SL1 Ibiza 12.3.9 Release Notes

SL1 version 12.3.9

SL1 Ibiza 12.3.9 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 SL1 12.3.9.

The SL1 Ibiza 12.3.9 release includes updates to the Enterprise Key Management Service (EKMS) and Skylar AI, as well as package updates to improve security and system performance. It also addresses several 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 12.3.9 release.

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

- *12.3.0*
- *12.3.1*
- *12.3.2*
- *12.3.3*
- *12.3.4*
- *12.3.5*
- *12.3.6*
- *12.3.7*
- *12.3.8*

NOTE: *AP2 version 8.16.1-43 (Halwa.02)* is installed by default in SL1 12.3.9.

This document covers the following topics:

Before You Proceed

If you are planning to consume SL1 Ibiza 12.3.9, be advised of the following:

- The 12.3.9 release is available only as a patch; there is no ISO version.
- The recommended upgrade paths to version 12.3.9 are outlined below. Be advised that you can perform upgrades from one minor version to a subsequent minor version within the 12.3.x series. However, as with all updates, ScienceLogic strongly recommends that you perform such upgrades in a test environment before implementing the upgrades in production environments.

  The following are the recommended upgrade paths:

  - 12.3.8 > 12.3.9
  - 12.3.7 > 12.3.9
  - 12.2.7 > 12.3.9
  - 12.1.2 (OL8) > 12.3.9

> **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.

- 12.2.x and 12.3.x STIG-compliant users can upgrade to this release via one of the support upgrade paths so long as you have not consumed or upgraded to the 12.3.0 STIG release. If you previously deployed or upgraded to 12.3.0 STIG, you cannot upgrade to 12.3.9 STIG due to a known technical issue.
- If you are on an 11.x MUD system, you cannot upgrade directly to this release; you must first follow the approved conversion process from 11.x MUD to 12.2.1.1 STIG and then upgrade to 12.3.9 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 you must perform a post-upgrade Aurora 2 to 3 conversion.
- SL1 12.3.9 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 12.3.9

This section describes the new features and enhancements that are included in SL1 Ibiza 12.3.9.

EKMS

- Made the following updates to the Enterprise Key Management Service (EKMS):
    - Ensured that EKMS properly syncs with Data Collectors
    - Made updates to support three or more High Availability initializations
    - Addressed additional common issues

Platform and Security

- SL1 version 12.3.9 includes package updates to improve security and system performance. Among other things, these updates address critical vulnerability CVE-2025-49844.

Skylar AI

- Skylar now ingests additional event-related metadata from SL1, including event policy name.

Issues Addressed in SL1 Ibiza 12.3.9

This section describes the issues that were addressed in SL1 Ibiza 12.3.9.

Reporting

- Resolved an issue that caused unhandled exception errors when generating a "PowerPack Information" report. (Jira ID: EM-76056)

Skylar AI

- Resolved an issue that caused the Skylar metadata exporter to crash due to large batch sizes. (Jira IDs: EM-76565, EM-76596)

System Upgrade

- Ensured the MariaDB service fully stops before upgrading packages to prevent the service from crashing. (Case: 00516395) (Jira ID: EM-74025)

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

Upgrading SL1

IMPORTANT: You can consume SL1 12.3.9 only if you are upgrading from an earlier SL1 version that *supports upgrades to this release*. There is no ISO version for version 12.3.9.

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 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 12.3.9

This section includes important notes for upgrading existing SL1 systems to the Ibiza 12.3.9 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 12.3.9.

Recommended Upgrade Paths

The recommended upgrade paths to version 12.3.9 are outlined below. Be advised that you can perform upgrades from one minor version to a subsequent minor version within the 12.3.x series. However, as with all updates, ScienceLogic strongly recommends that you perform such upgrades in a test environment before implementing the upgrades in production environments.

The following are the recommended upgrade paths:

- 12.3.8 > 12.3.9
- 12.3.7 > 12.3.9
- 12.2.7 > 12.3.9
- 12.1.2 (OL8) > 12.3.9

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 Support

Users who are currently on an 11.x MUD system cannot upgrade directly 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.

12.2.x and 12.3.x STIG-compliant users can upgrade to this release via one of the support upgrade paths so long as you have not consumed or upgraded to the 12.3.0 STIG release. If you previously deployed or upgraded to 12.3.0 STIG, you cannot upgrade to 12.3.9 STIG due to a known technical issue.

NOTE: When deploying a STIG-compliant 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.

