SL1 Ibiza 12.3.0 Release Notes

SL1 version 12.3.0

SL1 Ibiza 12.3.0 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 12.3.0.

The SL1 Ibiza 12.3.0 release includes the following updates and enhancements:

- Support for the *Beta version of Skylar Analytics*, based on the Skylar AI engine, which analyzes SL1 data for anomaly detection, predictive alerting, and new data visualizations.
- Updates to meet requirements for the Federal Risk and Authorization Management Program, better known as *FedRAMP*.
- Multiple *package updates to improve security and system performance*.
- *Global Manager SSO configuration updates and stackDiff options*.
- Improved database performance and scalability with *MariaDB 10.6*.
- Enhanced Python capabilities with *Python 3.11*.
- Updates to the SL1 user interface from AP2 releases Espresso, French Toast, Gelato, and Halwa, including the following new features:
  - A new *Skylar AI page*, and a *rebrand of Zebrium to Skylar Automated RCA*.
  - A new *Skylar Analytics Summary widget* on the **Event Investigator** page.
  - Enhancements to the *Service Investigator page user interface*.
  - A new *Relationships and Membership panel* on the **Device Investigator** page.
  - Improved data visibility and management for *dashboard widgets*.

These release notes provide a comprehensive list of the features, enhancements, and addressed issues that are included in the SL1 Ibiza 12.3.0 release.

NOTE: Some of the features, enhancements, and addressed issues that are included in this SL1 platform release were originally included in the following SL1 AP2 releases:

- *8.7.37 (Espresso)*
- *8.7.96 (French Toast*)
- *8.14.26 (Gelato)*
- *8.16.1.14 (Halwa)*

AP2 version 8.16.1.14 (Halwa) is installed by default in SL1 12.3.0.

This document covers the following topics:

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 12.3.0, be advised of the following:

- You must currently be on a version of SL1 with all appliances running on Oracle Linux 8 (OL8) before you can upgrade to this release.
- You can upgrade to this release directly from SL1 12.1.2, 12.2.1.1, and 12.2.1.2.
- Due to release timing, SL1 12.1.3 cannot upgrade directly to any release prior to 12.3.1 (future release).
- Due to release timing, 12.2.4 cannot upgrade directly to 12.3.0.
- For customers deployed on DoDIN, 12.3.0 is not yet DoDIN-certfied.

For more information, see the ***Important Upgrade Notes*** and ***Known Issues*** sections.

New Features and Enhancements in SL1 Ibiza 12.3.0

This section describes the new features and enhancements that are included in SL1 Ibiza 12.3.0.

Skylar AI (Beta)

- What's new: ***The Skylar AI page in SL1 represents the Skylar AI engine, which gathers and analyzes data from SL1 for anomaly detection and predictive alerting***. Added the new **Skylar AI** page to the left-hand navigation and the **Advanced Menu** page. This page lets you directly access key Skylar AI components.
- The following list contains some of the types of data that SL1 can send to the Skylar AI platform, where the data is analyzed and used by Skylar Automated RCA, anomaly detection, and predictive alerting:
    - Alert and event logs
    - Availability data collected by SL1
    - Business service health, availability, and risk metrics
    - Class-Based Quality-of-Service (CBQoS) metadata and CBQoS time series data
    - Data from Gen 1 SL1 agents, which use the SL1 Distributed Architecture
    - Data from Gen 3 SL1 agents, which use the SL1 Extended Architecture. For more information on how to configure the Gen 3 SL1 agent for Skylar AI, see the ***Monitoring with the SL1 Agent*** manual.
    - Dynamic Application performance data
    - Topology data for L2, L3, CDP, LLDP, and ad hoc relationships between devices
    - DCM(+R) relationships
    - Metadata for web content, SOAP/XML transaction, and domain name monitors
    - Process and service data
- Added a ***Skylar AI Status*** column to the **Organizations** page (Registry > Accounts > Organizations) that displays whether the Skylar AI is enabled or disabled for a specific organization. By default, the Skylar AI features are disabled. You can select one or more organizations and use the ***Select Action*** drop-down to enable or disable Skylar AI.
- **For more information**: See *Introduction to Skylar Analytics*.

Additional Skylar AI Updates

- Added the "Enterprise Database: Skylar Alerts Poller" process to the **Admin Processes** page (System > Settings > Admin Processes). This process polls for all types of existing SL1 alerts, including Skylar AI alerts, and adds the alerts to the corresponding SL1 alert table.
- The **anomaly-alerts-poller** process was renamed **skylar-alerts-poller**. You can monitor this service on the **Admin Processes** page (System > Settings > Admin Processes).

- The Skylar AI logo in the main navigation menu now adjusts its color based on whether you are using a light or dark theme.

Anomaly Detection

- **What's new:** The **Machine Learning** page was renamed **Anomaly Detection**, and the **Machine Learning Thresholds** page was renamed **Anomaly Detection Thresholds**.

> **NOTE:** To access the **Anomaly Detection** page and the **Anomaly Detection Thresholds** page, go to the **Skylar AI** page in SL1 and click the corresponding button.

- The **Anomaly Detection** page (formerly the **Machine Learning** page) now lists every Dynamic Application metric with its Anomaly Detection status, including metrics that will not alert when the anomaly score goes too high.
- For an SL1 system that is connected to a Skylar AI system, the ***Anomaly Detection*** column was removed from the **Anomaly Detection** page, as this column is no longer relevant with this release. Any devices listed on the **Anomaly Detection** page have anomaly detection enabled by default. This column was also removed from the **Device Investigator**, **Event Investigator**, and **Service Investigator** pages that contain anomaly detection data.
- **For more information**: See *Introduction to Anomaly Detection*.

Additional Anomaly Detection Updates

- All instances of the "Anomaly Index" were renamed to "Anomaly Score".
- The **Anomaly Detection** page contains a ***Last Modified*** column with the localized date and time that a metric was last changed.
- To assist with troubleshooting, the **Audit Log** page (System > Monitor > Audit Logs) is updated when an anomaly detection metric is enabled or disabled, and includes the user who performed the action.

