



SL1 8.12.1.4 Release Notes

SL1 version 8.12.1.4

Table of Contents

Overview	0
Caveats	1
Best Practices	2
Issues Addressed in 8.12.1.4	3
The following issues are addressed in the 8.12.1.4 Unified UI:	3
New Features in 8.12.1.3	4
8.12.1.3 Unified UI includes the following new features:	4
Issues Addressed in 8.12.1.3	4
The following issues are addressed in the 8.12.1.3 Unified UI:	4
The following issues are addressed in the 8.12.1.2 Unified UI:	5
Issues Addressed in 8.12.1.1	6
The following issues are addressed in the 8.12.1.1 Unified UI:	6
New Features in 8.12.1	6
8.12.1 Unified UI includes the following new features:	6
8.12.1 Next UI includes the following new features:	7
Issues Addressed in 8.12.1	10
The following issues are addressed in the 8.12.1 Unified UI:	10
The following issues are addressed in the 8.12.1 Next UI:	13
PowerPacks Released with 8.12.1	13
New and Updated Packages in 8.12.1	14
Beta Features	14
Disabling the Knowledge Base	16
Special Upgrade Process for FIPS-Compliant System	17
Upgrade Process for Systems Running 8.1.0 and Earlier	17
Upgrade to 8.9.0	17
Features Not Currently Supported by the 8.x Releases	18
Upgrade Process for Systems Running 8.4.0 and Later	18
Manual Updates for 8.4.x Systems Updated to 8.12.1.4	25
Upgrading MariaDB	26
Two Database Servers Configured for High Availability	26
Two Database Servers Configured for Disaster Recovery	27
Three Database Servers Configured for HA and DR	28
Single Database Server/All-In-One Appliance/Data Collector/Message Collector	29
Rebooting Appliances	30
Administration Portal	30
Data Collectors and Message Collectors	31
Standalone All-In-One Appliances and Database Servers	32
Two Database Servers Configured for Disaster Recovery	32
Two Database Servers in a High Availability Cluster	33
Three Database Servers Configured for High Availability and Disaster Recovery	34
Deprecated Features	35
Known Issues	37

Overview

This document describes:

- [Caveats](#)
- [Best Practices](#)
- The [Issues Addressed](#) in the 8.12.1.4 release
- The [New Features](#) in the 8.12.1.3 release
- The [Issues Addressed](#) in the 8.12.1.3 release
- The [Issues Addressed](#) in the 8.12.1.2 release
- The [Issues Addressed](#) in the 8.12.1.1 release
- The [New Features](#) in the 8.12.1 release
- The [Issues Addressed](#) in the 8.12.1 release
- The [PowerPacks](#) included in the 8.12.1 release
- [New and Updated Packages](#) in the 8.12.1 release
- [The Beta Features available with the 8.12.1 release](#)
- [Disabling the Knowledge Base](#)
- [Special Upgrade Process for FIPS-Compliant Systems](#)
- [Upgrade Process for Systems Running 8.1.0 and Earlier](#)
- [Upgrade Process for Systems Running 8.4.0 and Later](#)
- [Manual Updates for 8.4.x Systems Updated to 8.12.1.4](#)
- [Upgrading MariaDB](#)
- [Rebooting Appliances](#)
- The [features deprecated](#) in this release
- The [Known Issues](#)

TIP: 8.12.1.4 includes delta-less updates. If you have already deployed 8.6.0 or later, you can import, stage, and deploy a single update file to update to 8.12.1.4.

Caveats

Consider the following caveats before deploying 8.12.1.4:

- **SL1 updates overwrite changes to the configuration file `opt/em7/nextui/nextui.env`.** This is a known issue (see <https://support.sciencelogic.com/s/article/1161> and <https://support.sciencelogic.com/s/article/1423>). ScienceLogic recommends that you backup this file before applying an update and then re-apply your changes to this file.
- **Do not import any releases from the 8.12.x line if you do not plan to immediately consume the 8.12.x line of releases.** After you import an 8.12.x release, all appliances in your SL1 system will now use the **new system update**. After you import an 8.12.x release, you will not be able to stage and deploy any

versions of SL1 previous to 8.12.0 or apply patches to versions of SL1 previous to 8.12.0. For details on the new system update, see the release notes for 8.12.0.

- **To install 8.12.x and its new System Updates tool, you must have already imported, staged, and deployed 8.4.0 or a later release.**
- 8.12.1 included important security updates that require you to reboot all appliances after installing 8.12.1. **If you have not previously installed 8.12.1 and rebooted all appliances, you must reboot all appliances after installing 8.12.1.4.** If you would like assistance in planning an upgrade path that meets your security needs while minimizing downtime, please contact your Customer Success Manager.
- 8.10.0 and later releases do not support Data Collectors and Message Collectors running the CentOS operating system. **If your system includes Data Collectors and Message Collectors running the CentOS operating system, contact your Customer Success Manager for details on upgrading Data Collectors and Message Collectors to Oracle Linux before installing 8.12.1.4.**
- The Knowledge Base includes known vulnerabilities for cross-site scripting and SQL injection. **If your first installation of SL1 was 8.9.1 or earlier, ScienceLogic strongly recommends that you [disable the Knowledge Base](#).**
- If you are running 8.4.0 or earlier and require access to all ticket notes immediately after upgrading, contact ScienceLogic Customer Support for details on manually updating the database schema before you upgrade.
- If you are running 8.4.0 or earlier and have added one or more custom firewall rules, such as a non-standard port for Phone Home Collectors, you must migrate these rules to firewalld before upgrading. Please contact ScienceLogic Support for more information.
- ScienceLogic recommends that Systems running an AP2 version earlier than 5.55.1.3 upgrade their version of AP2 before upgrading to 8.12.1.4. For details, see the manual *Introduction to SL1*, section on *Managing New Features on the Content Management Page*.
- 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 ScienceLogic releases during a maintenance window.
- The ScienceLogic 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.

Best Practices

Consider the following best practices before deploying 8.12.1.4:

- Before you install a ScienceLogic release, ScienceLogic recommends reviewing the hardware specifications of all the appliances in your system to ensure they meet the requirements for the current usage of your system. For more information, see <https://support.sciencelogic.com/s/system-requirements>.
- Before installing a release, ScienceLogic recommends that you verify that recent backups are available for your system.

- To apply updates to an existing Data Collector, that Data Collector must be a member of a Collector Group. In some SL1 systems, users might have to create a Collector Group for a single Data Collector.
- If your system is not currently running a recent release, the upgrade process includes importing multiple upgrade files. You must wait until an update file has imported successfully (i.e. the **Import Status** column displays *Complete* in both the EM7 Release pane and the ScienceLogic OS pane) before importing the next update file.
- ScienceLogic regularly uploads new and updated PowerPacks to the Customer Portal before packaging those PowerPacks in a system update file. For more information, see <https://portal.sciencelogic.com/portal/powerpacks>.

Issues Addressed in 8.12.1.4

The following issues are addressed in the 8.12.1.4 Unified UI:

NOTE: The Unified UI includes pages from the SL1 Classic UI that have been ported to the SL1 Next UI and pages developed in the Next UI.

Platform

- When SL1 is installed on AWS instances, the SL1 process "The Enterprise Database: Collector Task Manager" no longer generates an unhandled exception related to mysql internal tables. (Case: 47605) (Support ID: 180138) (JIRA ID: EM-32144))

Scheduler

- Improved the performance of the scheduler at scale. Improved the query that starts the scheduler process to prune invalid schedules and therefor avoid outages. (Case: 43708) (Support ID: 180208) (JIRA ID: 32180)

SNMP Dynamic Applications

- In SNMP Dynamic Applications, if a Collection Object is user-disabled or auto-disabled, SL1 will not process alert policies that reference that disabled Collection Object. If the disabled Collection Object uses the "special compatibility mode" (comparison to "--"), then SL1 will substitute "None" for the collected value during alert evaluation. (Case: 19860) (Support ID: 175,328) (JIRA ID: 28779)
- In an SNMP Dynamic Application, if a Collection Object references another Collection Object that has been auto-disabled, collection will not fail with an unhandled exception. (Case: 47262) (Support ID: 180207) (JIRA ID: EM-32177)
- If Collection Objects are auto-disabled or user-disabled, Alert Formulas dependent on those objects no longer fail with Python "name errors". (Case: 45544) (Support ID: 180451) (JIRA ID: EM-32225)

New Features in 8.12.1.3

8.12.1.3 Unified UI includes the following new features:

NOTE: The Unified UI includes pages from the SL1 Classic UI that have been ported to the SL1 Next UI and pages developed in the Next UI.

Network Interfaces

- In the **Network Interfaces** page (Registry > Networks > Interfaces > Select Actions), users can now bulk enable or bulk disable updates to interface speed/counter type.

Security

- Added restrictions to prevent users from viewing system files from the MIB browser.

