



SL1 10.2.6 Release Notes

SL1 version 10.2.6, Revision 1

Table of Contents

Upgrade Notes	5
Caveats	6
New Features in 10.2.6	7
Security	7
Issues Addressed in 10.2.6	7
Devices	7
New Features in 10.2.5	7
Security	7
WMI	8
New Features in 10.2.4	8
End-User Licensing Agreement	8
Security	8
Issues Addressed in 10.2.4	8
Concurrent SNMP Collection	8
Device Groups	9
Events	9
PowerShell Dynamic Applications	9
New Features in 10.2.3	9
Security	9
Issues Addressed in 10.2.3	10
Dashboards	10
Device Groups	10
Dynamic Applications	10
System Update	10
New Features in 10.2.2	10
Backups	10
Database Server	10
Security	11
System	11
Issues Addressed in 10.2.2	11
Devices	11
Internal Collections Dynamic Applications (ICDA)	11
IPv6	11
Logging	11
Issues Addressed in 10.2.1.1	12
Platform	12
New Features in 10.2.1	12
Authentication	12
New and Updated Packages in 10.2.1	12
Issues Addressed in 10.2.1	12
Agent	12
Reports	12
SSH Concurrent Collection	13
User Interface	13
SL1 Extended Architecture	14
PowerPacks in 10.2.6	15
Disabling the Knowledge Base	16
Upgrade Process for Systems Running 8.1.0 and Earlier	17
Upgrade Process for Systems Running 8.1.1 and Later	17
Downloading SL1 Updates on SL1 Systems running 8.1.x - 8.5.x	17

Downloading SL1 Updates on SL1 Systems Running 8.6.0 or Later	18
Recently Deprecated Features	18
8.14.0	18
10.1.0	19
Known Issues	19
Known Issue in 10.2.5	19
Known Issues in 10.2.0	20
Critical Known Issue with the Gen 1 Agent	20
Major Known Issue with Data Collection	20
Disable Concurrent SSH Collection	20
Manually Prune the files in /var	21

Overview

SL1 10.2.6 is a maintenance release that includes numerous package updates for improved security and platform performance.

This document covers the following topics:

<i>Upgrade Notes</i>	5
<i>Caveats</i>	6
<i>New Features in 10.2.6</i>	7
<i>Issues Addressed in 10.2.6</i>	7
<i>New Features in 10.2.5</i>	7
<i>New Features in 10.2.4</i>	8
<i>Issues Addressed in 10.2.4</i>	8
<i>New Features in 10.2.3</i>	9
<i>Issues Addressed in 10.2.3</i>	10
<i>New Features in 10.2.2</i>	10
<i>Issues Addressed in 10.2.2</i>	11
<i>Issues Addressed in 10.2.1.1</i>	12
<i>New Features in 10.2.1</i>	12
<i>New and Updated Packages in 10.2.1</i>	12
<i>Issues Addressed in 10.2.1</i>	12
<i>User Interface</i>	13
<i>SL1 Extended Architecture</i>	14
<i>PowerPacks in 10.2.6</i>	15
<i>Disabling the Knowledge Base</i>	16
<i>Upgrade Process for Systems Running 8.1.0 and Earlier</i>	17
<i>Upgrade Process for Systems Running 8.1.1 and Later</i>	17
<i>Recently Deprecated Features</i>	18
<i>Known Issues</i>	19

TIP: 10.2.6 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 10.2.6.

Upgrade Notes

CAUTION: SL1 version 10.2.5 included a new WMI client in response to Microsoft security updates. This change enables WMI Dynamic Applications to collect data from hardened Windows servers, but also has a major impact on system scalability.

This change significantly decreases the number of Microsoft Windows servers that can be supported on each Data Collector in your SL1 system. Users who need to monitor Windows devices using WMI should analyze their system resources and capacity before upgrading to 10.2.5 or later. For guidance about sizing, see the updated [Collector Sizing Guidelines for WMI Endpoints](#).

