



Restorepoint Integrations

Restorepoint PowerPack Version 103

Restorepoint Synchronization PowerPack Version 1.4.0

Restorepoint Automation PowerPack Version 102

Table of Contents

Introduction	3
Restorepoint Integrations	4
Introduction to the Restorepoint Synchronization PowerPack	5
Prerequisites for this Synchronization PowerPack	6
PowerFlow Applications Included in the Synchronization PowerPack	6
PowerFlow Applications	6
Configuration Object	7
Steps	7
Installing the Synchronization PowerPack	8
Downloading the Synchronization PowerPack	8
Importing the Synchronization PowerPack	8
Installing the Synchronization PowerPack	9
Installing and Configuring the Restorepoint PowerPack	10
Installing the PowerPack	10
Downloading and Compiling the Restorepoint MIB Files	10
Configuring Applications for the Restorepoint Synchronization PowerPack	12
Overview of Onboarding SL1 Devices to Restorepoint	13
Creating an SSH Credential in SL1 for Devices	14
Creating a Configuration Object in PowerFlow	15
Configuring the Restorepoint Applications in PowerFlow	18
Configuring the Restorepoint Applications	18
Configuring the "Restorepoint: Get the List of Logs from Restorepoint" Application	20
Discovering a Device in SL1 and Running the Sync Devices Application	21
Scheduling Applications	22
Introduction to the Restorepoint Automation PowerPack	26
What is the Restorepoint Automation PowerPack?	27
Installing the Restorepoint Automation PowerPack	27
Configuring Device Credentials	29
Creating a Credential	30
Aligning a Restorepoint Credential to the Restorepoint Automation Actions	31
Restorepoint Automation Policies	33
Standard Automation Policies	34
Creating and Customizing Automation Policies	37
Prerequisites	38
Creating an Automation Policy	38
Example Automation Configuration	41
Customizing an Automation Policy	42
Removing an Automation Policy from a PowerPack	44
Customizing Restorepoint Action Policies	45
Creating a Custom Action Policy	46
Customizing Automation Actions	47
Creating a New Restorepoint Automation Action	49

Chapter

1

Introduction

Overview

This manual describes how to use the *Restorepoint Synchronization PowerPack* to automatically add SL1 devices to Restorepoint when those devices are discovered in SL1 and collect backup events from Restorepoint. This manual also describes how to use the automation policies, automation actions, and custom action types found in the *Restorepoint Automation PowerPack*.

These PowerPacks require a subscription to one of the following solutions:

- SL1 Advanced or Premium solutions included in the 2020 pricing model
- SL1 Standard or Premium solutions in the Change and Configuration workflow automation option included in the 2022 pricing model

This manual covers the following topics:

Restorepoint Integrations

This manual describes content from the following PowerPack and Synchronization PowerPack versions:

- Restorepoint Synchronization PowerPack, version 1.3.0
- Restorepoint Automation PowerPack, version 102

Chapter

2

Introduction to the Restorepoint Synchronization PowerPack

Overview

This chapter describes how you can use the *Restorepoint Synchronization PowerPack* to automatically add SL1 devices to Restorepoint when those devices are discovered in SL1 and collect backup events from Restorepoint. The integration is unidirectional, from SL1 to Restorepoint.

This PowerPack requires a subscription to one of the following solutions:

- SL1 Advanced or Premium solutions included in the 2020 pricing model
- SL1 Standard or Premium solutions in the Change and Configuration workflow automation option included in the 2022 pricing model

NOTE: This version of the Synchronization PowerPack has been tested to sync up to 1,000 new devices at a time.

NOTE: After the 2.1.0 platform release, the *Integration Service* was rebranded as *SL1 PowerFlow*, and the *Automation Builder* was rebranded as *SL1 PowerFlow builder*.

NOTE: The label "SyncPack" is used in place of "Synchronization PowerPack" in the PowerFlow user interface.

For more information about integrating SL1 with Restorepoint, watch the [video](#).

This manual covers the following topics:

Prerequisites for this Synchronization PowerPack

The following table lists the port access required by PowerFlow and this Synchronization PowerPack:

Source IP	PowerFlow Destination	PowerFlow Source Port	Destination Port	Requirement
PowerFlow	SL1 API	Any	TCP 443	SL1 API Access
PowerFlow	Restorepoint API	Any	TCP 443	Restorepoint API Access
PowerFlow	SL1 Database	Any	TCP 7706	SL1 Database Access

PowerFlow Applications Included in the Synchronization PowerPack

This section lists the contents of the *Restorepoint* Synchronization PowerPack.

PowerFlow Applications

- **Restorepoint: Change detection for backed up devices.** This application queries the Restorepoint API to determine whether there was a change between the last two backups.
- **Restorepoint: Get List of Credentials from SL1.** This application queries SL1 for existing credentials and matches them against credentials in Restorepoint. If there is a change to the credential in SL1 and the credential exists in Restorepoint, the credential is updated with the new information.
- **Restorepoint: Get the List of Logs from Restorepoint.** This application queries the Restorepoint API to collect backup success and failure logs from Restorepoint to generate events in SL1.
- **Restorepoint: Onboard Device.** This application adds new devices and the associated elements to Restorepoint, including the domain and credential. The application gets details about how the device will be configured in Restorepoint, including the assigned agent and device type, from a mapping in the aligned configuration object.
- **Restorepoint: Sync Devices.** This application creates the Restorepoint custom attribute for the device and gets devices in the "Restorepoint" device group in SL1 and syncs them to Restorepoint by triggering the "Restorepoint: Onboard Device" application.
- **Restorepoint: Update Event info in SL1.** This application populates SL1 events with log and backup information that is collected from Restorepoint.

For more information about how to configure these applications, see [Configuring the Restorepoint Applications](#).

Configuration Object

- **Restorepoint Base Config.** This configuration object can be used as a template after the Synchronization PowerPack is installed on the PowerFlow system. The configuration object includes the following:
 - Details for connecting to the SL1 API, including the URL, username, and password.
 - Details for connecting to the Restorepoint API, including the URL, username, and password.
 - Details for connecting to the SL1 database, including the URL, username, and password.
 - A mapping between SL1 Device Class GUIDs and Restorepoint device types.
 - A default value for Restorepoint device types.
 - Mapping between SL1 collector appliance IDs and Restorepoint agents.
 - A default backup schedule for all new devices added to Restorepoint.
 - An option to add a custom link configuration to SL1, a user access URL, a timestamp, and the option to allow device change detection.

Steps

The following steps are included in this Synchronization PowerPack:

- Create Restorepoint Credential
- Restorepoint: Create Device
- Create Restorepoint Domain
- Determine the change in Restorepoint Logs
- Get backup data from RP
- Insert data in SL1 database
- Get device id from SL1
- Get Devices from SL1
- Transfer Data
- Select Device ID from SL1
- Get Logs from Restorepoint and save in PF cache
- Optional QueryGQL Call RP
- Select Custom Link
- Select devices from SL1
- Update Device Event Info
- Filter List of Credentials
- Get List of Basic/Snippet Credentials from SL1
- Get List of Credentials from Restorepoint

- Get List of SSH Credentials from SL1
- Save Edit Date to Cache

Installing the Synchronization PowerPack

A Synchronization PowerPack file has the **.whl** file extension type. You can download the Synchronization PowerPack file from the ScienceLogic Support site.

WARNING: If you are *upgrading* to this version of the Synchronization PowerPack from a previous version, make a note of any settings you made on the **Configuration** pane of the various integration applications in this Synchronization PowerPack, as these settings are *not* retained when you upgrade.

Downloading the Synchronization PowerPack

To locate and download the Synchronization PowerPack:

1. Go to the ScienceLogic Support Site at <https://support.sciencelogic.com/s/>.
2. Click the **[Product Downloads]** tab and select *PowerPack*.
3. In the **Search PowerPacks** field, search for the Synchronization PowerPack and select it from the search results. The **Release Version** page appears.
4. On the **[PowerPack Versions]** tab, click the name of the Synchronization PowerPack version that you want to install. The **Release File Details** page appears.
5. Click the **[Download File]** button or click the name of the **.zip** file containing the **.whl** file for this Synchronization PowerPack to start downloading the file.

After you download a Synchronization PowerPack, you can import it to your PowerFlow system using the PowerFlow user interface.

NOTE: If you are installing or upgrading to the latest version of this Synchronization PowerPack in an offline deployment, see "Installing or Upgrading in an Offline Environment" in the Synchronization PowerPack release notes to ensure you install any external dependencies.

Importing the Synchronization PowerPack

To import a Synchronization PowerPack in the PowerFlow user interface:

1. On the **SyncPacks** page of the PowerFlow user interface, click **[Import SyncPack]**. The **Import SyncPack** page appears.

2. Click **[Browse]** and select the **.whl** file for the Synchronization PowerPack you want to install.

TIP: You can also drag and drop a **.whl** file to the **Import SyncPack** page.

3. Click **[Import]**. PowerFlow registers and uploads the Synchronization PowerPack. The Synchronization PowerPack is added to the **SyncPacks** page.

NOTE: You cannot edit the content package in a Synchronization PowerPack published by ScienceLogic. You must make a copy of a ScienceLogic Synchronization PowerPack and save your changes to the new Synchronization PowerPack to prevent overwriting any information in the original Synchronization PowerPack when upgrading.

Installing the Synchronization PowerPack

To activate and install a Synchronization PowerPack in the PowerFlow user interface:

1. On the **SyncPacks** page of the PowerFlow user interface, click the **[Actions]** button () for the Synchronization PowerPack you want to install and select *Activate & Install*. The **Activate & Install SyncPack** modal appears.

NOTE: If you try to activate and install a Synchronization PowerPack that is already activated and installed, you can choose to "force" installation across all the nodes in the PowerFlow system.

TIP: If you do not see the PowerPack that you want to install, click the Filter icon () on the **SyncPacks** page and select *Toggle Inactive SyncPacks* to see a list of the imported PowerPacks.