Issues Addressed in 8.12.1.3

The following issues are addressed in the 8.12.1.3 Unified UI:

NOTE: The Unified UI includes pages from the SL1 Classic UI that have been ported to the SL1 Next UI and pages developed in the Next UI.

API

- In the ScienceLogic REST API, requests to the resource `data_performance_raw/interface` and `data_performance_raw/device/dynamic_app` no longer return null as the first value. (Case: 34889) (JIRA ID: EM-30779)
- The ScienceLogic REST API now successfully returns a value for the index label of a presentation object when that presentation object includes multiple collection objects. (Case: 12135) (Support ID: 159313) (JIRA ID: EM-24819)

Devices

- Critical Ping (Registry > Devices > Device Manager > wrench icon > Properties) now uses the following global default values: Ping Count is "1", Required Ping Percentage is "100" and Packet Size is "56 bytes". To adjust these global values or to allow Critical Ping to inherit the per-device values for ICMP Availability Thresholds (defined in Registry > Devices > Device Manager > wrench icon > Thresholds), contact ScienceLogic Customer Support. (Case: 37802) (Support ID: 178839) (JIRA ID: 31031)

Embedded Forms

- The Date & Time field in embedded forms (System > Customize > Form Fields > Embedded) now uses each user's local timezone. If the user's local timezone is not supported by the IANA database, SL1 substitutes the timezone for the operating system. (Support ID: 173176) (JIRA ID: EM-27604)

Network Interfaces

- In the unified UI, network interfaces no longer show a status of "up" when the interface is non-operational and "down" when the interface is operational. (Case: 35897) (Case: 34045) (Support ID: 178719) (JIRA ID: EM-30808)

Software Titles

- The Software Titles page (Registry > Devices > Software) now successfully displays the software title in the Software Title column and a date value in the Date of Install column. (Case: 26065) (Support ID: 178574) (JIRA ID: EM-30685)

Subscription Billing

- SL1 systems that use Aurora RDS can now successfully calculate and report usage. (JIRA ID: 25518)
- The process that calculates subscription usage is now assigned enough memory to ensure that it does not interfere with other SL1 processes. (JIRA ID: PTEL-374)
- A new option allows users to exclude device names from the payload of billing data that is sent to ScienceLogic daily. For details, contact ScienceLogic customer Support. (JIRA ID: PTEL-375)

Issues Addressed in 8.12.1.2

The following issues are addressed in the 8.12.1.2 Unified UI:

NOTE: The Unified UI includes pages from the SL1 Classic UI, displayed in either the SL1 Classic UI or ported to the SL1 Next UI.

Disaster Recovery

- In Disaster Recovery configurations, the primary Database Server is no longer automatically demoted to secondary during system update. (Case 00037880) (Support ID: 178841)

Dynamic Applications

- When collection for a Collection Object is auto-disabled or user-disabled, Alert Formulas that depend on those objects will no longer fail, and SL1 will no longer display an error message that states that the objects are not defined. (Case 00043732) (Case 42869) (Support ID: 179347)
- When collection for a Collection Object is auto-disabled or user-disabled, snippets that depend on those objects will fail. The error message states that the collection object "is not handled by this request" (Case 4294) (Support ID: 179342)

Events

- Inbound email messages with multiple addresses in the "To:" field no longer cause the Event Engine to crash. (Case 00039762) (Support ID: 179005)

System Update

- In the System Updates page, (System > Tools > Updates), after importing an update, the Staging Status no longer hangs with a status of "Scheduled".

Issues Addressed in 8.12.1.1

The following issues are addressed in the 8.12.1.1 Unified UI:

NOTE: The Unified UI includes pages from the SL1 Classic UI, displayed in either the SL1 Classic UI or ported to the SL1 Next UI along with pages developed for the next UI.

Security

- Closed an open port (443) on Data Collectors that was opened in the 8.12.0 release. (Support ID: 178985)

New Features in 8.12.1

8.12.1 Unified UI includes the following new features:

NOTE: The unified UI includes pages from the SL1 Classic UI, displayed in either the SL1 Classic UI or ported to the SL1 Next UI along with pages developed for the next UI.

Content Libraries

- Updated pip, setuptools, and wheel to latest versions, to support third-party content libraries.

Dynamic Applications

- Improved the performance of the Dynamic Application process that checks each auto-disabled collection object on a device and re-enables the collection object when appropriate.

Form Fields

- Improved custom form fields in the Application forms page (System > Customize > Form Fields). In the Form Creator modal page, the field types Varchar32, Varchar48 and Varchar64 have been replaced with a field of type TextArea. The new fields can include up to 64K characters

Logging

- Added new page PHP Developer Logs (System > Tools > PHP Developer Logs) to SL1. These logs aid ScienceLogic Customer Support when troubleshooting problems with the user interface.

PhoneHome

- In a High Availability system, only the Database Server that is also the PhoneHome control node may generate a PhoneHome token for the Data Collectors. (Support ID: 153173) (Support ID: 161661)(Support ID: 172370)(Case 00006471)

PowerShell

- If a PowerShell Dynamic Application terminates before closing its open connections, SL1 will automatically close the open PowerShell connections.
- PowerShell Dynamic Applications that are cache producers or cache consumer now successfully collect data from merged devices.

System Update

- Improved System Updates (System > Tools > Updates). After successful deployment or successfully staging a later version of an update, System Update now removes packages that were copied to each SL1 appliance during staging.

8.12.1 Next UI includes the following new features:

NOTE: Features in this section are not available in the SL1 Classic UI.

User Interface Version

- 8.12.1 includes the following version of the user interface:
 - AP2_5.125.44.

General

- When searching, you can click the menu icon to the right of the **Search** field to open a menu containing related search criteria. In that menu, you can select a search criteria and type additional search information.
- If you select a date-related search criteria from the list of criteria in Basic Search, you can use a drop-down calendar to select a specific date.
- Basic Search and Advanced Search were updated to include better search queries and usability.
- For an Administrator user, the End User License Agreement (EULA) appears the first time that user logs into SL1. The user must agree to the terms before using SL1.

Applications

- From the **Application Investigator** page, you can view the details of that application, view and add application components or devices to that application, and edit the status policy aligned with that application.

- The **[Rules]** button on the **[Devices]** tab for an application component lets you define the processes and arguments to monitor for that application component.
- The **[Define these with a Query]** button on the **[Devices]** tab for an application component lets you update the set of devices in that application component.
- You can edit an application component by clicking the **[Actions]** button for that component on the **Applications** page.
- You can create static or dynamic searches for the devices you want to add to an application component.
- You can view both statically defined and dynamically defined application components on the **Application Investigator** page.
- When creating an application or an application component, you can search for business, IT, and device services.
- Improved error messaging was added if you try to add non-devices to an application component.

Dashboards

- You can now create Application and Application Component widgets.
- The **Auto-Select** option was moved from the **All Filters** window to the widget creation process, where you can select the number of items that are automatically selected in the context-driving widgets.
- In a Service widget, you can link directly to another dashboard or item related to that service.
- The dashboard creator can choose a specific dashboard from a list that is linked to a leaderboard, so the user can specify a dashboard without copy and pasting a URL and using a parameter.
- If a dashboard creator doesn't enter a new name for a map widget, the name of the map will be used.
- The icon in a service tile widget is still visible even when the service is unavailable.
- Leaderboard bar chart widgets can now drive context.
- Event widgets can now drive context.
- Selecting items in a map widget will drive context in other widgets.
- Custom Attributes can now be selected under **Metrics and Properties** when creating a device table or event table widget.

Devices

- You can change the aligned Device Class from the **Info** drop-down on the **Device Investigator** page for a device.
- You can generate a report for a device from the **Device Investigator** page.
- The **[Settings]** tab on the **Device Investigator** page was updated with additional options.
- On the **[Events]** tab for the **Device Investigator** page, you can toggle between cleared and active events for a device.
- On the **[Events]** tab for the **Device Investigator** page, you can use the **Search** field to filter the list of events for that device.
- On the **[Interfaces]** tab for the **Device Investigator** page, you can click the interface name from the list of interfaces to open the **Interface Properties** page for that interface.

- If an SL1 system is configured to use Maps, the **[Map]** tab on the **Device Investigator** page displays by default.
- The **Tools** drop-down on the **Device Investigator** page does not display if the user does not have permissions for the device tools. The **Tools** drop-down now includes an Availability tool.
- You can drag and drop the various tabs on the Device Investigator page to rearrange the order of the tabs.
- Hovering over a column in the Devices page displays a ToolTip with the complete value if the value was cut off by the column width.
- You can now assign icons to devices.
- Users need proper permissions to edit Device Categories and Device Classes.