To avoid this impact, ScienceLogic recommends using SNMP collection for two-core Windows servers and PowerShell collection for four-core Windows servers. For more information, see this [Support Knowledge Base article](#).

CAUTION: If your SL1 system is deployed on AWS, you will be unable to upgrade from 10.2.6 to the 11.2.x line or upcoming 11.3.x line at this time due to a known issue. If your system is deployed on AWS and you plan to consume a 11.2.x or 11.3.x release, do not install 10.2.6.

This issue does not impact other SL1 deployment types.

- After installing 10.2.6, if your SL1 system is not deployed on AWS, you have the following upgrade options:
 - You can upgrade to the 11.1.x line with the 11.1.4 release. You cannot upgrade from 10.2.6 to 11.1.0, 11.1.1, 11.1.2, or 11.1.3.
 - You can upgrade to the 11.2.x line with the upcoming 11.2.2 release. You cannot upgrade from 10.2.6 to 11.2.0 or 11.2.1.
 - You can upgrade to the upcoming 11.3.0 release.
- There is a Known Issue that is causing System Updates to the 10.2.x and 11.1.x lines to fail to load Docker images on Data Collector appliances and All-in-One Appliances. For details and the workaround, see the Known Issue article 5693: <https://support.sciencelogic.com/s/article/5693>
- **If you are running a version prior to 8.12.0, do not install 10.2.6 if you do not plan to immediately consume 10.2.6.** After you import the 10.2.6 release, all appliances in your SL1 system will now use the **new system update**. After you import the 10.2.6 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 10.2.6 and its new System Updates tool, you must have already imported, staged, and deployed 8.6.0 or a later release.**
- You can install 10.2.6 in AWS RDS/Aurora environments.
 - You can upgrade from 10.1.x running in AWS RDS/Aurora environments to 10.2.6 running in AWS RDS/Aurora environments.

- However, you cannot upgrade from 8.14.x running in AWS RDS/Aurora environments directly to 10.2.6 running in AWS RDS/Aurora environments.
- 10.2.6 includes important security updates. **After deploying 10.2.6, you must reboot all appliances in the SL1 Distributed Architecture.** If you would like assistance in planning an upgrade path that meets your security needs while minimizing downtime, please contact your Customer Success Manager.
- ScienceLogic strongly recommends that you review the [Known Issues](https://support.sciencelogic.com/s/known-issues#sort=relevancy) for SL1 (<https://support.sciencelogic.com/s/known-issues#sort=relevancy>) before installing a new update. For Known Issues specific to 10.2.x, see the [Known Issues](#) section of these release notes
- ScienceLogic strongly recommends that you review the instructions on planning an upgrade, best practices for upgrades, and executing an upgrade. To do so, see the chapter on **Upgrading SL1** in the [System Administration](#) manual.
- Some SL1 updates require you to reboot all SL1 appliances to apply important security updates and then to upgrade MariaDB..

The following table specifies which SL1 updates require you to reboot all SL1 appliances and the required MariaDB version for each SL1 version:

SL1 Release	Requires Reboot?	Required MariaDB Version
10.2.0	Yes	10.4.18
10.2.1	Yes	10.4.18
10.2.2	Yes	10.4.18
10.2.3	Yes	10.4.21
10.2.4	Yes	10.4.22
10.2.4.1	Yes	10.4.22
10.2.5	Yes	10.4.22
10.2.6	Yes	10.4.26

Caveats

Consider the following caveats before deploying 10.2.6:

- As of 10.1.0, SL1 no longer includes Flash.
- As of 8.12.2, ScienceLogic no longer updates the help that appears when you select the **[Guide]** button. The Unified UI provides a new tool for inline help. Under the user name in the upper right corner, click the down arrow and select **Help**. The browser will open a new window that displays the appropriate page from docs.sciencelogic.com.
- As of January 1, 2021, **new installations of SL1 Extended Architecture are available only on SaaS deployments.** For existing on-premises deployments of SL1 Extended Architecture, please contact ScienceLogic Customer Support for upgrade documentation and help with technical issues.

