ScienceLogic

Skylar Compliance Release Notes

Version 5.6 , revision 1

Overview

These release notes document the most recent Skylar Compliance (formerly Restorepoint) 5.6 version maintenance release, followed by previous maintenance release notes, sorted by release date.

This document covers the following topics:

Notices:

- Restorepoint has undergone a corporate re-brand and is now known as Skylar Compliance. Going forward, these maintenance release notes document the most recent updates for Skylar Compliance version 5.6.
- Old user interface reports (Information > Reports > **[Old UI Reports]**) will be deprecated in upcoming releases. To prevent any data loss, you should migrate any old reports to the new reports (Information > Reports). For more information, contact ScienceLogic Support.

Most Recent Release: 20251022

- Improved the Skylar Compliance Support Server to enhance operational security and communication with appliances.
- Renamed the ***ObjectName*** field to ***DeviceName*** on the *Configuration Changes Summary* report (Report > Add).
- Addressed an issue which prevented backups and command tasks from running and caused the ***Backup Now*** process to hang and display a *Loading* message.(Case: 00556250)
- Addressed an issue that caused a *Disk is Full* error message and prevented users from viewing Device Control outputs. (Case: 00565908)
- Addressed an issue that caused device plug-in fields, including credential fields, to clear when the **Device** page loaded. (Cases: 00562307; 00562318; 00562338)

For more information on Skylar Compliance, see the *Skylar Compliance manual* and the *Skylar Compliance Release Notes*.

Previous Issues Addressed

The following issues were addressed in 20250925

- Addressed an issue that prevented RPM agents from using the back connection after a restart. (Case: 0550709)

The following issues were addressed in 20250924

- Addressed an issue that caused the backup transcript to appear in the *Configure Changes Summary* report in the ***Data Type*** drop-down field (Reports > Add Report). (Case: 00552211)
- Addressed an issue that caused the ***Hostname*** field in the **Auto-Apply** modal (Edit Device > Compliance > Device Policies) to ignore "OR" operations and only respect the "AND" operations. (Case: 00540122)
- Updated the **Device Creation** page (Devices > Add) to utilize user-defined plug-in defaults for device plug-in field values.
- Addressed an issue that prevented appliances from checking and downloading new plug-ins or plug-in changes.

The following issues were addressed in 20250910

- Addressed an issue that prevented multiple devices from updating when they shared the same plug-in but had different protocols. (Case: 00540065)
- Updated the "EnforceMax jobs limit" protocol so that when you run a command against more than 10 devices, the commands are executed asynchronously. Note that the output is not displayed immediately but is available in the **[Output]** tab (Devices > Device Control > Output) and is updated as the commands complete.
- Addressed an issue that caused the ***DomainID*** field to display a zero value when used as a filter parameter on the **Device List** API.

The following issues were addressed in 20250827

- Updated the default ***Regex*** search buffer size to 5% of the available memory on the appliance.
- Addressed an issue that caused the ***Disabled*** check box on the **[Device Details]** tab (Devices > Device List) to scroll through dates erratically when selected, and also addressed an issue that prevented it from being cleared.(Cases: 00525208; 00540046)
- Added the infinite scroll function to Restorepoint templates to prevent the user interface from freezing when users created or edited large templates. (Case: 00521648)
- Addressed an issue that caused a command schedule to trigger all the commands for selected devices at the same time. Addressed another issue in which the retention policy was implemented incorrectly after running multi-device command schedules. (Case: 00528316)
- Migrated the ***Configuration Changes*** report from the old user interface location (Information > Reports > Old UI Reports) into the current user interface (Information > Reports).

The following issues were addressed in 20250813

- Addressed an issue that prevented "Configuration Compliance" reports from generating and exporting as PDF documents. (Case: 00529061)
- Removed unused files from `logrotate` so that it only rotates the logs. (Case: 00538105)
- Decreased the wait time that incurred when users selected all devices in the **Device** table. (Case: 00537054)
- Addressed an issue that prevented users from exporting and restoring legacy backup files.

- Addressed an issue that prevented Device policies (Compliance > Device Policies > Rules)from being able to test multiple runtime command rules when using the **[Test All Rules]** function. (Cases: 00494940; 00524825)

The following issues were addressed in 20250807

- Addressed an issue that caused the Advanced Debug Log to issue an error instead of producing the log.