Events

- You can view the automations that were run on a certain event by selecting *View Automation Actions* from the **Actions** menu on the **Events** page.
- From the **View** drop-down on the **Events** page, you can toggle the ability to group events generated from a Business Service, events from its IT Services and their Device Services, and events from the underlying devices.
- From the **View** drop-down on the **Events** page, you can specify a time frame for SL1 to auto-refresh and display new events. You can also click the Refresh icon at the top right of the **Events** page table to manually refresh the list of events.
- The **Actions** menu from the **Events** page is also available at the top right of the **Event Investigator** page for an individual event.
- The Card view for the Events page has been deprecated.
- Custom Attributes can now be selected to display as columns in the **Events** page.

Maps

- The **Design** pane for a map was updated and streamlined, and the configurable design options now include *Tiered Hierarchy*, *Hierarchy*, and *Force Directed*. For more information about changing the appearance of a map, see the **Maps** manual.
- The **Filters** pane for a map was updated and streamlined, and the counts for each node type now displays in a badge next to the node type.
- You can access the **Design** pane and **Filters** pane from the new **Settings** drop-down on the navigation bar in a **Maps** window.
- You can hover over a node in a map to view a pop-up **Properties** pane with the relevant details, or metadata, for that node. If you click to select a node and then click the **[Selections]** button, the metadata displays in a **Properties** pane to the right of the map.
- If you select a node in a map, you can click the **[Events]** tab in the **Properties** pane to monitor the events on that node. If you do not have the relevant permissions for viewing events, the **[Events]** tab does not appear.
- For a Service node or an Application node, the Availability, Health, and Risk values now appear on the **Properties** pane.
- You can use the **Search** field at the top of a map page to search for specific nodes on the current map. Nodes that do *not* meet the search criteria are grayed out in the map.

- The Zoom feature for viewing a map was updated to ensure that the node details display clearly when zooming in or out.
- On the **[Nodes]** tab of the **Design** pane, if you have the **Show External Labels** toggle selected, you can expand the **Label Fields** section and edit the type of label that displays under each node. For example, you could edit the external labels to display the organization name for each node.
- Just like Dashboards, any Maps that you create can be *Private* (viewable only to you), *Public* (viewable to users in all organizations using SL1), or viewable by *Specific Organizations*. You must have the relevant permissions to create a map, and the state of a new map is *Private* by default.
- Depending on the permissions assigned to users, some users will be able to create and edit maps and select the default layout. Meanwhile, other users will only be able to view and filter existing maps and update the layout of existing maps.
- To create a copy of an existing map, open the map, click the **Save Map** drop-down, and select *Save As Copy*.

Issues Addressed in 8.12.1

The following issues are addressed in the 8.12.1 Unified UI:

NOTE: The Unified UI includes pages from the SL1 Classic UI, displayed in either the SL1 Classic UI and ported to the SL1 Next UI.

Asset Records

- The BIOS/EPROM field in the Asset Configuration page (Registry > Assets > Asset Manager > create/edit > Configuration) can now include up to 64 characters. (Support ID: 177307)(case 00022795)

Collector Groups

- In the Collector Group Management page (System > Settings > Collector Groups), renamed the field **Max Allowed Collector Outage** to **Collectors Available For Failover** and addressed an issue where SL1 was not following the failover rules defined in this page. If Collector Failover is enabled, and the number of available Data Collection servers is less than the value in the Collectors Available For Failover field, SL1 will not failover within the Collector Group.

Dashboards

- The onboarding dashboard now tries authenticating with the "EM7 internal" method first and no longer displays spurious errors about LDAP authentication. (Support ID: 175680)(case 20793)
- Dashboard widgets of type iframe that use host name-base proxies now load without security errors. (Support ID: 177222) (case 24860)

NOTE: If you have enabled the Force Secure HTTPS field in the Behavior Settings page (System > Settings > Behavior), when you supply a URL in the iframe widget, that URL must also use HTTPS. If you chose not to enable Force Secure HTTPS field in the Behavior Settings page (System > Settings > Behavior), you can use HTTP in the iframe widget and perform the following security work-around: `

1. Either go to the console of the Database Server or All-In-One appliance or open an SSH session to the Database Server or All-In-One appliance.
2. Use vi to edit the file /etc/nginx/conf.d/sm7ngx_web_ui.conf
3. After the last `listen` directive, add the following lines:

```
{code}
if ($scheme = http) {
return 301 https://$host$request_uri;
}
{code}
```

Documentation

- Edited the Installation and Initial Configuration manual. Edited the chapter for the PhoneHome configuration. (Support ID: 108082)
- Edited the Discovery and Credentials manual. Added Caution text that states that if you enter both the hostname and IP address of the same device, SL1 will discover two duplicate devices. (Support ID: 175871) (case 21902)
- Edited the System Administration manual, the Device Management manual and the Discovery and Credentials manual. The Ping and Poll Timeout field has been edited to include both discovery and availability monitoring. (case 0029032) (Support ID: 177881)
- Edited the System Administration manual. Added a new section on Disabling phpMyAdmin, with updated steps. (Support ID: 177863) (case 28748)
- The release notes for 8.12.1 and the System Administrators manual now specify that to apply updates to an existing Data Collector, that Data Collector must be a member of a Collector Group. (Support ID: 176540) (case 24412)
- I would tell you an IPv4 joke, but all the good ones have been exhausted.

Dynamic Applications

- Fixed problems with auto-disabling and auto-enabling of collection for collection objects. In the Dynamic Application Manager page, (System > Manage > Applications) the Subscribers column now accurately displays the number of subscribed devices. (Case 00025077) (Support ID: 152484) (Support ID: 176929) (Support ID: 159436)

IT Service Policies

- If one or more devices in an IT Service policy go into maintenance mode, with collection enabled, SL1 will continue aggregating health metrics for those devices, and those devices will not appear as unavailable to the IT Service. (Support ID: 176826) (case 25061)

Network Interfaces

- When an interface switches between 32-bit counters and 64-bit counters, SL1 will manage the new counter-value and will not produce unrealistic spikes in bandwidth usage. Bandwidth graphs, reports, and events will no longer show spikes in bandwidth usage when an interface switches counter type. (Support ID: 173458) (case 6457) (case 14275) (case 17686) (case 13677) (case 15309) (case 21949) (case 21489) (case 28186)
- All interface data (bandwidth, errors & discards, and packets) is now successfully collected with all possible combinations of Enable Variable Rate Interface Counters (in System > Settings > Behavior) and high_precision_if_collect (manually set in master.system_custom_config set field_value). (Support ID: 177371) (case 28392) (Support ID: 174594) (case 12174) (case 24323) (Support ID:174400) (case 15574)
- The SL1 process "Data Collection: Interface Bandwidth: no longer generates an unhandled exception when one or more network aliases include a forward-slash character ("/"). (Support ID: 160981) (case 00026692)

PhoneHome

- In a High Availability system, only the Database Server that is also the PhoneHome control node may generate a PhoneHome token for the Data Collectors. (Support ID: 153173) (Support ID: 161661)(Support ID: 172370)(Case 00006471)

Security

- All SL1 cookies now have their secure flag set to "yes". (Support ID: 177838) (Case 29364)
- The page <ip address>/em7/license.html no longer allows page caching. (Support ID: 177837) (case 00029365)

SNMP Traps

- If you create a trap filter in the SNMP Trap Filter page (Registry > Events > SNMP Trap Filters) and specify a value only in the Trap OID Filter field (and specify no values in the Varbind OID Filter field or the Varbind OID Pattern field), SL1 will successfully filter traps with a matching OID. When a trap is filtered, the Message Collector receives the trap, but does not store the trap, does not act on the trap, and does not pass the trap on to be examined by the ScienceLogic event engine.(Support ID: 178728) (Case 35100)

System Update

- The database processes that occur during system update and that were affecting high-frequency collection and medium-frequency collection have been improved for better performance. (Support ID: 178910) (Case 38635)

ScienceLogic API

- GQL queries and REST API queries for device relationships no longer run slowly, cause timeouts, and affect the performance of the Database Server. (Support ID: 178242) (case 00031725)
- You can now successfully create and update an asset record with a POST method. (Support ID: 178837) (case 37845)

The following issues are addressed in the 8.12.1 Next UI:

NOTE: Features in this section are not available in the SL1 Classic UI.

General

- Addressed an issue to ensure that SL1 properly handles user passwords with special characters such as "%" and "@".
- Addressed an issue where the Search feature did not provide results when searching for Custom Attribute labels or values.

Business Services

- Addressed an issue where the **[Overview]** page for a Device Service displayed an empty set of devices, stating that "Selected device services do not currently contain devices."

PowerPacks Released with 8.12.1

When patching to 8.12.1, please verify whether any PowerPacks that your system is currently running are "newer" than the PowerPacks included in this SL1 update. If the PowerPack on your system is "newer" than the one included with the SL1 update, you might see spurious error messages. To avoid spurious error messages:

1. Go to the **Device Components** page (Registry > Devices > Device Components).
2. Find each root device associated with the PP you do not want to update and select its checkbox.
3. Click the **Select Action** field and choose *Change Collection State: Disabled (recursive)*. Click the **[Go]** button.
4. Wait five minutes after disabling collection.
5. install the SL1 update.
6. Go to the **Device Components** page (Registry > Devices > Device Components).
7. Select the checkbox for all affected root devices.
8. In the Select Actions drop-down list, select *Change Collection State: Enabled (recursive)*.
9. Click the **[Go]** button.