Events

- **What's new:** ***New Skylar Analytics Summary panel***. Added a new **Skylar Analytics Summary** panel to the **Event Investigator** page to show predictive alerts from Skylar AI. Predictive alerts work like events in SL1, except they forecast when a future event could happen, instead of reporting on an event that has already occurred. The **Skylar Analytics Summary** panel displays a graph of data from Skylar AI that corresponds with the event ID.
- Added *Skylar AI* to the ***Event Source*** drop-down option. You can also filter your search by events sourced by Skylar AI on the **Event Policies** pages.
- On the **Event Policy Editor** page, the ***Skylar AI Severity*** drop-down for *Skylar AI*-sourced events now defaults to *Disregard Severity*.
- **For more information**: See *Defining and Editing Event Policies*.

Additional Event Updates

- SL1 de-duplicates the events generated by Skylar AI that align to the same device and file system (sub-entity).
- Replaced the text editor on the **Event Policy Editor** page with a front-end HTML editor for enabling text-editing capabilities for web applications and related software.
- You can now search event notes in both the basic and advanced search on the **Events** page.
- Updated the error messages in the **[Suppression]** tab on the **Event Policies** page for policies with invalid device IDs.
- A new *Event Table Preferences* sub-menu is now available on the **Grid Settings** menu on the **Events** page. This sub-menu includes the following toggles:

    - *View Event Masking*. Shows or hides the ***Masked Events*** column.
    - *Row Severity Highlighting* Show or hides color-coded highlights to rows on the events inventory table that correspond to the severity color of the event.

- Added a notification window to the **Events** page that explains the changes to sorting on the page. You can close the notification window, and you can dismiss it permanently by checking the **Don't show this again** checkbox.

Business Services

- **What's new:** ***Enhancements to the Service Investigator and Business Services pages.*** The **Business Services** and **Service Investigator** pages have been updated to include new features, such as new information in the **Timeline** panel on the **Service Investigator** page.

  The following updates were made to support this enhancement:

  - Updated the Zebrium icon to the Skylar AI icon in the **Timeline** panel of the **Service Investigator** page.
  - The ***Last Edited*** field in the **Overview** panel at the top of the **Service Investigator** page now displays the date the service was last edited.
  - Added a ***Refresh Interval*** column to the **Business Services** page. This column, also known as the polling frequency, displays the frequency at which data is communicated between a device and another system.
  - Added a new ***Predictions*** field to the **Skylar AI** section on the **Timeline** panel. This field also appears in the pop-over modal when moving your cursor over a certain point in time on the panel. The ***Predictions*** field shows predicted future events in the form of visual swim lanes, which are visual flowcharts that show a process from start to finish for an event.
  - Renamed the **[Log Insights]** tab to **[Skylar AI]** at the bottom of the **Timeline** panel. The **[Skylar AI]** tab includes events that are predicted by Skylar AI.
  - Consolidated the ***Confirmed*** and ***Suggestions*** fields to create a single ***Log Insights*** field in the **[Skylar AI]** tab of the **Timeline** panel.

- **What's new:** ***Improved Service Policies page.*** The **Policies** page was renamed the **Service Policies** page, and the following columns were added to the page: ***Status***, ***Service Count***, ***Date Edited***, and ***Last Edited By***.
- Updated the status policies for "Aggregate," "Business," and "IT" services and their corresponding rules for calculating health, availability, and risk values.
- You can now enable or disable services in bulk on the **Business Services** page.
- The "onDemand" process currently retrieves data by calculating the "lastValue" in the last three intervals. If the value of the two most recent intervals is null, the system will log the calculation as incomplete because metrics did not exist during that time.
- **For more information**: See *Using the Service Investigator*.

Additional Business Service Updates

- The **Timeline** panel on the **Service Investigator** page now shows the health, availability, and risk statuses of your events in the last 7 days by default.

- Updated the default Business Services policy so that device availability reflects the active status of constituent devices for physical and component devices.

  The following updates were made to support this enhancement:

  - Replaced availability vital metrics and the "All Devices" filter with "isActive=True".
  - Replaced the aggregation type of "Availability" with "Count".
  - Set the rule to "Available" if at least one device in the service has the "IsActive=True" filter.
  - Updated the default aggregation factor for IT, Business, and Services Model service policies from "Average" to "Minimum".
- On the **[Service Policy]** tab for a service, when you try to delete a service policy, the **Delete Policy** dialog displays if any services are currently using that policy; if the policy is deleted, those services will revert to using the default service policy.
- Enabled auto-clear for the ServiceNow event policies, which can be found in the "Integration Service Action Type" PowerPack version 105.

Device Management

- **What's new:** ***Added a new Relationships and Membership panel to the Device Investigator***. Added a new **Relationships and Membership** panel to the **Device Investigator** page. The new panel displays details about the other devices and services that have relationships to the selected device.
- You can now edit Device Investigator layouts, copy layouts, and save existing layouts with different names.
- The Device Investigator **[Machine Learning]** tab was renamed **[Anomaly Detection]**.
- **For more information:** See ***Using the Device Investigator.***

Additional Device Updates

- Updated the method for performing bulk actions to multiple devices on the **Devices** page. Previously, you could select from several action-specific icons at the top of the page. With this update, those icons have been replaced by an ***Actions*** drop-down menu that includes a list of the following available bulk actions:
  - *Add to Device Group*
  - *Align SNMP Read Credential*
  - *Change Collection State*
  - *Change Collector Group*
  - *Change User Maintenance Mode*
  - *Clear Device Logs*
  - *Schedule Maintenance*
- In the Basic Menu and Advanced Menu, the **Device Manager** option was relabeled to **Classic Devices**.