2. Click **[Yes]** to confirm the activation and installation. When the Synchronization PowerPack is activated, the **SyncPacks** page displays a green check mark icon () for that Synchronization PowerPack. If the activation or installation failed, then a red exclamation mark icon () appears.
3. For more information about the activation and installation process, click the check mark icon () or the exclamation mark icon () in the **Activated** column for that Synchronization PowerPack. For a successful installation, the "Activate & Install SyncPack" application appears, and you can view the Step Log for the steps. For a failed installation, the **Error Logs** window appears.
4. If you have other versions of the same Synchronization PowerPack on your PowerFlow system, you can click the **[Actions]** button () for that Synchronization PowerPack and select *Change active version* to activate a different version other than the version that is currently running.

Installing and Configuring the Restorepoint PowerPack

The following topics describe how to install and configure the *Restorepoint* PowerPack and the *Restorepoint* Synchronization PowerPack.

Installing the PowerPack

The *Restorepoint* PowerPack includes the following tools, which you will use with the *Restorepoint* Synchronization PowerPack:

- The "Restorepoint Connectivity" Dynamic Application, which tests SSH connectivity and indicates devices to be onboarded in Restorepoint.
- Event Policies for Restorepoint.
- A Device Class for Restorepoint devices.
- A Device Group called "Restorepoint Devices", which includes a dynamic rule that matches devices with aligned Dynamic Applications, including the "Restorepoint Connectivity" Dynamic Application.
- The Restorepoint MIB is available in your Restorepoint system. The MIB must be loaded before you can use the PowerPack. For more information, see [Downloading and Compiling the Restorepoint MIB Files](#).

To install the *Restorepoint* PowerPack:

1. Download the latest version of the PowerPack from [the ScienceLogic Support Site](#) to a local computer.
2. In SL1, log in and go to the **PowerPack Manager** page (System > Manage > PowerPacks).
3. Click **[Actions]** and select *Import PowerPack*.
4. Click **[Browse]** and navigate to the PowerPack file from step 1.
5. Select the PowerPack file and click **[Import]**. The **PowerPack Installer** modal page displays a list of the PowerPack contents.
6. Click **[Install]**. After the installation is complete, the PowerPack appears on the **PowerPack Manager** page.

Downloading and Compiling the Restorepoint MIB Files

After installing the *Restorepoint* PowerPack, you will need to download the following MIB files from Restorepoint and compile the MIB files in SL1:

- **RESTOREPOINT-APPLIANCE-MIB.txt**
- **RESTOREPOINT-MIB.txt**

You can access the Restorepoint MIB files from your Restorepoint system.

To download the MIB files in Restorepoint:

1. In your Restorepoint system, go to the **Systems Settings** page (Administration > System Settings).
2. Click the **[SNMP]** tab and navigate to the **Download MIBs** field.

3. Click both of the MIB file names to download them to your local drive.

To compile the Restorepoint MIB files in SL1:

1. Go to the **MIB Compiler** page (System > Tools > MIB Compiler) and click the **[Import]** button.
2. In the **MIB Import** modal page, navigate to the location of the MIB file on your local computer and click the **[Import]** button. The new MIB file appears in the list of MIB files in the **MIB Compiler** page.
3. Repeat steps 1-2 to upload the second MIB file.
4. You must compile both MIB files before SL1 can use them. To compile a MIB, click its lightning bolt icon ().
5. To enable Restorepoint to send trap events to SL1, go to **Administration > System Settings > Logs/Alerts** in the Restorepoint user interface and change the following:
 - **SNMP Traps**: Check this checkbox.
 - **SNMP Server**: Enter the IP address of the SL1 All-In-One or Data Collector.

Chapter

3

Configuring Applications for the Restorepoint Synchronization PowerPack

Overview

This chapter describes how to set up the PowerFlow applications for the *Restorepoint Synchronization PowerPack*.

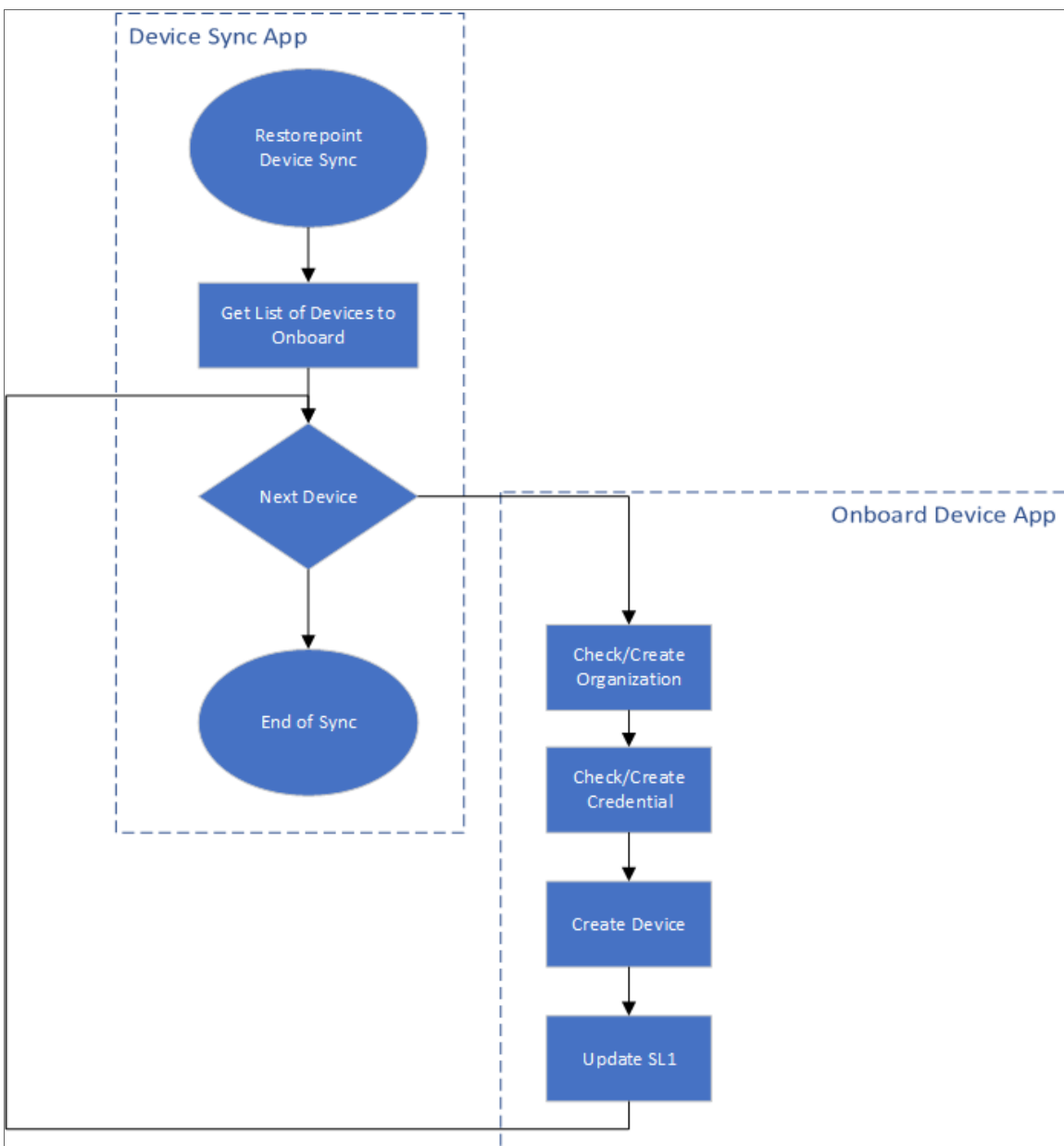
This chapter covers the following topics:

<i>Overview of Onboarding SL1 Devices to Restorepoint</i>	13
<i>Creating an SSH Credential in SL1 for Devices</i>	14
<i>Creating a Configuration Object in PowerFlow</i>	15
<i>Configuring the Restorepoint Applications in PowerFlow</i>	18
<i>Discovering a Device in SL1 and Running the Sync Devices Application</i>	21
<i>Scheduling Applications</i>	22

Overview of Onboarding SL1 Devices to Restorepoint

You can configure the *Restorepoint* Synchronization PowerPack to automatically add SL1 devices to Restorepoint when those devices are discovered in SL1. The integration is unidirectional, from SL1 to Restorepoint.

The following workflow describes the process for adding SL1 devices to Restorepoint:



See the following topics for detailed steps that cover how to configure settings in SL1 and PowerFlow before you can enable these applications and more.

Creating an SSH Credential in SL1 for Devices

In SL1, create an SSH credential for the devices that you want to discover and add to Restorepoint. SL1 uses this credential to automatically align the "Restorepoint Connectivity" Dynamic Application, which is used when you discover a device and add it to Restorepoint.

NOTE: If needed, create a new organization in SL1 for the device you want to discover. For more information, see the *Creating and Editing Organizations* chapter in the **Organizations and Users** manual.

To create an SSH/Key credential:

1. Go to the **Credentials** page (Manage > Credentials or System > Manage > Credentials in the classic user interface).
2. Click the **[Create New]** button and then select *Create SSH/Key Credential*. The **Edit Credential** modal page appears.
3. Supply values in the following fields:
 - **Name.** Name of the credential. Can be any combination of alphanumeric characters.
 - **All Organizations.** Toggle on (blue) to align the credential to all organizations, or toggle off (gray) and then select one or more specific organizations from the **What organization manages this service?** drop-down field to align the credential with those specific organizations.
 - **Timeout (ms).** Time, in milliseconds, after which SL1 will stop trying to communicate with the device from which you want to retrieve data. The default is 1500.
 - **Hostname/IP.** Hostname or IP address of the device you want to discover.
 - You can include the variable **%D** in this field. SL1 will replace the variable with the IP address of the current device (device that is currently using the credential).
 - You can include the variable **%N** in this field. SL1 will replace the variable with hostname of the current device (device that is currently using the credential). If SL1 cannot determine the hostname, SL1 will replace the variable with the primary, management IP address for the current device.
 - **Port.** Port number associated with the data you want to retrieve. The default TCP port for SSH servers is 22.

