



---

# SL1 Hollywood 12.2.7 Release Notes

SL1 version 12.2.7 (Document revision 1)

# SL1 Hollywood 12.2.7 Release Notes

**IMPORTANT:** ScienceLogic strongly recommends that you review the [upgrade instructions](#), important notes about [upgrading](#) SL1, and [known issues](#) for this release before upgrading to SL1 12.2.7.

**WARNING:** SL1 no longer supports the legacy version of Data Pull. If you are upgrading from a version of SL1 prior to 12.2.1.2, you will need to update all of your SL1 appliances to 12.2.7, including your Data Collectors and Message Collectors, to avoid potential data loss. When all appliances are successfully upgraded to 12.2.7, SL1 will automatically deprecate legacy Data Pull. If you do not update SL1 appliances after 60 days, the data on those appliances will be lost, and you will need to redeploy the appliances.

The SL1 Hollywood 12.2.7 release includes package updates to improve security and system performance and addresses multiple issues from previous releases.

These release notes provide a comprehensive list of the features, enhancements, and addressed issues that are included in the SL1 Hollywood 12.2.7 release.

To view the updates that are included in previous SL1 Hollywood releases, see the following release notes:

- [12.2.0](#)
- [12.2.1.1](#)
- [12.2.1.2](#)
- [12.2.3](#)
- [12.2.4.1](#)
- [12.2.5](#)
- [12.2.6](#)

This document covers the following topics:

<a href="#">Before You Proceed</a>	<a href="#">3</a>
<a href="#">New Features and Enhancements in SL1 Hollywood 12.2.7</a>	<a href="#">4</a>
<a href="#">Issues Addressed in SL1 Hollywood 12.2.7</a>	<a href="#">4</a>
<a href="#">Recently Deprecated Features</a>	<a href="#">7</a>
<a href="#">Upgrading SL1</a>	<a href="#">9</a>
<a href="#">Important Upgrade Notes for SL1 Hollywood 12.2.7</a>	<a href="#">9</a>
<a href="#">Known Issues for SL1 Hollywood 12.2.7</a>	<a href="#">15</a>

---

## Before You Proceed

If you are planning to consume SL1 Hollywood 12.2.7, be advised of the following:

- The 12.2.7 release is available only as a patch; there is no ISO version.
- SaaS deployments cannot upgrade to 12.2.7; this release is limited to on-premises deployments only.
- You can upgrade to 12.2.7 directly from the following SL1 versions:
  - 12.1.2, if all appliances are running on Oracle Linux 8 (OL8)
  - 12.2.1.2 through 12.2.6
- On-premises STIG-compliant users can upgrade to 12.2.7.
- Users who currently use Python 3.9 execution environments for Dynamic Applications and Run Book Automations should not upgrade to 12.2.7. Due to a known issue, Python 3.9 is not supported in this release.

For more details about these items and other potential issues you might experience, see the [Important Upgrade Notes](#) and [Known Issues](#) sections.

---

# New Features and Enhancements in SL1 Hollywood 12.2.7

## Platform and Security

- SL1 version 12.2.7 includes package updates to improve security and system performance.
- You can now change the token time-to-live (`token_ttl`) setting for EKMS to a range of values from "1h" to "48h". If you do this in high-availability (HA) systems, you must use the same `token_ttl` value for all active or passive nodes.

## PowerPacks

- The "EM7 Credential Tests" PowerPack was updated to version 104, which contains fixes for the SSH credential test, along with removal of deprecated features that led to errors in previous versions.

## ScienceLogic Libraries and Execution Environments

- The "sl1\_snippet\_api" library was updated to version 3.1.1. This update introduces a default value feature, which includes predefined configurations for various SSL components such as protocols.