- When adding devices using the guided discovery process from the **Discovery Sessions** page (Devices > Discovery Sessions), devices for which your SL1 system does not have the required entities will now appear in a secondary section at the bottom with a new warning note. This note will specify why you cannot add the selected device and the necessary prerequisites.
- On the **Devices** page, a new ***Asset ID*** column displays the ID of any asset associated with a device in the list. The asset ID displays as a hyperlink that you can click to view the asset's properties.
- When deleting one or more devices that have associated asset records, you now have the option to delete the associated assets at the same time.
- Device discovery now encodes all data using JSON instead of pickle.
- Added an API endpoint for device groups that enables you to filter by the device group's collective state using a scale of 0 to 4, where 0 is healthy, 1 is notice, 2 is minor, 3 is major, and 4 is critical. For example, if you wanted the API to return a list of no more than 10 device groups with a collective state of major, listed in ascending order by their device group ID, then you could enter the following URI into the API browser: `/api/device_group?extended_fetch=1&limit=10&filter.0.state=3&order._id=asc.`

Dashboards

- **What's new: *Improved data visibility and management for Dashboard widgets*.** Improved data visibility and management for widgets on the **Dashboards** page. Widgets can display different scale prefix options for non-percentage-based metrics. You can select one of these scale prefixes, such as *Kilo*, *Mega*, *Giga*, or *Tera*, if you want dashboards to auto-scale the visualization of metrics that have the same metric unit prefix.

  To use this feature, select the ***Scale prefix*** drop-down field in the ***Metrics & Properties*** column of the **Edit Widget** page, then select a unit of measurement to use from the drop-down field.

  The following updates were made to support this enhancement:

  - The widgets that use the following visualizations allow you to select different scale prefix options for non-percentage-based metrics: Bar Chart, Table, Line Chart, Number, Leaderboard, Leaderboard Bar Chart, and Forecast.
  - The ***Select Visualization*** drop-down list on the **Create Widget** page now lists the available visualization options in alphabetical order.

- **For more information**: See *Creating and Editing Dashboards*.

Additional Dashboard Updates

- Added navigation in SL1 to the **Device Dashboards** page (System > Customize > Device Dashboards) in the classic SL1 user interface.
- Removed the 50-return limit for ***Interface*** widgets with the *Table* visualization and added infinite scrolling.
- Updated and organized information in the footer of tables, such as the total, selected, and filtered counts.

- Added a new Device Groups widget to the Dashboards page. This widget contains a table visualization with the following columns: ***Name***, ***Severity***, and ***Device Count***. You can sort the table by ***Name*** and ***Severity***, but you will not be able to sort the table by Device Count until a future release.

Additional New Features and Enhancements in SL1 Ibiza 12.3.0

This section describes the new features and enhancements that were added in SL1 Ibiza 12.3.0.

Agent

- Updated the "Host Agent" PowerPack to v103, which includes the Python 3 execution environment. The PowerPack also updates the "Host Agent: System Config" and the "Host Agent: System Perf" Dynamic Applications to run Python 3.
- In the "ScienceLogic: Agent" PowerPack, updated the execution environment to Python 3 for the "ScienceLogic: Agent System Configuration" and "ScienceLogic: Agent System Performance" Dynamic Applications.
- Added the **agent_gen_type** field to the **master_dev.legend_device** database table. This field is set to 1 when adding a Gen1 agent or to 3 when adding a Gen 3 agent.
- If an agent did not successfully upgrade in the user interface, the installation process will now stop trying to upgrade and the agent will resume streaming with the previously installed version.
- For agent-based log collection on a device with a Windows agent, the minimum Windows agent is version 108. For agent-based log collection on a device on Linux, the minimum Linux agent is version 147. You can perform an upgrade by clicking the **[Upgrade]** button on the **Agent** page in SL1 or by downloading and upgrading the agent manually.
- Dogs can't operate MRI machines. But cats can.

Billing and Telemetry Collection

- Removed "Feature usage metrics collection complete" from the system log.

Credentials

- SL1 12.3.0 includes package updates to the Enterprise Key Management Service (EKMS) to improve security and performance.
- When creating a new credential, a search box displays that lets you review a list of credential types organized by *Core Credentials* and *Universal Credentials*.

Data Collection

- As part of the future deprecation of Python 2 support in SL1, the "EM7 Core: Python Env Deploy" admin process is now disabled.

Database Tool (DB Tool)

- For non-STIG environments, the **Database Tool** page (System > Tools > DB Tool) is available with this release of SL1.

FedRAMP Compliance

- SL1 now logs appliance IP address changes in the audit logs.
- Audit logging was enhanced to include session ID renewal events.
- The new **/etc/cron.d/credentialsrotate cron** job lets you schedule an Enterprise Key Management System (EKMS) credentials rotation. Additionally, the `slsctl credentials rotate` command will not run unless executed on the active Database Server to ensure the command properly runs. This job is disabled by default.
- An event will be generated on the **Events** page whenever the Enterprise Key Management Service (EKMS) experiences a fatal error.
- On a STIG system, you can use the ***Command Line Interface Login Message (STIG only)*** field on the **Login Alert Message** page (System > Settings > Login Alert Message) to change the banner text that appears after you sign into an account that has access to the SL1 command-line user interface. You cannot enter or input HTML code in the text banner.

Global Manager

- The single sign-on (SSO) configuration process is now the default configuration for all Global Manager systems. For more information, see the ***SL1 Global Manager*** manual.
- Changing the name of your global manager stack will retrieve and return the correct version information.

GraphQL

- Updated the GraphiQL browser-based user interface to match the SL1 theme, and added the GraphiQL user interface to SL1 on the **GQL Browser** page (System > Tools > GQL Browser). You can also make GraphQL queries or mutations using the GraphQL Yoga engine.
- Removed both the **enabled** and **status** fields from "aiMachineLearningMetricAnomalies" device queries in GraphQL and added an **alerting** status. The **alerting** status will send an alert whenever the anomaly score exceeds a set threshold, and then send an alert that maps to an event of the appropriate severity.
- Added a "deviceGroup" search parameter to the "relatedNodes" query in GraphQL to support the **Relationships and Memberships** panel in the **Device Investigator**.
- Updated the "deviceMetrics" API by adding new endpoints that enable any monitor-related data to be queried as a new "collectionType" object.
- In Global Manager mode, the "organizationsByGUID" query now has a stackDiff type that can also be queried.
- In Global Manager mode, when making a query to PowerPacks or device categories, a stackDiff will be accessible on any of the fields in for that query.
- The SL1 "stack" identification field in GraphQL is now discoverable. This update allows Global Manager to more effectively manage stacks.