- **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.
- 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 10.2.6.***
- 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](#).***
- Global Manager, SL1 Extended Architecture, the new UI, and PowerFlow do not provide MUD support in 10.2.x release.
- 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.

New Features in 10.2.6

Security

- 10.2.6 includes package updates that improve security and performance.

Issues Addressed in 10.2.6

Devices

- Improved the process for deleting large numbers of devices. (Case: 00268318) (Jira ID: EM-52468)

New Features in 10.2.5

Security

- Updated packages to address several security vulnerabilities.

WMI

- SL1 collection via WMI Dynamic Applications was refactored in response to Microsoft security updates. WMI Dynamic Applications can now collect data from hardened Windows servers.

CAUTION: This change significantly decreases the number of Microsoft Windows servers that can be supported on each Data Collector in your SL1 system. Users who need to monitor Windows devices using WMI should analyze their system resources and capacity before upgrading to 10.2.5. For guidance about sizing, see the updated [Collector Sizing Guidelines for WMI Endpoints](#).

To avoid this impact, ScienceLogic recommends using SNMP collection for two-core Windows servers and PowerShell collection for four-core Windows servers. For more information, see this [Support Knowledge Base article](#).

New Features in 10.2.4

End-User Licensing Agreement

- Updated the text of the End-User Licensing Agreement.

Security

- General package updates to address security issues and SL1 performance.
- Updated the packages on the containerized service (Streamer Push) that "pushes" collected data from the Data Collector to the Compute Node cluster on SL1 Extended systems. The package updates address security issues and SL1 performance.
- Updated packages for all containerized services for events. The package updates address security issues and SL1 performance.
- Updated packages for the containerized service that ingests Dynamic Application data in SL1 Extended systems. The package updates address security issues and SL1 performance.

Issues Addressed in 10.2.4

Concurrent SNMP Collection

- Concurrent SNMP collection no longer drops polls and creates data gaps when querying SNMPv3 devices with large latency. (Case: 00187707) (Case: 00205232) (Jira ID: EM-45866) (Jira ID: EM-47111) (Jira ID: EM-45093)

Device Groups

- The Device Group Editor page (Registry > Devices > Device Groups > create/edit) now loads successfully regardless of the number of devices or the complexity of the dynamic rules. (Case: 00202034) (Jira ID: EM-46387) (Jira ID: EM-46223) (Jira ID: EM-47100)

Events

- Event Suppression now works as expected on devices in Device Groups. (Case: 00220570) (Case: 0022963) (Jira ID: EM-48084) (Jira ID: EM-48016)

PowerShell Dynamic Applications

- Made improvements to the performance of legacy PowerShell Dynamic Applications:
 - If a PowerShell command takes longer than 90 seconds to execute on a device, SL1 will terminate that PowerShell command, and the collection data for that PowerShell command on that specific device during that collection session will be lost.

NOTE: In most cases, PowerShell commands take 2-5 seconds to execute on a device. The new 90-second timeout prevents "hung" responses from blocking the execution of other PowerShell commands in the same Dynamic Application. If you require a longer timeout, please see the Knowledge Base Article <KBA link>

- This new behavior will not affect:
 - any other PowerShell commands from the same Dynamic Application during the same collection session
 - the next collection session for that Dynamic Application for that device
 - any other Dynamic Applications for that device
- If SL1 terminates a PowerShell command, SL1 will create a log entry and also trigger an event.
- In addition, if a connection to a Windows server is closed without closing the PowerShell command, the orphaned PowerShell command will continue to exist on the Windows device for 2 minutes and then will automatically close. (Jira ID: EM-47819) (Jira ID: EM-47835) (Jira ID: EM-36579) (EM-47835)

New Features in 10.2.3

Security

- Package updates in response to Critical CVE-2021-43527.
- Package updates to address security issues and SL1 performance.

