



---

# Skylar One Juneau 12.5.1 Release Notes

Skylar One version 12.5.1

---

# Skylar One Juneau 12.5.1 Release Notes

**IMPORTANT:** ScienceLogic strongly recommends that you review the [installation and upgrade instructions](#), [important upgrade notes](#), and [known issues](#) for this release before installing or upgrading to Skylar One 12.5.1.

The Skylar One Juneau 12.5.1 release includes the following new features and enhancements:

- [With this release, SL 1 has been rebranded to Skylar One](#)
- [Role-based access control](#) for Skylar One appliance management, authentication profiles, and authentication resources
- Improved processes for creating and editing [business service policies](#)
- New actions on the [Devices page](#) and improvements to the Device Investigator
- A redesigned [Event Policy Editor](#) and the ability to [align event policies with specific organizations](#)
- The introduction of [Geographic Maps](#) that visualize devices on a map and provide at-a-glance insights of those devices
- Additional [exportable data types from Skylar One to Skylar AI](#) and easier service connections for exporting data
- [New topology options](#) at the system and device level for more context about device relationships
- Plus [many additional updates](#) and [addressed issues](#) from previous releases

These release notes provide a comprehensive list of the features, enhancements, and addressed issues that are included in the Skylar One Juneau 12.5.1 release.

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

- [8.17.23-45 \(Ice Pop\)](#)
- [8.18.43-81 \(Jelly Bean\)](#)
- [8.20.2-72 \(Key Lime Pie\)](#)
- [8.20.70-45 \(Lokma\)](#)
- [8.26.4-45 \(Mochi\)](#)

AP2 version 8.26.4-45 (Mochi) is installed by default in Skylar One 12.5.1.

This document covers the following topics:

<i>Before You Proceed</i> .....	4
<i>New Features and Enhancements in Skylar One Juneau 12.5.1</i> .....	5
<i>Issues Addressed in Skylar One Juneau 12.5.1</i> .....	27
<i>Installing and Upgrading Skylar One</i> .....	42
<i>Important Upgrade Notes for Skylar One Juneau 12.5.1</i> .....	43
<i>Known Issues for Skylar One Juneau 12.5.1</i> .....	51

---

## Before You Proceed

If you are planning to consume Skylar One Juneau 12.5.1, be advised of the following:

**WARNING:** If you are upgrading to 12.5.1 from a 12.1.x or 12.2.x release, you **must** run a script on your active or primary Database Server or Data Engine **before** you import the 12.5.1 patch bundle. Failure to do so will cause the upgrade to fail. For instructions, see the section [12.1.x and 12.2.x Pre-Import Script to Prevent Patching Issues](#) in the [Important Upgrade Notes](#).

Alternatively, you can upgrade to a 12.3.x release and then to 12.5.1, as this issue does not affect the 12.3.x to 12.5.1 upgrade path.

- All Python 2 functionality has been removed from Skylar One with this release. If you still use Python 2 for custom code, you cannot upgrade to this or any later releases until your custom code is Python 3-compatible.
- Be advised that you can perform upgrades from one minor version to a subsequent minor version in most cases. 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 validated upgrade paths for 12.5.1:
  - 12.3.8 > 12.5.1
  - 12.3.7 > 12.5.1
  - 12.2.7 > 12.5.1
  - 12.1.2 (OL8) > 12.5.1

**WARNING:** If you are upgrading from a version prior to 12.2.3, then after upgrading Skylar One, you must also upgrade MariaDB 10.4.x to version 10.6.21. Failure to perform this MariaDB upgrade can cause major functionality issues in Skylar One.

- 12.2.x and 12.3.x STIG-compliant users cannot upgrade to this release. 12.5.1 STIG is available only as an ISO.
- AWS deployments that are using Aurora 3 can upgrade to this release.
- When upgrading Skylar One to version 12.5.1, PowerPacks will be temporarily read-only until the update is complete.
- The Enterprise Key Management Service (EKMS) is enabled by default in 12.5.1.

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

---

# New Features and Enhancements in Skylar One

## Juneau 12.5.1

This section describes the new features and enhancements that are included in Skylar One Juneau 12.5.1.

### Rebranding

- **What's new: *SL1 is now Skylar One!*** With this release, ScienceLogic has rebranded SL1 to Skylar One. You will notice this rebranding throughout the platform. This change, as well as similar branding changes to the other products offered by ScienceLogic, reflects ScienceLogic's commitment to delivering intelligence that accelerates outcomes through service-centric observability, AI-driven operations, and intelligent automation.
- **For more information:** See the ScienceLogic website (<https://sciencelogic.com/platform/overview>).

### Authentication and Access Control

- **What's new: *Role-based access control for Skylar One appliance management, authentication profiles, and authentication resources.*** Added the ability to determine whether Skylar One appliances, authentication profiles, and authentication resources are shared with all organizations or if they are private. They are shared with all organizations by default, but if made private, they are visible only to Administrator users and users assigned to the System organization. These changes were made to facilitate role-based access control over certain tasks that should be performed only by Skylar One administrators. The following changes were made to support this enhancement:
  - Added a new **Sharing Permissions** field that enables Administrator user accounts and user accounts assigned to the System organization to determine whether an appliance, authentication profile, or authentication resource is shared or private. This field now appears on the following pages, but is visible only to those user types:
    - **Appliance Manager** page (System > Settings > Appliances)
    - **Authentication Profile Editor** modal (System > Settings > Authentication > Profiles > create or edit)
    - **Auth Resource Editor** modal (System > Settings > Authentication > Resources > create or edit)
  - Added a new **Access** column to indicate whether the listed appliances, authentication profiles, or authentication resources are shared with all organizations or are private. This column now appears on the following pages, but is visible only to Administrator user accounts and user accounts assigned to the System organization:
    - **Appliance Manager** page (System > Settings > Appliances)
    - **Authentication Profiles** page (System > Settings > Authentication > Profiles)
    - **Authentication Resource Manager** page (System > Settings > Authentication > Resources)

- **For more information:** See the chapters on "Role-based Access Control" in the *Organizations and Users* manual and "Global Settings" in the *System Administration* manual.

### **Additional Authentication and Access Control Updates**

- Added three new access hooks:
  - PLAT\_SETTINGS\_EMAIL\_EDIT, which enables users to edit the *Email Gateway* and *Email Gateway Alt* fields on the **Email Settings** page (System > Settings > Email).
  - PLAT\_SETTINGS\_PROCS\_EDIT, which enables users to edit the *Operating State* and *Frequency* fields for a process on the **Process Editor** page (System > Settings > Admin Processes > wrench icon).
  - RBK\_ACTIONS\_SNIPPET, which enables users to edit the snippet code for run book actions.
- Added a new "Platform Administration" access hook category and a new "Platform - Administration" access key. This key will be assigned by default to Administrator user accounts and grants permissions for some specific Skylar One platform items. The following access hooks are assigned to this new access hook category and access key:
  - PLAT\_SETTINGS\_EMAIL\_EDIT
  - PLAT\_SETTINGS\_PROCS\_EDIT
  - SYS\_SETTINGS\_BACKUP\_PAGE
  - SYS\_TOOLS\_DB
- Added a new "Tenant - Administration" access key, which allows you to grant permissions for tenant items. All access hooks are aligned to the "Tenant - Administration" access key, with the exception of those access hooks that are aligned to the "Platform - Administration" access key as well as the SYS\_ACCESS\_CONTROL\_KEY\_MANAGER access hook.
- Existing custom access keys that use the following access hooks will have new access hooks automatically added to them upon upgrading to 12.5.1 so users maintain their same access rights post-upgrade:
  - SYS\_SETTINGS\_EMAIL\_PAGE
  - IP\_INTERFACES\_EDIT
  - DEV\_TEMPLATE\_EDIT
  - SYS\_SETTINGS\_PROCS\_PAGE
  - SYS\_SETTINGS\_BEHAVIOR\_PAGE

## Business Services

- **What's new: *Improvements to service policy creation*.** This release includes a revamped experience for creating and editing service status policies. This change is designed to clarify service policy configuration and make rule-building more intuitive. The following changes were made to improve the service policy creation and editing process:
    - The **[Service Policy]** tab now includes distinct panels for **Health**, **Availability**, and **Risk**. Each panel shows the number of associated rules in parentheses, provides a list of the associated rules, and enables you to add, duplicate, or delete rules when in edit mode.
    - When adding or editing a rule in the **Edit Rule** modal, you can now:
      - Choose the metric, aggregation method, and timespan for each rule, including a number of new metrics.
      - Insert new conditions and establish specific condition thresholds that will trigger alert messages when crossed. The alert messages will become events if the matching event policy is enabled.
- NOTE:** You must select a metric and set a minimum of two thresholds for each rule. The available metrics differ depending on whether you are editing service policies for business services, IT services, or device services.
- View a line graph that visualizes the threshold ranges for each rule.
  - You can now align a service policy that generates Skylar AI Prediction events with a device service and set the risk value to reflect the severity of the prediction event.
  - When editing a rule for a device service, an error message will appear if the service does not have current raw data to display.
  - **For more information:** See the chapter on "Creating Services and Service Policies" in the ***Business Services*** manual.

### Additional Business Services Updates

- Made the following changes to the **Business Services** page:
  - Relabeled the ***RCA Options*** column to ***Service Analysis***.
  - Redesigned the **Preview** pane for building service hierarchies while creating custom service models.
  - Added the ability to update the refresh interval for services in bulk. To do so, select the checkboxes next to the services you want to update, then select ***Update Refresh Interval*** from the ***Actions*** field.
  - Updated the ***Policy*** column to display by default.

- Made the following changes to the **Service Investigator** page:
  - In the **Overview** panel:
    - Updated the ***Last Edited*** field to display the date the service was last edited.
    - Relabeled the ***RCA Options*** field to ***Service Analysis***.
  - In the **Timeline** panel:
    - Added a new ***Anomalies*** row under the **[Skylar AI]** heading to display events marked as anomalies over time.
    - Updated Skylar AI event icons to display in the color matching their event severity.
    - Updated the swim lane headers by adjusting text size and adding divider lines to create a clearer visual distinction between different header sections.
- Updated the default service policy condition values for both health and risk values.
- Removed the **Business Services Thresholds** page.
- When troubleshooting services that fail to generate "Health", "Availability", and "Risk" values, the "onDemandProcessing" GraphQL query now displays timing data. This includes the total number of services examined, the maximum time required to calculate these values for all included services, and the individual time taken for each service.

## Device Management

- **What's new: *New actions on the Devices page.*** You can now perform a number of new actions from the **Devices** page that previously were available only on the **Classic Devices** page. The following updates were made to support this enhancement:
  - On the **Devices** page, a new drop-down arrow button now appears next to the **[Add Devices]** button. Clicking this button displays a list of actions you can take with your device list. In this release, the following device actions are available:
    - *Create Physical Device*
    - *Create a Physical Device from File*
    - *Create Virtual Device*
    - *Download/Install Agent*



- From the **Devices** page, you can now perform several additional bulk actions on one or more selected devices by clicking the **[Actions]** button and selecting one of the following options:

- *Create Asset Record*
- *Align Device Investigator Layout*

**NOTE:** When bulk-aligning a Device Investigator layout to one or more devices, you can apply the layout to all users only if you have the permissions to do so. Otherwise, the layout change will be applied only for you.

- When you add one or more devices to a device group using the **[Actions]** button on the **Devices** page, you can now click the column headings on the **Add to Device Group** modal to sort the list of selectable device groups.
- You can now create reports for individual devices from the **Devices** page.
- The following new columns were added to the **Devices** page:
  - ***SL Agent***, which indicates whether an Skylar One agent is installed on the devices in the list. If an agent is installed on a device, you can click the **Yes** hyperlink in the ***SL Agent*** column to display a modal where you can update the agent's configuration.
  - ***SNMP Credential***, which displays the name of the SNMP credential used to monitor the devices in the list.
  - ***SNMP Version***, which displays the version of SNMP used to monitor the devices in the list.
  - Additionally, if you have defined any custom attributes for your devices, you can add those custom attributes as filterable columns that appear on the **Devices** page.
- **For more information:** See the chapter on "Using the Devices Page" in the ***Device Management*** manual.

#### **Additional Device Management Updates**

- On the **Device Investigator**, the **Events** panel now displays event ID links and changes the border color of each event based on its severity.
- The **[Configs]** tab of the **Device Investigator** now includes date and time stamps for Dynamic Applications that have one or zero snapshots, in addition to those with multiple snapshots.
- Removed the ***Process Runtime Threshold Low*** and ***Process Runtime Threshold High*** settings from the **[Thresholds]** tab of the **Device Investigator** as well as the **Device Thresholds** page (Devices > Classic Devices > wrench icon > Thresholds).

- Made the following changes to the **[Anomaly Detection]** tab of the **Device Investigator**:
  - The **[Add Alert Policy]** button was replaced with the **[Skylar Anomaly Detection]** button. Previously, clicking this button enabled anomaly detection events for the device; now, doing so now takes you to the **Skylar AI** page in Skylar One.

**NOTE:** For this change to take effect, you must use the `updateFeatureToggle` mutation in GraphQL and set the `AP2_DEVICEDETAIL_AD_TAB_BUTTON` toggle to "enabled". Otherwise, the former button and its functionality will persist.

- The ***Metric Type*** column was relabeled ***Dynamic Application Metric***.
- The ***Last Modified*** column was relabeled ***Date Enabled***.
- The ***ML Enabled by User*** column was relabeled ***Anomaly Score Alert Enabled By***.
- The items on the page are now sorted from the most number of anomalies to the least by default.