- Added the ability to search Dynamic Applications associated with specific presentation IDs by adding "presentationID" as an "IDSearch" variable for the existing "DynamicApplicationSearch" function. This update enables you to search Dynamic Applications by finding the corresponding APIs associated with specific presentation IDs.
- Added a new status variable to the GQL API for device groups. This variable represents the device statuses within a device group as a singular unit.
- When you run a GraphQL query for an "Appliance" type, you will also get the current operating system version for that appliance.
- Added a "createAssetsForDevices" mutation that allows device assets to be created through GQL.
- Added an "addDevicesToDeviceGroups" mutation that can add one or more devices to a device group in GQL.
- Removed the "experimental" labels from several GraphQL resources that are now standard fields.
- The **Business Services** page now uses a new GraphQL query that collects metric anomalies for your devices.
- Added a "powerPack" field to the guidedDiscoveryWorkflow(s) GraphQL queries. This field displays the PowerPack ID. If the guided discovery workflow contains a reference to a PowerPack that is not installed on the system, it will return a placeholder object with its "powerPack", with the "name" displaying as "N/A" and the "id" as "-1".
- Added the "accessKey" resource to GQL. An "accessKey" will have "accessKeyHooks" as sub-resources, and both have their own type of Category as sub-resources.
- Added an "id" field to the "systemInformation" query. The "id" field contains a value that represents the system or stack ID. The system ID is only available on systems running SL1 version 12.3 or later.

Inbound Messaging

- Added the ability to enable TLS encryption for incoming email. For more information, see the ***General Inbound and Outbound Email Settings*** in the ***Configuring Inbound and Outbound Email*** manual.

MariaDB

- Updated SL1 to enable upgrading MariaDB from the 10.4 line to the 10.6 line.
- Updated the `vimysql` command to handle configuration changes for MariaDB 10.6. The `vimysql` command automatically removes deprecated options from the configuration upon saving.
- Upgrades to the MariaDB server and client package are now handled in a single transaction during the MariaDB upgrade phase. The client package is no longer upgraded during the system update on most SL1 appliance types, with the exception of Administration Portals and Data Engines.
- When upgrading MariaDB, the "module_upgrade_mariadb" script that was previously used has been deprecated. With this release, users should now use the command "siloupdate upgrade-mariadb" to upgrade MariaDB packages on appliances in your SL1 stack.

Platform and Security

- This release includes multiple package updates to improve security and system performance.
- The FedRAMP deployment on Amazon RDS will enforce that all connections made to the MySQL database must use TLS. The "nextui" service is now responsible for regulating all secure connections to the database.
- Added primary keys to specific database tables to improve performance of queries during medium-frequency collection. The improved queries prevent medium-frequency collection from falling behind and causing an outage.
- When logging in for the first time with a new SL1 user account, a **Notice** dialog appears, prompting you to accept an agreement that you may use the product only in accordance with the applicable contract and within the scope of the rights purchased by your organization. To accept, check the box and then click **[Agree]**.
- Deployments on AWS now utilize Aurora 3.04.0 (MySQL 8.0) and RDS R7g.
- This release includes upgrades to Kubernetes 1.29.
- Updated the Config Push command so that users have the option to disable cleanup of temporary files by setting the value of "clean" in a [CONFIG_PUSH] section in the **/etc/silo.conf** file.
- When deploying or upgrading to SL1 12.1.2 or later, the root partition has been increased from 10 GB to 20 GB and now uses GPT as the default partitioning scheme.

PowerPacks

- Updated the "EM7 Dashboards Widget" PowerPack to version 7.6.
- The "ScienceLogic Support Pack" PowerPack version 107 was updated to use Python 3.
- The 12.3.0 ISO includes the following updated PowerPacks:
  - Host Agent version 103
  - ScienceLogic: Agent version 102
  - SL1 Core Reports version 119, which includes updates from the Interface Billing report
  - Generic Switch/Router MIB Support version 105
  - Host Resource Core Pack version 108.1
  - F5 BIG-IP version 105
  - ScienceLogic: PowerFlow Monitoring version 107

Python 3 Support

- Additional core SL1 features have now been updated to support Python 3. Unless otherwise noted in the SL1 documentation, this does not result in any behavior change.
- Removed support for Python 3.9 and added support for Python 3.11 for SL1 12.3.0 and execution environments so that they are more independent and deploy more reliably.

- The script that updates the database schema post-update now runs in Python 3. The `pcli list-patches` command is deprecated, but the equivalent command `siloupdate list-patches` is now be available.
- The SL1 SNMP Agent was updated to support Python 3.
- As part of the future deprecation of Python 2 support in SL1, the "EM7 Core: Python Env Deploy" admin process is now disabled.
- Why are the pyramids in Egypt? Because they were too heavy to take to the British Museum!

Run Book Automation

- Snippet action policies can only include object types that can be serialized and deserialized by JSON data formats.
- Added proxy support for the run book action type of "Send an AWS SNS message".
- Added the "%_service_investigator_url" variable option for automation actions that run against events aligned with business services.
- In the classic user interface, you can now align a run book automation policy with one or more SL1 business services.

ScienceLogic Libraries and Execution Environments

- Removed support for Python 3.9 and added support for Python 3.11 for SL1 12.3.0 and execution environments so that they are more independent and deploy more reliably.

NOTE: The option to use Python 3.9 execution environments is limited to SL1 12.2.1.1 and later 12.2.x releases. Any Dynamic Applications that use Python 3.9 execution environments will stop working after upgrading to SL1 12.3.0 or later. If you are currently using Python 3.9 execution environments, then after updating to 12.3.0 or later, you ***must*** create a Python 3.11 execution environment and align any Dynamic Applications that are currently aligned to the Python 3.9 execution environments to the Python 3.11 execution environment to make them work again.

