



SL1 Ibiza 12.3.1 Release Notes

SL1 version 12.3.1 (Document revision 10)

SL1 Ibiza 12.3.1 Release Notes

IMPORTANT: ScienceLogic strongly recommends that you review the [installation and upgrade instructions](#), [important upgrade notes](#), and [known issues](#) for this release before installing or upgrading to SL12.3.1.

The SL1 Ibiza 12.3.1 release adds the ability to export additional interface data to Skylar AI, includes package and security updates, and addresses issues from previous releases.

These release notes provide a comprehensive list of the features, enhancements, and addressed issues that are included in the SL1 Ibiza 12.3.1 release.

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

- [12.3.0](#)

NOTE: [AP2 version 8.16.1.14 \(Halwa\)](#) is installed by default in SL1 12.3.1.

This document covers the following topics:

Before You Proceed	3
New Features and Enhancements in SL1 Ibiza 12.3.1	4
Issues Addressed in SL1 Ibiza 12.3.1	4
Recently Deprecated Features	7
Installing and Upgrading SL1	7
Important Upgrade Notes for SL1 Ibiza 12.3.1	8
Known Issues for SL1 Ibiza 12.3.1	15

Before You Proceed

IMPORTANT: As of version 12.2.0, SL1 no longer supports deployment on Oracle Linux 7 (OL7). Users who are upgrading from a version of SL1 that runs on OL7 **must** first upgrade to SL1 12.1.2 and then convert all appliances to OL8 before they can upgrade to 12.2.0 or later. For more information, see the [Supported Upgrade Paths](#) section.

If you are planning to consume SL1 Ibiza 12.3.1, be advised of the following:

- You can upgrade to this release directly from SL1 12.2.1.1, 12.2.1.2, 12.2.3, 12.2.4.1, 12.2.5, and 12.3.0.
 - You can also upgrade directly from SL1 12.1.2 if all of your SL1 appliances have been converted to OL8. If you are already on 12.1.2, you should upgrade directly to 12.3.1 without consuming the 12.2.x releases. If you are on 12.1.0.2 or 12.1.1, you should upgrade to 12.1.2, convert to OL8, and then upgrade directly to 12.3.1.
 - You should not upgrade from 12.2.6 to 12.3.1.

WARNING: If you are upgrading from a version prior to 12.2.3, then after upgrading SL1, you must also upgrade MariaDB 10.4.x to version 10.6.18. Failure to perform this MariaDB upgrade can cause major functionality issues in SL1.

- STIG-compliant users can deploy this release; 12.2.x and 12.3.0 STIG-compliant users can upgrade to this release. Users who are on an 11.x MUD system cannot upgrade to this release; they must first follow the approved conversion process from 11.x MUD to 12.2.1.1 STIG. For more information, see the section on [STIG Support](#).
- AWS deployments that are using Aurora 3 can upgrade to this release.
 - If you are currently deployed using Aurora 2, you can upgrade to this release but must perform a post-upgrade Aurora 2 to 3 conversion.
- SL1 12.3.1 is Department of Defense Information Network (DoDIN)-certified.

For more information, see the [Important Upgrade Notes](#) and [Known Issues](#) sections.

New Features and Enhancements in SL1 Ibiza 12.3.1

This section describes the new features and enhancements that are included in SL1 Ibiza 12.3.1.

Platform and Security

- SL1 version 12.3.1 includes package updates to improve security and system performance. These package updates include the following security updates that address known vulnerabilities: ELSA-2023-6939, ELSA-2024-2988, ELSA-2024-2098, ELSA-2024-3254, ELSA-2024-0752, CVE-2024-37891, ELSA-2024-5258, ELSA-2024-4246, ELSA-2024-3968, ELSA-2024-12191.
- When upgrading to 12.3.1, the Enterprise Key Management Service (EKMS) will remain enabled or disabled based on whether it was already enabled or disabled in the version from which you are upgrading. If you are installing a new deployment of 12.3.1, EKMS will be disabled by default.
- Addressed an issue with EKMS that caused the token time-to-live (`token_ttl`) setting to not be honored by `sl-vaultmngt` when creating tokens. With this update, you can change the `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. For instructions, see the [Setting the EKMS Token Time to Live Value for All Nodes](#) section in the *Important Upgrade Notes*.

PowerPacks

- The "SL1: System Upgrade Assessment" PowerPack was removed from the SL1 12.3.1 ISO.