- Package updates for the following CVEs and ELSAs:
 - CVE-2019-11244, CVE-2019-11246, CVE-2019-11249, CVE-2019-9512, CVE-2019-9514, CVE-2019-9946, CVE-2019-1002101 CVE-2019-11251, CVE-2019-11247, CVE-2020-8555, CVE-2020-10749, CVE-2020-13379, CVE-2020-8554, CVE-2020-8555, CVE-2020-10749, CVE-2020-16845, CVE-2020-28914
 - ELSA-2019-4816, ELSA-2019-4593, ELSA-2020-5725, ELSA-2020-5726, ELSA-2020-5727, ELSA-2020-5825, ELSA-2020-5827, ELSA-2020-5828, ELSA-2021-9028

Issues Addressed in 10.2.3

Dashboards

- In Dashboards, map widgets now correctly auto-refresh. (Case: 00201978) (Jira ID: EM-46200) (Jira ID: EM-46261)

Device Groups

- Addressed an issue where the rules for dynamic Device Groups caused SL1 to slow down and eventually display a "502 Bad Gateway" error. (Case: 00212985) (Jira ID: EM-47295) (Jira ID: EM-47565)

Dynamic Applications

- Dynamic Applications are no longer mis-aligned to Microsoft Windows servers. (Jira ID: EM-47464) (Jira ID: EM-46419) (Jira ID: EM-47465)

System Update

- The timeout value has been increased to prevent multiple timeouts during upgrade. Moved the timeout setting for OS processes to the master.system_custom_config table, in the os_process_timeout column, instead of using the value in the credential. (Case: 00186868) (Case: 00181625) (Jira ID: EM-46551) (Jira ID: EM-46095) (Jira ID: EM-47003) (Jira ID: EM-45197) (Jira ID: EM-45291)

New Features in 10.2.2

Backups

- Configuration backups now include the RSA host key for the Database Server.

Database Server

- SL1 Database Servers now includes kubectl for k8s 1.16 and supporting packages.

Security

- Update packages to improve security and performance.)
- Security updates to address CVE 2021-33909.
- Made security improvements to logging. (Jira ID: EM-45137) (Jira ID: EM-45136) (Case: 00187629)
- Made security improvements to Log Monitoring Policies (System > Manage > Log File Monitoring Policies). (Jira ID: EM-45136) (Case: 00187629)

System

- 10.2.2 includes an improvement to database tables for normalized performance data from Dynamic Applications. In 10.2.2 and later releases, SL1 indexes the tables of normalized performance data during the post-upgrade process. Reports and dashboards that use normalized performance data will no longer lag and will now load large data-sets within seconds.

Issues Addressed in 10.2.2

Devices

- You can now manually purge vanished devices from the Vanished Device Registry page. (Jira ID: EM-39360) (Case: 00089588)

Internal Collections Dynamic Applications (ICDA)

- Internal Collections Dynamic Applications (ICDA) no longer cause false alerts for process inventory, services inventory, and file system inventory. (Jira ID: EM-43553) (Jira ID: EM-43756) (Jira ID: EM-43783) (Jira ID: EM-44090) (Jira ID: EM-44091) (Jira ID: EM-44175) (Jira ID: EM-45218) (Case: 00157364) (Case: 00161944) (Case: 00164303) (Case: 00167935) (Case: 00169232) (Case: 00175579) (Case: 00179779)

IPv6

- Addressed an issue that was preventing users from adding IPv6 addresses in the IP Address field on the Device Properties page in the classic SL1 user interface. With this update, you can now add an IPv6 IP address and Subnet Mask to a discovered device. (Case: 00157887) (Jira ID: EM-43805) (Jira ID: EM-42730)

Logging

- Added additional details to the powershell_collector.log to enable troubleshooting. (Jira ID: EM-43200) (Case: 00162182)