- Added the new library, "sl-snippet-api", to SL1 version 12.3.0. This library is a clone of the current "silo-apps" library used for both SL1 platform and PowerPack updates.

System Update

- A new package, "sciencelogic-release", has been added to SL1. This package carries the GnuPG (GPG) public key that is used for verifying package signatures. This RPM is included in the patch hook package. If you are upgrading from a previous version of SL1 and you receive an error indicating that the public key was not installed during pre-upgrade, then you must run the patch hook package again after installing the latest version of siloupdate to ensure the new "sciencelogic-release" package is included in your system.

User Interface

- Throughout SL1, references to "Zebrium" have been changed to "Skylar AI."
- Throughout SL1, references to "Machine Learning" and "Metric Anomalies" have both been changed to "Anomaly Detection".
- Added a footer to the user interface that includes the current SL1 version and build number. Optionally, if you have selected the ***Display Previous Login In Footer*** checkbox on the **Behavior Settings** page (System > Settings > Behavior), this footer can also display the time stamp of your last successful or failed login attempt.

Webhooks

- Removed the webhook container service from SL1 and replaced it with a new RPM that gets installed as part of the SL1 upgrade. The webhook collector service no longer appears in Docker images or containers on SL1 message collectors or All-in-One systems. Added a systemd alias so that `systemctl` commands will work for both service names (webhook-collector and webhook_collector) for backwards compatibility. For example: `sudo systemctl webhook-collector` and `sudo systemctl webhook_collector` commands will provide the same output.

Issues Addressed in SL1 Ibiza 12.3.0

This section describes the issues that were addressed in SL1 Ibiza 12.3.0.

Agent

- Addressed an issue for Gen 3 Agents where hidden file systems no longer generate alerts when their thresholds are exceeded. (Case: 00397779) (Jira ID: EM-62221)
- Addressed an issue in which the agent did not appear updated in the user interface due to an improper return value from the agent version request. (Case: 00452046) (Jira ID: AP-2858)
- Addressed an issue in which agent installation impacted proper process monitoring on Linux servers. (Case: 00422712) (Jira ID: EM-64110)
- Addressed an issue with case-sensitivity that affected process monitor matching. (Case: 00415514) (Jira ID: EM-62573)

Assets

- Addressed an issue where an asset with the highest precedence was not getting assigned the expected collection object value. (Case: 00452509) (Jira ID: EM-67910)

Authentication

- Addressed an issue that occurred after updating your Database Server and/or Administration Portal passwords using the Web Configuration Utility on port 7700. Before this update, you might have experienced an "Unexpected end of JSON input" error when you attempted to log in to the default SL1 user interface (AP2). (Jira ID: EM-64285)
- Resolved an issue that was preventing users from logging in using the default login page if the ***Single Instance Login*** setting was enabled. (Jira ID: SLS-1228)
- Resolved an issue in which users could not log in to the default user interface if their password contained a colon (:) character. (Cases: 00271595, 00298673) (Jira ID: SLS-549)
- Updated access logs to ensure the session duration value is correct for expired sessions. (Case: 00323782) (Jira ID: EM-57920)

Billing and Telemetry Collection

- Addressed an issue with the billing process to ensure data delivery to ScienceLogic generates proper billing. (Case: 00415301) (Jira ID: PTEL-1795)

Business Services

- Resolved an issue where the classic "Custom IT Service" widget was not displaying the health, availability, and risk values. (Case: 00396418) (Jira ID: EM-62196)
- Resolved an issue where business service status policies were incorrectly calculating the health state of services. (Case: 00421078) (Jira ID: SLUI-19584)

Credentials

- The "Enterprise Database: Subscription Usage Crunch" process now starts up without an SL1 Data Collector being added to the SL1 environment. (Case: 00441230) (Jira ID: EM-65230)
- SSH credential tests that use a private key now work in SL1 environments using a STIG-compliant or Military Unique Deployment (MUD) configuration. (Case: 00353453) (Jira ID: EM-58881)
- Updated the ***SNMP Credential Read/Write*** fields to display empty fields and values correctly. (Case: 00223980) (Jira IDs: EM-66571, EM-67909, EM-49241)
- The Credential Tester for SSH credentials now supports both RSA and ECDSA keys in PEM format. (Case: 00425786) (Jira ID: EM-63927)

Data Collection

- SL1 now clears out orphaned data in the **last_config_poll** table when a Dynamic Application is unaligned from an agent on Extended SL1 systems. (Case: 00393205) (Jira ID: EM-61998)
- Moved a "noisy" log message that SL1 generates during the post-processing of performance Dynamic Applications to Debug level to prevent SL1 from generating unwanted events and sending unnecessary information to the logs. (Case: 00426127) (Jira ID: EM-64286)

- Addressed an issue where an exception occurred when sending data that contained a non-UTF character to a collector. (Case: 00431098) (Jira ID: EM-65135)
- When SL1 encounters a device whose neighbor has an IP address that is an empty string, it will no longer create an unhandled exception in the system log. (Case: 00453299) (Jira ID: EM-66229)
- Addressed an issue that was causing a "PowerShell Communication" error, followed by one or more "PowerShell Request" errors, whenever the pypsrp module was enabled and events relating to a failure to connect to a Windows device were triggered in SL1. With this change, only the communication error is now generated, which is in line with the behavior expected when pypsrp is not being used. (Cases: 00397479, 00419026) (Jira ID: EM-64179)
- Addressed an issue in which the **device_processes** table lacked a primary key, resulting in degraded performance. (Case: 00368813) (Jira ID: EM-60403)
- The Cisco Discovery Protocol (CDP) process no longer stops data collection upon receiving invalid IP addresses. Instead, the CDP process collects and returns data found on the next Cisco device or hardware it finds. (Case: 00422541) (Jira ID: EM-64160)
- Improved the performance of MySQL queries in systems with a large number of component devices with dynamic component map (DCM) relationships. (Case: 00457073) (Jira ID: EM-66343)