NOTE: The protocol attribute of your device in Restorepoint is set based on the port specified in this credential. If the port is 23, the attribute is set to telnet/tftp. For all other ports, the attribute is set to ssh/tftp.

- **Username.** Username for an SSH or user account on the device to be monitored.
- **Password.** Password for an SSH or user account on the device to be monitored.

- **Private Key (PEM Format)**. Enter the SSH private key that you want SL1 to use, in PEM format.

4. Click **[Save]**.

Creating a Configuration Object in PowerFlow

For this Synchronization PowerPack, you can make a copy of the "Restorepoint Base Config" configuration object, which is the sample configuration file that was installed with the *Restorepoint Synchronization PowerPack*.

TIP: The "Base Config" configuration object contains all of the required variables. Simply update the variables from that object to match your SL1 and Restorepoint settings.

To create a configuration object based on the "Restorepoint Base Config" configuration object:

1. In the PowerFlow user interface, go to the **Configurations** page (⚙️).
2. Click the **[Actions]** button (⋮) for the "Restorepoint Base Config" configuration object and select *Edit*.

The **Configuration** pane appears:

The screenshot shows the 'Configurations' page in the PowerFlow user interface. The 'Restorepoint Base Config' configuration object is selected and its details are displayed in a modal window. The configuration includes the following fields:

Name	Value	Encrypted
sl1_url	https://<HOST_URL>	☐
sl1_user	<SL1_USER>	☐
sl1_password	sZs//MYb0boqIP+P46uk4jS7ysx	☒
sl1_db_host	<SL1_DB_HOST>	☐
sl1_db_user	<SL1_DB_USER>	☐
sl1_db_password	FZzLGx3b1E6ElFwxzAKYeyrxa/	☒
restorepoint_url	https://<DOMAIN-URL>	☐

The modal window also includes a 'Description' field with the text 'Base config for Restorepoint syncpack', a 'Version' field with the value '1.0.0', and a 'Toggle JSON Editor' button. At the bottom right, there are 'Copy as' and 'Save' buttons.

3. Click **[Copy as]**. The **Create Configuration** pane appears.
4. Complete the following fields:
 - **Friendly Name**. Name of the configuration object that will display on the **Configurations** page.
 - **Description**. A brief description of the configuration object.
 - **Author**. User or organization that created the configuration object.
 - **Version**. Version of the configuration object.
5. In the **Configuration Data** field, update the default variable definitions to match your PowerFlow configuration:
 - **sl1_url**. Type the URL for your associated SL1 system.
 - **sl1_user**. Type the username for your SL1 system.
 - **sl1_password**. Type the password for your SL1 system.
 - **sl1_db_host**. Type the URL for your associated SL1 database.
 - **sl1_db_user**. Type the username for your SL1 database.
 - **sl1_db_password**. Type the password for your SL1 database.
 - **restorepoint_url**. Type the URL for your associated Restorepoint system.
 - **restorepoint_user**. Type the username for your Restorepoint system.
 - **restorepoint_password**. Type the password for your Restorepoint system.
 - **default_restorepoint_device_type**. Type the default device type for your Restorepoint system.
 - **default_backup_interval**. Type the default time for the Backup Interval for your Restorepoint device.

NOTE: The value for the `default_backup_interval` field uses the following format: `second minute hour ****@0@@0@0`.

- **create_custom_link**. Type a value to create an optional custom link from SL1 to Restorepoint.

NOTE: If you are running SL1 platform version 10.2.0 or later and have custom links enabled, you can set the value to `1` to automatically add the custom link definition for Restorepoint. The default value is `False/0`.

- **restorepoint_ui_url**. Type an optional user access URL that is different than the Restorepoint URL that is used to integrate with PowerFlow.
- **restorepoint_config**. Type `Enable` or `Disable` to allow device change detection.

NOTE: The **restorepoint_config** feature requires SL1 platform version 11.2.0 or later. If you are using an earlier version of SL1, this field should always be set to its default value: *Disable*.

- **timestamp.** The "Restorepoint: Get List of Credentials" application queries SL1 for updated credentials and stores the last time that SL1 was queried. Type a value that specifies the number of hours for the application to query SL1 for updated credentials, if no previous time stamp is available (e.g. the first execution of the application). The application will update the credentials in Restorepoint that have been updated in SL1 within the specified number of hours.
 - **default_monitoring_monitor_device.** Type *True* or *False* to enable or disable device monitoring. The default value is *True*.
 - **default_monitoring_fail_after.** Type how many failed attempts to onboard a device before PowerFlow will stop attempting to discover the device.
 - **default_monitoring_is_ping_type.** Type *True* or *False* to enable or disable ICMP ping rather than TCP connection. The default value is *True*.
 - **default_monitoring_email_when_down.** Type *True* or *False* to enable or disable sending an email when the device is down. The default value is *False*.
 - **default_monitoring_email_when_up.** Type *True* or *False* to enable or disable sending an email when the device is back up. The default value is *True*.
6. The other optional values in the Configuration Data field require JSON code to edit their values. Click **[Toggle JSON Editor]** to show the JSON code.
 7. In the **Configuration Data** field, be sure to include the required block of code to ensure that the applications aligned to this configuration object do not fail:

```
{
  "encrypted": false,
  "name": "s11_db_host",
  "value": "${config.s11_host}"
}
```

For example:

```
{
  "encrypted": false,
  "name": "s11_db_host",
  "value": "10.2.11.42"
}
```

8. To create a configuration variable, define the following keys:
 - **encrypted.** Specifies whether the value will appear in plain text or encrypted in the JSON file. If you set this to "true", when the value is uploaded, PowerFlow encrypts the value of the variable. The plain text value cannot be retrieved again by an end user. The encryption key is unique to each PowerFlow system. The value is followed by a comma.
 - **name.** Specifies the name of the configuration file, without the JSON suffix. This value appears in the user interface. The value is surrounded by double-quotes and followed by a comma.

- **value**. Specifies the value to assign to the variable. The value is surrounded by double-quotes and followed by a comma.

9. Click **[Save]**. You can now align this configuration object with one or more applications.

Configuring the Restorepoint Applications in PowerFlow

You can use this Synchronization PowerPack to automatically add an SL1 device, along with associated credential and organization details, to Restorepoint. You can also use this Synchronization PowerPack to automatically collect backup events from Restorepoint. You will need to align the Restorepoint applications with the relevant configuration object in PowerFlow, and, if needed, update any other fields on the **Configuration** pane for the applications.

To run this Synchronization PowerPack, you must "align" the configuration object to run with the following PowerFlow applications:

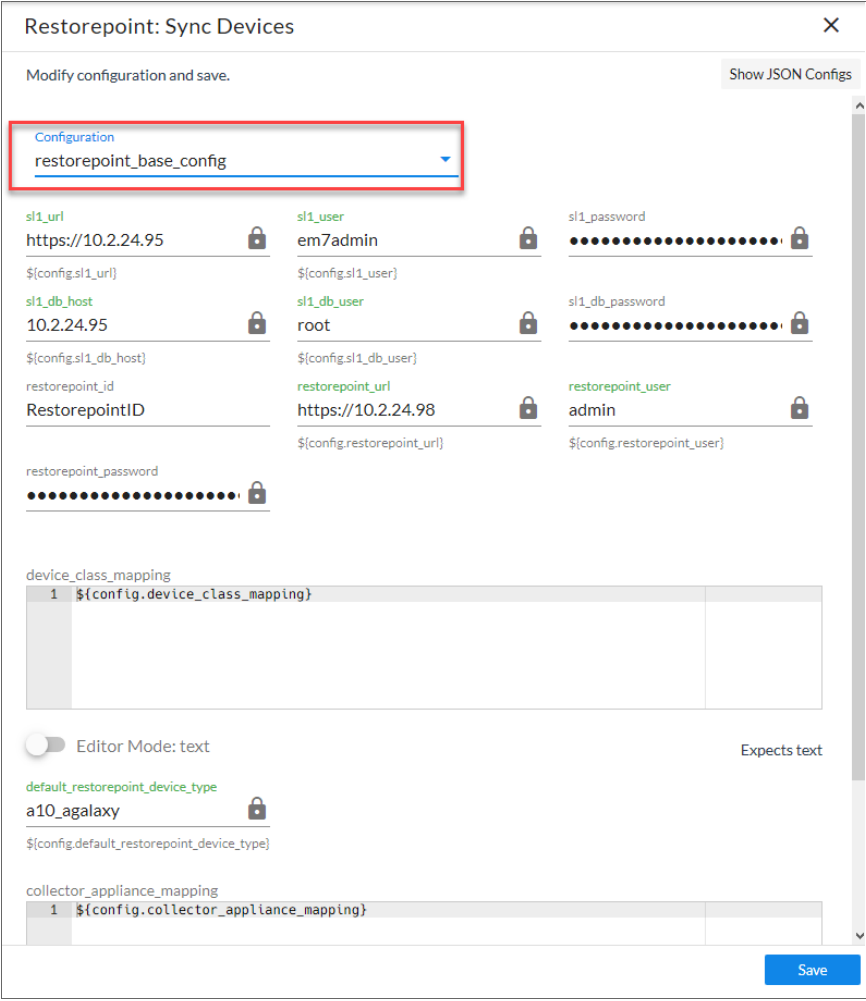
- "Restorepoint: Change detection for backed up devices"
- "Restorepoint: Get List of Credentials from SL1"
- "Restorepoint: Get the List of Logs from Restorepoint"
- "Restorepoint: Onboard Device"
- "Restorepoint: Sync Devices"
- "Restorepoint: Update Event info in SL1"

Configuring the Restorepoint Applications

To configure the applications in the PowerFlow user interface:

1. In the PowerFlow user interface, go to the **Applications** page and select the application you want to configure.

- Click the **[Configuration]** button . The **Configuration** pane appears:



Restorepoint: Sync Devices

Modify configuration and save. Show JSON Configs

Configuration
restorepoint_base_config

sl1_url
https://10.2.24.95

sl1_user
em7admin

sl1_password
.....

sl1_db_host
10.2.24.95

sl1_db_user
root

sl1_db_password
.....

restorepoint_id
RestorepointID

restorepoint_url
https://10.2.24.98

restorepoint_user
admin

restorepoint_password
.....

device_class_mapping

1	\$(config.device_class_mapping)

Editor Mode: text Expects text

default_restorepoint_device_type
a10_agalaxy

collector_appliance_mapping

1	\$(config.collector_appliance_mapping)

Save

- In the **Configuration** drop-down, select *the configuration object you created earlier*. The fields with a padlock icon () are updated with values from the configuration object.
- Update any of the other fields that do not have a padlock icon, and then click **[Save]**.