Skylar AI

- The following data can now be exported to Skylar from SL1:
 - Interface billing metrics and metadata
 - Network interface IPv4 and IPv6 address and netmask metadata
- The Skylar Management script can now run as a new asynchronous system process, "Enterprise Database: Skylar Management." This process is enabled by default.
- A new `master_events.skylar_lookup.subtype` database field was added to indicate the subtype of alerts sent from Skylar to SL1.

Issues Addressed in SL1 Ibiza 12.3.1

This section describes the issues that were addressed in SL1 Ibiza 12.3.1.

Agent

- Resolved an issue that caused timeout errors when multiple Gen-1 agents were deployed on different collector groups. (Case: 00390933) (Jira ID: EM-67890)
- Updated agent log file monitoring policies for Linux/AIX agents to ensure the policies respect case-sensitivity in log names. (Case: 00468003) (Jira ID: EM-70780)

API

- Addressed an issue in SaaS/PaaS deployments that utilize Aurora 3 where API queries against the data_performance resource were not returning device IDs in their responses due to a schema issue. (Case: 00476368) (Jira ID: EM-71329)
- Resolved an issue that prevented users from filtering devices by device group in the REST API. (Case: 00472441) (Jira ID: EM-71052)

Data Collection

- Addressed an issue where the filesystem statistics process caused an unhandled exception. (Case: 00450992) (Jira ID: EM-71464)
- Resolved several issues that caused critical unhandled exception events to occur with the "Data Collection: Interface Bandwidth: Traceback" process during collection, as well as when Internal Collections Dynamic Applications from the "Microsoft: Windows Server" PowerPack were used to collect data. (Cases: 00429936, 00463088, 00447219) (Jira IDs: EM-71465, EM-70802)
- When the "Microsoft: Windows Server IC Interface Inventory" Dynamic Application collects both IPv4 and IPv6 addresses from interfaces on a Windows device, those addresses will now all be displayed in the **IP Address** drop-down field of the **Device Properties** page (Devices > Device Manager > wrench icon). (Case: 00376135) (Jira ID: EM-70574)

Data Pull

- Improved the Job Scheduler process 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-65598)
- Addressed an issue that prevented SL1 from storing the result of ModuleCmdStorage in system logs. (Cases: 00466380, 00470300) (Jira ID: EM-67223)

Discovery

- During SNMP device discovery, SL1 now converts any control characters that are returned for the "sysname" Object ID (OID) to UTF-8 so the characters are properly displayed in the user interface. (Case: 00452024) (Jira ID: EM-66235)

- 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 with their initial execution during discovery. (Case: 00462791) (Jira ID: EM-71421)
- Addressed an issue that caused duplicate device components when saving a device component that included a backslash (\) for the GUID or unique_id. (Case: 00473348) (Jira ID: EM-70760)

Events

- Increased time-to-live (TTL) from 1 minute to 5 minutes for cached device group suppression in the event engine to prevent scenarios where too many queries cause excessive load on the database, which resulted in queries to seemingly get stuck. (Cases: 00459999, 00462563) (Jira ID: EM-66517)

Platform and Security

- Added an option for customers with large numbers of SL1 Collectors to increase the open file descriptor limit through a new `open_file_limit` configuration option in the `/etc/silo.conf` file under the `[CONFIG_PUSH]` heading. This new option defaults to a value of "1024". (Case: 00460017) (Jira ID: EM-70972)
- 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)

Reports

- Resolved an issue that prevented the proper generation of reports with embedded images. (Case: 00469311) (Jira ID: EM-71633)

System Updates

- Ensured that the appropriate appliances display as intended when you click the **[Appliance List]** button from the **System Updates** page (System > Tools > Updates) if you are on a SaaS/PaaS deployment that utilizes Aurora 3. (Cases: 00475665, 00477537) (Jira ID: EM-71417)

Topology

- Resolved an issue with the Layer-2 topology crunch process to avoid errors on connections marked as "override". (Case: 00469796) (Jira ID: EM-67876)
- Ensured that Link Layer Discovery Protocol (LLDP) relationships are created properly based on device name. (Case: 00471899) (Jira ID: EM-70782)
- Updated the manner in which Layer-3 topology results are collected and handled to ensure Layer-3 topology collection runs successfully. (Case: 00478864) (Jira ID: EM-71175)

User Interface

- Ensured that the **OID Browser** page (System > Tools > OID Browser) properly displays symbolic names for newly added OIDs when large MIBs are compiled. (Case: 00457239) (Jira ID: EM-71419)
- Resolved an issue that sometimes prevented the **Device Processes** page (Devices > Processes) from loading properly, resulting in HTTP 504 Gateway Timeout errors. (Case: 00429969) (Jira ID: EM-65340)