Data Maintenance and Retention

- Updated the SL1 product documentation to explain that setting a threshold of 0 for the ***Device Logs Max*** field on the **Data Retention Setting** page will result in all device entries being deleted. (Case: 00264306) (Jira IDs: EM-52283, EM-52749)
- Resolved an issue where the daily maintenance process started in debug mode despite turning it off. (Case: 00353450) (Jira ID: EM-59121)
- The Dynamic App Frequency override table in the SL1 central database will be cleaned up when a device is deleted from SL1 to prevent orphaned records. (Case: 00439434) (Jira ID: EM-65206)
- Resolved an issue that was causing hourly maintenance to end abruptly while updating component device availability statuses. (Case: 00443537) (Jira ID: EM-65600)

Device Management

- The **Device Groups** modal, from the **Actions** menu of the **Device Properties** view, now shows device groups where the device is a static member and where the device matches on a dynamic rule for device group. (Cases: 00329711, 00363057, 00401505) (Jira ID: EM-57212)
- On the **Device Properties** view (Devices > Classic Devices > wrench icon or Registry > Devices > Device Manager > wrench icon), the list of collector groups in the second ***Collection*** field now display in alphabetical order. (Case: 00318934) (Jira ID: EM-56116)
- The process of deleting of a log monitoring policy now completes successfully and automatically update the **Log File Monitoring** page (Registry > Monitors > Logs). (Case: 00416759) (Jira ID: EM-63379)
- You are now prevented from deleting a log monitoring policy in the user interface if that policy is still aligned to a device template. (Case: 00419711) (Jira ID: EM-63550)
- Addressed an issue where, when deleting a device from the **Devices** page from the ***Actions*** menu, the **Delete Devices** modal displayed for an indefinite period of time. (Jira ID: SLUI-19738)

- Added an index to the spool process table, which enables the cleanup activity from a device deletion to complete in a shorter amount of time. (Case: 00396342) (Jira ID: EM-62175)
- Saving properties of a component device no longer display an error that there were incorrect properties sent. (Case: 00329722) (Jira ID: EM-57376)
- Addressed an issue that was impacting the ability to configure PHP developer log settings in **/opt/em7/backend/silo_php/php_devlog_config.php**. (Case: 00434698) (Jira ID: EM-64787)
- User-initiated changes in maintenance mode that are performed on one or more devices are now logged in the SL1 Audit Logs. (Case: 00308320) (Jira ID: EM-55115)
- Added a task that handles orphaned DCM+R links for deleted devices to the "EM7 Core: Daily Maintenance" process. (Case: 00425487) (Jira IDs: EM-64127, EM-64562)
- Addressed an issue where an unhandled exception occurred when the "Enterprise Database: Topology Crunch" process encountered a network interface with no physical address discovered. (Case: 004461878) (Jira ID: EM-65537)

Discovery

- Addressed an issue that was causing high-frequency rows behind exceptions during nightly discovery due to the creation of a large number of storage objects. (Case: 00431977) (Jira ID: EM-65195)
- An interface with unexpected characters in its properties no longer blocks SL1 from discovering the device that contains that interface. (Case: 00411856) (Jira ID: EM-62795)

Events

- Resolved an issue that caused high latency when loading events on the **Events** page. (Case: 00455708) (Jira ID: SLUI-20411)
- Events raised for an expired SSL certificate on a device are now properly cleared when the certificate is renewed and an event for this is raised. (Cases: 00316477, 00336592, 00422336) (Jira ID: EM-56192)
- Addressed an issue that caused event suppression to stop working with device groups after upgrading from an SL1 11.x release. (Cases: 00376097, 00377769, 00379446) (Jira IDs: EM-60621, EM-61157)

Global Manager

- Resolved an issue that was causing some Global Manager pages to not load due to child stacks returning an HTTP 502 error, resulting in users having to manually disable monitoring of those child stacks. (Case: 00466624) (Jira IDs: EM-66978, SLUI-20184)

GraphQL

- Addressed an issue that caused several device-related GraphQL fields to always be null, which was resulting in a mismatch in the device data that displayed in the default SL1 user interface (AP2) compared to what displayed in the classic SL1 user interface. (Case: 00461621) (Jira ID: SLUI-20515)

Inbound Messaging

- Addressed an issue where incoming emails have unexpected newline characters in the subject, which could cause run book automations to fail. (Case: 00414903) (Jira ID: EM-63707)
- Addressed an issue where unhandled exceptions occurred when processing incoming email with text/html type. (Case: 00446967) (Jira ID: EM-65550)

Logs

- Addressed an issue with PHP log rotation that created a large number of empty php-error*.backup log files. (Case: 00463868) (Jira ID: EM-70694)

Platform and Security

- Addressed cross-site scripting vulnerabilities on the **Domain Name Monitoring** page (Registry > Monitors > Domain Name). (Jira ID: EM-65918)
- Created a ping6 symlink to ping to address IPv6 ICMP-based latency monitoring. (Case: 00434419) (Jira ID: EM-65261)
- Added additional error-handling and debug logging to L2 topology collection. (Case: 00444011) (Jira ID: EM-65416)
- Addressed misspellings in the **event_print_ajax.inc** file. (Case: 00434738) (Jira ID: EM-64781)
- Addressed an issue where the "Support: Configuration File Validation" Dynamic Application failed to work after converting the Database Server to Oracle Linux 8 (OL8). (Case: 00445813) (Jira ID: EM-65529)
- Addressed an issue where a duplicate policy was created when a user tried to apply a new Windows service monitoring policy to a device where there is already a policy for the same service. (Case: 00307995) (Jira ID: EM-55205)
- Updated access logs to ensure the session duration value is correct for expired sessions. (Case: 00323782) (Jira ID: EM-57289)
- Addressed an issue that was causing race conditions in the em7 scheduler service. (Case: 00461925) (Jira ID: EM-66634)

PowerPacks

- Addressed an issue with the Oracle client cx_oracle that prevented the "Oracle: Database" PowerPack v105 from working on SL1 12.2.1.x. (Jira ID: EM-64241)
- Resolved an issue where a query was causing delays when deleting PowerPacks. (Case: 00412935) (Jira ID: EM-62958)