## Event Management

- **What's new: Redesigned Event Policy Editor.** The **Event Policy Editor** page (Events > Event Policies > create or edit an event policy) has been redesigned to make the process of creating event policies more intuitive for users. As part of this redesign, the **Event Policy Editor** has been reorganized into three new tabs:
  - The **[Basic]** tab is the starting point when creating a new event policy. It allows you to define the fundamental requirements, such as ***Event Policy Name***, operational state, ***Event Source***, and the resulting ***Event Severity*** and ***Event Message***, along with commonly used alert evaluation criteria to configure if and when an alert converts into an active event.
  - The **[Advanced]** tab contains more advanced configuration options such as topology masking and device sub-entity settings, as well as external system integration fields and event auto-clear mapping.
  - The **[Summary]** tab is the landing page when navigating to view or edit an existing event policy. It provides an at-a-glance view of the event policy properties and highlights the linked alert. The **Troubleshooting Tips and Links** section of this tab is a rich text editor including the event policy description and probable cause.

- **What's new: *Organization Alignment for Event Policies*.** You can now align event policies to specific organizations on the **Event Policy Editor** page. All event policies are "Global" by default and apply to all devices unless specified. To change the alignment of an event policy, click **[Global Policy]**, select the ***Specific Organizations*** radio button, select the checkbox next to each organization to which you want to align the event policy, and then click the **[Apply]** button. In addition, the following updates were also made to support this enhancement:
  - A notification window was added to the **Event Policy Editor** page that explains the new organization alignment feature. The notification window will display when creating or editing an event policy. You can close the notification window or you can dismiss it permanently by selecting the ***Don't show this again*** checkbox.
  - Added an ***Event Policies*** column to the **Organizations** page (Registry > Accounts > Organizations) to indicate the number of event policies that are aligned to each organization in the list.
  - Added a new ***Alignment*** column to the **Event Policies** page (Events > Event Policies) to indicate the organization alignment for each event policy listed on the page.
  - Updated the GraphQL API for event policies to support aligning event policies to organizations.

**NOTE:** Changing the alignment of an event policy to a specific organization will result in the event policy applying only to devices in the chosen organization.

**NOTE:** If an event policy has been aligned to specific organizations and is included in a PowerPack, the event policy cannot retain its organization-specific alignment and will automatically align to "Global" upon installation into another Skylar One environment.

- **For more information:** See the topic on "Defining and Editing Event Policies" in the ***Events*** manual.

#### **Additional Event Management Updates**

- Added the following new capabilities to the **Events** page to provide you with more flexibility when viewing and managing events:
  - Updated the way sorting works on the **Events** page. Now, when you add a new sort to the **Events** page, such as ***Message***, the selected sort is the only one applied. You can revert to the default sort (by ***Severity*** and then ***Last Detected***) by clicking the **[Apply Default Sort]** button from the **Multi Sort** modal. A new notification window explains these changes to sorting; you can close the notification window, and you can dismiss it permanently by checking the "Don't show this again" checkbox.
  - You can now search event notes in both the basic and advanced search on the **Events** page.

- Skylar One can now differentiate between Skylar AI subtypes in events. To support this change:
  - You can now filter events by Skylar AI subtypes on the **Events** and **Devices** pages using the advanced search feature that is available on both pages.
  - When you click on a Skylar AI event from the **Events** page, the details that appear on **Event Overview** page now differ based on the subtype of Skylar AI event. For predictive events, a **Skylar Analytics Summary** panel appears on the page. That panel does not appear for anomaly detection events; instead, a **[View Skylar Anomaly Details]** button appears on the **Device Details** panel. Clicking this button opens the **[Anomaly Detection]** tab of the impacted device's **Device Investigator**.
  - Added a new `master_events.skylar_lookup.subtype` database field that indicates the subtype of alert sent from Skylar to Skylar One.
- If you add a user display name to your account on the **User Accounts** page (Registry > Accounts > User Accounts), that display name now appears in place of your username in the following areas:
  - On the **Events** page, under the **Acknowledge** column for acknowledged events. In addition, you can filter this column by displayed username.
  - On the **Event Policies** page (Events > Event Policies), under the **Edited By** column.
  - On the **Event Investigator** page, next to the **[Clear]** button for acknowledged events.
  - On the **Events** and **Events Details** pages, when hovering your cursor over the **[Acknowledge]** button.
- Updated the Event Engine to Python 3.11.
- Added error handling for unhandled exceptions with the Event Engine.

## Maps

- **What's new: Introduction of Geographic Maps.** A new **Geographic Maps** page (Maps > Geographic Maps) allows you to create and manage custom geographic maps that visualize devices on a map and provide location-based insights of those devices at a glance. The following updates were made to support this new feature:
  - A sortable, filterable table on the **Geographic Maps** page lists all geographical maps associated with your organization. The table consists of three columns:
    - **Map name.** The name of the geographical map.
    - **Organization.** The organizations to which the associated geographical map is aligned.
    - **Map Region.** The geographic area (countries and states).
  - You can create custom geographic maps from your existing devices from the **Geographic Maps** page by selecting devices that have been associated with a location. If no devices are available for selection, you will need to load location data first. In this release, location data can be uploaded in bulk, and this process can be repeated at any time to add more location data to devices. Once the location data for devices are added, they will appear as options when creating a new map.

- Geographic maps can be aligned with one or more organizations.
- Geographic maps include the following interactive capabilities that allow you to engage with mapped devices directly and explore device data visually:
  - **Hover behavior:** When you hover your cursor over a node, it displays a list of all devices (by device name) associated with that location.
  - **Zoom behavior:** If multiple locations with devices are in close proximity, the map displays a single node showing the number of locations in that area. As you zoom in, the clustered node separates into individual nodes labeled by their specific location names. You can then hover your cursor over each location-specific node to see the devices in that particular area.
  - **Single-location behavior:** If there is only one location with devices in a region of the map, even when zoomed out, the map will display a single node marked by that location's name. Hovering over it with your cursor will show all devices in that location.
- **For more information:** See the chapter on "Geographic Maps" in the *Maps* manual.

## Skylar AI Platform

- **What's new: *Additional exportable data types and easier service connections for exporting data.***  
The following additional data types can now be exported to Skylar AI from Skylar One:
  - Additional event and alert data
  - Basic asset data
  - Device category data
  - Device group data
  - Email round trip data
  - Event policy name
  - Interface billing metrics and metadata
  - Internal Collection processes
  - Internal Collection services
  - Internal Collection CBQoS
  - Journal Dynamic Application data
  - Thresholds

- Additionally, the following updates now make it easier to establish service connections for exporting data from Skylar One to Skylar AI:
  - From the **Service Connections** page (Manage > Service Connections), you can now create a Skylar AI Engine service connection to enable the export of data from Skylar One to Skylar. To do so, click the **[Add Service Connection]** button, then select *Skylar AI Engine* from the drop-down menu that appears. When you create or edit a Skylar AI Engine service connection, a command-line interface (CLI) script will automatically run to manage Skylar configurations. This script generates configuration files and initiates the service that exports Skylar One data to Skylar AI. In the past, you needed to run this script manually.
  - A new generic, internal alert definition was added to Skylar One to indicate whenever a Skylar connection is successful or encounters a problem.
- **For more information:** See the chapter "Introduction to Skylar AI" in the *Getting Started with Skylar AI* manual.

### Additional Skylar AI Platform Updates

- Added an event policy for Skylar management failures to the "SL1 Default Internal Events" PowerPack. If you installed Skylar One version 12.5.1 from an ISO file, this PowerPack will be included with the installation. If you are upgrading to Skylar One version 12.5.1, you will need to download the "SL1 Default Internal Events" PowerPack from the ScienceLogic Support site and then install the PowerPack first.
- Anomaly detection alerts now appear in Skylar One as "Skylar" alerts rather than "API" alerts.
- Added a new **Skylar Options (JSON)** text field on the **Behavior Settings** page (System > Settings > Behavior) that enables you to override the hard-coded default options for exporting metadata to Skylar. To do so, the values entered must be in the same JSON structure as those that appear in the `config.py` file:
 

```
DEFAULT_OPTIONS = { "metadata": { "intervals": {"snapshot": 60,
"cleared_events": 5}, "snapshot": { "batch_sizes": { "asset_basic":
500, "asset_ip_config": 10000, "perf_index_label": 5000, "device_
config": 20000, }, }, "cleared_events": { "query_range": 60, }, } }
```
- On the **Anomaly Detection** page, the **[Enable]** button was relabeled **[Create Alert Policies]** and the **[Disable]** button was relabeled **[Delete Alert Policies]**.
- As part of the rebranding effort across ScienceLogic's entire product line, all references to "Zebrium" throughout the platform have been updated to "Skylar Automated RCA" or "Skylar RCA," including on the **Service Connections** page (Manage > Service Connections) and in various dashboard options.

- Added three new columns to the **Service Connections** page (Manage > Service Connections):
  - **Service Check**, which displays the **[Run Test]** button if the service type is "Skylar AI Engine". Clicking **[Run Test]** runs a script to check the status of the Skylar AI connection and display the results in a modal.
  - **Status**, which displays one of the following values depending on the results of the latest service connection test:
    - Status Unknown.
    - Enabled. Exporting.
    - Enabled. Not Exporting.
    - Exporting Paused.
  - **Status Updated**, which displays the date and time the service connection was last tested.
- After creating or editing a Skylar AI service connection, a modal now appears with a "Select Organizations" link that navigates to the **Organizational Account Administration** page to encourage setting up organization export to Skylar AI. This modal can be closed if you want to set up organization export to Skylar AI later.
- You can now search for Skylar AI events by subtype through the Advanced Search feature throughout Skylar One.
- You can now use the "skylarConnectorStatus" GraphQL query to find the latest status of the Skylar management script when it is being created or updated.
- Added the following GQL mutations, which are accessible to only users with administrator privileges:
  - checkSkylarConnector
  - enableSkylarConnector
  - pauseSkylarConnector
- The following configuration options were added to the Skylar management script start-up command:
  - `--verify-cert false`, which allows users in on-premises environments to connect to Skylar using self-signed certificates
  - `--ca-bundle /path/to/bundle.pem`, which allows users to specify a path to a .pem file and assign it to the `REQUESTS_CA_BUNDLE` environment variable
- When running the Skylar management script, administrators can now pause Skylar by running the following command: `sudo sl-otelcol-mgmt.py -vv skylar`. Pausing sets all Skylar toggle fields to disabled; restarts the event engine and data pull services to reflect the changed configuration; stops Skylar One managed services such as the Metadata Exporter, Alerts Poller, and sl-otelcol.timer; and stops and disables the sl-otelcol systemd service.
- Added a `--skylar-disable` flag to the Skylar management script that enables administrators to stop all Skylar-related exports and services. This flag performs the same operations as the pause command and also removes any Skylar-related pages from the user interface.
- A warning message was added to debug logs for the metadata export process for cases where a large device configuration table might cause a memory issue.

- When updating Skylar-related settings in the **nextui.conf** file on a Database Server, those changes are now automatically replicated to other nodes in your stack.
- After clicking the **[Run Test]** button for a service connection, the **Skylar Connection Debug** modal will now appear and display the script's status output. You can re-run the status check by clicking the **[Run Again]** button.

## Topology

- **What's New: *Enhanced topology options*.** Added new topology options at the system and device level that make it easier for Skylar One to form relationships between devices. This enhancement enables Skylar One to provide additional context about device relationships, better topology maps, and enhanced event correlation. To support this new feature, the following updates were made:
  - Added the following new fields to the **Behavior Settings** page (System > Settings > Behavior) under the heading "Network Topology":
    - Enable L2 Topology Collection from all VLANs
    - Enable L2 Topology Collection and Processing
    - Enable L3 Topology Collection and Processing
    - Enable CDP Topology Collection and Processing
    - Enable LLDP Topology Collection and Processing

These fields include checkboxes that, if selected, enable Skylar One to create relationships between devices system-wide, as long as the applicable devices, device classes, or device templates are configured to do so.



- Added ***L2 Topology***, ***L3 Topology***, ***CDP Topology***, and ***LLDP Topology*** fields at the device, device class, and device template levels. These fields enable you to override the system-wide topology settings from the **Behavior Settings** page at a more focused level. These new fields display on the following pages:

- **Device Properties** page (Devices > Classic Devices > wrench icon, or Registry > Devices > Device Manager > wrench icon)
- **Device Class Editor** page (System > Customize > Device Classes)
- **Device Template Editor** page (Devices > Templates > create or edit > Config)

On these pages, the following drop-down options are available in these fields to provide you with more granular control over topology behavior at the device, device class, or device template level:

- *Disabled*. Disables that topology collection and processing type for the device, device class, or device template.
- *Processing Enabled*. Enables that topology processing type for the device, device class, or device template using the standard topology crunch process.
- *Collection and Processing Enabled*. Enables that topology collection and processing type for the device, device class, or device template using the standard topology crunch process.
- *Enhanced Processing Enabled*. Enables the new, more robust topology processing for that topology type for the device, device class, or device template. This option is available for devices and device classes only if enhanced topology is enabled system-wide.
- *Collection and Enhanced Processing Enabled*. Enables the new, more robust topology processing and collection process for that topology type for the device, device class, or device template. This option is available for devices and device classes only if enhanced topology is enabled system-wide.

