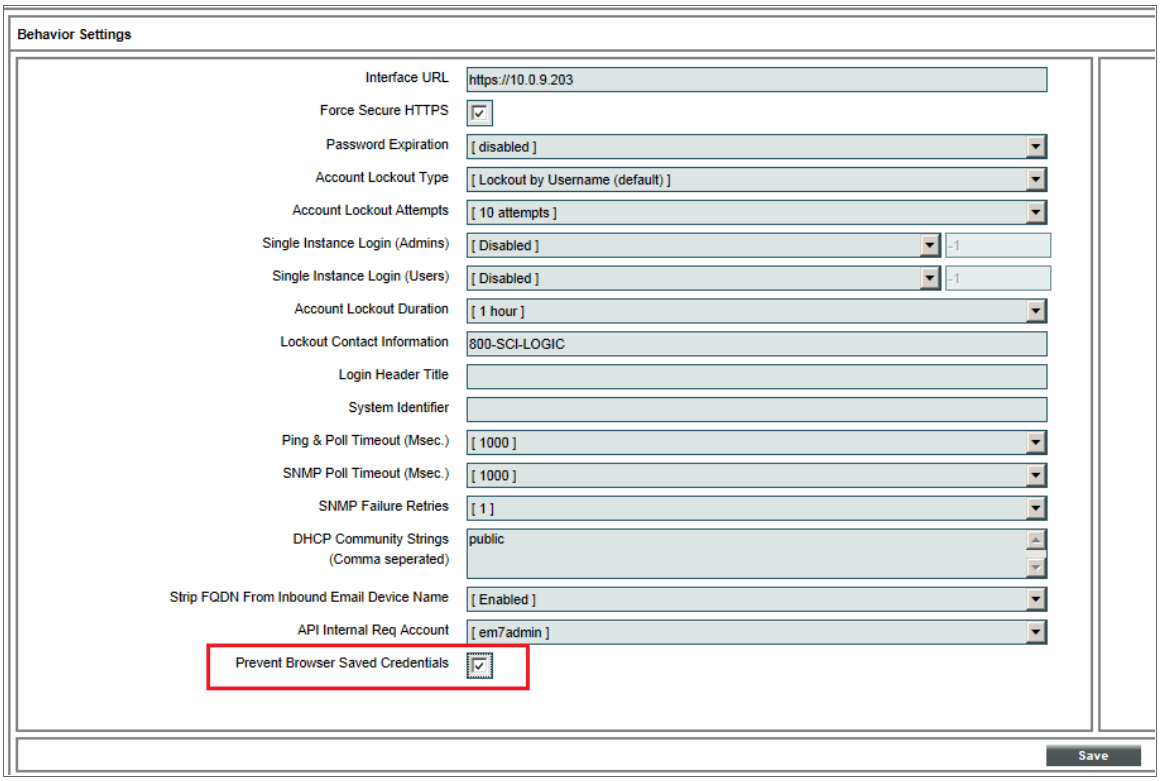


Configuring SL1 to Disable Auto-Complete

To comply with PCI DSS, you must disable the auto-complete feature in the login page for SL1. To do this, you must disable the feature that allows the browser to save ScienceLogic credentials in the browser cache.

To disable the auto-complete feature in SL1:

1. Go to the **Behavior Settings** page (System > Settings > Behavior).
2. Click the checkbox for ***Prevent Browser Saved Credentials***.
3. Click the **[Save]** button.


Behavior Settings
Interface URL
https://10.0.9.203
Force Secure HTTPS
Password Expiration
[disabled]
Account Lockout Type
[Lockout by Username (default)]
Account Lockout Attempts
[10 attempts]
Single Instance Login (Admins)
[Disabled]
-1
Single Instance Login (Users)
[Disabled]
-1
Account Lockout Duration
[1 hour]
Lockout Contact Information
800-SCI-LOGIC
Login Header Title
System Identifier
Ping & Poll Timeout (Msec.)
[1000]
SNMP Poll Timeout (Msec.)
[1000]
SNMP Failure Retries
[1]
DHCP Community Strings
(Comma seperated)
public
Strip FQDN From Inbound Email Device Name
[Enabled]
API Internal Req Account
[em7admin]
Prevent Browser Saved Credentials
Save

Chapter 3

Installing an SSL Certificate

Overview

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

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 the menu options, click the Advanced menu icon ( ).