TIP: You should schedule the "Get List of Credentials from SL1", "Sync Devices", and "Update SL1 Event Info" applications to run on a regular basis. This will ensure that credentials are updated, new SL1 devices are added to Restorepoint, and SL1 events are updated automatically. For more information, see [Scheduling Applications](#).

- Click **[Save]**.

Configuring the "Restorepoint: Get the List of Logs from Restorepoint" Application

To align the configuration object with the relevant PowerFlow applications:

1. In the PowerFlow user interface, go to the **Applications** page and select the "Restorepoint: Get the List of Logs from Restorepoint" application.
2. Click the **[Configuration]** button (⚙️). The **Configuration** pane appears:

Restorepoint: Get The List Of Logs From Restorepoint

Modify configuration and save. [Show JSON Configs](#)

Configuration
restorepoint_base_config

sl1_url
https://<HOST_URL>

sl1_user
<SL1_USER>

sl1_password
.....

sl1_db_host
<SL1_DB_HOST>

sl1_db_user
<SL1_DB_USER>

sl1_db_password
.....

restorepoint_url
https://<DOMAIN-URL>

restorepoint_user
<RESTOREPOINT_USER>

restorepoint_password
.....

sl1_read_timeout
20

restorepoint_config
☒ Enable
☐ Disable

Save

3. In the **Configuration** drop-down, select *the configuration object you created earlier*. The fields with a padlock icon (🔒) are updated with values from the configuration object.
4. In the **restorepoint_config** field, select *Enable* or *Disable* to allow device change detection. You should select the same value you entered in the selected configuration object.

NOTE: The `restorepoint_config` feature requires SL1 platform version 11.2.0 or later. If you are using an earlier version of SL1, this field should always be set to its default value: *Disable*.

5. Click **[Save]**.

TIP: You should schedule the "Get the List of Logs from Restorepoint" application to run on a regular basis to ensure that backup events are collected automatically. For more information, see [Scheduling Applications](#).

Discovering a Device in SL1 and Running the Sync Devices Application

The next time you discover a device in SL1 and run the "Restorepoint: Sync Devices" application, any devices you discovered in SL1 that are aligned with the "Restorepoint Connectivity" Dynamic Application get added to Restorepoint. Those devices are also part of the Restorepoint Device Group.

If you include the SSH or telnet credential you created earlier in a discovery session, the "Restorepoint Connectivity" Dynamic Application is automatically aligned. Optionally, you can manually align the Dynamic Application with your devices using the credential. Based on the Dynamic Application alignment, the device is also automatically included in a Restorepoint Device Group. For more information about discovering a device in SL1, see the **Discovery and Credentials** manual.

To run the "Restorepoint: Sync Devices" application:

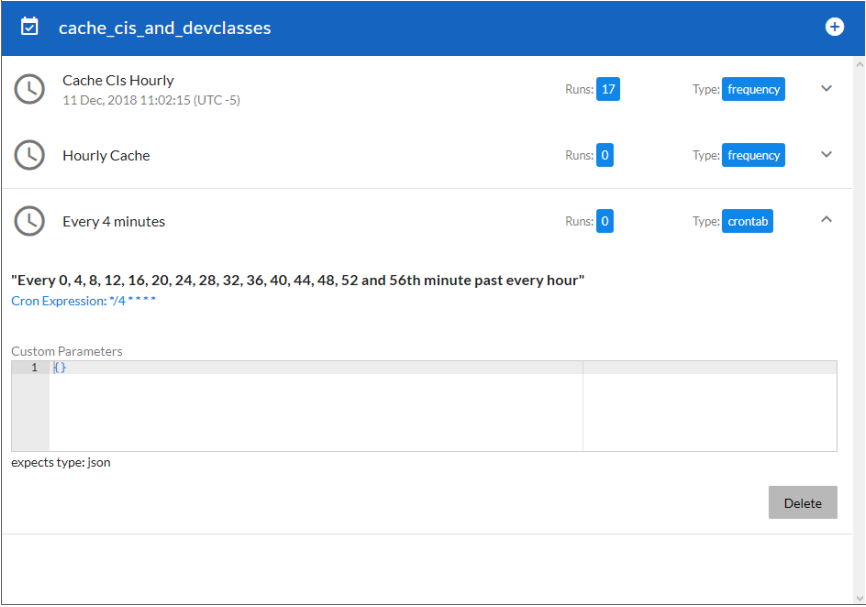
1. Go to the **Applications** page and select the "Restorepoint: Sync Devices" application.
2. Click the **[Run]** button (). The following actions occur:
 - If the SL1 organization exists as a domain in Restorepoint, the device is added to that domain. Otherwise, a new domain is created in Restorepoint that maps to the SL1 organization.
 - If needed, a new credential is created in Restorepoint that maps to the new SL1 credential.
 - A new device is added in Restorepoint that maps to the new device in SL1 :
 - The device is associated with the appropriate domain and credential.
 - The device is associated with an agent that maps to the SL1 Data Collector monitoring that device, using a pre-defined mapping from the "Restorepoint Base Config" configuration object.
 - The device is configured with a plugin that maps to the SL1 Device Class for that device, using a pre-defined mapping from the "Restorepoint Base Config" configuration object.

Scheduling Applications

You can create one or more schedules for a single application in the PowerFlow user interface. When creating each schedule, you can specify the queue and the configuration file for that application.

To schedule an application:

1. On the **Applications** page () , click the **[Schedule]** button for the application you want to schedule. The **Schedule** window appears, displaying any existing schedules for that application:



cache_cis_and_devclasses	
 Cache CIs Hourly 11 Dec, 2018 11:02:15 (UTC -5)	Runs: 17 Type: frequency
 Hourly Cache	Runs: 0 Type: frequency
 Every 4 minutes	Runs: 0 Type: crontab
"Every 0, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52 and 56th minute past every hour" Cron Expression: <code>*/*4 * * * *</code>	
Custom Parameters	
1 { }	
expects type: json	
<button>Delete</button>	

NOTE: If you set up a schedule using a cron expression, the details of that schedule display in a more readable format in this list. For example, if you set up a cron expression of `*/*4 * * * *`, the schedule on this window includes the cron expression along with an explanation of that expression: "Every 0, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, and 56th minute past every hour".

2. Select a schedule from the list to view the details for that schedule.
3. Click the + icon to create a schedule. A blank **Schedule** window appears:

cache_cis_and_devclasses

Schedule Name
Schedule Name

Switch to Cron Expression

Frequency secs

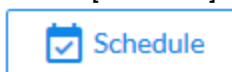
Custom Parameters

1	+	
2		()
3		

expects type: json

Save Schedule

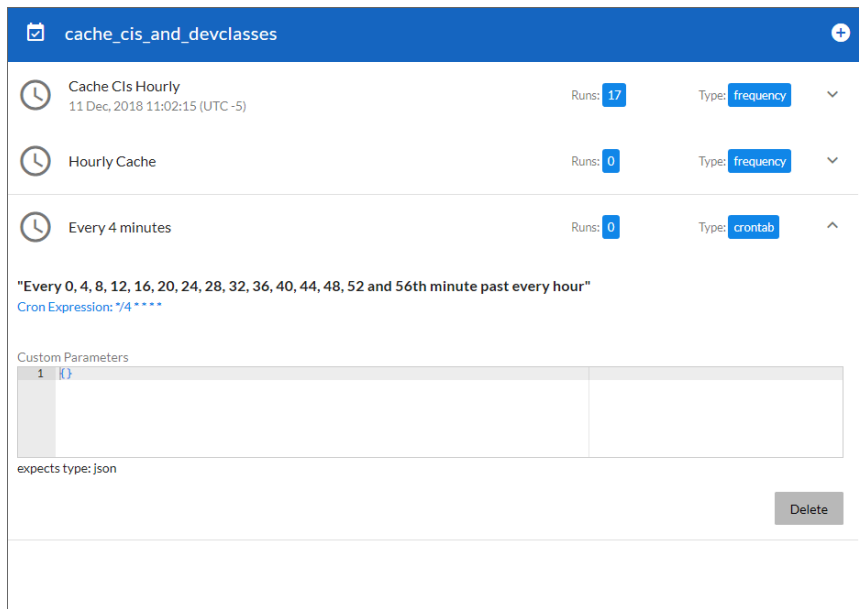
4. In the **Schedule** window, complete the following fields:
 - **Schedule Name.** Type a name for the schedule.
 - **Switch to.** Use this toggle to switch between a cron expression and setting the frequency in seconds.
 - **Cron expression.** Select this option to schedule the application using a cron expression. If you select this option, you can create complicated schedules based on minutes, hours, the day of the month, the month, and the day of the week. As you update the cron expression, the **Schedule** window displays the results of the expression in more readable language, such as *Expression: "Every 0 and 30th minute past every hour on the 1 and 31st of every month", based on */30 * */30 * **.
 - **Frequency in seconds.** Type the number of seconds per interval that you want to run the application.
 - **Custom Parameters.** Type any JSON parameters you want to use for this schedule, such as information about a configuration file or mappings.
5. Click **[Save Schedule]**. The schedule is added to the list of schedules on the initial **Schedule** window. Also, on the **Applications** page, the word "Scheduled" appears in the **Scheduled** column for this application, and the **[Schedule]** button contains a check mark:



NOTE: After you create a schedule, it continues to run until you delete it. Also, you cannot edit an existing schedule, but you can delete it and create a similar schedule if needed.