Aurora 3 Support

AWS deployments that are using Aurora 3 can upgrade to SL1 12.3.9. If you are currently deployed using Aurora 2, you can upgrade to SL1 12.3.9 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 SL1* 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?
12.3.9 (Upgrade only)	10.6.18	Yes
12.3.8 (Upgrade only)	10.6.18	Yes
12.3.7	10.6.18	Yes
12.3.6 (Upgrade only)	10.6.18	Yes
12.3.5 (Upgrade only)	10.6.18	Yes
12.3.4 (Upgrade only)	10.6.18	Yes
12.3.3 (Upgrade only)	10.6.18	Yes
12.3.2 (Upgrade only)	10.6.18	Yes
12.3.1	10.6.18	Yes
12.3.0	10.6.18	Yes
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
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

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 12.3.9, you should clear your system cache to remove cached items from 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 SL1 appliance, see the section on *Required Ports for SL1* 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 until the release of the 12.5.x line.

CAUTION: The upcoming SL1 12.5.1 Juneau release will 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 will proactively migrate 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 upcoming 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.

Use of tmux When Using SSH

Starting with SL1 version 12.3.4, the tmux utility is disabled by default if you are on a non-STIG SL1 deployment and access an SL1 system using SSH. ***This is a change in behavior from versions 12.2.1.1 through 12.3.3, where the tmux utility was enabled by default.***

If you are on a STIG-compliant SL1 deployment, the tmux utility is enabled by default. ScienceLogic encourages non-STIG users enable the tmux utility as well.

The 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.

If tmux is enabled, 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.

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

To enable the tmux utility in non-STIG deployments:

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 to edit the silo.conf file:

```
sudo visilo
```

4. Change the following line in the `[OS_HARDENING]` section of the file to enable tmux:

```
TMUX = true
```

> **NOTE:** If the `[OS_HARDENING]` heading does not already exist in the silo.conf file, you must add that immediately above the `TMUX = true` setting.

5. Save and quit the file. (`:wq`).
6. Log out of SL1 and then log back in. The tmux utility is now enabled.

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.

Known Issues for SL1 Ibiza 12.3.9

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 12.3.9:

System Upgrade

- 12.2.x and 12.3.x STIG-compliant users can upgrade to this release via one of the supported upgrade paths so long as you have not consumed or upgraded to the 12.3.0 STIG release. If you previously deployed or upgraded to 12.3.0 STIG, you cannot upgrade to 12.3.9 STIG due to a known technical issue.
- The `post_update` script might show errors referencing scripts in incorrect directories. A fix for this issue is included in the SL1 12.5.1 release. For more information, see https://support.sciencelogic.com/s/article/16189. (Case: 00481367) (Jira ID: EM-71361)
- In systems that have consumed a large number of SL1 patch imports, the `master_filestore.storage_system_patch` database table might grow too large in size. If this occurs, then when you attempt to log in to SL1, you will be unable to do so and will instead receive an error message stating "The table 'organizations_log' is full" if logging in via the default user interface (AP2), or without an error message if logging in via the classic user interface. To address this issue, you should clean up any previous patch import files after deploying a new version on your SL1 stack. (Jira ID: EM-76040)
- An intermittent issue sometimes causes the database connection to Amazon RDS instances to become unavailable for a brief amount of time during the upgrade process, which causes deployment to be marked as failed in the user interface. If this occurs, re-run the upgrade; doing so should update all backend metadata to register as successfully completed and update the latest version in the user interface. (Jira ID: EM-66627)

Authentication

- 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)

- The use of a percentage character (%) in a password will prevent firstboot from completing. (Jira ID: EM-72924)
- SNMP v3 default authentication sometimes fails on new Message Collectors. A fix for this issue is included in the SL1 12.5.1 release. For more information, see https://support.sciencelogic.com/s/article/16042. (Case: 00482414) (Jira ID: EM-71374)
- The ***Single Instance Login*** setting, which can be set on the **Behavior Settings** page (System > Settings > Behavior), is not working as designed for user accounts that utilize ASCII ADFS authentication. (Jira IDs: SLS-1559)
- Users with expired passwords will get stuck in a loop of transferring sessions and updating their password in the classic user interface. If this occurs, go to the **Behavior Settings** page (System > Settings > Behavior) and set the ***Single Instance Login*** to *Instant* or *Disabled*. (Case: 00520860) (Jira ID: EM-74760)
- If you attempt to reset your SL1 password from the default user interface (AP2), the email link that is provided will direct you to the incorrect page. A fix for this issue is included in the SL1 12.5.1 release. (Jira IDs: SLS-1544)

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.