This chapter includes the following topics:

Certificates for SL1 Servers

When installing an SSL certificate, you can either purchase a commercial SSL certificate or (if your security requirements allow a self-signed certificate) you can create your own certificate.

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

- For each Administration Portal, you must purchase ***two*** certificates, one for the standard user interface and one for the Configuration Utility.
- For each Database Server, you must purchase one certificate, for use with 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.
- For each Integration Server, you must purchase one certificate to allow secure cURL communication with the server.

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 Administration Portal. Log in as "root".

NOTE: For details on enabling and using SSH, see the manual ***System Administration***. For details and warnings about root access and instructions on how to make root access secure, see the manual ***System Administration***.

2. First, you must generate a private key for the server. To do this, enter the following at the shell prompt:

```
openssl genrsa -des3 -out keyname.key 1024
```

where *keyname.key* 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 files are NOT named ***em7.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 passphrase and store both in a secure location.
5. 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:

   ```
   openssl req -new -key keyname.key -out keyname.csr
   ```

   where *keyname.csr* 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*.

6. 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.
7. 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 ScienceLogic server.

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 each SL1 appliance in your SL1 system and also remember to create two key pairs for each Administration Portal server in your SL1 system. For a list of required certificates, see the section *Certificates for ScienceLogic Servers*.

If your organization is a Certificate Authority, see your organization's internal documentation on creating a certificate for Apache2.

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

1. First, you must generate a private key for the server. To do this, enter the following at the shell prompt:

   ```
   openssl genrsa -des3 -out keyname.key 1024
   ```

   where *keyname.key* 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 files are **not** named ***em7.key***. This is the name of the pre-existing ScienceLogic self-signed certificate file.

2. You will be prompted to enter a passphrase for the key.
3. Best practice is to make a backup copy of the key file and the passphrase and store both in a secure location.
4. 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:

   ```
   $ 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 and *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*.

5. The resulting .crt file is the public key that matches your private key for the SL1 appliance.

Installing the Certificate on an SL1 Server

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.

Chapter 4

Disabling phpMyAdmin

Overview

This chapter describes how to disable phpMyAdmin.

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 the menu options, click the Advanced menu icon ( ).

This chapter includes the following topics:

What is phpMyAdmin?

The phpMyAdmin interface provides a web interface for viewing and managing MySQL databases. By default, you can log in to the Database Server server using the phpMyAdmin interface to view and manage the MySQL databases on all Database Servers, Data Collectors, and Message Collectors in the system.

Disabling phpMyAdmin

To disable phpMyAdmin, you must disable the service and then disable the ports on which the service runs. To do this:

1. If you are using a distributed system, either go to the console of the Database Server or use SSH to access the Database Server. Open a shell session on the server. Log in as "root".
2. If you are using an All-In-One Appliance, either go to the console of the All-In-One Appliance or use SSH to access the All-In-One Appliance. Open a shell session on the server. Log in as "root".

> **NOTE**: For details on enabling and using SSH, see the manual ***System Administration***. For details and warnings about root access and instructions on how to make root access secure, see the manual ***System Administration***.

3. Open a vi session to edit the file /etc/siteconfig/firewalld-rich-rules.siteconfig
4. Add the following lines:

```
rule service name="phpmyadmin" reject
rule port port="8008" protocol="tcp" reject
```

5. Save your changes and exit the file.
6. Tell SL1 to pick up the changes to firewalld. To do this, type the following at the command line:

```
sudo /opt/em7/share/scripts/update-firewalld-conf.py
```

7. Restart the firewall services so that the phpMyAdmin service and port 8008 will no longer be allowed. To do this, type the following at the command line:

```
sudo systemctl restart firewalld
sudo systemctl restart nginx
```

Chapter 5

Installing Patches

Overview

This chapter describes how to install patches 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 the menu options, click the Advanced menu icon ( ).

This chapter includes the following topics:

System Updates

To maintain the security of SL1, you must install the latest updates and patches. You must also consult the release notes for each update and patch to ensure that you have performed any required manual configuration.

The **System Updates** page allows you to update the software on your SL1 Appliances. You must first download the update file to the local computer where you are running the browser. You can then load the software update through the user interface. After the software is loaded, you can install the software or schedule the software to be installed at a later time.

The **System Updates** page also maintains a list of installed updates and the date and time at which each update was applied.

Downloading a Patch

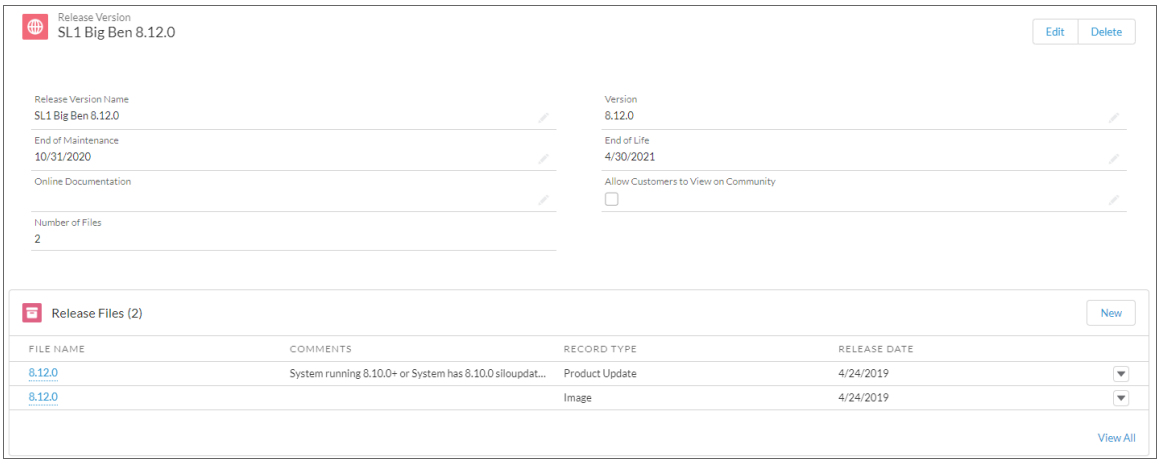
> **NOTE:** To download updates for previous the SL1 systemGlobal Manager systemsoftware versions that have reached their End of Life date and are no longer supported by ScienceLogic, contact ScienceLogic Support or a designated Customer Success Manager to get the update files.

Before you can load a patch or update onto your instance of the SL1 systemGlobal Manager system, you must first download the patch or update to your local computer. To do this:

> **NOTE:** These steps do not affect the performance of the SL1 systemGlobal Manager system. ScienceLogic recommends that you perform these steps at least 3 days before upgrading.

1. Log in to https://support.sciencelogic.com. Use your ScienceLogic customer account and password to access this site.

2. Select the **[Product Downloads]** button, select the ***Product Downloads*** menu, and choose *Platform*.
3. Find the release you are interested in and click its name.



4. In the ***Release Version*** article, click on the link for the release image or release patch you want to download. Scroll to the bottom of the page.
5. Under **Files**, select the link for the file you want to download. The file is then downloaded to your local computer.

Loading an Update onto the Platform

For information on updating an existing SL1 system, see the section on *Updating, Monitoring, and Maintaining SL1* in the System Administration manual. The *Updating, Monitoring, and Maintaining SL1* manual describes how to update the software on your SL1 appliances.

Contact ScienceLogic to get access to the ***Updating, Monitoring, and Maintaining SL1*** manual.

Chapter 6

Security Scans

Overview

Approved Scanning Vendors are companies that make software that performs vulnerability scans and helps organizations validate adherence to PCI DSS. For a list of all companies and scanning software approved by PCI DSS, see https://www.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors.

In our example, we used Rapid7 to test SL1 for compliance with PCI DSS ***before*** we performed the configuration steps in this document. If you use a scanning tool ***before*** performing the steps in this document, you might see some vulnerabilities like the following:

Vulnerability ID	Vulnerability Description	Vulnerability Solution
ssh-openssh-x11-forwarding-info-disclosure	OpenSSH 4.3p2, and probably other versions, allows local users to hijack forwarded X connections by causing ssh to set DISPLAY to :10, even when another process is listening on the associated port, as demonstrated by opening TCP port 6010 (IPv4) and sniffing a cookie sent by Emacs.	False positive. SL1 does not use X or OpenBSD.