The 8.12.1 release includes the following PowerPacks that are new or updated and included with the release:

- Net-SNMP Base pack, v101
- F5 BIG-IP, v102

Documentation and release notes for each PowerPack are available on the [ScienceLogic Portal](#).

CAUTION: If you are currently using the Amazon Web Services PowerPack included in the 8.1.0 platform release or included in an earlier platform release, please read the release notes for Amazon Web Services before migrating to later versions Amazon Web Services PowerPack. You must first migrate to Amazon Web Services, v100 before upgrading to later versions of the Amazon Web Services.

CAUTION: If you are currently using the VMware: vSphere Base Pack, v202 or earlier, please read the migration instructions in the release notes for VMware: vSphere Base Pack, v203 and migrate to v203 before upgrading to later versions of the PowerPack.

NOTE: The "Microsoft SharePoint" PowerPack is no longer included with platform releases. The PowerPack is superseded by the "Microsoft: SharePoint Server" PowerPack.

NOTE: The "Microsoft SQL Server" PowerPack is no longer included with platform releases. The PowerPack is superseded by the "Microsoft: SQL Server" and "Microsoft: SQL Server Enhanced" PowerPacks.

NOTE: The "Microsoft Exchange" PowerPack is no longer included with platform releases. The PowerPack is superseded by the "Microsoft: Exchange Server 2010" and "Microsoft: Exchange Server 2013" PowerPacks.

NOTE: The "Microsoft HyperV" PowerPack is no longer included with platform releases. The PowerPack is superseded by the PowerPack "Microsoft: Hyper-V Server".

New and Updated Packages in 8.12.1

The 8.12.1 release includes multiple kernel updates and security updates.

WARNING: *8.12.1 includes important security updates that require you to reboot all appliances after installing 8.12.1. If you have not previously installed 8.12.1 and rebooted all appliances, you must reboot all appliances after installing 8.12.1.2.* If you would like assistance in planning an upgrade path that meets your security needs while minimizing downtime, please contact your Customer Success Manager.

Beta Features

The following beta features are included in the 8.12.1.2 release:

- **Manual Device Discovery**

- This beta feature allows monitored devices to be added manually instead of via a discovery session.


- **Run Book Actions: Custom Action Type**

- A Run Book Action of type "Custom Action Type" executes a reusable snippet. Unlike the Action Type "Snippet", a Custom Action Type can accept input parameters (in a JSON format) and create output (in a JSON format). A Custom Action Type allows a single snippet to be used in multiple Action Policies, each time with different inputs and different outputs. A Custom Action Type is associated with an Execution Environment. An Execution Environment contains the supporting modules and code (Content Libraries) required by the Custom Action Type. Content Libraries allow snippet developers to isolate the "heavy weight", re-usable code and write "light weight" snippets that call the Content Libraries.

- **PowerPacks:** Beta versions of the following PowerPacks are available. You can download them from the Customer Portal and import them into SL1 :

- Alibaba Cloud: Aliyun
- AMQP: RabbitMQ
- Cisco: ACI Multi-Site Manager
- Cisco: Cloud Center
- Cisco: Contact Center Enterprise
- Cisco: Hyperflex
- Cisco: Medianet/Mediatrace
- Cisco: Meraki (API)
- Cisco: Tetration
- Cisco: UC Ancillary PowerPack. Includes Dynamic Applications for monitoring Cisco CUBE devices.
- Cisco: UCS Director
- Cisco: Unity Express (Download from the Customer Portal and Import into SL1)
- Docker (Download from the Customer Portal and Import into SL1)
- ELK: AWS CloudTrail
- ELK: Azure Activity Log
- F5: BIG-IP DNS
- Google Cloud Platform
- Hitachi Data Systems: VSP
- Kubernetes
- Link Layer Neighbor Discovery (Download from the Customer Portal and Import into SL1)
- Microsoft: Office 365
- Microsoft: Windows Server Event Logs
- Palo Alto (Download from the Customer Portal and Import into SL1)

To install a beta PowerPack:

1. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).
2. Select the **[Actions]** menu and select *Install PowerPack*. The **PowerPack Installer** modal page is displayed.
3. Select the lightning-bolt icon () for the PowerPack you want to install. Information about the contents of the PowerPack and the installation process is displayed.
4. Select the **[Install]** button.

TIP: By default, installing an updated version of a PowerPack will overwrite all content in a PowerPack that has already been installed on the target system. You can use the **Enable Selective PowerPack Field Protection** setting in the **Behavior Settings** page (System > Settings > Behavior) to prevent new PowerPacks from overwriting local changes for some commonly customized fields.

Disabling the Knowledge Base

The Knowledge Base includes known security vulnerabilities. ScienceLogic no longer supports the Knowledge Base


- If your first installation of SL1 was 8.9.1 or earlier, ScienceLogic strongly recommends that you disable the Knowledge Base. SL1 provides a setting in the silo.conf file to disable the Knowledge Base.
- For newer installations where the first installation was 8.9.2 or later, the Knowledge Base will be disabled by default.

WARNING: The Knowledge Base includes known vulnerabilities for cross-site scripting and SQL injection. ScienceLogic strongly recommends that you disable the Knowledge Base.

To disable the Knowledge Base:

1. Use SSH to connect to the Administration Portal and Database Server or All-In-One (all SL1 appliances that provide a web interface).
2. Use an editor like vi and edit the file `/etc/silo.conf`. In the LOCAL section, add the line:

```
kbase_disabled=1
```
4. Use an editor like vi and edit the file `/etc/siteconfig/siloconf.siteconfig`. In the LOCAL section, add the line:

```
kbase_disabled=1
```
5. Open a browser session and log in to the SL1
6. From the hamburger menu () in the upper right, select **Clear SL1 System Cache**.

7. Upon your next login, the Knowledge Base tab will not appear. Attempts to access the tab will result in an "Access Denied" error message.

Special Upgrade Process for FIPS-Compliant System

FIPS-compliant systems should use the classic SL1 user interface. The Unified User Interface is not yet FIPS-compliant.

FIPS-compliant systems (those that are FIPS 140-2 enabled) should *manually upgrade to the latest version of MariaDB*.

The platform patch will automatically update MariaDB-client, MariaDB-common, and MariaDB-shared RPMs but will not update the MariaDB Server.

Upgrade Process for Systems Running 8.1.0 and Earlier

WARNING: ScienceLogic strongly suggest you contact Customer Support or your Customer Success Manager to plan your migration from CentOS (versions of SL1 prior to 8.1.1) to 8.12.1.4.

The 8.1.1 release included a complete update of the ScienceLogic appliance operating system from CentOS 5.11 to Oracle Linux. Major operating system components, including the database, web server, and High Availability/Disaster Recovery packages have been updated or replaced by new industry-standard packages.

When upgrading from a version prior to 8.1.1, each appliance must be migrated to 8.9.0 and the Oracle Linux 7.5 operating system.

Upgrade to 8.9.0

The process of migrating an existing system to 8.9.0 includes multiple additional steps that will vary depending on your architecture. Please contact your Customer Success Manager to begin a discussion on the migration plan that is appropriate for your system.

The following is the general process for migrating to 8.9.0. This is a high-level description only. For details, contact Customer Support or your Customer Success Manager.

- The existing system must be upgraded to at least 7.8.5 before the migration.
- Run the 8.9.0 migration patch.

NOTE: See the separate Migration document for detailed instructions on how to perform the migration steps. Before you migrate to 8.9.0, please contact your Customer Success Manager.

- Use the 8.9.0 ISO to reinstall all Database Servers or All-In-One Appliances. Data is migrated using a logical backup while the database on the existing system is stopped. The downtime of this operation can be mitigated in several ways depending on your current architecture.
- Use the 8.9.0 ISO to reinstall all Administration Portal appliances.
- After reinstalling all Database Servers and Administration Portals, the system is operational.
- If you want to upgrade to a version later than 8.9.0, you must use the 8.9.0 ISO to reinstall all Data Collectors and Message Collectors. 8.10.0 and later versions do not support "mixed-mode", where the Database Servers and Administration Portals are running Oracle Linux and the Data Collectors and Message Collectors are running CentOS.
- To upgrade to 8.12.1.4, see the section on [Upgrade Process for Systems Running 8.4.0 and Later](#).
- Perform the steps listed in the [Other Manual Updates](#) section.