# Additional New Features and Enhancements in Skylar One Juneau 12.5.1

## Agent

- Skylar One version 12.5.1 includes Linux Agent v196 and Windows Agent v154, which include the following enhancements since the previous versions that were pinned to a Skylar One release:
  - Linux Agent v194:
    - Linux agents can now be entered into maintenance mode or suspended. When suspended, the agent cannot upload metric data files, which saves bandwidth.
  - Linux Agent v195:
    - Linux Agent v195 includes updates to improve security and agent performance.
  - Linux Agent v196:
    - In the **scilog\_proxy.conf** file, you can now specify as many as four Linux proxy server configurations when installing the agent. If the connection through the primary proxy fails or the proxy is unavailable, the agent will attempt to make the connection through the other specified proxies.
  - Windows Agent v151:
    - Windows agents can now be entered into maintenance mode or suspended. When suspended, the agent cannot upload metric data files, which saves bandwidth.
    - Added a new, editable LogMonitorUserServerTime setting in the **scilog.conf** file, which enables you to localize Windows log monitoring event time stamps to your timezone.
  - Windows Agent v152:
    - Updated the Windows agent service to prevent it from entering a "stop pending" state that required you to force-quit and restart the agent.
  - Windows Agent v153:
    - In the **scilog\_proxy.conf** file, you can now specify as many as four Windows proxy server configurations when installing the agent. If the connection through the primary proxy fails or the proxy is unavailable, the agent will attempt to make the connection through the other specified proxies.
  - Windows Agent v154:
    - If the LogMonitorUserServerTime setting in the **scilog.conf** file is not defined, the "UTC" suffix is not added to Windows log monitoring event time stamps.

**IMPORTANT:** Windows Agent v151, v152, and v153 are not compatible with versions prior to 12.5.1. Windows Agent v154 added backwards-compatibility for SL1 12.3.x releases for those features.

- Updated the agent so that when it is disabled or suspended, it does not continue to collect metric data and waste bandwidth that should not be consumed.
- Added "success" and "failed" events to Dynamic Application alignment that will appear on the **Events** page, the Device's **[Events]** tab, and the Device's **[Logs]** tab.
- Added "suspend support" so the agent limits data sent while in maintenance.
- Added the agent value to enable agents to use the local server time for log monitoring policies, which will appear in the log line of the device logs. You must have permissions to enable this feature via SQL query. For more information, contact ScienceLogic Support to request this feature.
- Updated delivery and consumption for the Streamer Prime service to ensure future updates can be delivered via an RPM file and dependencies can be used without affecting the platform as a whole.
- Normalized timestamps for agent data uploads to ensure the system consumes agent data that is uploaded at unexpected intervals.

## Credentials

- The **Credentials** page (Manage > Credentials) has been reorganized into two new tabs: **[Summary]** and **[Types]**.
  - The **[Summary]** tab contains all the information related to your credentials, including but not limited to the **Category** (previously known as **Type**), which indicates the category for each credential, and **Type** (previously **Subtype**), which denotes the type of vendor-specific credential to which each universal credential belongs.
  - The **[Types]** tab presents a table listing just your credential types along with their respective categories.

**NOTE:** You can delete universal credential types on the **[Type]** tab, as long as they have not been used to create existing credentials.

- A **[Save As]** option is now available when editing a credential type in the **Edit Credential Type** modal (Manage > Credentials > Types > edit a credential type).
- In PowerShell credentials, the former **Encrypted** toggle field is now labeled **Use SSL (HTTPS)** to more accurately reflect the field's function.

- Added two new fields for PowerShell credentials:
  - **Certificate Validation.** This field is visible when the **Use SSL (HTTPS)** toggle field is enabled for the connection and enables you to select whether a certificate is validated for the credential. Choices are:
    - *Ignore.* Skylar One will not validate a certificate for the credential. This is the default setting.
    - *Validate.* Skylar One will require a validated certificate for the credential. If you select *Validate*, then the target device must include a non-expired certificate issued from a certificate authority.
  - **Message Encryption Setting.** This field is visible when the **Account Type** field is set to *Active Directory* and enables you to select whether Kerberos packages sent over PowerShell Remoting Protocol (PSRP) or Windows Remote Management (WinRM) are encrypted. Choices are:
    - *Auto.* Encryption is enabled if the package supports it; otherwise, encryption is disabled. This is the default setting.
    - *Never.* Messages are never encrypted. If selected, the target device must support this option.
    - *Always.* Messages are always encrypted. If selected, the target device must support this option.

**NOTE:** These field changes are included only in the PowerShell credential editor in the default user interface (AP2). They are not included in the classic user interface.

**IMPORTANT:** If your Skylar One system currently uses the following database fields from the `master.system_custom_config` table to control message encryption, these new credential fields will not override the following database settings:

- `powershell_msg_encrypt_http`
- `powershell_msg_encrypt_https`

If those database settings are used, then they should be removed and the associated credentials should be updated. This allows the credential updates to take place in a controlled manner, so Skylar One can continue monitoring the devices using those database fields until you have made the appropriate credential changes.

If either of these settings is in use, you can remove it with the following database statement:

```
DELETE FROM master.system_custom_config WHERE field = '<name>';
```

For example:

```
DELETE FROM master.system_custom_config WHERE field =  
'powershell_msg_encrypt_https';
```

- The Credential Tester process in Skylar One now allows tests to IPv6 addresses and has been updated to run in Python 3.11.
- The "EM7 Credential Tests" PowerPack was renamed "SL1 Credential Tests".
- The Enterprise Key Management Service (EKMS) is enabled by default in 12.5.1.
- Ensured that the rollback process for EKMS converts credentials stored in the `system_settings_licenses` table to non-vault credentials.

## Dashboards

- The **AIML Predictions** widget was renamed **Skylar Automated RCA** and the logo was updated to the Skylar AI logo. In addition, when creating the widget, the ***Zebrium Connection ID*** and ***Zebrium Service Groups*** fields have been renamed to ***Skylar Automated RCA Connection ID*** and ***Skylar Automated RCA Service Groups***, respectively, and the **Preview** pane now reads "Please provide a Skylar Automated RCA Connection ID for this widget."
- The table visualization for **Services** widgets now supports pagination and continuous scrolling, allowing you to view more services in a single table. This widget's table also includes many of the same capabilities and features as other tables in Skylar One, such as the ability to sort and filter the data within the table and to add or remove various properties such as service properties, organization properties, and service metrics.
- Improved widget visualizations and interactivity by upgrading the Highcharts integration to version 12.2.
- Updated GraphQL APIs using a variation of state or severity to add a new `SeverityLevel` enum type for queries.

## Data Collection

- In Skylar One version 12.5.1, Streamer Prime is distributed as an RPM file with refined permissions and files. As part of this update, the Streamer Push service now runs persistently and directly on Skylar One Collectors, rather than as a containerized service.
- Removed the Docker container for concurrent PowerShell collection and replaced it with a Python 3 system service.
- Concurrent PowerShell is now enabled for STIG environments.
- Optimized the "Enterprise Database: Collector Config Push process (`config_push.py`) by adding new filters to the internal Config Push managed tables, decreasing the volume of data sent to Skylar One Collectors.
- The "EM7 Core: Task Manager" process now stops core Skylar One services when a Database Server or data engine appliance becomes the passive node in a high-availability configuration.
- Updated PowerShell monitoring to ensure that if an IPv6 address cannot be resolved, Windows devices can still be monitored using local account credentials. However, if you use Active Directory credentials, the IPv6 address must always be resolved to a host or fully qualified domain name, because the computer name must exist in the Active Directory database.
- Added the `snmpEngineTime` OID as an option for uptime data collection. This OID measures in seconds rather than hundredths of seconds. You can edit device classes for supported devices to use the new OID.

- Updated the "Bandwidth usage exceeded threshold" alert message and formula to no longer alert when bandwidth is greater than 100%.
- Resolved multiple issues that were preventing some data from displaying correctly in **Device** dashboard widgets with *Leaderboard* visualizations whenever CPU or Memory were added. (Jira IDs: SLUI-20627, SLUI-20510)

## Deployment and Configuration

- New ISO installations of Skylar One will utilize Oracle Linux 8.10 to support installation on newer hardware platforms.
- STIG systems deployed in the cloud (AWS and Azure) now require a password when using `sudo` to run commands.
  - For newly installed Skylar One systems, you must set a password for the em7admin account before you can complete setup. The "Message of the Day" in the user interface will appear as a security warning to set the password on the account.
  - For Skylar One systems updated with a patch, the "Message of the Day" will appear as security warning stating that there is no password on the em7admin account. You will need to run the command listed in the "Message of the Day":

```
sudo /opt/em7/share/scripts/fix_sudo_passwd
```

## Documentation

- The ScienceLogic API and GraphQL documentation is now available at the [ScienceLogic Support site](#) (login required) under the **[Skylar One]** drop-down tab.

## Global Manager

- When running on a Global Manager stack, the "createDeviceCategory" GraphQL mutation, by default creates the device category on the Global Manager stack as well as on the enabled child stacks. New child stacks and modifications to the "mutateGlobalManager" mutation can alter this behavior, allowing it to be executed in the following ways:
  - Locally (on the Global Manager only)
  - Remotely (on one or more child stacks only)
  - Locally and remotely (on selected subsets of child stacks)
- Updated Global Manager to always display the globally unique identifier (GUID) for organizations, enabling you to manage organizations across stacks in your Global Manager system.
- The Organization query in GQL now supports the stackDiff and syncStatus fields for Global Manager systems. The stackDiff field returns a list of fields that are different between the stack node and the Global Manager, while syncStatus indicates whether the resource is synchronized across child stacks in the Global Manager system.

## GraphQL

- The "AccountPolicy" query now supports all policy fields.
- The "organizationsByGUID" query now allows searches for integer values, GUID values, or a combination of both.
- Updated the event GQL resource to indicate the subtype of alert sent from Skylar to Skylar One in user queries.
- The "createPhysicalDevicesFromCSV" mutation now requires the following CSV headers:
  - ip
  - name
  - organizationId
  - deviceClassId (GUID only)
  - collectorGroupId
- Removed deprecated timer functions from multiple GQL resources related to devices and Dynamic Applications.
- Added "lastValue" and "metrics" functions to the "monitorWebContents" query, enabling the **Dashboards** page to query a set of monitoring policies and retrieve the last value from monitorMetric data on the device associated with those policies.
- You can now use "skylarConnectorStatus" to query the latest status of the Skylar management script when it is being created or updated.
- Ensured that the "executeDeleteDevices" mutation indicates an error when you attempt to delete a device and the deletion fails.
- Removed the "createFeatureToggle" and "deleteFeatureToggle" mutations.
- You can now create account policies using the "createAccountPolicy" mutation.
- Removed the deprecated OrganizationInput argument from the Organization type.

## High Availability and Disaster Recovery

- Added additional validation to the silo-cluster-install process for High Availability and Disaster Recovery (HA/DR) configurations.

## Logging

- A "Notice" log entry now appears in the system log whenever a "Lock wait timeout exceeded" error occurs for the `master_events.events_active` database table.
- Refined debug log messages related to regular expression (RegEx) matching to reduce the volume of such log messages.

## PhoneHome Communication

- RSA256 and RSA512 algorithms can now be used for key authentication in PhoneHome configurations.

## Platform and Security

- Removed all remaining legacy Python 2.x code and functionality from Skylar One. As of this release, Skylar One only supports Python 3 code.

**WARNING:** If you still use Python 2 for custom code, you cannot upgrade to this or any later releases until your custom code is Python 3-compatible.

- Skylar One version 12.5.1 includes package updates to improve security and system performance. These package updates include the following security updates that address known vulnerabilities: ELSA-2023-6939, ELSA-2024-2988, ELSA-2024-2098, ELSA-2024-3254, ELSA-2024-0752, CVE-2024-37891, ELSA-2024-5258, ELSA-2024-4246, ELSA-2024-3968, ELSA-2024-12191, CVE-2025-1097, CVE-2025-1098, CVE-2025-1974, CVE-2025-24513, CVE-2025-24514, and CVE-2025-49844.
- Skylar One deployments in AWS now use Aurora RDS 3.08.2 (MySQL 8.0) and Aurora RDS R6g instances by default.
- STIG systems can no longer utilize PHPlibsec or Rijndael-256 encryption. If you attempt to install a PowerPack that uses this encryption, you will receive an error message.
- The "EM7 Core: Task Manager" process now stops the "em7\_scheduler" service when a Database Server becomes the passive node in a High Availability configuration.

## PowerPacks

- When upgrading Skylar One to version 12.5.1, PowerPacks will be temporarily read-only until the update is complete.
- The internal calls from the PowerPack Engine to Skylar One now obey the global TLS required setting when determining if the engine should use SSL.



- Added the "ScienceLogic Support Pack" PowerPack v109, which is installed as part of this release. This version of the PowerPack includes the following updates:
  - Fixed the use of the reserved MySQL keyword "function" in the "Support: Configuration File Validation" Dynamic Application snippet.
  - Updated the "Support: Appliance Validation" Dynamic Application to fix memory calculation for a Message Collector in the "Support: Appliance Validation Minimum MC Requirements Not Met" event.
  - Updated the "Support: Database DNS Configuration" Dynamic Application to ensure the DNS check will check all listed DNS servers.
  - Optimized the database query in the "Support: Device Group Performance" Dynamic Application.
  - Updated the "Support: VMware Performance" Dynamic Application.
  - Updated the default credential name.
  - Updated the device templates.
- Updated the "Supplemental Device Class" PowerPack version 105 to include the following devices classes that are supported by the Skylar One agent:
  - Ubuntu 18.04, 20.04, 22.04, 23.04
  - Oracle Linux 8, 9, 10
  - Debian 9, 10, 11, 12
  - CentOS 8
  - AIX 7.3
  - AlmaLinux
  - Amazon Linux
  - Rocky Linux
- The "SL1 Default Dashboards Base Pack" PowerPack was rebranded as "Skylar One Default Dashboards Base Pack" and all references to SL1 were updated to Skylar One.