The following issues were addressed in 20250730

- Addressed an issue that prevented Primary nodes from syncing data during a High Availability failover from Primary to Secondary Master. (Case: 00523718)
- Addressed an issue in the Asset report that caused assets from one device to populate in devices that do not contain those assets. (Case: 00524776)
- Addressed an issue preventing users from adding new device templates due to missing permissions. (Case: 00529067)
- Removed the **[Push]** button that appeared for users lacking the "Push Templates" permissions. (Case: 00529067)
- Added the ***Install Count*** and ***Max Devices Reported*** fields to the administrator server's appliance API.

The following issues were addressed in 20250716

- Addressed an issue that prevented the ***Regex*** search from searching for files in an archive. (Case: 00524071)
- Removed the *Telnet* option from the admin CLI ***Help*** command. (Case: 00524345)
- Addressed an issue that prevented offline users from updating their appliances.
- Updated the ***Log Retention Policy*** on the **[Logs/Alerts]** tab (Administration > System Settings > Logs/Alerts) to also apply to jobs in the database so that they are retained for a longer period of time. You can list or delete the historic jobs through two new endpoints: `GET /jobs/historic` and `DELETE /jobs/historic/{jobid}`.

The following issues were addressed in 20250702

- Restricted Lua device control commands and policy rules if they contain exploitable Lua functions or packages.

The following issues were addressed in 20250618

- Updated the **Create Agent** API spec to include an agent ***Address*** field.
- Updated the **Security** page (Administration > System Settings > Security tab) to include the **SSH Keys** pane so you can upload or generate new appliance SSH keys.
- Addressed an issue that caused an error message to appear when users with limited access opened the **View Device Configuration** page. (Case: 00521451)
- Updated the ***Limit Versions*** field to have a default value of *Last version* on the **Global Search** page (Devices > Global Search) and elsewhere throughout the user interface. In addition, this will be the default value in the API if the ***LimitVersions*** field is omitted.

- Added the following options to the **Request Settings** pane on the **[Security]** tab of the **System Settings** page (Administration > System Settings > Security) to allow you to configure the maximum body size for requests. These new option enhance system security:
    - ***Max body size (in MB)***, which sets the maximum request body size for all requests. The default is 100MB.
    - ***Max file size (in MB)***, which sets the maximum file size for requests that upload files. The default is 10MB.
- Added the following plug-in updates in the Restorepoint user interface:
    - Device details now show default plug-in options if those options appear in the default data for a plug-in.
    - Device configuration types (Devices > Edit/Add Devices > Device Details) that are configured as defaults in the plug-in now appear with a preselected checkbox near the bottom of the **Edit Device** page.
    - The default ***Backup Port*** field on the **[Connection]** tab (Devices > Edit Device > Connection) uses the default port for the plug-in unless it does not exist. If the default port does not exist, you can use the default port value for the protocol, which is shown as a placeholder when the ***Backup Port*** field is empty. (Case: 0051769)
- Updated the **Alerts** settings on the **[Logs/Alerts]** tab so that the ***Email From*** field value is always suffixed with the "no-reply" username to ensure that users can only alter the domain name that Restorepoint will use to send the emails from.

The following issues were addressed in 20250612

- Addressed an issue that prevented users from clearing the ***Disabled*** checkbox on the **[Device Details]** tab on a device. (Cases: 00521008; 00521316)
- Addressed an issue that caused permission errors for all users regardless of permission status when accessing the **Domains** page (Administration > Domains). (Cases: 00512886; 00520015; 00520411; 00520867)

The following issues were addressed in 20250604

- Added a hover-over message on the **[Submit]** button on the **Global Search** page to indicate that it is disabled when you have not entered search criteria or selected devices to search against.
- Replaced the compliance information message when saving a device compliance policy with a new static message on the **Compliance Policies Rule** modal to explain that modifying rules might impact the compliance score.
- Addressed an issue that prevented users from registering agents with pre-defined addresses.
- Updated the **Logs/Alerts** page (System Settings > Logs/Alerts) so that the input for SMTP credentials is visible when the new ***Change Creds*** checkbox is selected.
- Updated the Alert Settings API so that SMTP username and password are not returned.
- Addressed an issue to improve how .csv reports are generated, which significantly reduces memory usage on ***Compliance*** and ***Logs*** reports. (Case: 00495458)

- Implemented the following updates to the public domains API:
    - Created a public read-only API that returns only the ID and name of each domain.
    - Updated the non-public domain API with more strict permissions.
    - Updated the user interface to utilize the new public domains API when you require domain information.