Credential Management and Discovery

- The ***Search*** box that displays when creating a new credential during unguided discovery does not work. (Jira ID: SLUI-20777)
- 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)
- When selecting two or more SNMP credentials to discover a device, if the first credential with the lower ID number contains incorrect information and the second credential with a higher ID number contains the correct information, the discovery logs will not be able to get an SNMP response. (Cases: 00289639, 00292649, 00422558) (Jira ID: EM-39681)

- On SL1 systems with healthy EKMS installations enabled on a passive node, or in systems where EKMS is disabled altogether, the `slsctl health_check` might mistakenly return a `failure` value. (Jira IDs: SLS-1404)

Device Management

- Clicking the printer icon to print a report on either the **Device Processes** page (Devices > Processes) or **Windows Services** page (Devices > Services) results in a blank page appearing rather than a modal of report options. To work around this issue, go to the **Classic Devices** page (Devices > Classic Devices), click the bar graph icon for the device you want to print a processes or services report for, select either the **[Process]** tab or **[Services]** tab, and then click the printer icon. (Case: 00503774) (Jira ID: EM-73062)
- The ability to assign an icon to a device from the **Devices** page by clicking the **[Actions]** button (ellipsis menu) for that device and selecting *Assign Icon* is not working as intended. (Jira ID: SLUI-19763)
- You might encounter an issue where the **Device Investigator** is missing the options to add device vitals panels for CPU, Memory, or Swap. (Jira ID: EM-76034)
- In 12.3.x SL1 versions, enabling ***Interface index change detection*** in the device class settings of a device can cause missing Interface bandwidth collections if the device has the same MAC address across multiple interfaces. (Jira ID: EM-75060)

Discovery

- When discovering an SL1 appliance using SNMP v2 or v3 credentials, you might see one or both of the following unhandled exceptions in the system log: "UnicodeEncodeError: 'ascii' codec can't encode characters in position 0-2: ordinal not in range(128)" and "TypeError: Incorrect padding". (Jira ID: EM-74484)

Events and Alerts

- If you have an SNMP Trap Filter with a ***Host Filter*** longer than 64 characters, the Event Engine will cause an unhandled exception during trap filtering. To work around this issue, disable that trap filter. If you have multiple hosts in a single filter, you can split those hosts into multiple filters. (Jira ID: EM-74036)
- Any user with basic privileges who has the access hooks EVT_SUPPRESSION_ADDREM, EVT_SUPPRESSION_REG_PAGE, and EVT_MANAGER_REG_PAGE assigned to their user profile can delete event suppressions regardless of their organization membership. (Jira ID: EM-72912)
- SL1 might not generate a "Healthy" event for events that are remediated during a maintenance window. If this occurs, you can clear the event manually. (Jira ID: EM-74713)
- You might experience an issue where device log maintenance mode alerts do not have the correct Event ID or might be missing the Event ID entirely. (Jira ID: EM-74052)

High Availability and Disaster Recovery

- In disaster recovery configurations, Virtual IPs might not transition when promoting a secondary node to a primary node. (Jira ID: EM-76091)

Licensing

- You might encounter a "License record not found" critical event after an appliance's IP address changes, due to the Event Engine using the former IP address to verify the appliance's license information. If this occurs, log in to the appliance using SSH and restart the "EM7 Core: Event Processing Engine" process by running the following command:

  ```
  sudo systemctl restart em7_event
  ```

  (Jira ID: EM-74134)

Logging

- 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)

PowerPacks

- When installing or importing a PowerPack, you might not be able to adjust the PowerPack's embedded license or license key type. (Jira IDs: EM-71507, EM-72515, EM-72716)

Reporting

- 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)
- A new, non-administrator user that has all of the Reporting access keys aligned to their user account cannot create a new scheduler or see the archived reports. (Jira ID: EM-72259)
- Creating an ad-hoc report results in duplicate archived report jobs being created, and ad-hoc reports are deleted shortly after the archived job is created. (Jira IDs: EM-76543, EM-76550)

Skylar AI

- In systems with Skylar AI enabled, the sorting feature for columns on the **Anomaly Detection** page only sorts by the data currently displaying on the page, which might not include all anomaly detection data. (Jira ID: SLUI-22523)
- You might experience data pull "rows behind" events if you have Skylar AI enabled. (Jira ID: EM-76980)

- In systems with Skylar AI enabled, data will not get exported from SL1 to Skylar AI if the ***Time Factor*** field for the "Enterprise Database: Skylar Metadata Exporter" process is set too low. To prevent this situation, go to the **Admin Processes** page in SL1 (System > Settings > Admin Processes), locate the "Enterprise Database: Skylar Metadata Exporter" process, and update the ***Time Factor*** field to 90 minutes. (Jira ID: EM-77019)

System Tools

- On the **OID Browser** page (System > Tools > OID Browser), the *Where Symbolic is like* drop-down option for the ***Search where*** field might not work as intended. (Jira ID: EM-74326)