- The Skylar One 12.5.1 ISO also includes the following updated PowerPacks:
  - Cisco: Base Pack version 216
  - Cisco: IPSLA version 104
  - Datacenter Automations Utilities version 201
  - Entity MIB version 102
  - Generic Switch/Router MIB Support version 106
  - Host Resource Core Pack version 109
  - Linux SSH Automations version 107
  - Microsoft: Windows Server version 118
  - Net-SNMP Base Pack version 103
  - SL1: Collector Affinity version 101
  - VMware: vSphere Base Pack version 309
  - Windows PowerShell Automations version 105

**NOTE:** Due to a known issue, you might need to manually upgrade several of these PowerPacks. For more information, see the section on "System Upgrade" in the [Known Issues](#).

## Run Book Automation

- Added a new RBK\_ACTIONS\_SNIPPET access hook that enables users to edit the snippet code for run book actions. Users without this hook aligned who have the ability to view or edit run book actions can still create or edit actions, but they cannot edit the run book actions' snippet code.
- Updated the Run Book Automation Engine to ensure that the run book automations for ServiceNow events or incidents are not triggered prematurely. For more information, see the manuals for the "ServiceNow CMDB" SyncPack or the "ServiceNow Incident" SyncPack.

## ScienceLogic Libraries and Execution Environments

- You can no longer select Python 2 versions in the **Environment Type** drop-down field when creating or editing execution environments.
- Updated the "sl1\_snippet\_api" library to version 3.1.1. This update introduces a default value feature, which includes predefined configurations for various SSL components such as protocols.

## Subscription Billing

- Replaced the subscription usage crunch process with a more efficient Python 3-compatible process.

**IMPORTANT:** This new process requires a configuration change in the `/etc/silo.conf` file if you use the Secure (offline) Process. To enable this process, go to the console of the appliance or use SSH to access the server, then log in as `em7admin` with the appropriate password. Type `sudo visolo` to open the `etc/silo.conf` file, then add `mode=LOCAL` in the `SUBSCRIBER` block. When you are finished, type `:wq` to save your changes and exit the file.

## User Interface

- The **About** page now displays the AP2 release version name in addition to the existing AP2 release version number. The release name also appears for hotfix versions within the same release.
- The text editor that is embedded on pages throughout the classic Skylar One user interface was updated to the latest version, 4.2.2. This updated text editor includes a **[Template]** button, which gives you access to a variety of forms, like a Change Control Worksheet and an Escalation Process form.
- The **SL1 Developer Logs** page (System > Tools > SL1 Developer Logs) has been renamed to **AP2 Developer Logs** and the corresponding item in the left-hand navigation menu has also been updated to reflect this change.
- Added a confirmation dialog window that appears when you attempt to clear or delete a Dynamic Application from the **Dynamic Applications Manager** page (System > Manage > Dynamic Applications) in the classic user interface.

---

## Issues Addressed in Skylar One Juneau 12.5.1

This section describes the issues that were addressed in Skylar One Juneau 12.5.1.

### Agent

- Resolved an issue that caused base minute aggregator crashes if the payload was missing process data. (Case: 00466067) (Jira ID: EM-72119)
- Resolved an issue that prevented non-administrator users with appropriate permissions from aligning agent devices to a log monitoring policy because the option was missing from the **Device Select** drop-down field (Registry > Monitors > Logs > Create > Device Select). (Case: 00244802) (Jira ID: EM-50798)
- Updated agent log file monitoring policies to ensure the policies respect case-sensitivity in the log name. (Case: 00468003) (Jira ID: EM-70780)

- The **Interface Properties** page for Gen 3 agents is now grayed out because the agent interface data collection defaults to 5 minutes, and this value is not configurable. (Cases 00434062; 00477448) (Jira ID: EM-64812)
- Resolved an issue that prevented Skylar One from recognizing an operating system update on a Linux or Windows device that has a Gen 1 or Gen 3 agent installed. (Cases: 00388396, 00392928) (Jira ID: EM-61974)
- Updated the legacy Gen 1 agent pipeline to automatically update the device class to recognize the operating system resolving the pipeline's attempt to reclassify devices if the operating system or other details have changed. (Cases 00388396, 00392928) (Jira IDs: EM-71006, EM-61974)
- Resolved an issue that caused processes to stop updating, which resulted in a grayed out **[Process]** tab, false alerts, and error messages for the agent-vitals-process-store-logs. (Case: 00464759) (Jira ID: EM-66779)
- Updated the logic around how CPU resource limits are evaluated to ensure that an alert is triggered when usage exceeds the configured limit. (Case: 00513863) (Jira IDs: EM-73869, EM-74320)
- Resolved an issue that prevented users from upgrading or deploying the agent to stacks running the Extended Architecture in versions prior to 12.3.8. (Case: 00548279) (Jira ID: EM-76983)

## Anomaly Detection

- Ensured that anomaly detection prediction graphs display properly for on-premises accounts. (Jira ID: EM-73617)

## API

- Resolved an issue where Run-As accounts could be granted incorrect access hooks. (Jira ID: SLUI-21780)
- Added a new device\_group\_name filter for the device API endpoint and ensured that the existing device\_group and organization filters work as intended. (Case: 00505039) (Jira ID: EM-72774)
- Resolved an issue with Aurora 3 where you were unable to enable TLS verification through the user interface or API. (Jira ID: SLS-1834)

## Asset Management

- Addressed an issue where the Asset Record Maintenance process generated false-positive notices and log messages stating that an asset record was changed. (Case: 00492477) (Jira ID: EM-72269)
- Asset values from collection objects with a larger asset precedence setting are now honored during Dynamic Application collection. (Case: 00452509) (Jira ID: EM-66153)
- Removed incomplete software inventory records from processing when the "Enterprise Database: Software Title" inventory updater process runs. When the process is in DEBUG mode, users receive the log message for the incomplete software inventory result(s) in the **/var/log/sl1/software\_inventory\_update.log** file to denote which Dynamic Application and device has collected an incomplete inventory record that will not be processed. (Case: 00465611) (Jira ID: EM-66957)

- Resolved an issue that prevented the "Enterprise Database: Asset Record Maintenance" process from running properly, which resulted in fatal errors and empty records. (Case: 00502077) (Jira ID: EM-73078)

## Authentication and Access Control

- Addressed an issue where SNMP v3 default authentication failed on new Message Collectors. With this update, you can configure SNMPD community/user access using the `slmenu` feature. For more information, see the section on [Credentials Required for Self-Monitoring](#) in the **System Administration** manual. (Case: 00482414) (Jira ID: EM-71374)
- Fixed a typo in the names of several access hooks related to log file monitoring policies. (Case: 00466213) (Jira ID: EM-67028)
- Resolved an issue that directed users to the incorrect page when they attempted to reset their system password from the default user interface (AP2). (Jira ID: SLS-1544)

## Backups

- Addressed an issue that generated an error related to 'rclone\_proc' after successfully completing a backup. (Case: 00329757) (Jira ID: EM-57034)

## Business Services

- Resolved an issue that prevented the **Overview** panel at the top of the **Service Investigator** page from loading the sunburst chart when creating a device service. (Jira ID: SLUI-21084)
- Addressed an issue that caused the following error message when accessing the console of the Skylar One server after creating or editing existing device services: "Float cannot represent non numeric value: Infinity". (Jira ID: SLUI-21002)
- Resolved an issue that resulted in an error message if you attempted to duplicate a business, IT, or device service but that service included organizations you do not have access to. (Jira ID: SLUI-20008)
- Resolved an issue that caused business service "availability" metrics to be indicated by percentages rather than boolean or unitless values. (Jira ID: EM-71963)

## Classic IT Services

- Resolved an unhandled exception error in classic IT Service management caused by "KeyError: 'app\_id'" when using hardware metrics with virtual devices. (Cases: 00515724, 00515952) (Jira IDs: EM-73994, EM-74055)

## Credentials

- Resolved an issue where the Credential Tester on the **Credentials** page (Manage > Credentials) sometimes marked its progress as complete without finishing all steps, leading to missing expected error messages for failed credentials. (Case: 00467981) (Jira ID: SLUI-21086)

- Resolved an issue in the **Edit Credential** modal where, when editing or testing a credential, the **Select Credential Test** field in the **Credential Tester** panel was not showing the full list of credential tests. (Case: 00517459) (Jira ID: SLUI-22132)
- Updated the Enterprise Key Management Service (EKMS) to ensure the service syncs properly with Data Collectors. (Jira ID: SLS-1589)
- Ensured that existing SNMP credentials rotate as intended in systems that have EKMS enabled. (Jira ID: EM-72425)
- Resolved an issue that caused DNS resolution errors to appear in the system log when using a PowerShell credential, which could then result in data pull high frequency rows behind events. (Jira ID: EM-76485)

## Dashboards

- Resolved an issue where the **Device Group Editor** modal did not show any information after clicking a device group name in **Device Group** dashboard widgets. (Jira ID: SLUI-20703).
- Addressed multiple issues that impacted **Device** widgets that use the *Leaderboard* visualization option. (Case: 00489835) (Jira IDs: SLUI-20510, SLUI-20627, SLUI-20681, SLUI-21554)
- Resolved an issue where **Interface** widgets with the *Leaderboard* visualization option were not showing information about discovered network interfaces under the **Utilization In** and **Utilization Out** columns. (Jira ID: SLUI-20933)
- Resolved an issue where PowerPacks containing dashboards that used metric IDs to identify Dynamic Applications were resulting in incorrect matches. (Jira ID: SLUI-20924)
- Ensured that columns in **Device Groups** widgets can be properly sorted. (Jira ID: SLUI-20610)
- Resolved an issue where **Subscription License Reports** dashboard widgets inaccurately reported licenses in Skylar One when multiple instances of the **Dashboards** page were open at the same time. (Jira ID: SLUI-20951)
- Addressed an issue that caused multiple GraphQL errors when loading dashboards containing **File Systems** widgets over 1 TB. (Case: 00489856) (Jira ID: SLUI-21218)
- Resolved an issue where the **Dashboards** page malfunctioned when typing too quickly in the search field of a widget. (Case: 00496272) (Jira ID: SLUI-21561)
- Resolved an issue where **Filesystem** and **Services** widgets that were subscribed to other widgets capable of publishing filesystem and services data retained the data from the publishing widgets to which they were subscribed, even if all rows in those publishing widgets had been deselected. (Jira ID: SLUI-21548)
- Addressed an issue that caused Skylar One to generate an error when trying to narrow down the data displayed in a dashboard using the **[Filter]** button with a basic name query. (Jira ID: SLUI-21132)
- Resolved an issue where performance metric references in dashboard widgets could display incorrect or blank values when the dashboard was installed through a PowerPack. (Case: 00494949) (Jira IDs: SLUI-21486, SLUI-22044)
- Resolved an issue where auto-refreshing on the **Dashboards** page was not keeping user sessions active, even when the **Page Auto-Refresh Keeps User Session Active** field was set to *Enabled* on the **Behavior Settings** page (System > Settings > Behavior). (Case: 00503563) (Jira ID: SLUI-21787)

- Resolved an issue where **Device** widgets using the *Line Chart* visualization could not be saved when a negative value was entered in the **Threshold Line** field. (Case: 00488189) (Jira ID: SLUI-22119)
- Resolved an issue where selecting multiple devices for widgets using the *Forecast* visualization did not display information for all selected devices. (Case: 00526493) (Jira ID: SLUI-22344)
- Addressed an issue on the **Dashboards** page where widgets using the *Table* or *Bar Chart* visualizations did not update when the time span was adjusted. (Case: 00515942) (Jira ID: SLUI-22141)
- Ensured that filtering by device group works as intended in classic dashboard widgets. (Case: 00515536) (Jira ID: EM-74590)
- The **Total Network Traffic** widget in **Server** dashboards now displays data as intended without errors. (Case: 00516146) (Jira ID: SLUI-22206)

## Data Collection and Retention

- Addressed an issue that impacted PowerShell-based data collection. (Jira ID: EM-70764)
- Addressed an issue that caused false SNMP error events to appear for Windows and Linux devices for services that were not running. (Cases: 00472205, 00484057) (Jira ID: EM-71494)
- Added error handling when daily maintenance fails to create device log messages for asset service and warranty expirations. (Case: 00475225) (Jira ID: EM-71000)
- Resolved an issue that resulted in critical unhandled exceptions occurring during the data collection process. (Case: 00447219) (Jira ID: EM-65798)
- Addressed an issue that prevented SNMP Dynamic Applications from working when the default max repeat value was set at 10. (Case: 00089993) (Jira ID: EM-29003)
- Local credentials used for Concurrent PowerShell monitoring now all share a single child process, which reduces the resource requirements on the Skylar One Collector. (Cases: 00400476; 00404282) (Jira ID: EM-62374)
- Updated the "Host Resource: Storage" Dynamic Application to prevent a log message from continually appearing in the device log if an index does not have a value that can be used for deviation alerting. (Case: 00472966) (Jira ID: EM-71131)
- Resolved an issue that caused occasional unhandled exceptions in the Collector Task Manager process (em7\_ctaskman) due to a query deadlock with another Skylar One process. (Case: 00480458) (Jira ID: EM-71439)
- Addressed an issue that prevented Skylar One from storing the result of ModuleCmdStorage in system logs. (Cases: 00466380, 00470300) (Jira ID: EM-67223)
- Improved the Job Scheduler process stability to ensure database connection and transaction resources are initialized and cleaned up properly after every schedule activates, regardless of the schedule's status. (Cases: 00447556, 00448996) (Jira ID: EM-65598)
- Resolved an issue with CDP and LLDP topology that generated hundreds of minor system log messages per second. (Case: 00491695) (Jira ID: EM-72199)
- Ensured that the **OID Browser** page (System > Tools > OID Browser) properly displays symbolic names for newly added OIDs. (Case: 00457239) (Jira ID: EM-66400)