To view or delete an existing schedule:

1. On the **Applications** page, click the **[Schedule]** button for the application that contains a schedule you want to delete. The **Schedule** window appears.
2. Click the down arrow icon (▼) to view the details of an existing schedule:



3. To delete the selected schedule, click **[Delete]**.

NOTE: When either multiple SL1 stacks or multiple ServiceNow systems are involved with PowerFlow, you should create an individual configuration object for each SL1 stack or ServiceNow system. Next, create an individual schedule for each configuration object. Each schedule should use a configuration object that is specific to that single SL1 stack or ServiceNow system. Creating copies of a PowerFlow application from a Synchronization PowerPack for the purpose of distinguishing between domains is not supported, and will result in issues on upgrades.

The following image shows how you can schedule PowerFlow applications for multiple ServiceNow domains:

device_sync_sciencelogic_to_servicenow

Device Sync Domain A

n/a (UTC -4)

Runs: 63

Type: crontab

^

"02:00 every day"

Cron Expression: 0 2 * * *

Custom Parameters

1 {

2 "configuration": "now_domain_a"

3 }

expects type: json

Delete

Device Sync Domain B

n/a (UTC -4)

Runs: 63

Type: crontab

▼

Device Sync Domain C

May 19, 2021 00:00:00 (UTC -4)

Runs: 63

Type: crontab

▼

Chapter

4

Introduction to the Restorepoint Automation PowerPack

Overview

This chapter describes how to use the Run Book Automation policies, Run Book Action policies, and custom action types found in the *Restorepoint Automation* PowerPack.

This PowerPack requires a subscription to one of the following solutions:

- SL1 Advanced or Premium solutions included in the 2020 pricing model
- SL1 Standard or Premium solutions in the Change and Configuration workflow automation option included in the 2022 pricing model

For more information about integrating SL1 with Restorepoint, watch the video https://www.youtube.com/watch?v=PgXMYstd_g.

This manual covers the following topics:

What is the Restorepoint Automation PowerPack?

The *Restorepoint Automation* PowerPack includes automation policies that:

- Enrich SL1 events for devices managed by Restorepoint (for example, devices that have been synched using the *Restorepoint Synchronization* PowerPack) by automatically running diagnostic commands. The command output is added to the SL1 event log or associated incident.
- Start or revert a backup in Restorepoint and add the command output to the SL1 event log or associated incident.

The Restorepoint Automation actions are executed on the SL1 All-In-One Appliance or Database Server.

In addition to using the standard content, you can use the content in the *Restorepoint Automation* PowerPack to:

- Create your own automation policies that include the pre-defined actions that run different sets of diagnostic commands.
- Use the supplied "Restorepoint: Generic Action type" custom action type to configure your own automation action by supplying a set of commands.

Installing the Restorepoint Automation PowerPack

Before completing the steps in this manual, you must import and install the latest version of the *Restorepoint Automation* PowerPack.

IMPORTANT: You must install the *Datacenter Automation Utilities* PowerPack version 103 before using the Restorepoint Automation PowerPack.

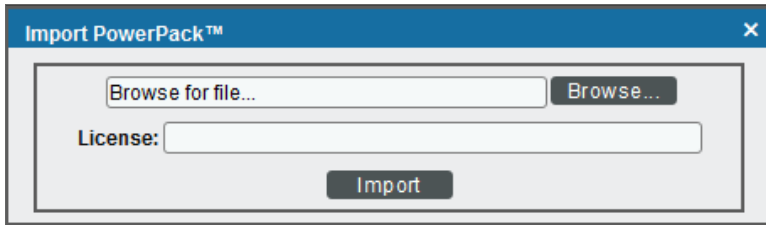
NOTE: The *Restorepoint Automation* PowerPack requires SL1 version 8.14.0 or later. For details on upgrading SL1, see the appropriate SL1 [Release Notes](#).

TIP: By default, installing a new version of a PowerPack overwrites all content from a previous version of 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. (For more information, see the *System Administration* manual.)

To download and install a PowerPack:

1. Download the PowerPack from the ScienceLogic Support Site at <https://support.sciencelogic.com/s/powerpacks>.
2. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).

3. In the **PowerPack Manager** page, click the **[Actions]** button, then select *Import PowerPack*. The **Import PowerPack** dialog box appears:



4. Click the **[Browse]** button and navigate to the PowerPack file.
5. When the **PowerPack Installer** modal appears, click the **[Install]** button to install the PowerPack.

NOTE: If you exit the **PowerPack Installer** modal without installing the imported PowerPack, the imported PowerPack will not appear in the **PowerPack Manager** page. However, the imported PowerPack will appear in the **Imported PowerPacks** modal. This page appears when you click the **[Actions]** menu and select *Install PowerPack*.

Chapter

5

Configuring Device Credentials

Overview

This chapter describes how to configure the credentials required by the automation actions in the *Restorepoint Automation* PowerPack.

This manual covers the following topics:

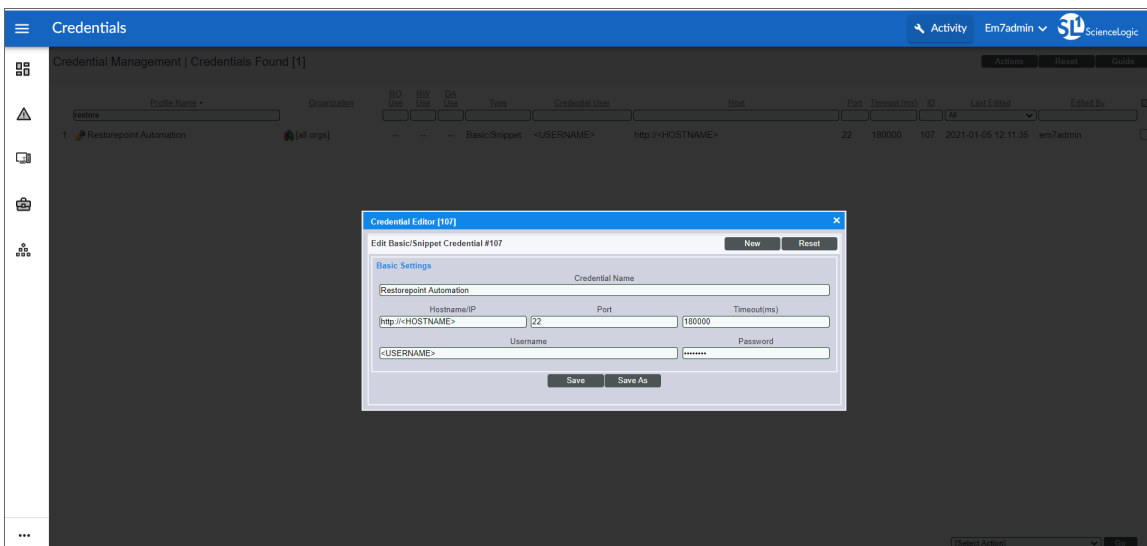
Creating a Credential

To use the automation actions in the PowerPack to collect data from a device, you must create a Restorepoint credential that includes the hostname/IP address, username, and password for your Restorepoint system. The *Restorepoint Automation* PowerPack includes a *Restorepoint Automation* credential template that you can use to create your own credential to communicate with your Restorepoint devices.

NOTE: The *Restorepoint Automation* PowerPack uses one credential for all devices in your Restorepoint system. Once you have created your Restorepoint Automation credential, you will need to modify the automation actions to update the credential ID parameter.

To create a Restorepoint Automation credential:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the *Restorepoint Automation* sample credential and click the wrench icon (). The **Credential Editor** modal page appears:



3. Enter values in the following fields:
 - **Credential Name.** Enter a new name for your Restorepoint credential.
 - **Hostname/IP.** Enter the URL for the Restorepoint device.
 - **Port.** Enter the port number associated with the data you want to retrieve. The TCP port for secure HTTP servers is 443.
 - **Timeout(ms).** Enter a timeout, in milliseconds, for the connection.

- **Username.** Enter the username for a user account on the Restorepoint device to be monitored.
 - **Password.** Enter the password for the user you entered in the **Username** field.
4. Click **[Save As]**.
 5. SL1 assigns the credential an ID number. Take note of the ID number that appears in the Credential Editor heading, as you will need this when [aligning a Restorepoint credential to the Restorepoint automation actions](#).

NOTE: You may also find the credential ID number on the **Credential Management** page under the "ID" column.

For more information about configuring credentials in SL1, see the *Discovery and Credentials* manual.

Aligning a Restorepoint Credential to the Restorepoint Automation Actions

Once you have created a Restorepoint credential that communicates with your Restorepoint devices, you must align the credential to the five default action policies included in this PowerPack. The aligned credential will work with the automation policy that is installed by default in this PowerPack to provide a working configuration.

To align the credential to the automation actions:

1. Navigate to the **Action Policy Manager** page (Registry > Run Book > Actions).
2. Locate a Restorepoint action policy and click the wrench icon (🔧). The **Action Editor** modal page appears:

Policy Editor | Editing Action [63] Reset

Action Name	Action State
Restorepoint: Difference between Last Two Backups	[Enabled] ▼
Description	
Show the difference between last two configuration backups for the triggered device	
Organization	Action Type
[System] ▼	Restorepoint : Generic Action type (1.0)
Execution Environment	
[-- Default Environment] ▼	
Action Run Context	
[Database] ▼	
Input Parameters	
<pre>{ "s11_credential_id": "", "max_log": "", "action": "recent_backups_diff" }</pre>	
Save Save As	

3. In the **Input Parameters** pane, add the credential ID to the "s11_credential_id" value. For example: "s11_credential_id": "235", .
4. Click **[Save]**.