Issues Addressed in 10.2.1.1

Platform

- A feature that was added to 10.2.0 to improve the performance of dashboards is causing upgrades and installations to hang. The feature added indexes to normalized data from Dynamic Applications. 10.2.1.1 removes this feature. The result of removing this feature is that dashboards that use very large sets of data might be slow. (Case: 00174619) (Case: 00172656) (Jira ID: EM-44059) (Jira ID: EM-34141)
- Addressed an issue where Docker images failed to load while updating collectors to 10.2.1.1. (Case: 00175811) (Jira ID: EM-44278)

New Features in 10.2.1

Authentication

- Existing SSH certificates are stored in SL1 with encryption.
- New SSH certificates are stored in SL1 with encryption and are not displayed during or after import.

New and Updated Packages in 10.2.1

10.2.1 includes multiple package updates to address security issues and improve performance. .

WARNING: *10.2.1 includes important security updates that require you to reboot all AIO appliances and all appliances in the Distributed stack after installing 10.2.1.* If you would like assistance in planning an upgrade path that meets your security needs while minimizing downtime, please contact your Customer Success Manager.

Issues Addressed in 10.2.1

Agent

- The Agent for classic UI now starts successfully on new installations. (Jira ID: [AP-1729](#))

Reports

- The vSphere Top Utilization report no longer fails with the error "PHP Fatal error: Call to undefined method groupsWrapper::shouldFilterByGroupId() in /dev/shm/codestore-master_reports.dynamic_reports_new.73.inc". (Jira ID: EM-43321) (Case: 00163026)

SSH Concurrent Collection

- SSH Concurrent Collection is disabled by default. Due to a known issue that can degrade collector performance, ScienceLogic strongly discourages you from enabling SSH Concurrent Collection in 10.2.1. This does not affect PowerPacks that use SSH for collection. When concurrent SSH collection is disabled, those PowerPacks will use standard SSH collection. (Jira ID: SOL-13728 (Case: 00170950))

User Interface

In 10.2.6, the default user interface is the Classic User Interface. To change the default user interface to the Unified UI:

To change the default user interface to the Unified UI:

1. Go to the console of the Administration Portal or open an SSH session to the Administration Portal.
2. Navigate to `/opt/em7/share/config/nginx.d`
3. At the shell prompt, enter the following:

```
sudo vi em7ngx_web_ui.fragment
```

4. Find this section in the file:

```
location / {
    root /usr/local/silo/gui/ap/www;
    index index.em7;
}
```

5. Edit as follows:

```
location = / {
    proxy_set_header Host $host;
    proxy_set_header X-Forwarded-For $remote_addr;
    proxy_set_header X-Forwarded-Proto $scheme;
    proxy_connect_timeout 10;
    proxy_read_timeout 300;
    proxy_pass http://localhost:3000;
}

location /em7 {
    server_name_in_redirect off;
    root /usr/local/silo/gui/ap/www;
    index index.em7;
}
```

6. Save your changes to the file (`:wq`).
7. Restart the web server. To do this, enter the following at the shell prompt:

```
sudo systemctl restart nginx
```

SL1 Extended Architecture

10.2.6 supports the SL1 Extended Architecture. *The following SL1 features require the SL1 Extended Architecture:*

- **Expanded Agent Capabilities.** You can configure the SL1 Agent to communicate with SL1 via a dedicated Message Collector. However, this configuration limits the capabilities of the SL1 Agent. If you configure the SL1 Agent to communicate with SL1 via a Compute Cluster, you expand the capabilities of the SL1 Agent to include features like extensible collection and application monitoring.
- **Data Pipelines.** Data pipelines transport and transform data. Data transformations include enrichment with metadata, data rollup, and pattern-matching for alerting and automation. The Data Pipelines provide an alternative to the existing methods of data transport (data pull, config push, streamer, and communication via encrypted SQL) in SL1. Data pipelines introduce message queues and communicate using encrypted web services.
- **Publisher.** Publisher enables the egress of data from SL1. Publisher can provide data for long-term storage or provide input to other applications that perform analysis or reporting.
- **Scale-out storage of performance data.** Extended Architecture includes a non-SQL database (Scylla) for scalable storage of performance data.
- **Anomaly Detection and future AI/ML developments.** Anomaly detection is a technique that uses machine learning to identify unusual patterns that do not conform to expected behavior. SL1 does this by collecting data for a particular metric over a period of time, learning the patterns of that particular device metric, and then choosing the best possible algorithm to analyze that data. Anomalies are detected when the actual collected data value falls outside the boundaries of the expected value range.