ScienceLogic API

- When doing an extended fetch, the interface API now returns the correct list of **interface_ips**. (Case: 00424505) (Jira ID: EM-63865)

System Update

- The patch import process now checks for the number of files associated with the patch file version ID, and will fail the import state if there are no packages associated with the version ID. This will prevent staging errors, because the staging button will not be enabled. (Case: 00155465) (JIRA IDs: EM-42122, EM-61356)

User Interface

- Resolved an issue where **Event Console** page was not accessible after upgrading SL1. (Case: 00380651) (Jira ID: EM-61214)
- Addressed an issue in which users experienced timeout errors when opening the **Subscribers** window for Dynamic Applications on the **Dynamic Applications** page (System > Manage > Dynamic Applications > Click "Subscribers" Button for an Application). (Jira ID: EM-63732) (Case: 00421340)
- Ensured that the ability to edit the Privilege Keys granted in a user account work as intended. Specifically, if a user has a "user" account type with a defined user policy assigned to their account, then the **Privilege Keys** section of their **Account Permissions** page (Registry > Accounts > User Accounts > wrench icon > Permissions) should be disabled. (Case: 00421121) (Jira ID: EM-63599)
- Addressed an issue where two pop-up windows or modals appeared on an iframed "classic" user interface (EM7) page in the SL1 user interface. (Case: 00426636) (Jira ID: EM-64507)
- Added the ability to expire 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: (Case: 00416571) (Jira ID: EM-63240)
  - 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)

Recently Deprecated Features

The 12.3.0 release deprecates the following PowerPacks and removes them from the ISO:

> **NOTE:** If you are upgrading from a previous version of SL1, the 12.3.0 upgrade will not remove any existing PowerPacks. The PowerPacks listed below are still available for download from the PowerPacks Support page.

- 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 only

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*** 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 12.3.0

This section includes important notes for upgrading existing SL1 systems to the Ibiza 12.3.0 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 12.3.0.

Supported Upgrade Paths

Review the following considerations:

- Because of the deprecation of the legacy version of Data Pull in SL1 version 12.1.2 and 12.2.1.1, before you can upgrade to 12.3.0, you must first upgrade to 12.1.2 or 12.2.1.2, or install 12.2.1.1 (12.2.1.1 is ISO only).
- If you are currently on SL1 12.1.0.x or 12.1.1 and all of your appliances are running on Oracle Linux 8 (OL8), you can upgrade to 12.1.2 or 12.2.1.2 and then upgrade to 12.3.0.

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.

If you take no action before January 30, 2025, all older SL1 systems with OL7 will continue to run, but ScienceLogic will not support 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

The following upgrade paths are not supported:

- You cannot upgrade from 12.2.4.x or 12.2.5.x to 12.3.0.
- You cannot upgrade from 12.1.3 to 12.3.0.

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?
12.3.0	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

SL1 Release	Required MariaDB Version	Requires Appliance Reboot?
12.1.0.2 ISO (OL8)	10.4.28	N/A
12.1.0.2 Upgrade (OL7)	10.4.29	Yes
11.3.2.1	10.4.28	Yes
11.3.2	10.4.28	Yes
11.3.1.3	10.4.28	Yes
11.3.1	10.4.28	Yes
11.3.0	10.4.26	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.

Aurora 3 Support

AWS deployments that are using Aurora 3 can upgrade to SL1 12.3.0, using a post-upgrade Aurora 2 to 3 conversion. The conversion is done by SRE, with additional steps in the *Upgrade* chapter of the ***System Administration*** 12.3.0 manual.

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 release. However, ScienceLogic will still include Python 2 in parallel with Python 3 until Q2 2025. 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 Q2 2025.

The SL1 12.5.0 release, which is the Q2 2025 release, will not include Python 2. Any Python 2 content will stop working when an instance is updated to version 12.5.0 and later.

For more information, see the ***Python 3 Resource Center*** on the ScienceLogic Support site.

Python 3.9 Execution Environment Support Deprecation

The option to use Python 3.9 execution environments is limited to SL1 12.2.1 and later 12.2.x releases. SL1 12.3.0 removes support for Python 3.9 and adds support for Python 3.11.

As a result, any Dynamic Applications that use Python 3.9 execution environments will stop working after upgrading to SL1 12.3.0 or later.

If you are currently using Python 3.9 execution environments, then after updating to 12.3.0 or later, you ***must*** create a Python 3.11 execution environment and align any Dynamic Applications that are currently aligned to the Python 3.9 execution environments to that Python 3.11 execution environment to make them work again.

MUD/STIG Deployments

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.

Enterprise Key Management Service (EKMS) Issues

You might experience the following EKMS-related issues upon upgrading to SL1 12.3.0:

- EKMS might not start due to issues with the configuration files
- EKMS might not start due to an issue where it remains encrypted upon startup.

Both of these issues are described in more detail below.

EKMS Configuration File Issues

In SL1 12.2.1.1 and later, if you are using a high-availability (HA) configuration and you re-ISO or rebuild one of the Database Servers, you might experience an issue where the EKMS vault service (`sl_vault`) does not start due to issues with the configuration files. If this occurs, you will experience the following issues:

- When you attempt to log in to the default user interface (AP2), you will receive an "Unexpected end of JSON" input error.
- When you attempt to log in to the classic user interface, you will receive a "502 Bad Gateway" error.
- The `sl_vault` service gets stuck on the following message: "Error checking seal status: Get "http://localhost/v1/sys/seal-status": dial unix /run/vault/vault.sock: connect: no such file or directory".
- The `/tmp/vault_conf.yml` file displays in plain text and the password displays as `###PASSWORD###`, which indicates that it is not set.

Before attempting to work around this issue, you should first ensure that the `clientdbuser` has the correct permissions. To do so, open an SSH session to the Database Server and run the following command:

```
silo_mysql -e "SELECT user, grant_priv FROM mysql.user WHERE user =
'clientdbuser'"
```

This should return a "`Y`" value. If it does not, contact your database administrator and request permissions for `clientdbuser` before attempting the workaround.