Recently Deprecated Features

PowerPacks

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

The 12.3.1 release removed the following PowerPack from the SL1 ISO:

- SL1: System Upgrade Assessment

The 12.3.0 release deprecated the following PowerPacks and removed them from the SL1 ISO:

- Blackberry Custom Reports
- Cisco: Wireless
- EM7 Base Themes
- OpenStack
- ScienceLogic Integration Service/PowerFlow Monitoring
- ScienceLogic Rules Engine Events
- VMware: vSphere Base Pack, versions 306 and 307

Installing and Upgrading SL1

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

For detailed instructions on performing a new installation of SL1, see the [Installation and Initial Configuration](#) 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](https://support.sciencelogic.com/s/known-issues#sort=relevancy) for SL1 at <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.

NOTE: New installations of SL1 Extended Architecture are available only on SaaS deployments.

Important Upgrade Notes for SL1 Ibiza 12.3.1

This section includes important notes for upgrading existing SL1 systems to the Ibiza 12.3.1 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 notes in their entirety before upgrading to version 12.3.1.

Supported Upgrade Paths

You can upgrade directly to 12.3.1 from the following SL1 versions:

- 12.3.0
- 12.2.5
- 12.2.4.1
- 12.2.3
- 12.2.1.2
- 12.2.1.1
- 12.1.2, if all SL1 appliances are running on Oracle Linux 8 (OL8)

CAUTION: If you are already on 12.1.2, you should upgrade directly to 12.3.1 without consuming the 12.2.x or 12.3.0 releases. If you are on 12.1.0.2 or 12.1.1 and want to upgrade 12.3.1, you

should upgrade to 12.1.2, convert to OL8 if you have not already done so, and then upgrade directly to 12.3.1.

WARNING: For versions 12.2.0 and later, the SL1 platform can be deployed *only* on Oracle Linux 8 (OL8) operating systems. All customers who are upgrading from a version of SL1 that runs fully or partially on OL7 *must* first upgrade to SL1 12.1.2 and then convert all appliances to OL8 before you can upgrade to SL1 12.2.0 or later.

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.

Unsupported Upgrade Paths

You should not upgrade from SL1 12.2.6 to 12.3.1 due to a known technical issue.

STIG Support

STIG-compliant users can deploy this release.

In addition, 12.2.x and 12.3.0 STIG-compliant users can upgrade to this release.

Users who are currently on an 11.x MUD system cannot upgrade to this release. 11.x MUD customers should follow the 11.3 MUD conversion to 12.2.1.1 STIG re-ISO migration path; this process is documented in the *ScienceLogic OL8 MUD Conversion Guide*. (Ask your ScienceLogic contact for this manual.) Once you are on 12.2.1.1 STIG, you can upgrade to later STIG releases, including this release.

NOTE: When deploying a STIG-compliant configuration—also known as a military unique deployment (MUD) configuration—port 7700, the Web Configuration Utility, and the **Database Tool** page are all disabled. In addition, concurrent PowerShell, concurrent SNMP, and concurrent network interface collection are not supported for these deployments.

Enabling the Enterprise Key Management Service (EKMS) on STIG Deployments

EKMS is not enabled by default in STIG deployments in versions of SL1 prior to 12.3.14. STIG users must manually enable EKMS. To do so:

1. Either go to the console of the active Data Engine or use SSH to access the active Data Engine.
2. To check the status of the EKMS, you can run the following command:

```
/opt/em7/backend/ha_status.py
```

3. Run the following command:

```
sudo silo_mysql -e "UPDATE master.system_settings_general SET value=1  
WHERE param='sl_vault_service';"
```

4. Run the first boot script for the vault service:

```
sudo /opt/em7/share/scripts/em7_firstboot.d/96_vault_init.sh
```

5. Run the following command to start the service:

```
sudo systemctl start sl_vault
```

6. Check the log file for errors:

```
sudo less /data/logs/sl_vault.log
```

7. Confirm the service is enabled and healthy:

```
slsctl health_check
```

8. Exit the shell session.
9. In Skylar One (SL1), go the **System Logs** page (System > Monitor > System Logs) and verify that there are no error or exceptions for the `slsctl` command.

Aurora 3 Support

AWS deployments that are using Aurora 3 can upgrade to Skylar One (SL1) 12.3.1. If you are currently deployed using Aurora 2, you can upgrade to Skylar One (SL1) 12.3.1 but must perform a post-upgrade Aurora 2 to 3 conversion. If you are on a SaaS-hosted AWS deployment, the ScienceLogic SRE team will complete this conversion. If you are on a customer-hosted AWS deployment, you must complete this conversion, with additional steps in the section on [Updating Skylar One](#) in the [System Administration](#) manual. Contact ScienceLogic Professional Services if you need assistance.