---

# Issues Addressed in SL1 Hollywood 12.2.7

## API

- Resolved an issue that prevented users from filtering devices by device group in the REST API. (Case: 00472441) (Jira ID: EM-71052)

## Authentication

- Resolved an issue that prevented Global Manager single-sign-on (SSO) authentication if the username included a special character other than a period ( . ) or a hyphen ( - ). (Case: 00495460) (Jira ID: EM-72487)
- Resolved an issue that impacted the behavior of the **Single Instance Login** setting for local non-administrator user accounts that utilize CAC or ADFS authentication. (Jira ID: SLS-1687)

## Data Collection

- Addressed an issue that caused data collection to fail for some SNMP Dynamic Application collection objects if they used certain advanced Object ID field features and PDU packing, or if concurrent SNMP collection was enabled. (Case: 00494992) (Jira ID: EM-73047)

- Removed incomplete software inventory records from processing when the "Enterprise Database: Software Title" inventory updater process runs. When the process is in DEBUG mode, users will receive the log message for the incomplete software inventory result(s) in the /var/log/sl1/software\_inventory\_update.log file to denote which Dynamic Application and device has collected an incomplete inventory record that will not be processed. (Case: 00465611) (Jira ID: EM-72218)
- Addressed an issue that caused false SNMP error events to appear for Windows and Linux devices for services that were not running. (Cases: 00472205, 00484057) (Jira ID: EM-72506)
- Improved the Job Scheduler process stability to ensure database connection and transaction resources are initialized and cleaned up properly after every schedule activates, regardless of the schedule's status. (Cases: 00447556, 00448996) (Jira ID: EM-71969)
- Resolved an issue that caused critical unhandled exception events to occur with the "Data Collection: Interface Bandwidth: Traceback" process during collection. (Cases: 00429936, 00463088) (Jira ID: EM-71465)
- Resolved an issue that caused the "Data Collection: Interface Bandwidth" process to terminate collection without completing (SIGTERM). (Cases: 00450353, 00480917) (Jira ID: EM-67148)
- Addressed an issue where the filesystem statistics process caused an unhandled exception. (Case: 00450992) (Jira ID: EM-71464)

## Discovery

- Addressed an issue that caused Dynamic Application discovery and auto-alignment to sometimes fail with KeyErrors when snippet or bulk snippet Dynamic Applications did not return a full or correct set of results during their initial execution during discovery. (Case: 00462791) (Jira ID: EM-71421)
- Addressed an issue that caused event redirects to sometimes not work properly or not show the correct organization ID when redirecting between devices in different collector groups. (Case: 00464589) (Jira ID: EM-71280)

## Events

- Resolved an issue that caused the "EM7 Core: Event Processing Engine" to experience an unhandled exception due to improper processing of a syslog message. (Case: 00489058) (Jira ID: EM-71830)

## High Availability and Disaster Recovery

- Updated the web server configuration for the vault service to improve behavior between multiple database and data engine appliances, to address an issue that caused false system events indicating that passive databases could not connect to SL1 Collectors in high availability (HA), disaster recovery (DR), or HA+DR configurations. This update might require users on HA / DR configurations to take action upon installing or upgrading to SL1 12.2.7. For more information, see the section on "Changes to High Availability and Disaster Recovery Configurations" in the [Important Upgrade Notes for SL1 Hollywood 12.2.7](#). (Cases: 00434477, 00435183) (Jira ID: EM-64808)

## Logging

- Updated access logs to ensure the session duration value is correct for expired sessions. (Case: 00323782) (Jira ID: EM-65755)

## Platform and Security

- Addressed an issue in post-processing with Dynamic Application index mapping. In this situation, if an existing index that had a non-accented character was replaced by an accented version of the same character, or vice versa, that replacement caused an infinite error loop. (Case: 00477206) (Jira ID: EM-72432)
- Increased time-to-live (TTL) from 1 minute to 5 minutes for cached device group suppression in the event engine to prevent scenarios long-running queries from getting stuck. (Cases: 00459999, 00462563) (Jira ID: EM-66517)

## PowerPacks

- Ensured that legacy PowerShell processing, including handling of the "Microsoft: SQL Server Enhanced" PowerPack, honors your message encryption settings. (Case: 00453220) (Jira ID: EM-71462)

## Reporting

- Resolved an issue that prevented SL1 from generating reports in PDF, XLSX, or HTML formats. (Cases: 00483912, 00485367, 00486679, 00493250, 00495240, 00501968) (Jira IDs: EM-64941, EM-66052, EM-71710, EM-72365, EM-72489)
- Resolved an issue that prevented the proper generation of reports with embedded images. (Cases: 00469311, 00492671) (Jira IDs: EM-71633, EM-72205)