- Resolved an issue that caused critical unhandled exception events to occur with the "Data Collection: Interface Bandwidth: Traceback" process during collection. (Cases: 00429936, 00463088) (Jira ID: EM-64487)
- Ensured that errors due to bad Internal Collections Dynamic Application (ICDA) data are handled with a stack trace message explaining what has failed during the ICDA collection. (Case: 00450992) (Jira ID: EM-65971)
- Addressed logic errors in critical ping storage and alerting, and also addressed an issue that was causing a unhandled exception. (Jira ID: EM-71776)
- "Index Label" class collection objects now properly store the index value when concurrent SNMP collection is enabled. (Case: 00510290) (Jira ID: EM-73945)
- Resolved an issue that caused collection to terminate without completing (SIGTERM) when adding overrides for class-based quality of service (CBQoS) alerts and thresholds. (Case: 00490191) (Jira ID: EM-71930)
- Resolved an issue that caused very high CPU usage, SIGTERMs, and other collection issues on Data Collectors due to the same query running multiple times. (Cases: 00502085, 00502942) (Jira ID: EM-73066)
- Decreased the likelihood of deadlocks occurring in high availability or disaster recovery deployments due to DCM storage errors caused by medium-frequency data pull processes. (Case: 00503245) (Jira ID: EM-72962)
- Resolved an issue that caused the "Data Collection: Interface Bandwidth" process to sometimes experience unhandled exceptions when upgrading from an Skylar One version using Python 2.7 for interface collection to one using Python 3.6. (Case: 00500434) (Jira ID: EM-72827)
- Resolved several issues with data collection in SOAP, XML, and XSLT Dynamic Applications. (Case: 00501856) (Jira IDs: EM-72949, EM-73096)
- Addressed an issue that caused data collection to fail for some SNMP Dynamic Application collection objects if they used certain advanced Object ID field features and PDU packing or concurrent SNMP collection was enabled. (Case: 00494992) (Jira ID: EM-73047)
- Ensured that failed or incomplete OS Process monitoring data collection does not result in false-positive alerts. (Case: 00485271) (Jira ID: EM-71756)
- Resolved inconsistencies in device component tree data that caused fatal errors in hourly maintenance. (Case: 00510037) (Jira ID: EM-73621)
- Improved logic to prevent false service monitoring alerts when internal collections Dynamic Applications data collection fails. (Case: 00517693) (Jira ID: EM-74564)
- Added caching capabilities to the scheduler service to reduce the risk of memory errors that could result in missed or late scheduled actions. (Case: 00509068) (Jira ID: EM-73513)
- Updated class-based quality of service (CBQoS) inventory collection to stop unnecessary collection attempts on disabled interfaces, which were resulting in issues on systems with a large number of interfaces. (Case: 00511842) (Jira ID: EM-74563)
- Resolved an issue with CBQoS data collection that resulted in MF rows behind issues on Data Collectors due to a large number of CBQoS queries. (Case: 00521312) (Jira ID: EM-75442)
- Updated CBQoS inventory collection to discard only invalid CBQoS objects rather than all collected objects for a device if the system encounters an invalid SNMP index on the device. (Case: 00523571) (Jira ID: EM-75171)



- Resolved an issue with data collection in XSLT Dynamic Applications. (Jira ID: EM-73096)

## Deployment and Configuration

- Addressed an issue that prevented users who were using a yum proxy from logging in to the Web Configuration Utility. (Case: 00515777) (Jira ID: EM-74126)
- Resolved an issue where attempting to update the Web Config Utility login passwords for your Skylar One appliances resulted in error messages. (Cases: 00504492, 00505294) (Jira IDs: EM-72698, EM-72959)
- Addressed an issue where the use of a percentage character (%) in a password prevented firstboot from completing. (Case: 00509045) (Jira IDs: EM-72924, EM-73391)

## Device Management

- Improved the load time for the **[Performance]** tab when users view device class-based quality of service (CBQoS) performance metrics. (Case: 00488049) (Jira ID: EM-71873)
- During SNMP device discovery, Skylar One now converts any control characters that are returned for the "sysname" OID to UTF-8 so the characters display properly in the user interface. (Case: 00452024) (Jira ID: EM-66235)
- Ensured that the process of merging a component device into a physical device works as intended, even if Dynamic Applications aligned to the component device have not collected any data. (Cases: 00473976, 00483167) (Jira ID: EM-70925)
- Improved indexing on the database table that stores device notes to enable faster API queries. (Case: 00428585) (Jira ID: EM-64156)
- Resolved an issue where deleting devices resulted in orphaned component devices. (Case: 00503030) (Jira ID: EM-72853)
- Resolved an issue that caused duplicate SNMP strings to appear in the **Availability Port** drop-down field on the **Device Properties** page (Registry > Devices > Device Manager > wrench icon). (Case: 00356953) (Jira ID: EM-59282)
- Updated a misleading response that was provided when using the API to delete a device. (Case: 00376359) (Jira ID: EM-60528)
- Updated the device **Collection State** value *Maintenance* to *Scheduled Maintenance*. This change is reflected throughout the Skylar One user interface. (Case: 00320884) (Jira ID: EM-56785)
- When you update a device class type that is assigned as the default element for an inbound email event rule, that default element information is now also updated accordingly. (Case: 00261651) (Jira ID: EM-52419)
- Addressed an issue with topology crunch that caused blank duplicate interfaces to display under the CDP heading in the **[Relationships]** tab of the **Device Properties** pane. (Case: 00474408) (Jira ID: EM-71018)
- Ensured that LLDP relationships are created properly based on device name. (Case: 00471899) (Jira ID: EM-70782)
- Updated the manner in which Layer 3 topology results are collected and handled to ensure Layer 3 topology collection runs successfully. (Case: 00478864) (Jira ID: EM-71175)

- Ensured that when a device group's maintenance schedule is configured with a **Scope** value of *Group and Children*, the devices included in the device group's subgroups also go into maintenance mode at the scheduled time. (Case: 00318136) (Jira ID: EM-55841)
- You can no longer save schedules where the duration of the schedule is longer than the recurrence interval. For example, you can no longer save a schedule that lasts one day but has a recurrence interval of two hours. (EM-71745)
- Added a new **Ignore Case** checkbox when defining a system process monitoring policy on the **[Proc Policies]** tab in a device template. This option enables you to determine if Skylar One should ignore case-sensitivity in the process name when determining whether to run the system process monitoring policy for devices that were created or modified using the device template. (Case: 00403914) (Jira ID: EM-62836)
- Resolved an issue on the **Devices** page where bulk action options under the **[Actions]** button were not sorted alphabetically in the Firefox browser. (Jira ID: SLUI-20870)
- Ensured that the **[Relationships and Memberships]** panel on the **Device Investigator** can properly display the table of services from the **[Services]** tab. (Jira ID: SLUI-20564)
- Resolved an issue on the **Devices** page that prevented columns from being hidden when the table was sorted or filtered by those columns. (Jira ID: SLUI-20413)
- Improved system performance around purging vanished device components during hourly maintenance processes. (Case: 00446959) (Jira ID: EM-65623)
- Resolved an issue where cleared Skylar AI events from the **[Events]** tab of the **Devices** page did not display when sorting the table by cleared events. (Jira ID: SLUI-20889)
- Ensured that you can duplicate or assign icons to device categories from the **Device Categories** page (Devices > Device Categories). (Jira ID: SLUI-21016)
- When the "Microsoft: Windows Server IC Interface Inventory" Dynamic Application collects both IPv4 and IPv6 addresses from interfaces on a Windows device, those addresses will now all be displayed in the **IP Address** drop-down field of the **Device Properties** page (Devices > Device Manager > wrench icon). (Case: 00376135) (Jira ID: EM-70574)
- The **Collector Groups** page (Manage > Collector Groups) now displays the correct number of Data Collectors in a collector group, rather than incorrectly indicating a maximum of 10 Data Collectors per collector group. (Case: 00501726) (Jira ID: SLUI-21874)
- Resolved an issue where searching for the location of an asset or device on the **Asset Manager** page (Registry > Assets > Asset Manager) resulted in an error. (Case: 00500159) (Jira ID: SLUI-21765)
- Addressed an issue that sometimes caused an exception in the system log after nightly auto-discovery completed for interfaces that did not have the `ifDescription`, `ifSpeed`, or `ifHighSpeed` properties set. (Case: 00508599) (Jira ID: EM-73545)
- When you select a collector group in the **[Config]** tab of a device template and then apply that template to a device, it now properly aligns the device to the selected collector group as intended. (Cases: 00471246, 00482918, 00506448) (Jira ID: EM-70819)
- Ensured that the "Update Device State" process to store the state of a device group completes successfully. (Case: 00521186) (Jira ID: EM-74930)
- Ensured that the columns on the **[Events]** tab of the **Device Investigator** are sortable. (Jira ID: SLUI-20991)

- Resolved an issue that caused a search on collectionState in the getInterfaces GQL query to return an error. (Case: 00523713) (Jira ID: SLUI-22466)

## Discovery

- Addressed an issue that caused duplicate device components when saving a device component that included a backslash (\) for the GUID or unique\_id. (Case: 00473348) (Jira ID: EM-70760)
- Resolved an issue that caused Dynamic Application discovery and auto-alignment to sometimes fail with KeyErrors when snippet or bulk snippet Dynamic Applications did not return a full or correct set of results during their initial execution that occurs during discovery. (Case: 00462791) (Jira ID: EM-66738)
- Interfaces with unexpected characters in their properties no longer block Skylar One from discovering the device that contains that interface. (Case: 00411856) (Jira ID: EM-62795)
- Resolved an issue that caused some bullet points on the guided discovery pages to appear as â€¢. (Jira ID: SLUI-20614)
- Ensured that SNMP timeouts or other errors occurring while attempting to retrieve a device's sysobjectid does not result in the removal of the device's device class. (Case: 00450503) (Jira ID: EM-71048)
- Updated the "Discovery: Nightly Update" process to ensure the process completes correctly and mitigate unhandled exceptions. (Case: 00480561) (Jira ID: EM-71440)

## Documentation

- Updated the **System Administration** manual chapter on "Skylar One Self-Monitoring" to address several issues with the instructions provided. (Case: 00443290) (Jira IDs: EM-65342, EM-65343)
- Updated the "Restoring Backups" topic in the "Backup Management" chapter of the **System Administration** manual to include additional procedures and information. (Cases: 00433223, 00495469) (Jira ID: EM-64688)
- Updated the **Device Management** manual chapter on "Creating a Physical Device without Running Discovery" to show the proper class\_type format when using a CSV file to create physical devices. (Case: 00386036) (Jira ID: EM-61542)

## Event Management

- Addressed an issue that caused event redirects to sometimes not work properly or not show the correct organization ID when redirecting between devices in different collector groups. (Case: 00464589) (Jira ID: EM-66990)
- Ensured that deleting a child event within a group deletes only that event and not its parent event when the **Event Clearing Mode** setting *Clear all in group* is selected. (Cases: 00278705, 00377687) (Jira ID: EM-53290)
- Events raised for an expired SSL certificate on a device are now properly cleared when the certificate is renewed. (Cases: 00316477, 00336592, 00422336) (Jira ID: EM-56192)
- Resolved an issue that caused message match to fail if the event message contained a backslash. (Case: 00448918) (Jira IDs: EM-65861, EM-66664)

- Deleting Dynamic Applications with a substantial amount of stored data no longer negatively affects handling of events or other system processes. (Case: 00467628) (Jira ID: EM-67099)
- Resolved an issue on the **Events** page that prevented columns from being hidden when the table was sorted or filtered by those columns. (Jira ID: SLUI-20413)
- Addressed an issue where the email round trip monitor did not work properly because emails were using the same auto-increment value. (Case: 0481116) (Jira ID: EM-71331)
- Addressed an issue that prevented the **Enable Event Policy** toggle from being visible when the top bar was set to a dark color while using a light theme in Skylar One. This issue was addressed as part of the [updates to the Event Policy Editor](#) by moving the **Enable Event Policy** option to the **[Basic]** tab and making it a checkbox instead of a toggle option. (Cases: 00321580, 00422365) (Jira ID: SLUI-21444)
- Updated the "Appliance Validation" Dynamic Application to fix Message Collector memory calculation in the "Support: Appliance Validation Minimum MC Requirements Not Met" event. (Jira ID: EM-65495)
- Resolved an issue that prevented the event engine from properly decoding some inbound email messages due to special characters. (Jira IDs: EM-72656, EM-72242)
- Addressed an issue that closed the browser window when the **[Create External Ticket]** button was clicked for an event listed on the **Events** page. (Case: 00469006) (Jira ID: SLUI-20898)
- Resolved an issue where users with limited permissions might have encountered an error message when clicking the **[Actions]** button (the ellipses icon) at the following locations:
  - The top-right corner of the **Event Overview** panel of the **Event Investigator** page
  - The **Events** table that appears on the **Events** page, **Service Investigator** page, or **Device Investigator** page
  - The **Changes** table on the **Service Investigator** page
  - The **Log Insights** table on the **Service Investigator** page
 (Case: 00498124) (Jira IDs: SLUI-21788, SLUI-21866)
- Resolved an issue that caused the event engine to crash if an internal event included a non-UTF-8 character. (Jira ID: EM-74969)
- Ensured the correct "yname" (sub-entity name) is set for each event policy when multi-match is enabled to confirm that event auto-clearing works as expected. (Case: 00474473) (Jira ID: EM-71282)
- Addressed an issue that prevented event notes from displaying in the exported CSV file created from the **Events** page or **Events** dashboard widgets. (Case: 00523119) (Jira ID: SLUI-22260)
- Updated the "notifierLogs" GraphQL query so that when an event search is executed, it will only return logs for events with event IDs included in the filter. (Case: 00524845) (Jira ID: SLUI-22340)