The following issues were addressed in 20250521

- Addressed an issue that prevented device reports from generating if you applied a filter. (Case: 00511414)
- Addressed an issue that prevented archive restoration when a new appliance shared the same serial number. (Case: 00512806)
- Updated the user interface for the **Global Search** page (Devices > Global Search) to include the ***RegEx*** search option and enhance usability.
- Updated the **Global Search** page (Devices > Global Search) with an **[Export]** button that allows you to export your ***RegEx*** search results to a .csv file.
- Modified the **Global Search** API to include the configuration lines that matched a given ***RegEx*** search.
- Updated the ***View Configuration*** pane (Global Search or Devices > Edit Device > Configurations > Configuration) to highlight the results of the newly added ***RegEx*** search. It was also updated to display line numbers and the backup name above the displayed configuration contents, and to improve the ***Wrap*** checkbox styling.

The following issues were addressed in 20250507

- Addressed an issue that caused runtime commands to be sent and received out of order by allowing users to use the `waitprompt` Lua function in the **Device Control**. (Case: 00507947)
- Addressed an issue that prevented agent SSH setting changes from being applied to the agent. (Case: 00484433)
- Addressed an issue that sent blank emails when the *Merge Output* option was selected. (Case: 00503241)
- Updated the ***Device Control Output*** link in the bottom of the email to point to the current Restorepoint user interface. (Case: 00503241)
- Addressed an issue to ensure the ***Manufacturer*** filter on the **Device Search** table filters properly in combination with other filters. (Case: 00495163)
- Added ***DomainID***, ***DomainName***, and ***PluginName*** fields to filter results in the **Global Search** API .
- Updated the Restorepoint user interface to improve speed and efficiency.

> **NOTE:** ScienceLogic recommends that you clear the Restorepoint cache to avoid any issues that might occur after the Restorepoint user interface update.

The following issues were addressed in 20250424

- Updated the checkboxes on the **Password Polices** page so they accurately reflect the values from the Restorepoint API.
- Implemented new API endpoints to allow users to create, update, view, and delete plug-in redaction rules.
- Addressed an issue to ensure that the agent switches to the secondary node when a High Availability failover occurs.
- Renamed the **Device Defaults** page (System Administration > Device Defaults) to **Device** page and updated the ***Group*** card. Added a new ***Plugins*** section that shows a table of plug-ins that shows users the correct permissions to click a plug-in for ***Plugin Options***. The ***Plugin Options*** modal currently only includes the ***Redact Rules*** section where users with the correct permissions can add, edit, or delete a plug-in's redact rules.
- Added an **[Information]** button (ⓘ) to the ***Redact Rules*** modal that pops up to explain the usage of regular expression capture groups for the redactions.
- Updated the **[Configurations]** tab (Devices > Configurations) to fetch file servers only when users have the correct permissions so the "Forbidden" error does not appear at the bottom of the page.
- Added a new permission: `ViewUnredactedBackup` to all users with the `ViewBackup` permission so that users can view unredacted backups.
- Applied the following redaction rules to backups: View Backup, Compare Config, Download Config and View Config on the Global Search.
- Addressed an issue that prevented asset information from being correctly displayed on new devices that were never backed up.

The following issues were addressed in 20250415

- Addressed an issue that prevented users from bulk editing multiple devices.

The following issues were addressed in 20250409

- Updated the global alert definitions so that administrators can specify backup sizes and receive notifications when backups exceed the defined limits.

The following issues were addressed in 20250331

- This release provides significant enhancements to **Domains**, allowing you to limit user access based on domain assignment. Domain support has been added in the release as follows:
    - You can now add a Domain ID to device commands, command schedules, reports, report schedules, and device policies.

      > **NOTE:** If a command is assigned to a command schedule, you cannot delete the command. Likewise, if a report is assigned to a report schedule, you cannot delete the report.

    - You can now add multiple Domain IDs to Commands and Reports.
    - When creating or editing a credential, agent, command, or policy, devices shown in the list are filtered based on the domain to which they belong.
    - If a device command, command schedule, report, report schedule, or device policy is in the global domain, any global domain user with the correct permissions can view or edit it.
    - Users assigned to the global domain with the appropriate permission within the global domain can create or change any element that belongs to more than one domain.
    - **Caveats**:
        - You cannot delete a label, command, policy, agent, or credential that is assigned to a device.
        - You cannot change the domain of a label, command, policy, agent, or credential when it is assigned to a device which shares that domain.
        - You cannot change the domain of a report when it is assigned to a report schedule which shares that domain.
        - If a user does not have access to the same domain as a report, report schedule, command, command schedule, or policy, the form appears disabled.