## User Interface

- Added the ability to set the expiration of user passwords after 365 days at the user account, user policy, or system level. With this change, a new 365 Days option was added to the **Password Expiration** drop-down field that appears on the following pages:
  - Account Properties (Registry > Accounts > User Accounts > create or edit)
  - User Policy Properties Editor (Registry > Accounts > User Policies > create or edit)
  - Behavior Settings (System > Settings > Behavior)(Case: 00416571) (Jira ID: EM-71136)
- Addressed an issue where, when running SL1 on a computer with limited hardware resources, using the **Bandwidth Billing Editor** page (Registry > Service Provider Utilities > Bandwidth Billing > create/edit) would cause some computers to experience an infinite redirect loop and lock up. (Case: 00494962) (Jira ID: EM-72445)
- Ensured that the **OID Browser** (System > Tools > OID Browser) properly displays symbolic names for newly added OIDs. (Case: 00457239) (Jira ID: EM-71419)
- Resolved an issue that was causing the **Device Processes** page (Devices > Processes) to sometimes not load properly. (Case: 00429969) (Jira ID: EM-65340)

---

## Recently Deprecated Features

### 12.2.0

The 12.2.0 release deprecates the following PowerPacks and removes them from the ISO:

- Citrix: Xen
- Dell EMC: Isilon
- Dell EMC: Unity
- Dell EMC: VMAX and PowerMax Unisphere API
- Dell PowerConnect Base Pack
- EMC: VMAX
- EMC: VNX
- Google Base Pack
- SMI-S: Array

**NOTE:** If you are upgrading from a previous version of SL1, the 12.2.7 upgrade will not remove any existing PowerPacks. The PowerPacks listed above are still available for download from the [PowerPacks Support](#) page.

### 12.1.0

The 12.1.0 release deprecates the following PowerPacks and removes them from the ISO:

- 3Com Device Classes Base Pack
- Alcatel-Lucent Base Pack
- Alteon Monitoring Base Pack
- APC Base Pack
- AskEM7 Query Widgets
- Attachmate Device Classes Base Pack
- Avaya Base Pack
- Avocent Base Pack
- Blue Coat Monitoring Base Pack
- Brocade: Base Pack
- Citrix Monitoring Base Pack
- Danaher Device Classes Base Pack
- DEC Device Classes Base Pack
- Dell OM Base Pack

- Dell PowerVault Event Policies
- D-Link Device Classes Base Pack
- Empire Device Classes Base Pack
- Enterasys Device Classes Base Pack
- Extreme Base Pack
- Fluke Networks
- Force 10 Monitoring
- Fortinet Base Pack
- Foundry Base Pack
- Google Base Pack
- Hitachi Base Pack
- HP-ISM Base Pack
- HP Pro Curve Base Pack
- HP-UX Base Pack
- Intel Base Pack
- Konica Minolta Base Pack
- LANCOM Systems Device Classes
- Lannair Device Classes
- Lantronix Device Classes
- Liebert Monitoring Base Pack
- Linksys Device Classes
- McAfee Monitoring
- MIB-2 Base Pack
- Microsoft: Azure Classic
- Motorola Device Classes
- NetBotz Base Pack
- NetScout Systems Device Classes
- Netscreen Base Pack
- Nokia Base Pack
- Printer Base Pack
- Riverbed Monitoring
- SNMP Research Base Pack
- UCD-SNMP Base Pack
- VMware: vSphere Reports
- Vyatta
- Xerox Base Pack

**NOTE:** If you are upgrading from a previous version of SL1, the 12.2.7 upgrade will not remove any existing PowerPacks. The PowerPacks listed above are still available for download from the [PowerPacks Support](#) page.

- With the [PHP updates](#) that were made in SL1 11.1.0, the classic SL1 Global Manager was supported only up to the 10.2.x line. Because the 10.2.x release line has now reached end of life, the **Classic Global Manager** manual was deprecated from [docs.sciencelogic.com](https://docs.sciencelogic.com).

---

## Upgrading SL1

**IMPORTANT:** You can consume SL1 12.2.7 only if you are upgrading from an earlier SL1 version that [supports upgrades to this release](#). There is no ISO version for version 12.2.7.

For a detailed overview of SL1, see the [Introduction to SL1](#) manual.

For detailed instructions on upgrading SL1, see the section on [Updating SL1](#) in the [System Administration](#) manual and the upgrade notes that are included in this document.