Support PowerPack

- 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. This issue is fixed in version 109 of the PowerPack, which is included in SL1 12.5.1. (Jira ID: EM-72266)

User Interface

- In the default 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)
- In the classic user interface, when a user is required to reset their password, the new password fields appear far above where they normally would appear. (Jira ID: EM-74342)
- After upgrading to 12.3.2 or later, custom themes and logos might not display on classic user interface pages. To work around this issue, clear the cache of your web browser. (Case: 00503523) (Jira ID: EM-72921)
- In the default user interface (AP2), when opening the **Account Permissions** page (Registry > Accounts > User Accounts > wrench icon) for an existing user account, the ***Theme/Brand*** drop-down field does not initially display on the page. To work around this issue, refresh the page. (Jira ID: EM-76478)
- 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)
- In STIG deployments, the ***DashSL1*** column does not display on the **PowerPack Manager** page (System > Manage > PowerPacks). A fix for this issue is included in SL1 12.5.1. (Case: 00465085) (Jira ID: EM-66815)
- The **Access Keys** page (System > Manage > Access Keys) might not count administrator users in the value displayed in the ***# Aligned Users*** column. To work around this issue, go to the **Account Permissions** page (Registry > Accounts > User Accounts > wrench icon) for the administrator users and re-save their permissions. (Jira ID: EM-74241)

- When you bulk-select multiple event policies to align with a run book automation policy, additional event policies that you did not select might become aligned with that automation policy as well. (Jira ID: EM-70690)
- On the **Organizations** page (Registry > Accounts > Organizations), the filter-while-you-type feature is not working as intended in the ***Skylar AI Status*** column. A fix for this issue is included in the SL1 12.5.1 release. (Jira ID: EM-71414)
- On the **Admin Processes** page (System > Settings > Admin Processes), the **Runtime Offset** column does not display any values. You can view the runtime offset value by editing the process. (Case: 00506663) (Jira ID: EM-73218)
- In the classic user interface, the filter for ***Edit Date*** is not working as intended on the **Inbound Email** page (Registry > Events > Inbound Email). (Jira ID: EM-75291)

Windows Monitoring

- You cannot monitor Windows devices with IPv6 addresses using WMI. You can use PowerShell or SNMP to monitor Windows devices that work with IPv6. (Jira ID: EM-73384)

Known Issues Resolved in Available Releases

Several known issues that are present in 12.3.9 are resolved in the following AP2 releases. You can optionally download and install these releases ***after*** upgrading to 12.3.9 to obtain the fixes to these known issues.

- The following known issues impacting this release are fixed if you upgrade to the *AP2 8.17.23-45 (Ice Pop)* release or later:
    - You cannot 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';`. (Jira ID: SLS-1500)
    - On the **[Events]** tab of the **Device Investigator**, Skylar AI-cleared events cannot be found if you filter for an ***Event Source*** of *Skylar AI* in the **[Cleared Events]** tab. (Jira ID: SLUI-20889)
    - The **Classic Maps** page fails to load properly whenever you attempt to log in to the default user interface (AP2) without accepting the End-User License Agreement (EULA). To work around this issue, create a "Grant All" user account, then sign in to AP2 with the newly created account. (Jira ID: SLUI-20801)
    - Password reset emails direct users to the classic SL1 user interface even when the password reset was requested from the default SL1 user interface (AP2). (Case: 00458525) (Jira ID: SLUI-20939)

- The following known issues impacting this release are fixed if you upgrade to the *AP2 version 8.18.43-81 (Jelly Bean)* release or later:
    - 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)
    - If you attempt to duplicate a business, IT, or device service but that service includes organizations you do not have access to, you will receive an error message. (Jira ID: SLUI-20008)
    - The **Skylar Analytics Summary** panel is displaying an error on Skylar AI-sourced events. (Jira ID: SLUI-22087)
- The following known issues impacting this release are fixed if you upgrade to the *AP2 version 8.20.2-72 (Key Lime Pie)* release or later:
    - In ISO deployments, on the guided discovery pages, bullet points might appear as â¢. A fix for this issue is included in an upcoming release. (Jira ID: SLUI-20614)
- The following known issues impacting this release are fixed if you upgrade to the *AP2 version 8.20.70-45 (Lokma)* release or later:
    - Dashboard auto-refreshing is not keeping user sessions active, even when the ***Page Auto-Refresh Keeps User Session Active*** field is set to *Enabled* on the **Behavior Settings** page (System > Settings> Behavior). For more information, see https://support.sciencelogic.com/s/article/16930. (Case: 00503563) (Jira ID: SLUI-21787)

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

International: +1-703-354-1010