ssh-openssh-cbc-mode-info-disclosure	Error handling in the SSH protocol in (1) SSH Tectia Client and Server and Connector 4.0 through 4.4.11, 5.0 through 5.2.4, and 5.3 through 5.3.8; Client and Server and ConnectSecure 6.0 through 6.0.4; Server for Linux on IBM System z 6.0.4; Server for IBM z/OS 5.5.1 and earlier, 6.0.0, and 6.0.1; and Client 4.0-J through 4.3.3-J and 4.0-K through 4.3.10-K; and (2) OpenSSH 4.7p1 and possibly other versions, when using a block cipher algorithm in Cipher Block Chaining (CBC) mode, makes it easier for remote attackers to recover certain plaintext data from an arbitrary block of ciphertext in an SSH session via unknown vectors.	False positive. SL1 does not use X or OpenBSD.

Vulnerability ID	Vulnerability Description	Vulnerability Solution
openssh-x11-cookie-auth-bypass	ssh in OpenSSH before 4.7 does not properly handle when an untrusted cookie cannot be created and uses a trusted X11 cookie instead, which allows attackers to violate intended policy and gain privileges by causing an X client to be treated as trusted.	False positive. SL1 does not use X or OpenBSD.
http-generic-sensitive-form-data-unencrypted	A web form contains fields with data that is probably sensitive in nature. This form data is submitted over an unencrypted connection, which could allow hackers to sniff the network and view the data in plaintext.	Fixed by *forcing HTTPS*.
http-cookie-secure-flag	The Secure attribute tells the browser to only send the cookie if the request is being sent over a secure channel such as HTTPS. This will help protect the cookie from being passed over unencrypted requests. If the application can be accessed over both HTTP and HTTPS, then there is the potential that the cookie can be sent in clear text.	Fixed by *forcing HTTPS*.
http-generic-webdav-enabled	WebDAV is a set of extensions to the HTTP protocol that allows users to collaboratively edit and manage files on remote web servers. Many web servers enable WebDAV extensions by default, even when they are not needed. Because of its added complexity, it is considered good practice to disable WebDAV if it is not currently in use.	False positive. SL1 does not enable webdav.
http-basic-auth-cleartext	The HTTP Basic Authentication scheme is not considered to be a secure method of user authentication (unless used in conjunction with some external secure system such as TLS/SSL), as the username and password are passed over the network as cleartext.	Fixed by *forcing HTTPS*.
http-cookie-http-only-flag	HttpOnly is an additional flag included in a Set-Cookie HTTP response header. If supported by the browser, using the HttpOnly flag when generating a cookie helps mitigate the risk of client side script accessing the protected cookie. If a browser that supports HttpOnly detects a cookie containing the HttpOnly flag, and client side script code attempts to read the cookie, the browser returns an empty string as the result. This causes the attack to fail by preventing the malicious (usually XSS) code from sending the data to an attacker's website.	Fixed by *forcing HTTPS*.
ssl-self-signed-certificate	The server's TLS/SSL certificate is self-signed. Self-signed certificates cannot be trusted by default, especially because TLS/SSL man-in-the-middle attacks typically use self-signed certificates to eavesdrop on TLS/SSL connections.	Fixed by *installing a commercial SSL certificate*.

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