**NOTE:** ScienceLogic strongly recommends that you review the [Known Issues](#) for SL1 (<https://support.sciencelogic.com/s/known-issues#sort=relevancy>) before installing a new update.

For known issues specific to this release, see the [Known Issues](#) section of this document.

## SL1 Extended Architecture

For existing on-premises deployments of SL1 Extended Architecture, see the section on [Upgrading SL1 Extended Architecture](#) in the [System Administration](#) manual for upgrade instructions. For help with technical issues, contact ScienceLogic Customer Support.

---

## Important Upgrade Notes for SL1 Hollywood 12.2.7

This section includes important notes for upgrading existing SL1 systems to the Hollywood 12.2.7 release.

Unless otherwise stated, the information in this section applies to all users who are upgrading from previous SL1 versions.

**CAUTION:** ScienceLogic strongly recommends that you review these upgrade notes in their entirety before upgrading to version 12.2.7.

## Supported Upgrade Paths

Previous SL1 releases included major updates that you must consume before you can upgrade to 12.2.7, if you have not done so already. Therefore, you might be required to upgrade to one or more earlier versions of SL1 before you can upgrade to 12.2.7.

You can upgrade directly to 12.2.7 from the following SL1 versions:

- 12.1.2, if all appliances are running on Oracle Linux 8 (OL8)
- 12.2.1.2 through 12.2.6

Additionally, users on STIG-compliant SL1 deployments can upgrade to this release if they are currently on one of the above versions.

## Unsupported Upgrade Paths

You cannot upgrade to SL1 12.2.7 in the following scenarios:

- You are on a SaaS deployment of SL1.
- You have not yet deployed or upgraded to an SL1 version in which all appliances are running on Oracle Linux 8 (OL8).

**WARNING:** All customers who are upgrading from a version of SL1 prior to 12.1.2 **must** first upgrade to SL1 12.1.2 and then convert to OL8 before upgrading to SL1 12.2.7.

All older SL1 systems with OL7 are still operable, but ScienceLogic no longer supports them, and the systems might not be secure.

For upgrade instructions and important notes about upgrading to 12.1.2, see the [SL1 Golden Gate 12.1.2 Release Notes](#). For more information, see the [OL8 Conversion Resource Center](#) on the ScienceLogic Support portal.

## Upgrading MariaDB and Rebooting SL1

Some SL1 versions include important security updates. To apply these updates, you must upgrade MariaDB and then reboot all SL1 appliances.

The following table specifies the required MariaDB version for each SL1 version and which SL1 updates require you to reboot all SL1 appliances:

SL1 Release	Required MariaDB Version	Requires Appliance Reboot?
12.2.7 (Upgrade only)	10.6.18	Yes
12.2.6 (Upgrade only)	10.6.18	Yes
12.2.5 (Upgrade only)	10.6.18	Yes

SL1 Release	Required MariaDB Version	Requires Appliance Reboot?
12.2.4.1 (Upgrade only)	10.6.18	Yes
12.2.3 (Upgrade only)	10.6.18	Yes
12.2.1.2 (Upgrade only)	10.4.31	Yes
12.2.1.1 (ISO only)	10.4.31	N/A
12.2.0	10.4.31	Yes
12.1.2 (OL8)	10.4.31	Yes
12.1.2 (OL7)	10.4.29	Yes
12.1.1 (OL8)	10.4.28	Yes
12.1.1 (OL7)	10.4.29	Yes
12.1.0.2 ISO (OL8)	10.4.28	N/A
12.1.0.2 Upgrade (OL7)	10.4.29	Yes

**NOTE:** For instructions on updating MariaDB or rebooting the SL1 system, see the section on [Updating SL1](#) in the *System Administration* manual.

If you would like assistance in planning an upgrade path that meets your security needs while minimizing downtime, please contact your Customer Success Manager.

## Deployment Limitations

SaaS deployments cannot upgrade to SL1 12.2.7; this release is limited to on-premises deployments only.

## Required Ports

Beginning with SL1 12.2.0, if you have a firewall between your Database Server, data engine, and Administration Portal appliances, you should open TCP port 8200 to facilitate communication between those appliances.

For a full list of ports that must be open on each SL1 appliance, see the section on [Required Ports for SL1](#) in the *Installation and Initial Configuration* manual.