- Updated permissions in this release are as follows:
    - The following permissions were added to allow for interactions with schedules, such as pausing or postponing schedules, on the **Schedules** page:
        - View All Schedules
        - Modify All Schedules
    - The following permissions replace **View Schedule** and **Modify Schedule**:
        - View Backup Schedule
        - Modify Backup Schedule
    - The following permissions were updated for **Schedule** groups to allow you to assign one or more domains to a report schedule:
        - View Device Report Schedule
        - Modify Device Report Schedule
    - The following permissions were added to control who can view or change Device Control commands:
        - View Device Command
        - Modify Device Command
    - The Command Device permission is enforced only when controlling or sending a command to a device.
    - The following permissions replace **View Rules**, **Modify Rules**, and **Apply Rules**:
        - View Device Policy
        - Modify Device Policy
        - Apply Device Policy
    - Renamed the **Old Report** permissions to **Legacy Permissions** to clarify the permissions interact with the ***Legacy Reports*** that reside in the old user interface.
- You can now filter **Device Control > Schedule** so command schedules are filtered based on the command's device type.
- Updated **Report Schedules** (Reports > Schedules) and **Reports** (Report > Reports) to be filtered by domain.

> **NOTE:** You can see schedules and reports only if you are a member of the same domain, unless you are a global domain user.

The following issues were addressed in 20250312

- Updated the storage protocols for back connection user passwords to ensure that the agent's back connection user password is encrypted and only the encrypted variant is stored in the configuration file.

- Addressed an issue that prevented multi-part archives from fully restoring which resulted in missing backup files.
- Addressed an issue that prevented global administrators from seeing command outputs on domain devices.
- Relocated the *Full transcript* global setting to the **[Notifications & Monitoring]** tab on the **Edit Devices** page as a new checkbox. When you enable the ***Full transcript*** checkbox, transcripts will not be truncated for that device.

The following issues were addressed in 20250311

- Addressed an issue that prevented correct reporting of the agent status.

The following issues were addressed in 20250305

- Addressed an issue that prevented appliance backup restores from correctly restoring any included device backup files.

The following issues were addressed in 20250226

- Updated the storage protocol to store Restorepoint users' passwords as their salted and hashed variants in the database instead of plain text.

The following issues were addressed in 20250213

- Addressed an issue to ensure that Restorepoint uses the latest sqlite version to restore archives.

The following issues were addressed in 20250212

- Addressed an issue that prevented the passphrase input in the ***Auto Export Policy*** form from working.
- Addressed an issue to ensure that when you view all past device configurations, regardless of if the configuration files exists or if there is an issue with just one configuration, the whole page will not issue an error.
- Addressed an issue in which devices that had their ***Location*** column set, but did not have a corresponding location device asset, had the location value migrated to the **Deviceassets** table.
- Updated the **Push Firmware** modal to ensure it displays only the devices with the same plugin as the target firmware.
- Addressed an issue in which the Restorepoint agent did not perform a failover if the primary was up and encrypted.
- Upgraded the sqlite3 version installed on the appliance to provide more advanced features for importing appliance backups from older appliances.

The following issues were addressed in 20250207

- Addressed an issue in which devices with older SSH versions caused backup failures.

The following issues were addressed in 20250203

- Addressed an issue in which the agent crashed after upgrading to agent version 20250129.

The following issues were addressed in 20250129

- Addressed an issue that prevented a backup saved on a CIFS fileserver from being restored on OL8 appliances.

- Addressed an issue to add validation ensuring domains will not be deleted while labels are assigned to that domain.
- Addressed an issue to ensure device policy auto-apply rules list all of the devices' domains and locations.
- Updated the error message to be more informative when clearing the debug log when debugging is active.
- Resolved an issue where the **[Fingerprint]** button displayed an error when you use devices on agents.
- Updated the ***Storage Dashboard*** widget to show the used site in the green section (without index size) and the gray section for index size. Total used space (gray and green) is now displayed as a percentage in the center of the widget.
- Addressed an issue with the Restorepoint agent in which core directories were being removed.
- Addressed an issue that disabled buttons on the **Schedule** page.
- Implemented the "AgentAddress" configuration to allow you to set the IP address that the agent should use to establish SSH connections to master.
- Addressed an issue that allowed two agents with the same IP address to connect to the same configured agent.
- Addressed an issue to ensure the SSH device key cache is able to clear even if there are errors in the *known_hosts* file.
- Addressed an issue to ensure that when you link a compliance rule with a context configuration type, the rule runs against all files generated from that context configuration type.
- Addressed an issue in which the **Device Location** asset was not being updated.
- Addressed an issue in which domain users were unable to disable multiple devices in the **Device List**.
- Addressed a number of edge cases involving SSH key validation handling to ensure SSH access and SSH connections operate on the agent and to allow you to delete SSH device keys that use non-default SSH ports.