## Global Manager

- Resolved a caching issue in the Global Manager NextUI service that temporarily stored user information, allowing subsequent different users to load the cached information. (Jira ID: SLUI-20931)

- Resolved an issue where the graph in the **Skylar Analytics Summary** widget of the **Event Investigator** page did not load or display correctly when viewed on a Global Manager system. (Jira ID: SLUI-21073)
- Resolved an issue in Global Manager where SAML SSO for Skylar One authentication was providing users with incorrect permissions, which resulted in increased or reduced access rights. (Case: 00492738) (Jira ID: SLUI-21564)

## GraphQL

- Addressed an issue where running the "GlobalManagerDeviceCategories" query with Global Manager enabled returned a null value for all queried fields, except for the "id" field. (Jira ID: SLUI-20601)
- Resolved an issue that caused device queries based on interfaces to fail. (Case: 00513430) (Jira IDs: SLUI-22069, SLUI-21560)
- Resolved an issue where the "createDiscoverySession" mutation produced an error when upgrading SL1 to version 11.3.1. (Case: 00360478) (Jira ID: SLUI-21434)
- Fixed an issue where creating discovery sessions using the "createDiscoverySession" mutation resulted in an error and the discovery session wasn't created. (Case: 00511630) (Jira ID: SLUI-22182)
- Resolved an issue where queries returned null results when searching for an organization with a null value, which caused an error during the query execution. (Case: 00522745) (Jira ID: SLUI-22442)

## Inbound Messaging

- Addressed an issue where the email setting for an authorized domain was not saved. (Case: 00509457) (Jira ID: EM-73388)
- Resolved an issue that was preventing SNMP trap messages from displaying correctly when the sequence is not a hex string. (Case: 00534742) (Jira ID: EM-75898)

## Logging

- 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)
- Ensured that log messages indicate whenever interfaces are removed from bandwidth billing policies. (Case: 00432744) (Jira ID: EM-66251)
- Resolved an issue that prevented non-administrator users in STIG deployments of Skylar One from sometimes viewing the system status log or run the system status script. (Jira ID: EM-71273)

## Maps

- Resolved an issue where the **Classic Maps** page failed to load properly whenever you attempted to log in to AP2 without accepting the End-User License Agreement (EULA). (Jira ID: SLUI-20801)

## Monitoring Policies

- Addressed an issue that prevented web content monitoring policies from decoding content if the system could not detect the encoding from the headers or content, which resulted in errors when the policies checked for expressions. (Case: 00534734) (Jira ID: EM-75892)

## PhoneHome Communication

- Improved responsiveness of the PhoneHome connection by enabling the "keepalive" option for the TCP connection. (Jira ID: EM-65069)
- Added a new, configurable keepalive timeout setting for PhoneHome collectors. This new setting, which can be set at the appliance command line using the command `sudo phonehome config set keepalive_timeout <value>`, enables you to adjust the timeout value for sending keepalive requests to the server, which can be helpful for PhoneHome collectors with high network latency. You can configure the `keepalive_timeout` setting to a value between 10 seconds (10s) and 10 minutes (10m). (Case: 00449593) (Jira ID: EM-65809)

## Platform and Security

- Updated the web server configuration for the vault service to improve behavior between multiple database and data engine appliances, to address an issue that caused false system events indicating that passive databases could not connect to Skylar One Collectors in high-availability (HA), disaster recovery (DR), or HA+DR configurations. This update might require users on HA / DR configurations to take action upon installing or upgrading to Skylar One 12.5.1. For more information, see the section on "Changes to High Availability and Disaster Recovery Configurations" in the [Important Upgrade Notes for Skylar One Juneau 12.5.1](#). (Cases: 00434477, 00435183) (Jira ID: EM-64808)
- Added an etype index for the `master_events.events_active` database table to address an issue that prevented run book queries from running successfully on AWS Aurora RDS deployments of Skylar One. (Cases: 00279302, 00418325) (Jira ID: EM-53171)
- Added an option to increase the open file descriptor limit through a new "open\_file\_limit" configuration option in the `/etc/silo.conf` file under the `[CONFIG_PUSH]` heading. This new option defaults to a value of 1024. (Case: 00460017) (Jira ID: EM-66579)
- Increased time-to-live (TTL) from one minute to five minutes for cached device group suppression in the event engine to prevent long-running queries from getting stuck. (Cases: 00459999, 00462563) (Jira IDs: EM-66517, EM-75455)
- Addressed an issue in post-processing with Dynamic Application index mapping that caused an infinite error loop whenever an existing index that had a non-accented character was replaced by an accented version of the same character, or vice versa. (Case: 00477206) (Jira ID: EM-71069)
- Events are no longer automatically triggered every minute when a Skylar One process that runs daily or less frequently terminates collection without completing (SIGTERM), to decrease the number of events and the amount of log "noise" generated for this condition. (Case: 00453028) (Jira ID: EM-66248)

- Ensured that legacy PowerShell processing, including handling of the "Microsoft: SQL Server Enhanced" PowerPack, honors your message encryption settings. (Case: 00453220) (Jira ID: EM-66122)
- Resolved an issue where Skylar One displayed a "Receiving 504 Gateway Time-out" error message when attempting to access the **Audit Logs** page (System > Monitor > Audit Logs). (Case: 00415120) (Jira ID: SLUI-21014)
- Addressed an issue that caused HF rows behind unhandled exceptions due to infrequent deadlocks. (Case: 00462819) (Jira ID: EM-66648)
- Resolved an issue that caused password reset emails that directed users to the classic Skylar One user interface even when the password reset was requested from the default Skylar One user interface (AP2). (Case: 00458525) (Jira ID: SLUI-20939)
- Resolved an issue that caused Skylar One services to sometimes experience an approximately 15-minute delay before restarting on the High Availability (HA) failover node if you performed a hard stop on a primary HA node. (Cases: 00459541, 00522323) (Jira ID: EM-66492)
- Addressed an issue where upgrades failed if a user had a hashtag character (#) in the database password. (Jira ID: EM-74737)

## PowerPacks

- On the **PowerPack Manager** page (System > Manage > PowerPacks), the ***DashSL1*** column now displays on STIG systems in addition to non-STIG systems. (Case: 00465085) (Jira ID: EM-66815)
- Resolved an issue that caused unhandled exceptions relating to two Dynamic Applications in the "ScienceLogic Support Pack" PowerPack that contained SQL queries with the keyword "function", which is a reserved keyword in MySQL 8.0. (Jira ID: EM-72266)

## Reporting

- Resolved an issue that prevented PDF and XSLX Ticketing report types from generating properly due to OL8 incompatibility issues. Also resolved an issue where those report types and ODS reports could not be generated on the **Classic Devices**, **Organizations**, or **Tickets** pages. (Jira IDs: EM-51131, EM-73498)
- Ensured that file names are properly aligned with user validation and that reports download successfully from the **Report Output Template** page. (Case: 00544908) (Jira ID: EM-76453)
- Resolved an issue that prevented reports with embedded images from properly generating. (Case: 00469311) (Jira ID: EM-71633)
- The "Performance Multi Object/Device Table" report now includes the ***Mounted On*** value for the "IBM: AIX FileSystem" Dynamic Application. (Case: 00507256) (Jira ID: EM-73338)
- Resolved an issue that caused unhandled exception errors when generating a "PowerPack Information" report. (Jira ID: EM-76056)

## Run Book Automation

- For users of the "ServiceNow CMDB" SyncPack and the "ServiceNow Incident" SyncPack, addressed an issue that occurred when an event was sent to PowerFlow and a run book automation was started as soon as the event was in the sync queue, instead of when the external ticket was created. (Case: 00428951) (Jira ID: EM-67235)
- Resolved an issue that limited the number of devices that could be aligned to a run book automation policy. (Case: 00465094) (Jira ID: EM-67035)

## ScienceLogic API

- Updated the ScienceLogic REST API to ensure that numerous queries against the "Device" endpoint would not result in heavy MySQL load. (Jira ID: EM-76429)
- Resolved an issue that prevented users from filtering devices by device group in the REST API. (Case: 00472441) (Jira ID: EM-71052)

## Skylar AI

- Addressed an issue where the **Metric Type** column on the **Anomaly Detection** page displayed the presentation ID for a metric instead of the presentation name for the metric. (Jira ID: SLUI-21510)
- Ensured that the Skylar metadata exporter does not crash when exporting large batches. (Jira IDs: EM-76565, EM-76596)
- Resolved an issue that caused Skylar AI service connections created from the **Service Connections** page (Manage > Service Connections) to not appear in the left sidebar on the **Skylar AI** page. (Jira ID: SLUI-22176)

## Subscription Billing

- Ensured that all device license usage counts appear on the **Subscription Usage** page (Manage > Subscription Usage). (Case: 00424541) (Jira ID: SLUI-19903)

## System Update

- Resolved an issue that caused the siloupdate process to become unresponsive while running a pre-upgrade check, despite appearing to be active. (Case: 00480680) (Jira ID: EM-74321)
- Addressed an issue with the pre-upgrade process where the process did not mark schedules as failed during exceptions, leading to endless loops. (Case: 00417775) (Jira ID: EM-63385)
- When a pre-upgrade failure caused by insufficient disk space occurs, the lines related to disk space are now highlighted in red in the user interface. (Cases: 00388051, 00389037) (Jira ID: EM-61886)
- Addressed an issue where the post-update script 60\_sshd\_config.sh failed when upgrading Skylar One. (Case: 00481367) (Jira ID: EM-71361)



- Ensured that the newer repository metadata is available for appliances that share a MariaDB instance with the primary Database Server, such as the Administration Portal and the secondary/disaster recovery databases. (Case: 00401840) (Jira ID: EM-62393)
- Resolved an issue that caused the post-update process to fail with the message "ha\_status: command not found". (Case: 00509644) (Jira ID: EM-73387)
- Added logs for the `locate-update` command output and the packages that are affected using this command to help you troubleshoot pre-upgrade failures on remote appliances during the staging process for system updates. (Case: 00419470) (Jira ID: EM-63452)

## Topology

- When interfaces that are not discovered in Skylar One are included in topology maps, records for those undiscovered interfaces are no longer created in the database. (Cases: 00377649, 00505904) (Jira ID: EM-61146)
- Lowered the logging trace level in LLDP topology collection to resolve an "Illegal mix of collations" error, which resulted in the Event Engine crashing. (Case: 00519994) (Jira ID: EM-74524)
- Resolved an issue that caused unhandled exceptions during L3 topology data collection when the system encountered a device without a primary IP address. (Case: 00473950) (Jira ID: EM-71630)
- Improved CDP and LLDP topology collection efficiency to enable more devices to be aligned to a Data Collector. (Case: 00515516) (Jira ID: EM-73998)
- Ensured that LLDP topology collection can make multiple relationships between the same devices. (Cases: 00444042, 00549735) (Jira ID: EM-6502)

## User Interface

- Addressed an issue that limited the amount of clickable space for the **[Delete]** button on the **Device Groups** page (Devices > Device Groups). (Case: 00479090) (Jira ID: EM-71302)
- Resolved an issue that caused the **Device Processes** page (Devices > Processes) to sometimes not load properly. (Case: 00429969) (Jira ID: EM-65340)
- Ensured that, in the classic user interface, when a user is required to reset their password, the new password fields appear in the proper location. (Jira ID: EM-74342)
- Resolved an issue where Skylar One appliances did not display as intended when clicking the **[Appliance List]** button on the **Updates** page (System > Tools > Updates). (Cases: 00475665, 00477537, 00488758, 00476368, 00465495) (Jira IDs: EM-66897, EM-71113, EM-71013, EM-66897)
- When adding or configuring **(base) Leaderboard/Top-N** widgets in the classic Skylar One user interface, these widgets can now display performance metrics if you select *Collection Name* from the **Title Label Options** field. (Case: 00422137) (Jira ID: EM-63653)
- Resolved an issue causing longer AP2 login times for non-administrative users or those with limited permissions when using LDAP for authentication. (Cases: 00477960, 00478182) (Jira ID: SLUI-21012)

- Addressed an issue that caused the filter-while-you-type feature to not work as intended for the **Skylar AI Status** column on the **Organizations** page (Registry > Accounts > Organizations). (Jira ID: EM-71414)
- Resolved an issue where the incorrect version number displayed in the system footer. (Jira ID: SLUI-20424)
- The **Agents** page (Devices > Agents) now loads properly when your system includes vanished agent-monitored devices. (Case: 00493976) (Jira ID: EM-79262)
- Addressed an issue where, when running Skylar One on a computer with limited hardware resources, using the **Bandwidth Billing Editor** page (Registry > Service Provider Utilities > Bandwidth Billing > create/edit) would cause some computers to experience an infinite redirect loop and lock up. (Case: 00494962) (Jira ID: EM-72445)

---

## Installing and Upgrading Skylar One

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

For detailed instructions on performing a new installation of Skylar One, see the [Installation and Initial Configuration](#) manual.

For detailed instructions on upgrading Skylar One, see the section on [Updating Skylar One](#) 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.

## Skylar One Extended Architecture

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

**NOTE:** New installations of Skylar One Extended Architecture are available only on SaaS deployments.

---

# Important Upgrade Notes for Skylar One Juneau

## 12.5.1

This section includes important notes for upgrading existing Skylar One systems to the Juneau 12.5.1 release.

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

**CAUTION:** ScienceLogic strongly recommends that you review these notes in their entirety before upgrading to version 12.5.1.

### 12.1.x and 12.2.x Pre-Import Script to Prevent Patching Issues

**WARNING:** *With the Skylar One 12.5.1 Juneau release, support for Python 2 is now deprecated in Skylar One.* Any custom Python 2 content you have developed will stop working if you upgrade to 12.5.1 or later. This includes all Dynamic Application snippets, Execution Environments, Run Book Actions, and ScienceLogic Libraries that use Python 2. These items must be recreated utilizing ScienceLogic-provided enablement tools or migrated to Python 3 **before** you upgrade to this release.