## Legacy Data Pull Deprecation

As of version 12.2.1.2, SL1 no longer supports the legacy version of data pull. If you are upgrading from a version of SL1 prior to 12.2.1.2, you will need to update all of your SL1 appliances to version 12.2.7, including your Data Collectors and Message Collectors, to avoid potential data loss. When all appliances are successfully upgraded to 12.2.7, SL1 will automatically deprecate legacy Data Pull. If you do not update SL1 appliances after 60 days, the data on those appliances will be lost, and you will need to redeploy the appliances.

## Future Python 2 Support Deprecation

Prior to SL1 11.3.0, all Dynamic Application snippets, Execution Environments, Run Book Actions, and ScienceLogic Libraries utilized Python 2.

With the introduction of Python 3 support in 11.3.0, ScienceLogic announced its intent to deprecate support for Python 2 in a future release. The core SL1 platform will switch to Python 3 with the 12.3.0 (Ibiza) release.

However, ScienceLogic will still include Python 2 in parallel with Python 3 until the 12.5.0 (Juneau) release, slated for release in Q2 2025, at which point it will be completely removed from SL1. At that time, customers still using Python 2 in any custom content—including customer-created PowerPacks—will be unable to update to the 12.5.0 (Juneau) release until their custom code is Python 3-compatible.

For more information, see the [Python 3 Resource Center](#) on the ScienceLogic Support site, as well as this knowledge base article: <https://support.sciencelogic.com/s/article/12014>.

## Python 3.9 Execution Environment Issues and Future Support Deprecation

Users who currently use Python 3.9 execution environments for Dynamic Applications and Run Book Automations should not upgrade to 12.2.7. Due to a known issue, Python 3.9 is not supported in this release. Additionally, the SL1 12.3.0 release removes support for Python 3.9 entirely and adds support for Python 3.11. For more information, see the section [Important Notes on Creating ScienceLogic Libraries](#) in the **ScienceLogic Libraries and Execution Environments** manual.

## Default Use of tmux When Using SSH

Starting with SL1 version 12.2.1.1, the tmux utility runs by default when you access an SL1 system using SSH.

The addition of this utility, which is a terminal multiplexer that enables a number of terminals to be created, accessed, and controlled from a single screen, strengthens session-control mechanisms and aligns with industry-wide security practices.

With this update, sessions are automatically locked after 15 minutes of idleness or if an unclean SSH disconnect or dropped SSH connection occurs. Upon login, SL1 checks for and attaches any detached tmux session if it finds them; otherwise, it starts a new session.

This update also introduces advanced features like scroll-back buffering with search, built-in clipboarding, multiple sessions and panes, detaching or attaching sessions, and session supervision or sharing.

***If you have turned off tmux in an earlier version of SL1 and upgrade to 12.2.7, be advised that you will need to turn tmux off again after upgrading.***

For more information about tmux shortcuts and usage, see <https://tmuxcheatsheet.com/>.

## Disabling the PowerPack Encryption Preupgrade Test

If you are upgrading an SL1 stack that originated on an 11.x version or earlier, then prior to upgrading to this release, you must run the following command on the Database Server to disable the PowerPack encryption preupgrade test:

```
silosql -e "update siloupdate.preupgrade_config set enabled = 0 where type = 'pp_encryption';"
```

If you are upgrading an SL1 stack that originated on a 12.x version, you do not need to complete this step.

## Enterprise Key Management Service (EKMS) Issues

You might experience the following EKMS-related issues upon upgrading to SL1 12.2.7:

- EKMS might not start due to an issue where it remains encrypted upon startup.
- You might need to change the EKMS token time to live (`token_ttl`) setting

Both of these issues are described in more detail below.

### EKMS Remains Encrypted Upon Startup

After upgrading to 12.2.1.2 or later, you might experience an issue where the Enterprise Key Management Service (EKMS) for your SL1 system is unable to start because it is still encrypted upon startup.

To check for this issue, use SSH to access your SL1 Database Server and run the following command:

```
sudo cat /tmp/vault_conf.yml
```

If the file is clear text, then this issue does not impact you, and you can ignore the rest of this known issue.