Features Not Currently Supported by the 8.x Releases

The following functionality that was available in previous releases is not currently available in the 8.12.1.4 release, but will be re-added in a future release:

- Configuring two All-In-One Appliances for Disaster Recovery
- Applying a patch manually with the `apply_patch` script

Upgrade Process for Systems Running 8.4.0 and Later

As of 8.12.0, SL1 uses an improved System Update tool (System > Tools > Updates). To upgrade to versions of SL1 of 8.12.0 or later, you must be running SL1 8.4.0 or later. For details on upgrading to 8.4.0 or later, see the section [Upgrade Process for Systems Running 8.1.0 and Earlier](#) or the release notes for 8.4.0.

The 8.12.1.4 release includes a delta-less update. Any system running 8.6.0 or later can be upgraded to the 8.12.1.4 release by importing, staging, and deploying a single update file.

To upgrade to the 8.12.1.4 release from an 8.4.0 or later release:

NOTE: Before upgrading, ensure that:

- Each SL1 Appliance has a valid license
- Each Data Collector is a member of a Collector Group
- Each Data Collector is "available" to the Database Server. To check, see the **Collector Status** page (System > Monitor > Collector Status).

NOTE: Staging and deploying SL1 patches is "hitless" and does not require a maintenance window.

1. Familiarize yourself with the [Known Issues](#) for this release.
2. **For systems running an SL1 version prior to 8.12.0**, go to the **System Updates** page and disable automatic staging (System > Tools > Updates > Actions > Disable automatic staging).
 - If you have previously used manual staging, perform these additional steps:
 - Select all updates in the EM7 Releases pane and select all updates in the ScienceLogic OS pane.
 - In the **Select Action** menu, select *Unstage Update (remove staging policy override)*. Click **[Go]**.
 - For software that was previously staged with automatic staging, *Unstage Update (remove staging policy override)* does not affect staging.

NOTE: For details on downloading, importing, staging, and installing system updates, see the manual **System Administration**.

4. **If you are currently running an 8.4 release:**

- If you are running 8.4.0 and require access to all ticket notes immediately after upgrading, contact ScienceLogic Customer Support for details on manually updating the database schema before you upgrade.
- If you are running 8.4.0 and have added one or more custom firewall rules, such as a non-standard port for Phone Home Collectors, you must migrate these rules to firewalld before upgrading. Please contact ScienceLogic Support for more information.
- Please note that 8.10.0 and later versions do not support "mixed-mode", where the Database Servers and Administration Portals are running Oracle Linux and the Data Collectors and Message Collectors are running CentOS. If your system uses "mixed-mode", you must use the 8.4.0 ISO to reinstall the Data Collectors and Message Collectors before upgrading to 8.12.1.4. **ScienceLogic strongly suggest that you contact Customer Support or your Customer Success Manager to plan your migration from mixed-mode to 8.12.1.4.**
- From the ScienceLogic portal, **download the updates for 8.5.0, 8.6.0, and 8.12.1.4** to a local computer. Unzip any zipped files.
- **Import the 8.5.0 system update file in the System Updates page (System > Tools > Updates > Import button)**. The system update file will load an update in both the EM7 Releases and the ScienceLogic OS section. You must wait until the update file has imported successfully (i.e. the **Import Status** column displays *Complete*) before importing the next update file.
- **Import the 8.6.0 system update file in the System Updates page (System > Tools > Updates > Import button)**. The system update file will load an update in both the EM7 Releases and the ScienceLogic OS section. You must wait until the update file has imported successfully (i.e. the **Import Status** column displays *Complete*) before importing the next update file.
- Review the following release notes to see what has changed between 8.4.x and 8.12.1.4:
 - Applicable 8.4.x release notes (8.4.2 and 8.4.3)
 - 8.5.0
 - 8.5.1.4

- 8.6.0
- 8.6.1
- 8.6.2.3
- 8.7.0
- 8.7.1.2
- 8.8.0.1
- 8.8.1.3
- 8.8.2.1
- 8.9.0
- 8.9.1.1
- 8.9.2.4
- 8.10.0
- 8.10.1.3
- 8.10.2.1
- 8.10.3.1
- 8.12.0.2
- 8.12.1.4
- **Go to step #12** and continue.

5. **If you are currently running an 8.5 release:**

- Please note that 8.10.0 and later versions do not support "mixed-mode", where the Database Servers and Administration Portals are running Oracle Linux and the Data Collectors and Message Collectors are running CentOS. If your system uses "mixed-mode", you must use the 8.5.0 ISO to reinstall the Data Collectors and Message Collectors before upgrading to 8.12.1.4. **ScienceLogic strongly suggest that you contact Customer Support or your Customer Success Manager to plan your migration from mixed-mode to 8.12.1.4.**
- From the ScienceLogic portal, **download the updates for 8.6.0 and 8.12.1.4** to a local computer. Unzip any zipped files.
- **Import the 8.6.0 system update file in the System Updates page (System > Tools > Updates > Import button).** The system update file will load an update in both the EM7 Releases and the ScienceLogic OS section. You must wait until the update file has imported successfully (i.e. the **Import Status** column displays *Complete*) before importing the next update file.
- Review the following release notes to see what has changed between 8.5.x and 8.12.1.4:
 - Applicable 8.5.x release notes (8.5.1.4)
 - 8.6.0
 - 8.6.1
 - 8.6.2.3
 - 8.7.0

- 8.7.1.2
- 8.8.0.1
- 8.8.1.3
- 8.8.2.1
- 8.9.0
- 8.9.1.1
- 8.9.2.4
- 8.10.0
- 8.10.1.3
- 8.10.2.1
- 8.10.3.1
- 8.12.0.2
- 8.12.1.4
- **Go to step #12** and continue.

6. *If you are currently running an 8.6 release:*

- Please note that 8.10.0 and later versions do not support "mixed-mode", where the Database Servers and Administration Portals are running Oracle Linux and the Data Collectors and Message Collectors are running CentOS. If your system uses "mixed-mode", you must use the 8.6.0 ISO to reinstall the Data Collectors and Message Collectors before upgrading to 8.12.1.4. **ScienceLogic strongly suggest that you contact Customer Support or your Customer Success Manager to plan your migration from mixed-mode to 8.12.1.4.**
- From the ScienceLogic portal, **download the update for 8.12.1.4** to a local computer. Unzip any zipped files.
- Review the following release notes to see what has changed between 8.7.x and 8.12.1.4:
 - Applicable 8.6.x release notes (8.6.1 and 8.6.2.3)
 - 8.7.0
 - 8.7.1.2
 - 8.8.0.1
 - 8.8.1.3
 - 8.8.2.1
 - 8.9.0
 - 8.9.1.1
 - 8.9.2.4
 - 8.10.0
 - 8.10.1.3
 - 8.10.2.1
 - 8.10.3.1

- 8.12.0.2
- 8.12.1.4
- **Go to step #12** and continue.

7. **If you are currently running an 8.7 release:**

- Please note that 8.10.0 and later versions do not support "mixed-mode", where the Database Servers and Administration Portals are running Oracle Linux and the Data Collectors and Message Collectors are running CentOS. If your system uses "mixed-mode", you must use the 8.7.0 ISO to reinstall the Data Collectors and Message Collectors before upgrading to 8.12.1.4. **ScienceLogic strongly suggest that you contact Customer Support or your Customer Success Manager to plan your migration from mixed-mode to 8.12.1.4.**
- From the ScienceLogic portal, **download the update for 8.12.1.4** to a local computer. Unzip any zipped files.
- Review the following release notes to see what has changed between 8.8.x and 8.12.1.4:
 - Applicable 8.7.x release notes (8.7.1.2)
 - 8.8.0.1
 - 8.8.1.3
 - 8.8.2.1
 - 8.9.0
 - 8.9.1.1
 - 8.9.2.4
 - 8.10.0
 - 8.10.1.3
 - 8.10.2.1
 - 8.10.3.1
 - 8.12.0.2
 - 8.12.1.4
- **Go to step #12** and continue.

8. **If you are currently running an 8.8 release:**

- Please note that 8.10.0 and later versions do not support "mixed-mode", where the Database Servers and Administration Portals are running Oracle Linux and the Data Collectors and Message Collectors are running CentOS. If your system uses "mixed-mode", you must use the 8.8.0 ISO to reinstall the Data Collectors and Message Collectors before upgrading to 8.12.1.4. **ScienceLogic strongly suggest that you contact Customer Support or your Customer Success Manager to plan your migration from mixed-mode to 8.12.1.4.**
- From the ScienceLogic portal, **download the update for 8.12.1.4** to a local computer. Unzip any zipped files.
- Review the following release notes to see what has changed between 8.9.x and 8.12.1.4:

- Applicable 8.8.x release notes (8.8.0.1, 8.8.1.3, 8.8.2.1)
- 8.9.0
- 8.9.1.1
- 8.9.2.4
- 8.10.0
- 8.10.1.3
- 8.10.2.1
- 8.10.3.1
- 8.12.0.2
- 8.12.1.4
- **Go to step #12** and continue.