If you have the proper permissions, you can follow these steps to work around this issue:

1. In your SSH session, stop the EKMS services and mask them so they do not restart during the reinitialization:

   ```
   sudo systemctl stop sl_vault sl-vaultmngt
   ```

   ```
   sudo systemctl mask sl_vault sl-vaultmngt
   ```

2. Remove the problematic EKMS files:

   ```
   sudo rm -f /tmp/vault_conf.yml /etc/sl_vault/vault_conf.yml /etc/sl_
   vault/encryption_key /opt/em7/services/sl_vault/config/hcl/vault.hcl
   ```

3. Copy the default `vault_conf` template:

   ```
   sudo cp -v /opt/em7/services/sl_vault/utils/vault_conf.yml /etc/sl_
   vault/
   ```

4. Set the permissions for the `vault_conf` file:

   ```
   sudo chown s-em7-security:s-em7-security /etc/sl_vault/vault_conf.yml
   ```

5. Delete the users. They should regenerate when EKMS reinitializes:

   ```
   silo_mysql -e "DROP USER IF EXISTS 'em7-security'"
   ```

   ```
   silo_mysql -e "DROP USER IF EXISTS 'em7-security02'"
   ```

> **NOTE:** You must run this step on both the active and passive Database Servers.

6. Re-enable the EKMS services:

   ```
   sudo systemctl unmask sl_vault sl-vaultmngt
   ```

   ```
   sudo systemctl start sl_vault sl-vaultmngt
   ```

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
   ```

Global Manager Deployment

When deploying or upgrading Global Manager systems, the Global Manager stack and all of its child stacks must run on the same SL1 build version, as well as the same versions of AP2 and Oracle Linux.

Obtaining a ScienceLogic Key for Agent RPM Packages

As of SL1 version 12.1.1, RPM installer packages are now signed. Therefore, when installing an RPM package, you might receive a warning message similar to the following one if the RPM store does not contain ScienceLogic's public GPG key:

```
warning: all silo-agent-x86_64.rpm: Header V4 RSA/SHA512 Signature, key ID
3a6131f6: NOKEY
```

To address or prevent this warning, you can obtain the ScienceLogic key and then add it to the RPM store. To do so:

1. Go to https://keys.openpgp.org/search?q=devops%40sciencelogic.com.
2. Download the key.
3. Import the key into the RPM store using the following command:

   ```
   rpm --import <file name>
   ```

Validating Agent TLS Connections to the SL1 Streamer Service

As of SL1 12.1.1, customers who use the SL1 Gen 3 agent with on-premises Extended Architecture systems have the option to turn on TLS certificate validation when deploying the Streamer service. This provides additional security to confirm that the agent's connection to SL1 is valid.

To enable this TLS validation, the extended cluster must be configured with a valid TLS certificate and the "requireTls" setting in the Streamer helm chart must be set to "true" when deploying the Streamer, such as in the following command:

```
helm upgrade --version 1.2.13 streamer sl1/sl1-streamer -f output-
files/steamer-values.yml --set requireTls=true
```

If you update this setting, the Streamer pods will restart and the agent will download the new configuration upon its next communication with the cluster.

CAUTION: This TLS validation is currently disabled by default for on-premises Extended Architecture deployments.

If you want to enable this feature, it is important to first ensure that the Streamer end point that is provided via the URLFRONT installation option is configured with a valid TLS certificate. If the agent is configured to validate the TLS connection but the cluster it is trying to communicate with does not have a valid TLS certificate, the agent will be unable to communicate with that cluster.

If this occurs, you can disable the validation by updating the Streamer deployment to disable the "requireTls" setting, updating the scilog.conf file to remove or alter the "RequireWebCert true" line, and then restarting the agent.

NOTE: This feature can be enabled on SaaS SL1 deployments by submitting a Service Request case to the SRE queue at the ScienceLogic Support site at https://support.sciencelogic.com/s/, or by contacting your ScienceLogic customer service manager.

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.

Verifying PowerPack Version Compatibility

Before consuming SL1 12.3.0, please verify whether any PowerPacks currently running on your system are newer than the PowerPacks included in this release.

If the PowerPack on your system is newer than the one included with this release, you might see spurious error messages.

To avoid spurious error messages:

1. Before installing the SL1 update, go to the **Device Components** page (Registry > Devices > Device Components).
2. Find each root device associated with the PowerPacks you do not want to update and select their checkboxes.
3. Click the ***Select Action*** field and choose *Change Collection State: Disabled (recursive)*, and then click the **[Go]** button.
4. Wait five minutes after disabling collection.
5. Install the SL1 update.
6. After the SL1 update is complete, go to the **Device Components** page (Registry > Devices > Device Components).
7. Select the checkbox for all affected root devices.
8. Click the ***Select Action*** field and choose *Change Collection State: Enabled (recursive)*, and then click the **[Go]** button.

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 12.3.0

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 12.3.0:

- 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.

- When upgrading, 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)

- 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 in 12.3.0 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';`. ScienceLogic is working to correct this known issue by the next AP2 release, Icepop. (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). (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'." (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 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)

- 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, 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. (Case: 00412497) (Jira ID: EM-62874)

- 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 "Running the Skylar SL1 Management Script" topic in the ***Skylar Analytics*** manuals. (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)

- 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)
  - Services that are added or created to the N-tier hierarchy have their ***RCA Options*** field set to *Disabled* by default. The current solution to this issue is to edit the service you wish to configure by manually updating the ***RCA Options*** field to *RCA Enabled (contributors only)*.(Jira ID: SLUI-18852)
  - 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 SL1 12.1.1 release set the maximum number of simultaneous user sessions to 300. With this change, some users have received an "HTTP Response code was 429 (Too Many Requests)" error in SL1. For more information about this error, see the section on ***Adjusting Maximum User Sessions*** and https://support.sciencelogic.com/s/article/12971.
- In new installations of SL1 12.3.0, 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 **[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)

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. For more information, see https://sciencelogic.com/company/legal.

ScienceLogic

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

International: +1-703-354-1010