In addition, because of the removal of Python 2 support, if you are upgrading to 12.5.1 from a 12.1.x or 12.2.x release, you must execute a script on your active or primary Database Server or Data Engine **before you import the 12.5.1 patch bundle**. Failure to do so will prevent you from upgrading to 12.5.1. This issue prevents the patch hook RPM from getting installed on the Skylar One appliances in your stack, which in turn prevents you from upgrading to the newer silouupdate RPM that is needed to complete the system update (deployment) process on your Skylar One appliances.

This section describes how to download and run this pre-import script.

For additional information, see the following knowledge base article: <https://support.sciencelogic.com/s/article/19093>

**IMPORTANT:** If you attempt to upgrade from 12.1.x or 12.2.x to 12.5.1 without first running the script, your upgrade will ultimately fail. If this occurs, you can [run a post-upgrade script](#) that will update the silouupdate RPM file on all of your appliances.

**NOTE:** This issue does not impact users upgrading to 12.5.1 from a 12.3.x release. Those users do not need to complete this step. As an alternative to the procedure documented below, current 12.1.x and 12.2.x can instead choose to upgrade to a 12.3.x release and then upgrade to 12.5.1.

To download and run the pre-import script required for users upgrading from a 12.1.x or 12.2.x release to 12.5.1:

1. Before importing the 12.5.1 upgrade file, go the **Release Files** page for 12.5.1 on the ScienceLogic Support site and download the `12-5-1-pre-import-fix.pyc` script: <https://support.sciencelogic.com/s/release-file/aBtVL0000001Dsr0AE/preupgrade-script>.

2. On the active or primary Database Server or Data Engine, verify the checksum:

```
sha512sum 12-5-1-pre-import-fix.pyc

9fb796859a9aef4e8053f6e904bfca35ebdc5dfbffc97f3e76aa08395a727670 12-
5-1-pre-import-fix.pyc
```

3. Set the correct permissions on the script:

```
chmod 755 12-5-1-pre-import-fix.pyc
```

4. Test that you are able to execute the script by running usage help:

```
sudo /opt/em7/bin/python3.6 12-5-1-pre-import-fix.pyc -h
```

5. Validate that you can see a usage help similar to this:

```
usage: 12-5-1-pre-import-fix.pyc [-h] [-v] [--timeout seconds]
```

```
[-m module_id [module_id ...]]
```

```
Fix patcher status script
```

```
optional arguments:
```

```
-h, --help show this help message and exit
```

```
-v, --verbose enable debug logs
```

```
--timeout seconds timeout in seconds
```

```
-m module_id [module_id ...], --mid module_id [module_id ...]
```

```
SL1 appliance ID to run the test on
```

6. Make sure that most of the appliances in the stack are available. The script fixes the problems only on the Data Collectors and Message Collectors that are available and skips any unavailable ones. Note that you might need to run the script again for appliances that were unavailable but became available later. You can also run it for a specific set of appliances by specifying their appliance/module IDs using the `-m` flag.

7. Execute the script. Module selection using the `-m` flag to specify one or more appliance IDs is optional. If you do not select any module, it will automatically select all available Skylar One appliances in the stack:

```
sudo /opt/em7/bin/python3.6 12-5-1-pre-import-fix.pyc [-m <mid_1>
<mid_2> ... <mid_n>]
```

**NOTE:** If you have a large stack, ScienceLogic recommends running the script as a background task as a root user, as shown below:

```
touch /tmp/12-5-1-pre-import-fix.log
```

```
chown em7admin:em7admin /tmp/12-5-1-pre-import-fix.log
```

```
chmod 644 /tmp/12-5-1-pre-import-fix.log
```

```
nohup sudo /opt/em7/bin/python3.6 12-5-1-pre-import-fix.pyc [-m
<mid_1> <mid_2> ... <mid_n>] 2>&1 >/tmp/fix-patcher-status.log &
```

You can then exit from the shell as the root user and can follow the progress of the script by tailing the log file `12-5-1-pre-import-fix.log`.

8. Validate if there are any errors in the log file or in the command output. You might need to look at any reported problem. Fix any issues and then re-run the script for the failing appliances.
9. After you have ensured that most of the appliances in your stack have been fixed by the script, you can import the 12.5.1 patch bundle and proceed with your upgrade.

## Running the Post-Upgrade Recovery Script

If you attempt to upgrade from 12.1.x or 12.2.x to 12.5.1 without first [running the pre-import script](#), your upgrade will ultimately fail. If this occurs, you can run a post-upgrade script to update the silouupdate RPM file on all of your Skylar One appliances.

To download and run the post-upgrade script:

1. Go the **Release Files** page for 12.5.1 on the ScienceLogic Support site and download the `12-5-1-recovery.pyc` script: <https://support.sciencelogic.com/s/contentdocument/069VL00000Xa57tYAB>.
2. On the active or primary Database Server or Data Engine, verify the checksum:

```
sha512sum 12-5-1-recovery.pyc
```

```
3cf3343e96d5d8eade8bf9a0cbf8ba7a1641c3fbaee39234cf7c6b72e239c822 12-
5-1-recovery.pyc
```

3. Set the correct permissions on the script:

```
chmod 755 12-5-1-recovery.pyc
```

4. Test that you are able to execute the script by running usage help:

```
/opt/em7/bin/python3 12-5-1-recovery.pyc -h
```

5. Execute the script. Module selection using the `-m` flag to specify one or more appliance IDs is optional. If you do not select any module, it will automatically select all available Skylar One appliances in the stack:

```
/opt/em7/bin/python3 12-5-1-recovery.pyc [-m <mid_1> <mid_2> ...  
<mid_n>] [-v]
```

**NOTE:** If you have a large stack, ScienceLogic recommends running the script as a background task as a root user, as shown below:

```
touch /tmp/12-5-1-recovery.log
```

```
chmod 644 /tmp/12-5-1-recovery.log
```

```
nohup /opt/em7/bin/python3 12-5-1-recovery.pyc [-m <mid_1> <mid_2> ...  
<mid_n>] [-v] 2>&1 >/tmp/fix-patch-hook.log &
```

You can then exit from the shell as the root user and can follow the progress of the script by tailing the log file: `tail -f /tmp/12-5-1-recovery.log`

## Supported Upgrade Paths

**WARNING:** See the section [12.1.x and 12.2.x Pre-Import Script to Prevent Patching Issues](#) before importing the 12.5.1 patch bundle. This section includes important warnings for users who still have Python 2 content in their Skylar One system or are upgrading from 12.1.x or 12.2.x versions of the platform.

Be advised that you can perform upgrades from one minor version to a subsequent minor version in most cases. 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 validated upgrade paths for 12.5.1:

- 12.3.8 > 12.5.1
- 12.3.7 > 12.5.1
- 12.2.7 > 12.5.1
- 12.1.2 (OL8) > 12.5.1

## STIG Support

STIG-compliant users can deploy this release as an ISO.

12.2.x and 12.3.x STIG-compliant users cannot upgrade to this release.

**NOTE:** When deploying a STIG-compliant configuration, port 7700, the Web Configuration Utility, and the **Database Tool** page are all disabled. In addition, 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 Skylar One 12.5.1. If you are currently deployed using Aurora 2, you can upgrade to Skylar One 12.5.1 but must perform a post-upgrade Aurora 2 to 3 conversion. If you are on a SaaS-hosted AWS deployment, the ScienceLogic SRE team will complete this conversion. If you are on a customer-hosted AWS deployment, you must complete this conversion, with additional steps in the section on [Updating Skylar One](#) in the [System Administration](#) manual. Contact ScienceLogic Professional Services if you need assistance.

## Upgrading MariaDB and Rebooting Skylar One

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

**WARNING:** If you are upgrading from a version prior to 12.2.3, then after upgrading Skylar One, you must also upgrade MariaDB 10.4.x to version 10.6.21. Failure to perform this MariaDB upgrade can cause major functionality issues in Skylar One.

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

Skylar One (SL1) Release	Required MariaDB Version	Requires Appliance Reboot?
12.5.1	10.6.21	Yes
12.3.10 (Upgrade only)	10.6.18	Yes
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

Skylar One (SL1) Release	Required MariaDB Version	Requires Appliance Reboot?
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 Skylar One system, see the section on [Updating Skylar One](#) 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 Cache Post-Upgrade

After upgrading to version 12.5.1, you should clear your system cache to remove cached items from Skylar One (SL1) and prevent several potential issues that can occur post-upgrade due to caching. To do so, go to Misc > Clear SL1 Cache.

## Required Ports

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

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

## Python 3.9 Execution Environment Support Deprecation

Users who are currently on 12.2.x releases and use Python 3.9 execution environments for Dynamic Applications and Run Book Automations are advised that the 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 Skylar One (SL1) version 12.3.4, the tmux utility is disabled by default if you are on a non-STIG deployment and access a Skylar One (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 Skylar One (SL1) deployment, the tmux utility is enabled by default. ScienceLogic encourages non-STIG users to 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, Skylar One (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 Skylar One (SL1) appliance or use SSH to access the 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 Skylar One (SL1) and then log back in. The tmux utility is now enabled.

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

## Changes to High Availability and Disaster Recovery Configurations

In Skylar One (SL1) 12.3.2, the web server configuration for the vault service was updated to improve behavior between multiple database and data engine appliances. This was done to prevent false system events indicating that passive databases could not connect to Skylar One Collectors in high-availability (HA), disaster recovery (DR), or HA+DR configurations. With this update:

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

## System Update Notes

- **Skylar One 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 Skylar One system before performing a system update.
- The Skylar One 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 Skylar One releases during a maintenance window.
- The Skylar One 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 Skylar One 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 Skylar One](#)" chapter of the [System Administration](#) manual.
- When upgrading Skylar One 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 Skylar One Juneau 12.5.1

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

The following known issues exist for Skylar One Juneau 12.5.1:

## Deployment and Configuration

- After deploying or upgrading to Skylar One Juneau 12.5.1, you might be unable to log in to the Web Configuration Utility or port 7700. To resolve this issue, reboot the data engine or restart the `em7_sladmin` service. (Jira ID: EM-73671)

## System Upgrade

**WARNING:** If you are upgrading to 12.5.1 from a 12.1.x or 12.2.x release, you **must** run a script on your active or primary Database Server or Data Engine **before** you import the 12.5.1 patch bundle. Failure to do so will cause the upgrade to fail. For instructions, see the section [12.1.x and 12.2.x Pre-Import Script to Prevent Patching Issues](#) in the [Important Upgrade Notes](#).

Alternatively, you can upgrade to a 12.3.x release and then to 12.5.1, as this issue does not affect the 12.3.x to 12.5.1 upgrade path.

- Support for Python 2 is deprecated in Skylar One as of this release. Any custom Python 2 content you have developed will stop working if you upgrade to 12.5.1 or later. This includes all Dynamic Application snippets, Execution Environments, Run Book Actions, and ScienceLogic Libraries that use Python 2. These items must be recreated utilizing ScienceLogic-provided enablement tools or migrated to Python 3 **before** you upgrade to this release.
- 12.2.x and 12.3.x STIG-compliant users cannot upgrade to this release. 12.5.1 STIG is available only as an ISO.
- When upgrading Skylar One to version 12.5.1, PowerPacks will be temporarily read-only until the update is complete. (Jira ID: EM-73018)
- 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)
- System updates sometimes fail on Data Collectors due to silouupdate not updating on them. For more information about this issue, including workaround procedures, see <https://support.sciencelogic.com/s/article/18508>. (Case: 00543539) (Jira ID: EM-76307)

- After updating your system, you might experience an issue where the user interface is not displaying or working as intended. If this occurs, clear your browser cache. (Jira ID: EM-73859)
- 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)

## Agent

- Clicking the **[Upgrade]** button on the **Agents** page results in a message indicating that the upgrade was successful immediately appearing at the bottom of the page when, in actuality, the upgrade was merely initiated. The actual upgrade process can take several minutes to complete. (Jira ID: EM-74365)
- When attempting to install a Gen 1 agent on an AWS stack, the installation user interface will display an incorrect IP for download, which will result in the download attempt failing. (Jira ID: EM-74307)
- You might experience a scenario where an agent's polled data configuration is cleared unintentionally. (Jira ID: EM-74364)

## Asset Management

- When creating or editing an asset, the values entered in the **Administrator** and **Technician** fields might not be saved. (Jira IDs: EM-74258, EM-76664)

## Authentication

- A known issue with session cache management might cause Skylar One 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 Skylar One user interface. For more information, see <https://support.sciencelogic.com/s/article/13701>. (Jira ID: SLUI-21011)
- The **Single Instance Login** setting, which can be set on the **Behavior Settings** page (System > Settings > Behavior), is not working as designed for local non-administrator user accounts that utilize CAC or 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 create an empty authentication resource with no values filled in and assign it to an empty authentication profile, upon logging out of the system, the user interface becomes inaccessible. (Jira ID: EM-76608)

## 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 have had a child service removed, Skylar One 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.