If the file is not clear text, then EKMS is still encrypted and you will need to perform the following workaround steps:

1. Decrypt the vault file:

```
sudo slsctl config --file /etc/sl_vault/vault_conf.yml --key /etc/sl_vault/encryption_key --decrypt
```

2. Run the command a second time to decrypt the file again, as this issue is caused by a double encryption.

3. Remove the previous configuration file:

```
sudo rm -rf /tmp/vault_conf.yml /opt/em7/services/sl_vault/config/hcl/vault.hcl
```

4. Restart the `sl_vault` service:

```
sudo systemctl start sl_vault
```

### Setting the EKMS Token Time to Live Value for All Nodes

As of SL1 12.3.1, you can change the EKMS token time to live (`token_ttl`) setting to a range of values from 1h to 48h. If you do this in high-availability (HA) systems, you must use the same `token_ttl` value for all active or passive nodes. To do so:

1. Decrypt the configuration file `/etc/sl_vault/vault_conf.yml`:

```
slsctl config --file /etc/sl_vault/vault_conf.yml --key /etc/sl_vault/encryption_key --out /etc/sl_vault/vault_conf_d.conf --decrypt
```

2. Change the `token_ttl` setting in the decrypted vault file.

3. Re-encrypt the file:

```
slsctl config --out /etc/sl_vault/vault_conf.yml --key /etc/sl_vault/encryption_key --file /etc/sl_vault/vault_conf_d.conf --encrypt
```

4. Remove the configuration file from `/tmp`:

```
sudo rm /tmp/vault_conf.yml
```

5. Restart `sl_vault` and `sl-vaultmngt`:

```
sudo systemctl restart sl_vault
```

```
sudo systemctl restart sl-vaultmngt
```

**NOTE:** The new `token_ttl` value will take effect after the previous token time to live has lapsed.

## Changes to High Availability and Disaster Recovery Configurations

In SL1 12.2.7, the web server configuration for the vault service was updated to improve behavior between multiple database and data engine appliances. This was done to prevent false system events indicating that passive databases could not connect to SL1 Collectors in high-availability (HA), disaster recovery (DR), or HA+DR configurations. With this update:

- On new installations, you must run the following command after all database and data engine appliances are licensed, to populate the list of allowed locations where vault could be running: `sudo /opt/em7/share/scripts/vault_add_servers.sh`. If the list is populated successfully, the output will tell you to restart nginx for it to take effect. Upon updating, this is generated automatically.
- If you are upgrading and you have not modified the default configuration file, then it will be updated to this new configuration automatically.
- If you are upgrading and you have modified the default configuration file, the updated web server configuration will be installed as `/etc/nginx/conf.d/vault.conf.rpmnew`, and you will need to merge your modifications into the new configuration and then remove the `.rpmnew` extension.

## System Update Notes

- **SL1 updates overwrite changes to the configuration file `/opt/em7/nextui/nextui.env`.** This is a known issue. (For more details, see <https://support.sciencelogic.com/s/article/1161> and <https://support.sciencelogic.com/s/article/1423>.) ScienceLogic recommends that you back up this file before applying an update and then reapply your changes to this file.
- The SL1 user interface will be unavailable intermittently during system update.
- During the normal system update process, multiple processes are stopped and restarted. This might result in missed polls, gaps in data, and/or unexpected errors. ScienceLogic recommends that you always install SL1 releases during a maintenance window.

- The SL1 system update process starts a background process that can perform any required post-upgrade tasks. The post-patch update process is automatically stopped after 24 hours. However, depending on the size of your database as well as the version from which you are upgrading, the post-upgrade tasks can take several days to perform. If the post-patch update process is stopped after 24 hours, the process will automatically re-start and continue processing from the point at which it was stopped. If you see an event that indicates the post-patch update process was stopped, you do not need to contact ScienceLogic support for assistance until you see the same event for three consecutive days.
- After upgrading, to ensure proper data collection, you should go to the **Appliance Manager** page (System > Settings > Appliances), locate one of the Data Collector or Message Collector appliances, and click the lightning bolt icon to force configuration push for that appliance.

## Upgrading from Oracle Linux 7 (OL7) Versions of SL1

If you are upgrading from a version of SL1 prior to 12.2.0 and first need to upgrade to 12.1.2 and/or convert all of your SL1 appliances to Oracle Linux 8 (OL8), ScienceLogic **strongly** recommends that you review the [Important Upgrade Notes](#) section of the [SL1 Golden Gate 12.1.2 Release Notes](#) prior to upgrading.