The SL1 Extended Architecture includes four additional types of SL1 Appliances:

- **Compute Cluster.** Compute nodes are the SL1 appliances run services that transport, process, and consume the data from Data Collectors and the SL1 Agent. SL1 uses Docker and Kubernetes to deploy and manage these services. The following services and features require the compute function:
- **Load Balancer.** The SL1 appliance that brokers communication with services running on the Compute Cluster. Services running on the Compute Cluster are managed by Kubernetes. Therefore, a single service could be running on one Compute node in the Compute Cluster; to provide scale, multiple instances of a single service could be running on one, many, or all nodes in the Compute Cluster. To provide scale and resiliency, you can include multiple Load Balancers in your configuration.
- **Storage Cluster.** SL1 Extended includes a Storage Cluster that includes multiple Storage Nodes and one Storage Manager node. These SL1 appliances provide a NoSQL alternative to the SL1 relational database. The Storage Cluster can store performance and log data collected by the Data Collectors and the SL1 Agent.
- **Management Node.** The Management Node allows administrators to install, configure, and update packages on the Compute Nodes cluster, Storage Nodes, and the Load Balancer. The Management Node also allows administrators to deploy and update services running on the Compute Cluster.
- Resiliency and redundancy can also be accomplished by adding additional appliances to these configurations.

PowerPacks in 10.2.6

Before upgrading to 10.2.6 , please verify whether any PowerPacks currently running on your system 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 10.2.0 release included the following PowerPacks that are new or updated and included with the release:

- Cisco: UC Ancillary v103
- Cisco: UCS Standalone Rack Server v103
- Microsoft Hyper-V v101
- Microsoft: Azure v112

For 10.2.0 and later releases, only "Base" PowerPacks will be included with the platform ISO. The following PowerPacks have been removed from the 10.2.0 ISO to comply with the new SL1 pricing model:

<p>NOTE: If you are upgrading from a previous version of SL1 , the 10.2.6 upgrade will not remove any existing PowerPacks.</p>

- Aruba Base Pack
- Avocent ACS Pack
- BlueCat Base Pack
- Cisco VPN Pack
- Cisco: AppDynamics
- Couchbase Base Pack
- Coyote Point Base Pack
- Dell OpenManage Old Base Pack
- H3C Base Pack

- IBM Director Base Pack
- LifeSize Endpoint
- Microsoft: Active Directory Server
- Microsoft: DHCP Server
- Microsoft: DNS Server
- Microsoft: Exchange Server
- Microsoft: Exchange Server 2010
- Microsoft: SharePoint Server
- Microsoft: SQL Server
- Microsoft: SQL Server Enhanced
- Tomcat

To upgrade your license and download PowerPacks, contact your Customer Success Manager.

Documentation and release notes for each PowerPack are available at the [PowerPacks Support](#) page.

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 `silos.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/silos.conf`. In the `LOCAL` section, add the line:

```
kbasedisabled=1
```
3. Use an editor like `vi` and edit the file `/etc/siteconfig/silos.conf.siteconfig`. In the `LOCAL` section, add the line:

```
kbasedisabled=1
```
4. Open a browser session and log in to SL1.

5. From the hamburger menu (☰) in the upper right, select *Clear SL1 System Cache*.
6. Upon your next login, the Knowledge Base tab will not appear. Attempts to access the tab will result in an "Access Denied" error message.

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 10.2.6.