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.

WARNING: If you are upgrading from a version prior to 12.2.3, then after upgrading SL1, you must also upgrade MariaDB 10.4.x to version 10.6.18. Failure to perform this MariaDB upgrade can cause major functionality issues in SL1.

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?
12.3.1	10.6.18	Yes
12.3.0	10.6.18	Yes
12.2.6 (Upgrade only)	10.6.18	Yes
12.2.5 (Upgrade only)	10.6.18	Yes
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.

Clearing SL1 Cache Post-Upgrade

After upgrading to version 12.3.1, you should clear your system cache to remove cached items from Skylar One (SL1) and prevent several potential issues that can occur post-upgrade due to caching. To do so, go to Misc > Clear SL1 Cache.

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 Skylar One (SL1) appliance, see the section on [Required Ports for Skylar One](#) in the [Installation and Initial Configuration](#) manual.

Python 2 Support Deprecation

Prior to SL1 11.3.0 Forum, 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 Forum, ScienceLogic announced its intent to deprecate support for Python 2 in a future release.

The core SL1 platform switched to Python 3 with the 12.3.0 Ibiza release. However, ScienceLogic will still include Python 2 in parallel with Python 3 on the 12.3.x line.

CAUTION: The Skylar One Juneau 12.5.1 Juneau release does not include Python 2 support. Any Python 2 content will stop working when an instance is updated to version 12.5.1 Juneau and later.

ScienceLogic has proactively migrated the product and the PowerPacks it supports to Python 3. However, any custom content in customer-created PowerPacks must be recreated utilizing ScienceLogic-provided enablement tools or migrated to Python 3 before consuming the 12.5.1 Juneau release.

For more information, see the [Python 3 Resource Center](#) on the ScienceLogic Support site.

Python 3.9 Execution Environment Support Deprecation

Users who currently use Python 3.9 execution environments for Dynamic Applications and Run Book Automations are advised that the SL1 12.3.0 Ibiza release removed support for Python 3.9 and added 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.

Enterprise Key Management Service (EKMS) Issues

You might experience the following EKMS-related issues upon upgrading to SL1 12.3.1:

- 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
```

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

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 12.3.1, 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/>.

System Update Notes

- ***SL1 updates overwrite changes to the configuration file /opt/em7/nextui/nextui.env.*** (For more details, see <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.
- ScienceLogic recommends that you run backups of your SL1 system before performing a system update.
- 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.
- 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.

- 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).
- 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 Ibiza 12.3.1

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 Ibiza 12.3.1:

- A critical vulnerability, CVE-2025-68615, can impact Net-SNMP in SL1 12.3.x versions prior to 12.3.13. ScienceLogic strongly recommends that all users running version 12.3.x upgrade to the 12.3.13 release, which includes a fix for this vulnerability. If you are unable to upgrade at this time, you can instead run an out-of-band script to patch the vulnerability on your 12.3.x stacks. However, be advised that, if you run this script on your 12.3.x stack, you cannot upgrade to releases prior to 12.5.6; you must upgrade to 12.5.6 or later. For more information, see <https://support.sciencelogic.com/s/article/19707> and <https://support.sciencelogic.com/s/article/19976>.
- Due to a known issue, you should not upgrade from SL1 12.2.6 to 12.3.1.
- In this release, the PhoneHome server does not correctly report the connection state information of PhoneHome collectors in MariaDB. (Jira ID: EM-65069)
- 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.
- 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).

- 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 IDs: EM-59433, EM-62316)
- If you deploy SL1 Global Manager with SAML single sign-on authentication, you might experience an issue where the Global Manager stack cannot access data from its child stacks if Enterprise Key Management Service (EKMS) encryption was disabled on the Global Manager system, resulting in the following error message: "Stack <#> <IP address> results excluded. Consider disabling it. Reason: Response code 401 (Unauthorized)." To work around this issue, EKMS should be enabled for the Global Manager stack. It can be enabled or disabled for the child stacks. (Jira ID: SLUI-21476)
- In STIG deployments, the Enterprise Key Management Service (EKMS) must be enabled manually. For more information, see the section on [Enabling EKMS on STIG Deployments](#).
- The "Support: Configuration File Validation" and "Support: Appliance Validation" Dynamic Applications in the "ScienceLogic Support Pack" PowerPack contain SQL queries with the keyword "function", which is a reserved keyword in MySQL 8.0. Because of this, you might see unhandled exceptions relating to those Dynamic Applications. (Jira ID: EM-72266)
- When performing a disaster recovery (DR) backup, the backup_retention cleanup process might fail with an unhandled exception. In this scenario, the DR backup is successful; it is only the cleanup that is failing. This issue does not impact config or full backups or their cleanup processes. To alleviate this issue, if you are backing up to a device with limited storage, you can delete older DR backups you no longer need to free up storage space. (Jira ID: EM-72403)
- A known issue with session cache management might cause SL1 to log you out unexpectedly, or prevent you from logging in again after a recent session. If you experience either issue, you can work around it by clearing the cache of your web browser before you log into the SL1 user interface. For more information, see <https://support.sciencelogic.com/s/article/13701>. (Jira ID: SLUI-21011)
- Due to an issue with Aurora 3, you can no longer enable TLS verification through the user interface or the API. To address this issue, update the `master.system_settings_general` database table by setting `value=1` where `param='require_tls_verification'`; This issue was addressed in the [AP2 8.17.23.18 \(Ice Pop\)](#) release. You can optionally download and install that release after upgrading to 12.3.1 to obtain the fix. (Jira ID: SLS-1500)
- 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 2008 or Windows 2012, 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)
- In AWS Extended Architecture upgrade deployments, the active Data Engine might display a banner message that indicates there is no active database after a failover has been performed. If there appear to be no other issues and everything otherwise seems to be working as expected, check the database for the following file: `/data.local/tmp/motd.pid`. If that file exists, delete it and wait for motd to run again. After it runs again, you can log out and log back in. The banner message should no longer appear. (Jira ID: EM-59194)
- The **Classic Maps** (Maps > Classic Maps) page is empty for users that have not accepted the End-user License Agreement (EULA). This issue is addressed in the [AP2 8.17.23.18 \(Ice Pop\)](#) release. You can optionally download and install that release after upgrading to 12.3.1 to obtain the fix. (Jira ID: SLUI-20801)
- On Safari browsers, when attempting to modify data retention settings within the "Subscription" section of the **Data Retention** page, the slider for adjusting retention values is not functioning. The system displays the following error message: "Cannot find the input with NAME='sliderValue29h'." This issue does not impact other web browsers, so you can use a different browser to work around this issue. (Jira ID: EM-66372)
- In the SL1 user interface, the End User License Agreement (EULA) page is displayed on all pages that were iframed from the classic user interface, even after the user agrees to the EULA. This issue is occurring for ADFS, CAC, and AD authentication methods. (Jira ID: EM-67851)
- 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)
- A known issue is causing PDF and XSLX Ticketing report types to fail to generate properly due to an OL8 incompatibility issue. For more information, see: <https://support.sciencelogic.com/s/article/11649>. (Jira IDs: EM-51131)
- After upgrading to 12.2.0 or later, 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 default ("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. (Case: 00412497) (Jira ID: EM-62874)
- Numerous queries against the "Device" endpoint in the ScienceLogic REST API might result in heavy MySQL load. (Jira ID: EM-76429)
- For an Unguided Device Discovery, the **Search** box that displays for creating a new credential does not work. (Jira ID: SLUI-20777)
- The Service Connection for Skylar AI is not available in SL1 12.3.0. For a workaround, see the section [Running the Skylar SL1 Management Script](#) in the **Skylar Analytics** manual. (Jira ID: SLUI-20362)

- The Beta version of Skylar AI does not support collection labels in SL1 when selecting metrics to generate alerts. (Jira ID: SLUI-19834)
- PowerPacks created in SL1 12.3.0 or later cannot be exported to 12.2.x or earlier SL1 systems due to a technical limitation. When creating a PowerPack, you should ensure that it is compatible with the oldest version of SL1 that you intend to install it on. (Case: 00523689) (Jira ID: EM-74812)
- 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.

- 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)
- Classic dashboard reports cannot be scheduled. Attempting to do so results in a "report is blank" error appearing in the system log. (Jira ID: EM-61778)

© 2003 - 2026, ScienceLogic, Inc.

All rights reserved.

ScienceLogic™, the ScienceLogic logo, and ScienceLogic's product and service names are trademarks or service marks of ScienceLogic, Inc. and its affiliates. Use of ScienceLogic's trademarks or service marks without permission is prohibited.

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 herein, the information provided in this document 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 herein at any time without notice.

ScienceLogic

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

International: +1-703-354-1010