## Known Issues for SL1 Hollywood 12.2.7

**NOTE:** ScienceLogic strongly recommends that you review all [Known Issues](#) for SL1. For more information, see <https://support.sciencelogic.com/s/known-issues#sort=relevancy>.

The following known issues exist for SL1 Hollywood 12.2.7:

- Prior to the release of SL1 12.2.7, five new common vulnerabilities and exposures (CVEs) were released for Ingress-nginx, the highest being CVE-2025-1794, rated a 9.8 CVSS. This allows anything on a Kubernetes pod network to exploit configuration injection vulnerabilities via the Validating Admission Controller. When combined with other vulnerabilities, CVE-2025-1794 means that anything on the pod network has a good chance of taking over your Kubernetes cluster, with no credentials or administrative access required. In many deployments, the pod network is accessible to all workloads within the deployed VPC. This vulnerability has been fixed in 12.2.7 for AWS SL1 deployments but still persists for on-premises deployments. For on-premises deployments, users should follow the instructions provided by Kubernetes to remedy the issues: <https://kubernetes.io/blog/2025/03/24/ingress-nginx-cve-2025-1794/#your-next-steps> (Jira ID: DO-6413)
- Users who currently use Python 3.9 execution environments for Dynamic Applications and Run Book Automations should not upgrade to 12.2.7. Due to a known issue, Python 3.9 is not supported in this release. A fix for this issue is planned for a future release. (Jira ID: EM-70867)
- If you are upgrading an SL1 stack that originated on an 11.x version or earlier, then prior to upgrading to this release, you must run the following command on the Database Server to disable the PowerPack encryption pre-upgrade test:

```
silosql -e "update silupdate.preupgrade_config set enabled = 0
where type = 'pp_encryption';"
```

- In this release, the PhoneHome server does not correctly report the connection state information of PhoneHome collectors in MariaDB. (Jira ID: EM-65069)
- When upgrading SL1 on AWS stacks, you might receive an error message that the Data Engines failed to patch correctly. If this occurs, re-run the pre-upgrade tests and then run the patch again; this should result in the Data Engines updating correctly and the correct version then being reflected on the **Appliance Manager** page (System > Settings > Appliances).
- The preupgrade expiry check might fail for Database Servers that utilize out-of-the-box licenses, even when the license is set to expire after the configured expiration period. This issue does not impact appliances that use licenses procured from ScienceLogic. For more information, including a workaround for this issue, see: <https://support.sciencelogic.com/s/article/12914>. (Jira ID: EM-61746)
- When upgrading a large number of SL1 appliances, you might encounter an issue where the deployment summary shows that deployment timed out for many of the appliances but, upon further inspection, you discover that the appliances actually deployed correctly. This is due to a lag in the deployment status reaching the Database Server after the default timeout value of 3600 seconds (1 hour). If you check back later, the issue should fix itself. If you would rather work around this issue, you can increase the timeout value. For instructions, see the section on [Adjusting the Timeout for Slow Connections](#) in the "[Updating SL1](#)" chapter of the [System Administration](#) manual. (Jira ID: EM-62316)
- After upgrading to 12.2.1.2 or later, you might experience an issue where the Enterprise Key Management Service (EKMS) for your SL1 system is unable to start because it is still encrypted upon startup. For more information including a workaround, see the upgrade note about [EKMS issues](#). (Jira IDs: EM-66508, EM-66487)
- Some upgraded 12.2.x instances do not have `api_expanded` option listed for the `eventmanager` in the `silos.conf` file, which in turn is causing Skylar events to not trigger in SL1. To work around this issue:
  1. Either go to the console of the SL1 appliance or use SSH to access the SL1 appliance.
  2. Open a shell session on the server.
  3. Type the following at the command line:
 

```
sudo visilo
```
  4. Locate the line for "eventmanager" and update it to include "api\_expanded". For example:
 

```
eventmanager = internal,api,dynamic,syslog,trap,api_expanded
```
  5. To save your changes and exit the file, enter `:wq` and then confirm that you want to save.