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 Process for Systems Running 8.1.1 and Later

TIP: For detailed instructions on planning an upgrade, best practices for upgrades, and executing an upgrade, see the chapter on *Upgrading SL1* in the *System Administration* manual or view that chapter [online](#).

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 you upgrade**. Please contact ScienceLogic Support for more information.

If you are upgrading from a version of SL1 prior to 8.6.0, you will have to import, stage, run the pre-upgrade script, and deploy the update twice: once to upgrade to 8.6.0 and then again to use a delta-less upgrade to the latest update release.

Downloading SL1 Updates on SL1 Systems running 8.1.x - 8.5.x

To download updates for previous SL1 software versions that have reached their End-of-Life date and are no longer supported by ScienceLogic, contact ScienceLogic Support or a designated Customer Success Manager to get the update files.

You must upgrade your system to 8.6.0 and then upgrade again with the newer deltaless upgrade process.

Store the update files in a location that you can use to upload files to the SL1 system.

NOTE: These steps do not affect the performance of SL1. ScienceLogic recommends that you perform these steps at least 3 days before upgrading.

TIP: For detailed instructions on planning an upgrade, best practices for upgrades, and executing an upgrade, see the chapter on **Upgrading SL1** in the [System Administration](#) manual or view that chapter [online](#).

Downloading SL1 Updates on SL1 Systems Running 8.6.0 or Later

If your SL1 System is running version 8.6.0 or later, you can download a single update file and update your SL1 system to the latest release.

Before you can load a patch or update onto your instance of SL1, you must first download the patch or update to your local computer:

1. Log in to the [ScienceLogic Support](#) site. Use your ScienceLogic customer account and password to access this site.
2. Select the **[Product Downloads]** button, select the **Product Downloads** menu, and choose *Platform*.
3. Find the release you are interested in and click its name.
4. In the **Release Version** article, click on the link for the release image or release patch you want to download. Scroll to the bottom of the page.
5. Under **Files**, select the link for the file you want to download. The file is then downloaded to your local computer.

NOTE: These steps do not affect the performance of SL1. ScienceLogic recommends that you perform these steps at least 3 days before upgrading.

TIP: For detailed instructions on planning an upgrade, best practices for upgrades, and executing an upgrade, see the chapter on **Upgrading SL1** in the [System Administration](#) manual or view that chapter [online](#).

Recently Deprecated Features

8.14.0

- Deprecated the SNMP-based version of the ScienceLogic Support PowerPack (EM-30510)
- The SSH Tool has been removed from the Device Toolbox (Registry > Devices > Device Manager > wrench icon > Toolbox). (Case 00022135) (Support ID: 176020), (EM-29178)

- The Content Management page appears in the user interface but has been deprecated. Updates to the user interface are now included in platform updates.

10.1.0

- The Content Management page no longer appears in the user interface.
- Deprecated harProviderSearch and deviceSearch and replaced with override search. (SLUI-7404)
- The Video Reports PowerPack is no longer included with ISO builds. (SOL-6778)
- The Devices > Agent tab is now part of Device Settings (SLUI-6386)

Known Issues

ScienceLogic strongly recommends that you review all Known Issues for SL1 at <https://support.sciencelogic.com/s/topic/0TO0z000000E6w7GAC/known-issues>.

Known Issue in 10.2.5

- If you are using SL1 Extended Architecture and have enabled Machine Learning for one or more devices, there is a Known Issue. If you have changed the default administrator's username or password, there is a Known Issue when starting the services for Machine Learning. The remediation steps are in this Knowledge Base article:

https://sciencelogic.lightning.force.com/lightning/r/Knowledge__kav/ka04z000000HCczAAG/view

- 10.2.2 includes a performance improvement to database tables for normalized performance data from Dynamic Applications. In 10.2.2 and later releases, SL1 indexes the tables of normalized performance data during the post-upgrade process. After indexing, reports and dashboards that use normalized performance data will no longer lag and will now load large data-sets within seconds.