Chapter

6

Restorepoint Automation Policies

Overview

This chapter describes how to use the automation policies, action policies, and custom action types found in the *Restorepoint Automation* PowerPack.

This manual covers the following topics:

Standard Automation Policies

The *Restorepoint Automation* PowerPack includes three standard automation policies. The "Restorepoint Event Enrichment" policy triggers three different automation actions that collect diagnostic data and formats an output. The "Start Restorepoint Backup" and "Revert Restorepoint Backup" automation policies trigger automation actions that start or revert a user initiated backup. All of the automation actions use the custom action type "Restorepoint: Generic Action type", which is supplied in the PowerPack.

Editing PowerPack™ Restorepoint Automation									
▼ Manage PowerPack™ Properties Build / Export Features / Benefits Technical Notes Documentation ▼ Contents Dynamic Applications Event Policies Device Categories Device Classes Device Templates Device Groups Reports Dashboard Widgets Dashboards Dashboards SL1 Run Book Policies Run Book Actions Run Book Action Types Ticket Templates Credentials Credential Tests Proxy XSL Transformations IT Services Log File Monitoring Policies Credential Fields Guided Discovery Workflow AP Content Objects	Embedded Run Book Policies [3]								
	Automation Policy Name	ID	Policy State	Organization	Devices	Events	Actions	Edited By	Last Edited
	1. Restorepoint Event Enrichment	107	Enabled	System	1 group	All	4	em7admin	2022-03-10 11:06:02
	2. Revert Restorepoint Backup	109	Enabled	System	All	All	1	em7admin	2022-03-10 11:06:04
	3. Start Restorepoint Backup	108	Enabled	System	All	All	1	em7admin	2022-03-10 11:06:04
Available Run Book Policies [0]									
Automation Policy Name ID Policy State Organization Devices Events Actions Edited By Last Edited									
No results to display.									

The following table shows the standard automation policies, the aligned events, and the automation actions that run in response to the events:

Automation Policy Name	Aligned Events	Aligned Device Group	Automation Action
Restorepoint Event Enrichment	All events in your SL1 system are aligned to this policy	Restorepoint Devices	- Restorepoint: Difference Between Last Two Backups - Restorepoint: Link to Last Configuration Backup - Restorepoint: Recent Logs
Start Restorepoint Backup	All events	All devices	Restorepoint: Start Backup
Revert Restorepoint Backup	All events	All devices	Restorepoint: Revert Backup

The following figure shows a file system usage threshold exceeded event with major criticality on the **Events** page. Click the **[Actions]** button (**...**) for an event, and select *View Automation Actions* to see the automation actions triggered by the event.

Events											
9 Critical 374 Major 8 Minor 1 Notice 6 Healthy 398 Events Type to search events											
	ORGANIZATION	SEVERITY	NAME	MESSAGE	AGE	TICKET ID	COUNT	EVENT NOTE	MASKED EVENTS	ACKNOWLEDGE	CLEAR
☒	System	Healthy	bl-db	swap memory usage of 0% is below threshold of 20%	1 hour 11 minutes		1			☒ Acknowledge	☒ Clear
☒	System	Healthy	SL1	SL1: Tree Maintenance Component Updates	1 hour 16 minutes		1			☒ Acknowledge	☒ Clear
☒	Network	Major	10.64.172.187	Backup Error Message: Device2: nll device : unknown proto...	1 hour 25 minutes		1			☒ Acknowledge	☒ Clear
☒	System	Major	cisco26	Backup Error Message: SL1 Collector: Function won't comp...	1 hour 29 minutes		1			☒ Acknowledge	☒ Clear
☒	System	Major	Restonpoint Appliance	Backup Error Message: Device1: Timeout. Failed 304 times ...	1 hour 58 minutes		1			☒ Acknowledge	☒ Clear
☒	Network	Major	10.64.172.187	Backup Error Message: Device2: nll device : unknown proto...	2 hours 11 minutes		1			☒ Acknowledge	☒ Clear
☐	System	Minor	System	EM7 minor event: Non-digits in oid with object id: 19995, d...	2 hours 11 minutes		1			☐ Acknowledge	☐ Clear
☒	System	Major	cisco26	Backup Error Message: SL1 Collector: Function won't comp...	2 hours 15 minutes		1			☒ Acknowledge	☒ Clear
☒	System	Major	Restonpoint Appliance	Backup Error Message: Device1: Timeout. Failed 303 times ...	2 hours 46 minutes		1			☒ Acknowledge	☒ Clear
☒	Network	Major	10.64.172.187	Backup Error Message: Device2: nll device : unknown proto...	2 hours 57 minutes		1			☒ Acknowledge	☒ Clear
☒	System	Major	cisco26	Backup Error Message: SL1 Collector: Function won't comp...	3 hours 1 minute		1			☒ Acknowledge	☒ Clear
☒	System	Major	Restonpoint Appliance	Backup Error Message: Device1: Timeout. Failed 302 times ...	3 hours 34 minutes		1			☒ Acknowledge	☒ Clear
☒	Network	Major	10.64.172.187	Backup Error Message: Device2: nll device : unknown proto...	3 hours 43 minutes		1			☒ Acknowledge	☒ Clear
☒	System	Major	cisco26	Backup Error Message: SL1 Collector: Function won't comp...	3 hours 47 minutes		1			☒ Acknowledge	☒ Clear
☒	System	Major	Restonpoint Appliance	Backup Error Message: Device1: Timeout. Failed 301 times ...	4 hours 22 minutes		1			☒ Acknowledge	☒ Clear
☒	Network	Major	10.64.172.187	Backup Error Message: Device2: nll device : unknown proto...	4 hours 29 minutes		1			☒ Acknowledge	☒ Clear
☒	System	Major	cisco26	Backup Error Message: SL1 Collector: Function won't comp...	4 hours 33 minutes		1			☒ Acknowledge	☒ Clear
☒	System	Major	Restonpoint Appliance	Backup Error Message: Device1: Timeout. Failed 300 times ...	5 hours 10 minutes		1			☒ Acknowledge	☒ Clear
☒	Network	Major	10.64.172.187	Backup Error Message: Device2: nll device : unknown proto...	5 hours 15 minutes		1			☒ Acknowledge	☒ Clear
☒	System	Major	cisco26	Backup Error Message: SL1 Collector: Function won't comp...	5 hours 19 minutes		1			☒ Acknowledge	☒ Clear
☒	System	Major	Restonpoint Appliance	Backup Error Message: Device1: Timeout. Failed 299 times ...	5 hours 58 minutes		1			☒ Acknowledge	☒ Clear

The results shown for this event, in the **Event Actions Log**, include an executed automation policy (shown at the top of the following figure), along with the automation actions (commands). Results for each command are also displayed. The following figure shows an example of this output:

Event Actions Log | For Event [167503]
Refresh
Guide

2021-03-01 14:06:34
Automation Policy Restorepoint Event Enrichment action Datacenter Automation: Format Output as HTML ran Successfully
Message Snippet (557) executed without incident
Result: [formatted_output: 'Enrichment Command Output'

Command: Recent Logs from Restorepoint
UserName:Auto, Action:Backup, Dt:2021-03-01T14:01:10.519616867Z, Message:Version 5
UserName:Auto, Action:Backup, Dt:2021-03-01T14:00:45.516075877Z, Message:Started
UserName:Auto, Action:Backup, Dt:2021-03-01T13:01:11.527920692Z, Message:Version 5
UserName:Auto, Action:Backup, Dt:2021-03-01T13:00:45.514732167Z, Message:Started
UserName:Auto, Action:Backup, Dt:2021-03-01T12:01:11.076132052Z, Message:Version 5
UserName:Auto, Action:Backup, Dt:2021-03-01T12:00:45.51377585Z, Message:Started
UserName:Auto, Action:Backup, Dt:2021-03-01T11:01:10.355008506Z, Message:Version 5
UserName:Auto, Action:Backup, Dt:2021-03-01T11:00:45.515095109Z, Message:Started
UserName:Auto, Action:Backup, Dt:2021-03-01T10:01:11.148938966Z, Message:Version 5
UserName:Auto, Action:Backup, Dt:2021-03-01T10:00:45.51954914Z, Message:Started

Command: Last configuration changes, between 2021-02-24T22:46:49Z and 2021-03-01T14:01:10Z
running: snmp-server user public read_all v2c
snmp-server view all 1 included
Line references: 32 and 32
Current: snmp-server community public RO
...
Previous: snmp-server community public RW
snmp-server location Mordor
control-plane

}]

2021-03-01 14:06:28
Automation Policy Restorepoint Event Enrichment action Restorepoint: Link to Last Configuration Backup ran Successfully
Message CustomActionType (543) executed without incident
Result: Restorepoint Last Backup Link: https://10.2.11.16/#viewconfig/114'

2021-03-01 14:06:26
Automation Policy Restorepoint Event Enrichment action Restorepoint: Difference between Last Two Backups ran Successfully
Message CustomActionType (544) executed without incident
Result: [command_list_out: [Last configuration changes, between 2021-02-24T22:46:49Z and 2021-03-01T14:01:10Z, 'running: snmp-server user public read_all v2c\nsnmp-server view all 1 included\nLine references: 32 and 32\nCurrent: snmp-server community public RO\n...\nPrevious: snmp-server community public RW\nsnmp-server location Mordor\ncontrol-plane\n\n', 'False']])

2021-03-01 14:06:24
Automation Policy Restorepoint Event Enrichment action Restorepoint: Recent Logs ran Successfully
Message CustomActionType (542) executed without incident
Result: [command_list_out: [Recent Logs from Restorepoint', 'UserName:Auto, Action:Backup, Dt:2021-03-01T14:01:10.519616867Z, Message:Version 5\nUserName:Auto, Action:Backup, Dt:2021-03-01T14:00:45.516075877Z, Message:Started\nUserName:Auto, Action:Backup, Dt:2021-03-01T13:01:11.527920692Z, Message:Version 5\nUserName:Auto, Action:Backup, Dt:2021-03-01T13:00:45.514732167Z, Message:Started\nUserName:Auto, Action:Backup, Dt:2021-03-01T12:01:11.076132052Z, Message:Version 5\nUserName:Auto, Action:Backup, Dt:2021-03-01T12:00:45.51377585Z, Message:Started\nUserName:Auto, Action:Backup, Dt:2021-03-01T11:01:10.355008506Z, Message:Version 5\nUserName:Auto, Action:Backup, Dt:2021-03-01T11:00:45.515095109Z, Message:Started\nUserName:Auto, Action:Backup, Dt:2021-03-01T10:01:11.148938966Z, Message:Version 5\nUserName:Auto, Action:Backup, Dt:2021-03-01T10:00:45.51954914Z, Message:Started']]

To learn more about which commands are executed by default for a given automation action, see [Customizing Restorepoint Action Policies](#).