(Jira ID: SLUI-18754)

- On SL1 Oracle Linux 8 (OL8) appliances, after upgrading or after deploying a new HA, DR, or HA+DR stack, the following WARNING messages might appear when issuing commands using `crm` or any script/utility that utilizes `crm`, such as:

```
WARNING: could not get the pacemaker version, bad installation?
```

```
WARNING: list index out of range
```

These warnings can be safely ignored. For more information, see: <https://support.sciencelogic.com/s/article/14388>. (Jira ID: EM-63091)

- If your SL1 system is running Windows and you are using PowerShell collections that have the **Encrypted** field set to Yes in the credentials, those collections will stop working. For more information, see [Users with Windows 2008 R2 Servers or Windows 2012 Servers](#) in the SL1 Product Documentation. (Jira ID: EM-61204)
- After installing or upgrading to SL1 12.2.7, each time the system status script (system\_status.sh) runs, you might notice that error/traceback messages appear stemming from the SL1 siloupdate service. These messages can be safely ignored. For more information, see: <https://support.sciencelogic.com/s/article/11591>. (Jira ID: EM-65832)
- A known issue might cause high swap usage in excess of 95% to be observed on appliance types running SL1 12.1.x and Oracle Linux 8. This impacts all appliance types, but is most frequently observed on Database Servers or appliances that are under heavy memory pressure. For more information about this issue, including a workaround, see: <https://support.sciencelogic.com/s/article/11598>. (Jira ID: EM-59269)
- A known issue might cause several log configuration files to conflict, which could cause you to see errors for the `sl_vault` and `slsctl` logs or potentially block log rotation in some cases, depending on the order in which the files are executed. To work around this issue, delete the config files `~sl_vault` and `~slsctl`. (Jira IDs: SLS-1105, EM-62134)
- When using the SNMP Public V2 credential to discover devices, you might see an unhandled exception in the system log near the end of the discovery session, despite the devices being discovered successfully. (Jira ID: EM-59380)
- After upgrading to 12.2.x, you might be unable to delete devices from the **Devices** page. If this occurs, you can work around this issue by deleting the device from the **Device Manager** page in either the current ("AP2") SL1 user interface (Devices > Device Manager) or the classic user interface (Registry > Devices > Device Manager), or you can delete the device from the Database Server. (Jira ID: EM-62874, Case: 00412497)
- The following known issues impact Business Services:
  - The **[Anomalies]** tab on the **Service Investigator** page for device services might incorrectly display devices that have anomaly detection disabled, rather than showing only those devices with anomaly detection enabled. (Jira ID: EM-62884)
  - Organizations must have at least one or more accounts assigned to them to ensure the relevant services are saved. (Jira ID: SLUI-17810)
  - For services that have their **RCA Options** field enabled, and has had a child service removed, SL1 will not compute the health, availability, and risk values until the Service Topology Engine returns an updated topology, which occurs every 5 minutes by default. (Jira ID: SLUI-18853)

**IMPORTANT:** Before deleting child services in a 3-tier hierarchy, check if the parent service has the **RCA Options** field *Enabled*, then set this field to *Disabled* if it is not already.

- In new installations of SL1 12.2.7, the "EM7 Web Server" PowerPack that is normally installed by default is not being installed. You can manually install this PowerPack after SL1 has been installed and configured. For instructions, see the section on [Installing a PowerPack](#) in the [PowerPacks](#) manual. This issue does not impact SL1 instances that have been upgraded from earlier releases. (Jira ID: SOL-24609)
- The CyberArk credential gateway service integration is incompatible with SL1's Concurrent PowerShell feature. If you are using the CyberArk credential integration, you must have Concurrent PowerShell disabled. To disable Concurrent PowerShell, go to the **Behavior Settings** page (System > Settings > Behavior), ensure that the **Enable Concurrent PowerShell Collection** checkbox is not selected, and click **[Save]**. (Jira ID: EM-63205)
- The **[Expand]** and **[Contract]** buttons are not working as intended on the **Dynamic Application Collections** page (Devices > Device Manager > wrench icon > Collections). You can still expand and contract individual items on the page. (Jira ID: EM-64420)

© 2003 - 2025, 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](mailto:legal@sciencelogic.com). For more information, see <https://sciencelogic.com/company/legal>.



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

International: +1-703-354-1010