## Concurrent PowerShell

- Resolved an issue that was sometimes causing a minor event and the message "Updated PowerShell credential schema V2 not available, fallback to V1" to appear in the system log for users who utilize concurrent PowerShell. (Jira ID: EM-74551)

## Credential Management and Discovery

- You might experience a "red bell" error on the **Credentials** page, indicating that the page cannot load. This occurs when a credential GUID length is less than 32 characters. To work around this issue, recreate the credential with the incorrect GUID length, realign all impacted Dynamic Applications and Run Book Automations to that new credential, and then delete the original credential. (Cases: 00568449, 00568858) (Jira ID: EM-77246)
- For an unguided device discovery, the **Search** box that displays for creating a new credential 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)
- The **Credentials** page in the default user interface (AP2) fails to display credentials that are not aligned with an organization, but displays these credentials correctly in the classic Skylar One user interface on the **Credential Management** page. (Jira ID: SLUI-20947)
- On the **Credentials** page, if you have more than 50 credentials and at least one of the first 50 credentials is not aligned with an organization, the page will display duplicates of these credentials. (Jira ID: SLUI-20947)

- On 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)
- When creating or editing a credential, the **Select Credential Test** field in the **Credential Tester** panel might display only a small number of potential credential tests rather than the full list. (Jira ID: SLUI-22754)
- When attempting to discover Oracle devices with Native Network Encryption (NNE) enabled or using secure communication (TCPS), you might receive an error stating that the system failed to initialize Oracle Instance Client libraries, preventing those devices from being discovered. (Jira ID: EM-74110)
- You might get an error when trying to open SOAP/XML credentials that have been imported from a PowerPack. (Jira ID: EM-74291)
- In SOAP/XML credentials that use cURL options, the system might not replace %D or %N variables in the URL with the appropriate IP or hostname value. (Jira ID: EM-72620)



## Dashboards

- Creating an **Interface** widget with the *Leaderboard* visualization, applying an advanced filter, and adjusting the data time span using the **Time span filter** results in an error. (Jira ID: SLUI-22200)
- When editing the scale prefix of a **Device** widget using the *Leaderboard* visualization, the **Storage Used** column does that update in that widget's table. (Jira ID: SLUI-22198)
- When editing an **Events** widget and setting the **Refresh Mode** field to *None*, the widget's events table shows the refresh mode as automatic, despite the change. (Jira ID: SLUI-21947)
- In classic dashboards, if you create a Traffic Light widget, the ability to control context in other subscribing widgets is not working as intended. (Jira ID: EM-76527)

## Data Collection and Retention

- If you include an invalid or incorrectly typed value in `silos.conf`, such as a word or phrase where it should be an integer, the data pull process crashes and cannot start. (Jira ID: EM-74238)
- If you add the `enable_cudaps_service_default` field to the `master.system_custom_config` database table and concurrent SNMP and concurrent PowerShell collection options are disabled, collection output is terminated with the message "Skipping scheduling of non-collectable Discovery and Label (Config Group) objects." (Jira ID: EM-74309)
- You might experience a "float division by zero" unhandled exception during collection if the "Data Collection: Interface Bandwidth" process encounters a "0" value. (Jira ID: EM-76138)
- When aligning a Dynamic Application that discovers a dynamic component map tree using Latin-1 and UTF-8 encoded device names and identifiers, you might receive "Illegal mix of collations" data storage errors in the system logs. (Jira ID: EM-74263)

## 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)
- On the **Devices** page, when sorting your search by the **Organization** column, the inventory table will sort by **Organization ID** instead. (Jira ID: SLUI-21459)
- The assigned organization for devices might not always update, even after performing a bulk alignment organization action on the **Devices** page. To work around this issue, refresh your browser immediately after completing the bulk alignment action. (Jira ID: SLUI-21483)
- The column widths on the **Device Investigator** page do not adjust when resized. (Jira ID: SLUI-20081)
- On the **Devices** page, devices are unable to align with newly created organizations. (Jira ID: SLUI-20941)
- Filtering the **Collector Groups** column on the **Device Investigator** page with multiple group names can cause the page to not load correctly. (Jira ID: SLUI-21035)
- When sorting by columns on the **Device Investigator** page in Firefox, the table might continuously attempt to retrieve results unsuccessfully. (Jira ID: SLUI-21095)
- The **Device Categories** page (Devices > Device Categories) fails to load properly whenever there is a category with a null ID. To work around this issue, go to the **Device Categories** page (System > Customize > Device Categories), locate the category with the null ID, and then remove that category by clicking the delete icon (  ) next to the category. (Jira ID: SLUI-20731)
- On the **Devices** page, the **Clear Filters** option does not remove search filters from the **Asset ID** column and does not update whenever the page is reloaded. To work around this issue, click the **Select columns** icon (  ) on the **Devices** page, select **Column Preferences**, and then click "Show All". Once you have done so, you can click the **Select columns** icon again and then select **Clear Filters** from the drop-down menu. (Jira ID: SLUI-20779)
- The number of unacknowledged events in the **Device Overview** panel of the **Device Investigator** page does not update despite acknowledging alerts on a device. To work around this issue, add a new "unackEvents" subquery to the "Device Insights" query, then use that subquery to collect and retrieve information on unacknowledged events. (Case: 00471966) (Jira ID: SLUI-20858)
- When attempting to bulk delete devices or device components, a dialog message might indicate that some or all of the devices or components failed to delete, when in fact they were actually deleted. (Jira ID: EM-74351)
- Device reports generated from the **Classic Devices** page (Devices > Classic Devices) might result in an "Uncaught TypeError" message appearing in the browser console, despite most reports generating correctly. However, if you export the report to PDF, it might render the device names as long scientific notation strings. (Jira IDs: EM-74225, EM-74231)
- HTML device journal reports might generate with no data. (Jira ID: EM-74286)

- The checkbox to select all items on the **Device Dashboards** page (System > Customize > Device Dashboards) might select only the items that appear on your current page rather than all available device dashboards. (Jira ID: EM-74215)
- Event messages in device logs for multi-match events might display with the incorrect event ID . Additionally, the device logs might not indicate how many times an event has repeated. (Jira IDs: EM-74409, EM-74381)

## Events and Alerts

- Deviation alerting does not support the use of double quotes in indices. To work around this issue, use single quotes. (Jira ID: EM-72050)
- The **[Edit Note]** button on the **Events** page does not work when multiple events are selected for editing notes in Global Manager. (Jira ID: SLUI-21131)
- The events on the **Events** page cannot be sorted by the **Organization** column. (Jira ID: SLUI-20903)
- From the **Event Policies** page (Events > Event Policies), you can delete only a single event policy at a time, even if you select multiple event policies for bulk deletion. (Jira ID: SLUI-20853)
- Event messages derived from incoming email substitute "\xc2" for the character Å. (Jira ID: EM-73551)

## Global Manager

- The devices on the **Devices** page in Global Manager systems cannot be sorted by the **IP Address** column. (Jira ID: SLUI-21108)
- On Global Manager systems, the *View Event Policy* option in the **Actions** menu (⋮) on the **Events** page does not work as expected. (Jira ID: SLUI-21133)
- On Global Manager systems, the **Events** page does not display events from child stacks. To work around this issue, clear all system caches on both the child stacks and the Global Manager parent stack, then restart the NextUI service. (Jira ID: SLUI-21134)

## GraphQL

- The "harProviderOnDemanProcessing" GQL query incorrectly creates a service table in the "data\_har" database when executed with invalid or non-existent service IDs. (Jira ID: SLUI-21135)
- Clicking the **[Run Now]** button for any Dynamic Application on the **[Collections]** tab of the **Device Investigator** will display the following GQL error message in the Skylar One server console: "Variable "\$proclD" of non-null type "ID!" must not be null." (Jira ID: SLUI-21070)



## High Availability and Disaster Recovery

- You might encounter an issue where the Distributed Replicated Block Device (DRBD) does not detect the high availability (HA) secondary and disaster recovery (DR) connection after the primary node is rebooted with the secondary HA and DR nodes shut down. The problem appears to be related to the DRBD proxy version and its management during node restarts. To work around this issue, SSH into the primary HA node as a root user and run the following commands:

```
systemctl restart drbdproxy;
```

```
drbdadm adjust r0;
```

(Case: 00573719) (Jira ID: EM-77561)

- When EKMS is enabled in a high-availability (HA) configuration, the EKMS vault service might be unable to start after a failover due to bad configuration files. This issue is seen when a user has a working HA setup configuration, then later re-ISOs or rebuilds one of the Database Servers. One source of the rebuilt Database Server is swapping active node with DR node. For more information about this issue, see <https://support.sciencelogic.com/s/article/15486>. (Jira ID: SLS-1341)
- When upgrading in an Extended Architecture, on-premises, high-availability environment, the maximum connections configuration might be updated only in the primary Database Server and not in the passive node. (Jira ID: EM-76627)

## 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 upgrading Skylar One to version 12.5.1, PowerPacks will be temporarily read-only until the update is complete.
- Due to a known issue, you might need to manually upgrade to the following PowerPack versions after installing or upgrading to Skylar One 12.5.1:
  - "Net-SNMP Base Pack" PowerPack v103 (Jira ID: EM-73518)
  - "Microsoft Base Pack" v110 (Jira ID: EM-73516)
  - "Microsoft: Windows Server" v118 (Jira ID: EM-73516)
- 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 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)

- Reports that include images or charts fail to generate properly in ODS format. (Jira ID: EM-75401)
- Some information from the Device Combo report might not appear at the top of the generated report output. (Jira ID: EM-74144)

## Schedule Management

- A large number of stored procedure calls over time can lead to memory growth in the scheduler process as well as delays in processing schedules. (Jira ID: EM-76720)

## Skylar AI

- You might experience data pull "rows behind" events if you have Skylar AI enabled. (Jira ID: EM-76980)
- Presentation objects, labels, and metrics collected by Dynamic Applications that include SNMP index collection objects are not exported to Skylar AI. (Jira ID: EM-76641)
- If you have connected your Skylar One system with a Skylar AI system, data will not get exported from Skylar One 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 Skylar One (System > Settings > Admin Processes) and edit the "Enterprise Database: Skylar Metadata Exporter" process by setting the **Time Factor** field to 90 minutes. (Jira ID: EM-77019)

## System Administration

- When editing a collector group from the **Collector Groups** page (Manage > Collector Groups) by clicking its **Actions** menu (ellipsis icon) and unchecking two or more organizations in the **Limit access to specific organizations** field of the **Edit Collector Group** modal, the **Organizations** column on the **Collector Groups** page will show that only one organization was deselected, even if multiple were. (Jira ID: SLUI-22167)
- Message Collectors on the **Collector Groups** page (Manage > Collector Groups) cannot be sorted by the **Message Collectors** column. (Jira ID: SLUI-22099)

## User Interface

- In the Skylar One 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)
- 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)
- 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)

- 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-72421)
- 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 **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)
- On the **Custom Attributes** page (Manage > Custom Attributes), you might not be able to view more than the first 20 custom attributes unless you zoom in or change the size of your browser to force Skylar One to fetch additional attributes. You also might not be able to select the "Select All" checkbox on the page. (Jira IDs: SLUI-21449, EM-74251)
- Name changes to nodes on the **Nodes** page (Manage > Nodes) are not saved. (Jira ID: SLUI-22248)
- 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)
- 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)
- 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)
- You might experience several issues relating to collection labels and presentation objects, including the incorrect precedence value displaying or updates to the precedence level not being reflected in the user interface. (Jira ID: EM-76620)
- When using a dark mode theme, if you click on a calendar icon to select a date, some dates might not be visible on the calendar. (Jira ID: EM-76629)
- The final row might not appear on the **Select Objects** page (System > Customize > Select Objects) when viewed in the default user interface (AP2) using a Firefox browser. (Jira ID: EM-74222)
- When using Active Directory Federation Services (ADFS) to authenticate, the system opens to the default landing page rather than the last page the user visited. (Jira IDs: SLS-1764, SLS-1765)
- On the **TCP/IP Port Editor** page (System > Customize > TCP-IP Ports), if you search for a port name or port number and then click the wrench icon for the port found, the system does not retrieve its data for editing. (Jira ID: EM-76667)
- If you create a new network on the **IPv4 Networks** page (Registry > Networks > IPv4 Networks), it might not appear on the page after you save it. However, the network should still be available for selection in other operations. (Jira ID: EM-76666)
- In AWS deployments, the **% Used** column on the **IPv4 Networks** page (Registry > Networks > IPv4 Networks) might erroneously display values over 100%. (Jira ID: EM-76672)

- When saving a change on the **Quality of Service Threshold Defaults** page (System > Settings > Thresholds > Quality of Service), the page might continuously state that it is saving until you refresh the page. Despite this messaging issue, the system should save the changes correctly. (Jira ID: EM-74336)
- If you select a normalized option for a service usage graph, the **Date Range Selection** pane changes to the year 1970 and the graph will not be visible, even if you correct the start and end dates. (Jira ID: EM-74331)
- When creating an uptime OID, the system might display an error alert if the OID is invalid but still save the OID anyway. (Jira ID: EM-74227)
- On the **Process Manager** page (System > Settings > Admin Processes), if you deselect the appliance type(s) that a process should run on and then save that change, it will prevent that process from starting in the future. (Jira ID: EM-74236)
- If you click the **[Save]** button on the **User Policy Properties Editor** page (Registry > Accounts > User Policies > create or edit) for an existing user policy, the system mistakenly saves the user policy again as a separate entry rather than overwriting the existing policy with the updated information. (Jira ID: SLS-1773)
- When adding a new Access Key on the **Key/Hook Alignment Editor** page (System > Manage > Access Keys > Key Manager), the form might not reset if you click the **[New]** button. (Jira ID: EM-76407)

© 2003 - 2025, ScienceLogic, Inc.

All rights reserved.

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

ALL INFORMATION AVAILABLE IN THIS GUIDE IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED. SCIENCELOGIC™ AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT.

Although ScienceLogic™ has attempted to provide accurate information herein, the information provided in this document may contain inadvertent technical inaccuracies or typographical errors, and ScienceLogic™ assumes no responsibility for the accuracy of the information. Information may be changed or updated without notice. ScienceLogic™ may also make improvements and / or changes in the products or services described herein at any time without notice.



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

International: +1-703-354-1010