9. ***If you are currently running an 8.9 release:***

- Please note that 8.10.0 and later versions do not support "mixed-mode", where the Database Servers and Administration Portals are running Oracle Linux and the Data Collectors and Message Collectors are running CentOS. If your system uses "mixed-mode", you must use the 8.9.0 ISO to reinstall the Data Collectors and Message Collectors before upgrading to 8.12.1.4. ***ScienceLogic strongly suggest that you contact Customer Support or your Customer Success Manager to plan your migration from mixed-mode to 8.12.1.4.***
- From the ScienceLogic portal, ***download the update for 8.12.1.4*** to a local computer. Unzip any zipped files.
- Review the following release notes to see what has changed between 8.10.x and 8.12.1.4:
 - Applicable 8.9.x release notes (8.9.1.1, 8.9.2.4)
 - 8.10.0
 - 8.10.1.3
 - 8.10.2.1
 - 8.10.3.1
 - 8.12.0.2
 - 8.12.1.4
- **Go to step #12** and continue.

10. ***If you are currently running an 8.10 release:***


- From the ScienceLogic portal, ***download the latest update for 8.12.1.4*** to a local computer. Unzip any zipped files.
- Review the following release notes to see what has changed between 8.12.0 and 8.12.1.4:
 - Applicable 8.10.x release notes (8.10.1.3, .8.10 2.1, 8.10.3.1)
 - 8.12.0.2
 - 8.12.1.4


- **Go to step #12** and continue.

11. **If you are currently running an 8.12.x release:**

- From the ScienceLogic portal, **download the update for 8.12.1.4** to a local computer. Unzip any zipped files.
- Review the following release notes to see what has changed between 8.12.x and 8.12.1.4:
 - Applicable 8.12.x release notes (8.12.0.2, 8.12.1.4)
- **Go to step #12** and continue.

12. Import the 8.12.1.4 system update file in the **System Updates** page (System > Tools > Updates > **[Import]** button).

13. Select the staging icon () for 8.12.1.4.


14. When staging has completed, select the lightning-bolt icon () to deploy 8.12.1.4.

15. Clear your browser's cache.

16. Clear the SL1 cache.

- Go to the **Cache Management** page (System > Tools > Cache).
- From the hamburger menu (), select **Clear EM7 System Cache**.

CAUTION: An update included in 8.12.1 requires that you clear the EM7 System Cache. Until you clear the EM7 System Cache, you might experience errors with credentials that can affect discovery, calls to the ScienceLogic API, and calls to GQL.

17. Go to the **PowerPack Manager** page (System > Manage > PowerPacks) and install all updated PowerPacks. Updated PowerPacks are loaded on your ScienceLogic system by the patch process. To install an updated PowerPack, find the PowerPack in the **PowerPack Manager** page and select the installation icon () in the **Update** column for the PowerPack or use the *Update PowerPacks* option in the **Select Action** drop-down list.

TIP: By default, installing an updated version of a PowerPack will overwrite all content in that PowerPack that has already been installed on the target system. You can use the **Enable Selective PowerPack Field Protection** setting in the **Behavior Settings** page (System > Settings > Behavior) to prevent new PowerPacks from overwriting local changes for some commonly customized fields.

18. If you are monitoring devices using the ScienceLogic Agent, follow the steps listed in the **Agent Monitoring** manual to upgrade to the latest version of the Agent.
19. If you upgraded from an 8.4.x release, perform the steps listed in the **Other Manual Updates** section.

CAUTION: *Upgrading MariaDB* and the *rebooting all SL1 appliances* should be performed during a maintenance window. If you would like assistance in planning an upgrade path that minimizes downtime, please contact your Customer Success Manager.

20. If you have not previously upgraded to 8.12.0, you must upgrade MariaDB to the latest version. To do so, perform the steps in the **Upgrading MariaDB** section.
21. **8.12.1 included important security updates that require you to reboot all appliances after installing 8.12.1. If you have not previously installed 8.12.1 and rebooted all appliances, you must reboot all appliances after installing 8.12.1.4.** If you would like assistance in planning an upgrade path that meets your security needs while minimizing downtime, please contact your Customer Success Manager.

Manual Updates for 8.4.x Systems Updated to 8.12.1.4

If you upgraded from an 8.4.x system to 8.12.1.4, after 8.12.1.4 is installed, you must manually apply the following changes to every Message Collector and All-In-One Appliance in your system:

1. Either go to the console or use SSH to access the server.
2. Log in as user **em7admin** with the appropriate password.
3. Enter the following at the command line:

```
sudo vi /etc/siteconfig/siloconf.siteconfig
```
4. Locate the following line:

```
eventmanager = syslog,trap,internal
```

NOTE: On an All-In-One Appliance, this line will include additional entries in the comma-delimited list.

5. Add ",agent" to the end of the line. The line should now look like this:

```
eventmanager = syslog,trap,internal,agent
```
6. Save the file and exit vi (:wq).
7. At the command line, enter the following command to rebuild the configuration file:

```
sudo /opt/em7/share/scripts/generate-silo-conf.py > /etc/silo.conf
```

Upgrading MariaDB

Version 8.12.0 requires updates to MariaDB that address security and performance issues. If you have not previously installed an 8.12.x version, the 8.12.x platform patch will automatically update MariaDB-client, MariaDB-common, and MariaDB-shared RPMs but will not update the MariaDB Server RPM. You must manually update the MariaDB Server RPM. You can download the latest approved MariaDB updates at <https://portal.sciencelogic.com/portal/miscellaneous>.

NOTE: To address security issues, download the latest MariaDB updates. Earlier MariaDB updates remain on the portal to support users who have not yet migrated to the latest release.

The following sections describe how to perform this upgrade for different appliance types and architectures.

Two Database Servers Configured for High Availability

To upgrade a High Availability cluster, perform the following steps:

WARNING: The system will be unavailable when performing these steps.

1. Copy the MariaDB RPMs to the file system of both appliances.
2. Log in to the command-line of both Database Server appliances as em7admin.
3. Execute the following command on the secondary Database Server:

```
sudo systemctl stop pacemaker.service
```
4. Execute the following command on the primary Database Server to determine the current installed version of the RPMs:

```
sudo rpm -qa ^MariaDB-*
```
5. Execute the following command on the primary Database Server:

```
sudo systemctl stop mysql
```
6. On the primary Database Server, navigate to the directory that you copied the RPMs.
7. For each RPM that the output from step 5 showed at an earlier version, execute the following command on the primary Database Server:

```
sudo rpm -Uvh <file name of RPM>
```
8. Execute the following command on the primary Database Server to validate that the RPMs installed correctly:

```
sudo rpm -qa ^MariaDB-*
```
9. Execute the following command on the primary Database Server:

```
sudo systemctl start mysql
```

10. Execute the following command on the primary Database Server, replacing the password for the root database user when prompted:

```
sudo mysql_upgrade -u root -p
```
11. On the secondary Database Server, execute the following command to determine the current installed version of the RPMs:

```
sudo rpm -qa ^MariaDB-*
```
12. On the secondary Database Server, navigate to the directory where you copied the RPMs.
13. For each RPM that the output from step 11 showed at an earlier version of MariaDB, execute the following command on the secondary Database Server:

```
sudo rpm -Uvh <file name of RPM>
```
14. Execute the following command on the secondary Database Server to validate that the RPMs installed correctly:

```
sudo rpm -qa ^MariaDB-*
```
15. Execute the following command on the secondary Database Server:

```
sudo systemctl start pacemaker.service
```

Two Database Servers Configured for Disaster Recovery

To upgrade two Database Servers configured for disaster recovery, perform the following steps:

WARNING: The system will be unavailable when performing these steps.

1. Copy the latest RPMs to the file system of both appliances.
2. Log in to the command-line of both Database Server appliances as em7admin.
3. Execute the following command on the primary Database Server to determine the current installed version of the RPMs:

```
sudo rpm -qa ^MariaDB-*
```
4. Execute the following command on the primary Database Server:

```
sudo systemctl stop mysql
```
5. On the primary Database Server, navigate to the directory that you copied the RPMs.
6. For each RPM that the output from step 4 showed at an earlier version, execute the following command on the primary Database Server:

```
sudo rpm -Uvh <file name of RPM>
```
7. Execute the following command on the primary Database Server to validate that the RPMs installed correctly:

```
sudo rpm -qa ^MariaDB-*
```

- Execute the following command on the primary Database Server:

```
sudo resource start mysql
```

- Execute the following command on the primary Database Server, replacing the password for the root database user where indicated:

```
sudo mysql_upgrade -u root -p
```

- On the secondary Database Server, execute the following command to determine the current installed version of the RPMs:

```
sudo rpm -qa ^MariaDB-*
```

- On the secondary Database Server, navigate to the directory where you copied the RPMs.