TIP: Although you can edit the automation policies described in this section, it is a best practice to use "Save As" to create a new automation policy, rather than to customize the standard automation policies.

Creating and Customizing Automation Policies

Overview

This chapter describes how to create automation policies using the automation actions in the *Restorepoint Automation* PowerPack.

NOTE: The steps in this chapter are optional. The Restorepoint Automation PowerPack includes an automation policy that is installed by default. The default automation policy runs all automation actions in the PowerPack for all Minor, Major, and Critical events on devices that are in the "Restorepoint Devices" device group.

This manual covers the following topics:

Prerequisites

Before you create an automation policy using the automation actions in the *Restorepoint Automation* PowerPack, you must determine:

- Which set of commands you want to run on a monitored device when an event occurs. There are three automation actions in the PowerPack that run the "Restorepoint: Generic Action type" action type with different commands and output formats. You can also create your own automation actions using the custom action type supplied in the PowerPack.
- The event criteria you want to use to determine when the automation actions will trigger, or the set of rules that an event must match before the automation is executed. This can include matching only specific event policies, event severity, associated devices, and so on. For a description of all the options that are available in Automation Policies, see the *Run Book Automation* manual.

Creating an Automation Policy

To create an automation policy that uses the automation actions in the *Restorepoint Automation* PowerPack, perform the following steps:

1. Go to the **Automation Policy Manager** page (Registry > Run Book > Automation).

- Click **[Create]**. The **Automation Policy Editor** page appears.

The screenshot displays the 'Automation Policy Editor | Creating New Automation Policy' window. The interface is organized into several sections:

- Policy Configuration:** Includes fields for Policy Name (New Automation Policy), Policy Type (Active Events), Policy State (Enabled), Policy Priority (Default), and Organization (System).
- Criteria Logic:** A series of dropdown menus for defining event criteria, such as Severity (>=), Minor, and time-based conditions like 'and 5 minutes has elapsed'.
- Match Logic:** Includes Match Logic (Text search) and Match Syntax.
- Repeat Time:** A dropdown menu set to 'Only once'.
- Align With:** A dropdown menu set to 'Device Groups'.
- Include events for entities other than devices (organizations, assets, etc.):** An unchecked checkbox.
- Trigger on Child Rollup:** An unchecked checkbox.
- Available Device Groups:** A list of device groups including IPv4 Devices, IPv6 Devices, Linux Automation, Microsoft Hyper-V Automation, MOM VMWare Guests, NetFlow Devices, and ScienceLogic Data Collectors.
- Aligned Device Groups:** A list containing 'Restorepoint Devices'.
- Available Events:** A list of events including '[3007] Critical: AKCP: AC Voltage sensor detects no current', '[3016] Critical: AKCP: DC Voltage sensor High Critical', '[3017] Critical: AKCP: DC Voltage sensor Low Critical', '[3006] Critical: AKCP: Dry Contact Sensor Low Critical', '[3012] Critical: AKCP: Smoke Detector Alert!', '[3010] Critical: AKCP: Water Sensor has detected water', '[1938] Critical: APC: Diagnostic Test Failed', and '[4005] Critical: APC: UPS Battery Capacity'.
- Aligned Events:** A list containing '(All events)'.
- Available Actions:** A list of actions including 'Send Email [0]: Email for devices in 'ALL' Organization', 'SNMP Trap [1]: RBA Base Pack: Send Trap', 'SNMP Trap [1]: SL1 Event Trap', 'Create Ticket [2]: RBA Base Pack: Create Ticket', 'Create Ticket [2]: Test-RBA', 'Snippet [5]: All Output Test', and 'Snippet [5]: API VeloCloud initial disable'.
- Aligned Actions:** A list of actions including '1. Restorepoint : Generic Action type [114]: Restorepoint: Diff', '2. Restorepoint : Generic Action type [114]: Restorepoint: Lin', '3. Restorepoint : Generic Action type [114]: Restorepoint: Re', and '4. Format HTTP Action Output [108]: Datacenter Automation:'.

A 'Save' button is located at the bottom center of the form.

- Complete the following required fields:
 - Policy Name.** Enter a name for the automation policy.
 - Policy Type.** Select whether the automation policy will match events that are active, match when events are cleared, or run on a scheduled basis. Typically, you would select *Active Events* in this field.
 - Policy State.** Specifies whether the policy will be evaluated against the events in the system. If you want this policy to begin matching events immediately, select *Enabled*.
 - Policy Priority.** Specifies whether the policy is high-priority or default priority. These options determine how the policy is queued.

- **Organization.** Select one or more organizations to associate with the automation policy. The automation policy will execute only for devices in the selected organizations (that also match the other criteria in the policy). To configure a policy to execute for all organizations, select *System* without specifying individual devices to align to.
- **Align With.** Select *Device Groups*.
- **Aligned Device Groups.** The "Restorepoint Devices" device group needs to be aligned. To add the device group to the **Aligned Device Groups** field, select the "Restorepoint Devices" device group in the **Available Device Groups** field and click the right arrow (>).
- **Aligned Actions.** This field includes the actions from the *Restorepoint AutomationPowerPack*. To add an action to the **Aligned Actions** field, select the action in the **Available Actions** field and click the right arrow (>). To re-order the actions in the **Aligned Actions** field, select an action and use the up arrow or down arrow buttons to change that action's position in the sequence.

NOTE: You must have at least two Aligned Actions: one that runs the automation action and one that provides the output format. The actions providing the output formats are contained in the *Datacenter Automation Utilities PowerPack*, which is a prerequisite for running automations in this PowerPack. If you are selecting the "Difference Between Last Two Logs" or the "Restorepoint Recent Logs" collection actions, you may want to include the "Format Output as HTML" automation action, found in the *Datacenter Automation Utilities PowerPack*, in your automation policy.

4. Optionally, supply values in the other fields on this page to refine when the automation will trigger.
5. Click **[Save]**.

NOTE: You can also modify one of the automation policies included with this PowerPack. Best practice is to use the **[Save As]** option to create a new, renamed automation policy, instead of customizing the standard automation policies. For more information, see [Customizing an Automation Policy](#).

NOTE: If you modify one of the included automation policies and save it with the original name, the customizations in that policy will be overwritten when you upgrade the PowerPack unless you remove the association between the automation policy and the PowerPack before upgrading.

Example Automation Configuration

The following is an example of an automation policy that uses the automation actions in the *Restorepoint Automation PowerPack*:

The screenshot displays the 'Automation Policy Editor | Creating New Automation Policy' window. The interface is divided into several sections for configuring the policy:

- Policy Name:** Restorepoint: Run Recent Logs
- Policy Type:** [Active Events]
- Policy State:** [Enabled]
- Policy Priority:** [Default]
- Organization:** System
- Criteria Logic:** A series of dropdowns: [Severity >=], [Minor,], [and 5 minutes has elapsed], [since the first occurrence,], [and event is NOT cleared], and and all times are valid.
- Match Logic:** [Text search]
- Match Syntax:** (Empty field)
- Repeat Time:** [Only once]
- Align With:** Device Groups
- ☐ Include events for entities other than devices (organizations, assets, etc.)
- ☐ Trigger on Child Rollup
- Available Device Groups:** A list including IPv4 Devices, IPv6 Devices, Linux Automation, Microsoft Hyper-V Automation, MOM VMWare Guests, NetFlow Devices, and ScienceLogic Data Collectors Servers.
- Aligned Device Groups:** Restorepoint Devices
- Available Events:** A list of events such as [3007] Critical: AKCP: AC Voltage sensor detects no current, [3016] Critical: AKCP: DC Voltage sensor High Critical, [3017] Critical: AKCP: DC Voltage sensor Low Critical, [3006] Critical: AKCP: Dry Contact Sensor Low Critical, [3012] Critical: AKCP: Smoke Detector Alert!, [3010] Critical: AKCP: Water Sensor has detected water, [1938] Critical: APC: Diagnostic Test Failed, and [1926] Critical: APC: UPS Battery Capacity.
- Aligned Events:** (All events)
- Available Actions:** A list of actions including Run SNMP Walk [112]: Walk System MIB, Execute Commands via SSH [113]: Get and Truncate Large SL1 L..., Execute Commands via SSH [113]: Restart Service, Execute Commands via SSH [113]: Top and Pidstat Output, and several Restorepoint : Generic Action type [114] actions.
- Aligned Actions:** 1. Restorepoint : Generic Action type [114]: Restorepoint: Rec..., 2. Format HTTP Action Output [108]: Datacenter Automation:...
- Buttons:** Reset (top right), Save (bottom center).

The policy uses the following settings:

- **Policy Name.** The policy is named "Restorepoint: Run Recent Logs".
- **Policy Type.** The policy runs when an event is in an active state. *Active Events* is selected in this field.
- **Policy State.** *Enabled* is selected in this field. This policy is active and ready to use.