The following issues were addressed in 20250115

- Addressed an issue to ensure the public key on the **[Connection]** tab of the **Edit Device** page is correctly displayed and is passed on when a device is updated.
- Addressed an issue in which scrolling on the **Schedule** page to reveal more schedules did not work. Also addressed an issue in which scrolling on the **[Schedules]** tab on the **Device Control** page resulted in an error.
- Addressed an issue regarding testing the scheduled action output policy rule and added additional options to test these rules.
- Addressed an issue in which selecting the **[Enable]** or **[Disable]** buttons on **Allowed SSH Ciphers** (Administration > System Settings> Security > Allowed SSH Ciphers) duplicated the values. Also, updated the multi-select components in the user interface so users can better select multiple elements or deselect current elements (Administration > System Settings > Security > Allowed SSH Ciphers or Devices > Device List > Device > Compliance Tab > Compliance).

- Updated the validation on the devices endpoint to ensure the ***Monitor.AlertFail*** field is only required if `Monitor.Enabled` is set to `TRUE`. In cases, where `Monitor.Enabled` is set to `FALSE`, the ***Montior.AlertFail*** field is not required and set to the default value of 2.
- Addressed an issue regarding the Restorepoint FTP server and anonymous accounts and added an option to disable anonymous authentication on non-RPM agents. You can access this option by going to the VM Agent CLI > Advanced > Disable Anonymous FTP login or by configuring the Docker agent environment file.
- Addressed an issue regarding the device select component to ensure the application loads correctly when you select the ***Select All*** checkbox and the filter parameters change.
- Addressed a template configuration (Edit Device > Configuration) issue to disable the listed configurations if their file type is unsupported for templating (i.e. archive files and binary). A tool tip appears if you hover over disabled configurations indicating why they are disabled.
- Addressed an issue to ensure you can generate **Asset** reports if the asset fields referenced begin with a lowercase letter.
- Addressed an issue in which the same device appeared multiple times in the device listing.
- Addressed an issue with a runtime error on the Restorepoint agent causing it to restart which potentially prevented it from connecting to the secondary node on failover.

The following issues were addressed in 20250102

- Addressed an issue in which users were unable to select any option other than the debug options on the **Edit Agent**>**Details** page because the device selection checkboxes were caught in an automated shifting pattern between "select" and "deselect".
- Addressed an issue to ensure that when a user is deleted, the API tokens associated with that user are also deleted and the API validation returns an accurate error message to alert the user of the issue.
- Addressed an issue which resulted in an error message when users tried to postpone report schedules.
- Addressed an issue in which missing permission checks allowed unauthorized users to view and change data for which they were not authorized.
- Added a loading state to the Restorepoint user interface so users see progress when loading a template.
- Addressed an issue so that domain users executing a global search can view any device based on a user's domain visibility.
- Addressed an issue that prevented the device host key from clearing the file entry when the device address was a hostname instead of an IP address.
- Addressed an issue in which the ***Device Type*** on the **Edit/Add Rule** page of the **[Device Policy]** tab was grayed out and unavailable for users to change when creating a command from a runtime policy.
- Addressed an issue in which the **[Test Proxy]** button (Administration > System Settings > Network > Network Access) did not return an error message for a failed test. Updated the ***Test Proxy*** field to include the following entries: Hostname, IPv4, and IPv6 validations.
- Addressed an issue in which users without PushSoftware permissions were able to push firmware onto devices on which they did not have permissions.

Installing or Upgrading Skylar Compliance

For detailed steps about installing or upgrading to this version of Skylar Compliance (formerly Restorepoint), see the *Installing Skylar Compliance* chapter in the ***Skylar Compliance*** manual.

IMPORTANT: You should always upgrade to the most recent release of Skylar Compliance.