- For each RPM that the output from step 10 showed at an earlier version, execute the following command on the secondary Database Server:

```
sudo rpm -Uvh <file name of RPM>
```

- Execute the following command on the secondary Database Server to validate that the RPMs installed correctly:

```
sudo rpm -qa ^MariaDB-*
```

Three Database Servers Configured for HA and DR

To upgrade a High Availability cluster, perform the following steps:

WARNING: The system will be unavailable when performing these steps.

- Copy the latest RPMs to the file system of all three appliances.
- Log in to the command-line of all three Database Server appliances as em7admin.
- Execute the following command on the secondary Database Server in the HA cluster:

```
sudo systemctl stop pacemaker.service
```

- Execute the following command on the primary Database Server in the HA cluster to determine the current installed version of the RPMs:

```
sudo rpm -qa ^MariaDB-*
```

- Execute the following command on the primary Database Server in the HA cluster:

```
sudo systemctl stop mysql
```

- On the primary Database Server in the HA cluster, navigate to the directory that you copied the RPMs.

- For each RPM that the output from step 5 showed at an earlier version, execute the following command on the primary Database Server in the HA cluster:

```
sudo rpm -Uvh <file name of RPM>
```

- Execute the following command on the primary Database Server in the HA cluster to validate that the RPMs installed correctly:

```
sudo rpm -qa ^MariaDB-*
```

9. Execute the following command on the primary Database Server in the HA cluster:

```
sudo systemctl start mysql
```

10. Execute the following command on the primary Database Server in the HA cluster, replacing the password for the root database user where indicated:

```
sudo mysql_upgrade -u root -p
```

11. On the secondary Database Server, execute the following command to determine the current installed version of the RPMs:

```
sudo rpm -qa ^MariaDB-*
```

12. On the secondary Database Server, navigate to the directory where you copied the RPMs.

13. For each RPM that the output from step 11 showed at an earlier version, execute the following command on the secondary Database Server:

```
sudo rpm -Uvh <file name of RPM>
```

14. Execute the following command on the secondary Database Server in the HA cluster to validate that the RPMs installed correctly:

```
sudo rpm -qa ^MariaDB-*
```

15. Execute the following command on the secondary Database Server in the HA cluster:

```
sudo systemctl start pacemaker.service
```

16. On the Database Server for disaster recovery, execute the following command to determine the current installed version of the RPMs:

```
sudo rpm -qa ^MariaDB-*
```

17. On the Database Server for disaster recovery, navigate to the directory that you copied the RPMs.

18. For each RPM that the output from step 16 showed at an earlier version, execute the following command on the Database Server for disaster recovery:

```
sudo rpm -Uvh <file name of RPM>
```

19. Execute the following command on the secondary Database Server in the HA cluster to validate that the RPMs installed correctly:

```
sudo rpm -qa ^MariaDB-*
```

20. Execute the following command on the Database Server for disaster recovery to validate that the RPMs installed correctly:

```
sudo rpm -qa ^MariaDB-*
```

Single Database Server/All-In-One Appliance/Data Collector/Message Collector

To upgrade MariaDB on a single Database Server, All-In-One Appliance, Data Collector, or Message Collector, perform the following steps:

WARNING: The Database Server, All-In-One Appliance, Data Collector, or Message Collector will be inoperable when performing these steps.

1. Copy the latest RPMs to the file system of the appliance:
2. Log in to the command-line of the appliance as em7admin.
3. Execute the following commands:

```
sudo systemctl stop em7
sudo systemctl stop mariadb.service
```

4. Execute the following command to determine the current installed version of the RPMs:
5. Navigate to the directory that you copied the RPMs.
6. For each RPM that the output from step 4 showed at an earlier version, execute the following command:

```
sudo rpm -qa ^MariaDB-*
```

```
sudo rpm -Uvh <file name of RPM>
```

7. Execute the following command to validate that the RPMs installed correctly:

```
sudo rpm -qa ^MariaDB-*
```

8. Execute the following commands:

```
sudo systemctl daemon-reload
sudo systemctl start mariadb.service
```

9. Execute the following command, replacing the password for the root database user where indicated:

```
sudo mysql_upgrade -u root -p
```

10. Execute the following command to re-start SL1:

```
sudo systemctl start em7
```

Rebooting Appliances

Use the applicable steps listed in this section to reboot your appliances.

Administration Portal

If your SL1 system includes multiple Administration Portals, you can remotely reboot Administration Portals from another Administration Portal. To do so:

1. Go to the **Appliance Manager** page (System > Settings > Appliances).
2. Select the checkboxes for the appliances you want to reboot.
3. In the **[Select Action]** menu, select **Reboot** and click the Go button.
4. Click the OK button when the "Are you sure you want to reboot the selected appliances?" message is displayed.

5. During the reboot, the user interface for the affected Administration Portals is unavailable.
6. When the reboot has completed, the **Audit Logs** page (System > Monitor > Audit Logs) will include an entry for each appliance that was rebooted.

If your SL1 system include only a single Administration Portal, perform the following steps to reboot that Administration Portal:

1. Either go to the console of the Database Server or use SSH to access the server.
2. Log in as **em7admin** with the appropriate password.
3. At the shell prompt, execute the following:

```
python -m silo_common.admin_toolbox <appliance_ID> "/usr/bin/sudo /usr/sbin/shutdown -r +1"
```

where:

- *appliance_ID* is the appliance ID for the Data Collector, Message Collector, or Administration Portal.

Data Collectors and Message Collectors

You can reboot Data Collector and Message Collectors either from the user interface or from the command line.

From the SL1 user interface, perform the following steps to reboot a Data Collector or Message Collector:

1. Go to the **Appliance Manager** page (System > Settings > Appliances).
2. Select the checkboxes for the appliances you want to reboot.
3. In the **[Select Action]** menu, select **Reboot** and click the Go button.
4. Click the OK button when the "Are you sure you want to reboot the selected appliances?" message is displayed.
5. During the reboot, go to the **System Logs** page (System > Monitor > System Logs). You should see this message:

```
Major: Could not connect to module (5) database USING SSL=TRUE: Error attempting to connect to database with SSL enabled True: (2003, 'Can't connect to MySQL server on '10.2.12.77' (113 "No route to host")')
```

6. When the reboot has completed, the **Audit Logs** page (System > Monitor > Audit Logs) will include an entry for each appliance that was rebooted.

From the console of the Database Server or SSH to the Database Server, perform the following steps to reboot a Data Collector or Message Collector:

1. Either go to the console of a Database Server or SSH to access the server.
2. Log in as **em7admin** with the appropriate password.
3. At the shell prompt, execute the following:

```
python -m silo_common.admin_toolbox <appliance_ID> "/usr/bin/sudo /usr/sbin/shutdown -r +1"
```

where:

- `appliance_ID` is the appliance ID for the Data Collector, Message Collector, or Administration Portal.

Standalone All-In-One Appliances and Database Servers

Perform the following steps to reboot a standalone All-In-One Appliance or Database Server:

1. Either go to the console or use SSH to access the server.
2. Log in as **em7admin** with the appropriate password.
3. Execute the following commands on the appliance to pause the system and shutdown MariaDB. Enter the password for the em7admin user when prompted:

```
sudo touch /tmp/.proc_mgr_pause
sudo systemctl stop mariadb
```

4. Execute the following command on the appliance to reboot the appliance:
5. After the appliance has rebooted, log in to the appliance as the em7admin user using the console or SSH.
6. Execute the following command on the appliance to un-pause the system:

```
sudo rm /tmp/.proc_mgr_pause
```

7. Enter the password for the em7admin user and confirm the command when prompted.

Two Database Servers Configured for Disaster Recovery

Perform the following steps to reboot two Database Servers configured for Disaster Recovery:

1. Either go to the console of the primary Database Server or use SSH to access the server.
2. Log in as **em7admin** with the appropriate password.
3. First, you should check the status of the appliances. To do this, enter the following at the shell prompt:

```
cat /proc/drbd
```

4. Your output will look like this:

```
1: cs:Connected ro:Primary/Secondary ds:UpToDate/UpToDate C r----
ns:17567744 al:0 bm:1072 lo:0 pe:0 ua:0 ap:0 ep:1 wo:b oos:12521012
```

NOTE: If your output includes "ro:Primary/Secondary", but does not include "UpToDate/UpToDate", data is being synchronized between the two appliances. You must wait until data synchronization has finished before rebooting.

5. Execute the following commands on the **primary** appliance to pause the system and shutdown MariaDB. Enter the password for the em7admin user when prompted:

```
sudo touch /tmp/.proc_mgr_pause
sudo systemctl stop pacemaker
```

6. Execute the following command on the **primary** appliance to reboot the appliance:

```
sudo reboot
```

7. After the primary appliance has rebooted, log in to the console of the **primary** appliance again.
8. Execute the following commands on the **primary** appliance:

```
sudo rm /tmp/.proc_mgr_pause
```
9. Enter the password for the em7admin user and confirm the command when prompted.
10. Log in to the **secondary** Database Server as the em7admin user using the console or SSH.
11. Execute the following command on the **secondary** appliance to reboot the appliance:

```
sudo reboot
```
12. Enter the password for the em7admin user when prompted.

