Overview

These release notes document the most recent Restorepoint 5.6 version maintenance release, followed by previous maintenance release notes, sorted by release date.

This document covers the following topics:

Restorepoint Notices:

- 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: 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.

TIP: To view release notes and manuals for all major versions of Restorepoint, see *Restorepoint Documentation*.

Previous Issues Addressed

The following issues were addressed in 202500312

- 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 202500311

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

The following issues were addressed in 202500305

- 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 Restorepoint

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

> IMPORTANT: You should always upgrade to the most recent release of Restorepoint.