However, to see performance improvements, customers with very large database tables might have to increase the size of the /tmp directory on the Database Server or manually prune database tables for normalized performance data from Dynamic Applications.

For details, see the Known Issue article 6216: <https://support.sciencelogic.com/s/article/6216>

- There is a Known Issue with System Updates. System Updates to the 10.2.x and 11.1.x lines. System Updates can fail to load Docker images on Data Collector appliances and All-in-One Appliances.

For details and the workaround, see the Known Issue article 5693: <https://support.sciencelogic.com/s/article/5693>

Known Issues in 10.2.0

Critical Known Issue with the Gen 1 Agent

Upgrading to the 10.2.x causes a service outage with Gen 1 Agents. After upgrade to the 10.2.x line, SL1 can no longer communicate with Gen 1 Agents. ScienceLogic recommends that customers using the Gen 1 Agent not upgrade to the 10.2.x line.

For details on about the known issue and status updates on the fix, please contact ScienceLogic Customer Support.

Major Known Issue with Data Collection

10.2.0 includes a major Known Issue that can cause performance degradation and a potential outage for Data Collectors. (Case: 00170950)

The Concurrent SSH Collection feature is enabled by default on 10.2.0 systems, both upgrades and new installations. The Concurrent SSH Collection feature generates temporary files for each connection attempt to the monitored devices. These temporary files can eventually use all the space in the /var directory of each Data Collector, which can cause performance degradation and a potential outage.

Currently, only the Linux Base Pack PowerPack v103 and later uses concurrent SSH collection.


For full details, see the Knowledge Base Article: <https://support.sciencelogic.com/s/article/5498>

To prevent performance degradation and a potential outage, perform the following workaround steps:

- **Disable Concurrent SSH Collection.** This does not affect PowerPacks that use SSH. When concurrent SSH collection is disabled, the Linux Base Pack PowerPack will use standard SSH collection.
- **Manually prune the temporary files on each Data Collector.** Currently, only the Linux Base Pack PowerPack uses concurrent SSH collection. If you know which Data Collectors are performing collection for the Linux Base Pack PowerPack, you can perform these steps on those Data Collectors. If you do not know which Data Collectors are performing collection for the Linux Base Pack PowerPack, you can safely perform these steps on all Data Collectors.

Disable Concurrent SSH Collection

To disable Concurrent SSH Collection:

1. Log in to the Administration Portal.
2. Go to the Process Manager page (System > Settings > Processes).
3. Find the process "Data Collection: SSH Collector" and select its wrench icon (.
4. Set the **Operating State** to *Disabled*.
5. Save your change.
6. Wait 10 minutes for all collection processes to complete

CAUTION: : If you are monitoring a large number of Linux devices, for example, 100 devices or more, you must re-balance the Data Collectors after stopping Concurrent SSH Collector. For details, see the chapter on *Collector Groups and Load Balancing* in the **Systems Administration** manual.

Manually Prune the files in /var

Currently, only the Linux Base Pack PowerPack v103 and later uses concurrent SSH collection. If you know which Data Collectors are performing collection for the Linux Base Pack PowerPack, you can perform these steps on those Data Collectors. If you do not know which Data Collectors are performing collection for the Linux Base Pack PowerPack, you can safely perform these steps on all Data Collectors.

To manually prune the temporary files in the /var directory on each Data Collector:

1. Go to the console of the Data Collector or use SSH to access the Data Collector.
2. To delete all the temporary files in the Docker container for Concurrent SSH Collection, enter the following at the shell prompt:

```
for container in $(sudo docker ps -a | grep silo_ssh_collector | awk '{ print $1}'); do sudo docker rm -f $container; done
```
3. Notice that /var has more free space now.
4. Perform these steps on either each Data Collector performing collection for the Linux Base Pack PowerPack or on each Data Collectors in your SL1 system.

© 2003 - 2022, 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. For more information, see <https://sciencelogic.com/company/legal>.



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

International: +1-703-354-1010