Two Database Servers in a High Availability Cluster

Perform the following steps to reboot two Database Servers in a high availability cluster:

1. Either go to the console of the secondary Database Server or use SSH to access the server.
2. Log in as **em7admin** with the appropriate password.
3. First, you should check the status of the appliances. To do this, enter the following at the shell prompt:

```
cat /proc/drbd
```
4. Your output will look like this:

```
1: cs:Connected ro:Secondary/Primary ds:UpToDate/UpToDate C r----  
ns:17567744 al:0 bm:1072 lo:0 pe:0 ua:0 ap:0 ep:1 wo:b oos:12521012
```

NOTE: If your output includes "ro:Secondary/Primary", but does not include "UpToDate/UpToDate", data is being synchronized between the two appliances. You must wait until data synchronization has finished before rebooting.

5. Execute the following command on the **secondary** appliance to stop the cluster service:

```
sudo systemctl stop pacemaker
```
6. Enter the password for the em7admin user when prompted.
7. Log in to the **primary** Database Server as the em7admin user using the console or SSH.
8. Execute the following commands on the **primary** appliance to pause the system and stop the cluster service. Enter the password for the em7admin user when prompted:

```
sudo touch /tmp/.proc_mgr_pause  
sudo systemctl stop pacemaker
```
9. Execute the following command on the **primary** appliance to reboot the appliance:

```
sudo reboot
```
10. After the primary appliance has rebooted, log in to the console of the **primary** appliance again.

11. Execute the following command on the **primary** appliance:

```
sudo rm /tmp/.proc_mgr_pause
```

12. Enter the password for the em7admin user and confirm the command when prompted.
13. Ensure that the user interface is now available on the primary appliance.
14. Log in to the **secondary** Database Server as the em7admin user using the console or SSH.
15. Execute the following command on the **secondary** appliance to reboot the appliance:

```
sudo reboot
```
16. Enter the password for the em7admin user when prompted.

Three Database Servers Configured for High Availability and Disaster Recovery

Perform the following steps to reboot three Database Servers configured for high availability and disaster recovery:

1. Either go to the console of the **secondary Database Server in the HA cluster** or use SSH to access the server.
2. Log in as **em7admin** with the appropriate password.
3. First, you should check the status of the appliances. To do this, enter the following at the shell prompt:

```
cat /proc/drbd
```

4. Your output will look like this:

```
10: cs:Connected ro:Secondary/Primary ds:UpToDate/UpToDate C r----  
ns:17567744 al:0 bm:1072 lo:0 pe:0 ua:0 ap:0 ep:1 wo:b oos:12521012
```

NOTE: If your output includes "ro:Secondary/Primary", but does not include "UpToDate/UpToDate", data is being synchronized between the two appliances. You must wait until data synchronization has finished before rebooting.

5. Execute the following command on the **secondary Database Server in the HA cluster** to stop the cluster service:

```
sudo systemctl stop pacemaker
```
6. Enter the password for the em7admin user when prompted.
7. Log in to **primary** Database Server as the em7admin user using the console or SSH.
8. Execute the following commands on the **primary** appliance to pause the system and stop the cluster service. Enter the password for the em7admin user when prompted:

```
sudo touch /tmp/.proc_mgr_pause  
sudo systemctl stop pacemaker
```

9. Execute the following command on the **primary** appliance to reboot the appliance:

```
sudo reboot
```
10. After the primary appliance has rebooted, log in to the console of the **primary** appliance again.
11. Execute the following command on the **primary** appliance:

```
sudo rm /tmp/.proc_mgr_pause
```
12. Enter the password for the em7admin user and confirm the command when prompted.
13. Log in to the **secondary Database Server in the HA cluster** as the em7admin user using the console or SSH.
14. Execute the following command on the **secondary Database Server in the HA cluster** to reboot the appliance:

```
sudo reboot
```
15. Enter the password for the em7admin user when prompted.
16. Log in to the **Database Server for Disaster Recovery** as the em7admin user using the console or SSH.
17. Execute the following command on the **Database Server for Disaster Recovery** to reboot the appliance:

```
sudo reboot
```
18. Enter the password for the em7admin user when prompted.

Deprecated Features

As of the 8.2.0 release, the following PowerPacks are no longer included in the default ISO. These PowerPacks will not be automatically removed from an existing system during an upgrade and will remain available for download on the [ScienceLogic Portal](#):

- ADIC Base Pack
- Ascend Communications Base Pack
- Cabletron System Base Pack
- CloudKick Management
- GoGrid Base Pack
- Informant Cluster
- Informant Exchange
- Informant MS SQL
- Informant Windows OS
- NTI Base Pack
- Rackspace Base Pack
- Redback Base Pack
- RIM Blackberry Base Pack

- Sensatronics Base Pack
- SystemEdge Base Pack
- System Uptime
- Tipping Point Base Pack
- Xirrus Base Pack

The new user interface architecture requires API access for all users; API access is automatically granted to users. The following API-specific access hooks have been deprecated and removed from the product:

- API: Resource Indexes
- API: Server Access
- API: Virtual Device

The following functionality that was available in previous releases is no longer available in the 8.12.1 release:

- The process for generating rollup/normalized data has been updated to improve performance and scalability. This update deprecates the generation of frequent rollup data. The following user interface pages are affected:
 - The widgets Leaderboard/Top-N, Leaderboard/Top-N (secondary), and Multi-Series Performance no longer support Frequent normalization. If these widgets are used by older dashboards and are already configured to use Frequent normalization, the platform will automatically update these widgets to use hourly normalization.
 - In the Collection Labels page (System > Manage > Collection Labels), the Frequent Data column is deprecated.
- The Cisco Nexus PowerPack has been removed from the default build and is no longer supported. However, the PowerPack is not deleted during the upgrade process. The device classes for Cisco Nexus devices are now included in the Cisco: Base Pack PowerPack.
- The ScienceLogic Agent no longer supports 32-bit versions of Linux or Windows.
- The third-party Azure python library has been removed from the ISO build.
- The FTP, SFTP, NFS, and SMB backup options that stage locally are no longer supported.
- The EMC Base Pack PowerPack has been removed from the default build and is no longer supported. However, the PowerPack is not deleted during the upgrade process. If you are still using the EMC Base Pack PowerPack, ScienceLogic recommends using the EMC: VNX PowerPack instead.
- The SAN wizard is no longer supported. ScienceLogic will no longer provide direct support for configuring a SAN for data storage.
- Integration Server appliances are no longer supported.
- Root access is not enabled on any appliance.
- The VMware: vCloud PowerPack has been removed from the ISO build and is no longer supported.
- The "ifconfig" command is no longer supported by the new appliance operating system. The "ip addr" command must be used instead.
- NOC Screens (System > Manage > Screens) are no longer included in the platform. To re-enable this feature, contact ScienceLogic Customer Support.

- The Knowledge Base is no longer supported by ScienceLogic and will be disabled by default for new users.
- High-Availability and Disaster Recovery no longer support the command "drbd-overview". To check the status of drbd, use "cat /proc/drbd".
- System Update no longer supports the shell command "deploy_patch".

Known Issues

For a list of Known Issues and workarounds, see the ScienceLogic Customer Portal at <https://support.sciencelogic.com/s/topic/0TO0z000000E6w7GAC/known-issues>.

© 2003 - 2019, ScienceLogic, Inc.

All rights reserved.

LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

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

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

Copyrights and Trademarks

ScienceLogic, the ScienceLogic logo, and EM7 are trademarks of ScienceLogic, Inc. in the United States, other countries, or both.

Below is a list of trademarks and service marks that should be credited to ScienceLogic, Inc. The ® and ™ symbols reflect the trademark registration status in the U.S. Patent and Trademark Office and may not be appropriate for materials to be distributed outside the United States.

- ScienceLogic™
- EM7™ and em7™
- Simplify IT™
- Dynamic Application™
- Relational Infrastructure Management™

The absence of a product or service name, slogan or logo from this list does not constitute a waiver of ScienceLogic's trademark or other intellectual property rights concerning that name, slogan, or logo.

Please note that laws concerning use of trademarks or product names vary by country. Always consult a local attorney for additional guidance.

Other

If any provision of this agreement shall be unlawful, void, or for any reason unenforceable, then that provision shall be deemed severable from this agreement and shall not affect the validity and enforceability of any remaining provisions. This is the entire agreement between the parties relating to the matters contained herein.

In the U.S. and other jurisdictions, trademark owners have a duty to police the use of their marks. Therefore, if you become aware of any improper use of ScienceLogic Trademarks, including infringement or counterfeiting by third parties, report them to Science Logic's legal department immediately. Report as much detail as possible about the misuse, including the name of the party, contact information, and copies or photographs of the potential misuse to: legal@sciencelogic.com



ScienceLogic

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

International: +1-703-354-1010