- **Organization.** The policy executes for the System organization.
- **Criteria Logic.** The policy is configured to execute immediately when an event matches these criteria: "Severity >= Notice, and no time has elapsed since the first occurrence, and event is NOT cleared, and all times are valid".
- **Aligned With.** The policy is configured to align with devices in the selected device group.
- **Aligned Device Groups.** The policy is configured to trigger for devices in the "Restorepoint Devices" device group.
- **Aligned Events.** The policy is configured to trigger for All events.
- **Aligned Actions.** The automation includes the following actions. This action allows you to view the output of the diagnostic commands in the Automation Log, accessed through the SL1 **Events** page:
 - Restorepoint: Generic Action type [114]: Restorepoint: Recent Logs
 - Format HTTP Action Output [108]: Datacenter Automation: Format JSON as simple HTML

Customizing an Automation Policy

To customize an automation policy:

1. Go to the **Automation Policy Manager** page (Registry > Run Book > Automation).

- Search for the *Restorepoint Automation* automation policy you want to edit and click the wrench icon (🔧) for that policy. The **Automation Policy Editor** page appears:

The screenshot shows the 'Automation Policy Editor | Editing Automation Policy [450]' window. It contains several sections for configuring an automation policy:

- Policy Name:** Restorepoint Event Enrichment
- Policy Type:** [Active Events]
- Policy State:** [Enabled]
- Policy Priority:** [Default]
- Organization:** [System]
- Criteria Logic:** [Severity >=] [Minor,]
- Match Logic:** [Text search]
- Match Syntax:** (empty field)
- Repeat Time:** [Only once]
- Align With:** Device Groups
- Include events for entities other than devices (organizations, assets, etc.):** ☐
- Trigger on Child Rollup:** ☐
- Available Device Groups:**
 - MOM VMWare Guests
 - NetFlow Devices
 - ScienceLogic Data Collectors
 - Servers
 - VMware Virtual Machines
 - Windows Automation
- Aligned Device Groups:** Restorepoint Devices
- Available Events:**
 - [3007] Critical: AKCP: AC Voltage sensor detects no current
 - [3016] Critical: AKCP: DC Voltage sensor High Critical
 - [3017] Critical: AKCP: DC Voltage sensor Low Critical
 - [3006] Critical: AKCP: Dry Contact Sensor Low Critical
 - [3012] Critical: AKCP: Smoke Detector Alert!
 - [3010] Critical: AKCP: Water Sensor has detected water
 - [1939] Critical: ABC: Diagnostic Test Failed
- Aligned Events:** (All events)
- Available Actions:**
 - Send Email [0]: Email for devices in 'ALL' Organization
 - SNMP Trap [1]: RBA Base Pack: Send Trap
 - SNMP Trap [1]: SL1 Event Trap
 - Create Ticket [2]: RBA Base Pack: Create Ticket
 - Create Ticket [2]: Test-RBA
 - Snippet [5]: All Output Test
 - Snippet [5]: API/oloCloud initial disable
- Aligned Actions:**
 - 1. Restorepoint : Generic Action type [114]: Restorepoint
 - 2. Restorepoint : Generic Action type [114]: Restorepoint
 - 3. Restorepoint : Generic Action type [114]: Restorepoint
 - 4. Snippet [5]: Datacenter Automation: Format Output as

At the bottom, there are 'Save' and 'Save As' buttons.

- Complete the following fields as needed:

- Policy Name.** Type a new name for the automation policy to avoid overwriting the default policy.
- Policy Type.** Select whether the automation policy will match events that are active, match when events are cleared, or run on a scheduled basis. Typically, you would select *Active Events* in this field.
- Policy State.** Specifies whether the policy will be evaluated against the events in the system. If you want this policy to begin matching events immediately, select *Enabled*.

- **Policy Priority.** Specifies whether the policy is high-priority or default priority. These options determine how the policy is queued.
- **Organization.** Select the organization that will use this policy.
- **Aligned Actions.** This field includes the actions from the Restorepoint Automation PowerPack. You should see "Restorepoint" actions in this field. To add an action to the **Aligned Actions** field, select the action in the **Available Actions** field and click the right arrow (> >). To re-order the actions in the **Aligned Actions** field, select an action and use the up arrow or down arrow buttons to change that action's position in the sequence.

NOTE: You must have two Aligned Actions: one that runs the diagnostic or remediation commands and one that provides the output format. The actions providing the output formats are contained in the *Datacenter Automation Utilities* PowerPack, which is a prerequisite for running Restorepoint automations. If you are selecting the "Difference Between Last Two Logs" or the "Restorepoint Recent Logs" collection actions, you may want to include the "Format Output as HTML" automation action, found in the *Datacenter Automation Utilities* PowerPack, in your automation policy.

4. Optionally, supply values in the other fields on the **Automation Policy Editor** page to refine when the automation will trigger.
5. Click [Save As].

Removing an Automation Policy from a PowerPack

After you have customized a policy from a *Restorepoint Automation* PowerPack, you might want to remove that policy from that PowerPack to prevent your changes from being overwritten if you update the PowerPack later. If you have the license key with author's privileges for a PowerPack or if you have owner or administrator privileges with your license key, you can remove content from a PowerPack.

To remove content from a PowerPack:

1. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).
2. Find the *Restorepoint Automation*PowerPack. Click its wrench icon (.
3. In the **PowerPack Properties** page, in the navigation bar on the left side, click **Run Book Policies**.
4. In the **Embedded Run Book Polices** pane, locate the policy you updated, and click the bomb icon () for that policy. The policy will be removed from the PowerPack and will now appear in the bottom pane.

Chapter

8

Customizing Restorepoint Action Policies

Overview

This manual describes how to customize the automation action policies embedded in the *Restorepoint Automation* PowerPack to create automation actions to meet your organization's specific requirements.

For more information about creating automation policies using custom action types, see [Creating and Customizing Automation Policies](#).

This manual covers the following topics:

Creating a Custom Action Policy

You can use the "Restorepoint: Generic Action type" action type included with the *Restorepoint Automation PowerPack* to create custom automation actions that you can then use to build custom automation policies.

To create a custom action policy using the "Restorepoint: Generic Action type" action type:

1. Navigate to the **Action Policy Manager** page (Registry > Run Book > Actions).
2. In the **Action Policy Manager** page, click the **[Create]** button.
3. The **Action Policy Editor** modal appears.

The screenshot shows the 'Action Editor' modal window with the title 'Policy Editor | Creating New Action'. It contains several input fields and a dropdown menu. The 'Action Name' field is empty. The 'Action State' dropdown is set to '[Enabled]'. The 'Description' field is empty. The 'Organization' dropdown is set to '[System]'. The 'Action Type' dropdown is open, showing a list of options: 'Send an Email Notification', 'Send an SNMP Trap', 'Create a New Ticket', 'Send an SNMP Set', 'Run a Snippet', 'Execute an SQL Query', 'Update an Existing Ticket', 'Send an AWS SNS message', 'ServiceNow: Create, Update, Clear Ticket (1.2)', 'Restorepoint : Generic Action type (1.0)' (which is highlighted in blue), and 'Run Integration Service Application (1.0)'. The 'Execution Environment' dropdown is set to '[-- Default Environment]'. There is an 'Input Parameters' section with a large empty text area. A 'Save' button is at the bottom right, and a 'Reset' button is at the top right.

4. In the **Action Policy Editor** page, supply a value in each field.
 - **Action Name.** Specify the name for the action policy.
 - **Action State.** Specifies whether the policy can be executed by an automation policy (enabled) or cannot be executed (disabled).
 - **Description.** Allows you to enter a detailed description of the action.
 - **Organization.** Organization to associate with the action policy.

- **Action Type.** Type of action that will be executed. Select the "Restorepoint: Generic Action type" action type (highlighted in the figure above).
- **Execution Environment.** Select from the list of available Execution Environments. The default execution environment is *System*.
- **Action Run Context.** Select *Database* or *Collector* as the context in which the action policy will run.
- **Input Parameters.** A JSON structure that specifies each input parameter. Each parameter definition includes its name, data type, and whether the input is optional or required for this Custom Action Type. For more information about the available input parameters, see the table in [Creating a New Restorepoint Automation Action](#).

NOTE: Input parameters must be defined as a JSON structure, even if only one parameter is defined.

5. Click **[Save]**. If you are modifying an existing action policy, click **[Save As]**. Supply a new value in the **Action Name** field, and save the current action policy, including any edits, as a new policy.

Customizing Automation Actions

The *Restorepoint Automation* PowerPack includes five automation actions that use the "Restorepoint: Generic Action type" action type to request diagnostic information or remediate an issue. You can specify the host and the options in a JSON structure that you enter in the **Input Parameters** field in the **Action Policy Editor** modal.

NOTE: The Run Book automations only work against devices that have the Restorepoint ID custom attribute, which is automatically set when a device is synchronized from SL1 to Restorepoint. The automation actions share formatting actions with the *Datacenter Automation Pack*, so the output can be sent to Restorepoint using the same customization steps.

Policy Editor | Editing Action [63]
Reset

Action Name
Restorepoint: Difference between Last Two Backups

Action State
[Enabled]

Description
Show the difference between last two configuration backups for the triggered device

Organization
[System]

Action Type
Restorepoint : Generic Action type (1.0)

Execution Environment
[-- Default Environment]

Action Run Context
[Database]

Input Parameters

```

{
  "sl1_credential_id": "",
  "max_log": "",
  "action": "recent_backups_diff"
}

```

Save Save As

The following automation actions that use the "Restorepoint: Generic Action type" action type are included in the *Restorepoint Automation* PowerPack. Compare the commands run with the example in the image above. For more information about input parameter fields, see the table in [Creating a New Restorepoint Automation Action](#).

Action Name	Description
Restorepoint Recent Logs	Collects the last number of logs for the device associated with the triggering event. The number of logs is configurable.
Link to Configuration Backup	Creates a link to the Restorepoint UI that displays the last configuration backup from the device associated with the triggering event.
Difference between Last Two Backups	Collects the difference between the last two configuration backups for the device associated with the triggering event
Start Backup	Triggers a backup in Restorepoint
Revert Backup	Reverts a backup in Restorepoint

Creating a New Restorepoint Automation Action

You can create a new automation action or you can also use the existing automation actions in the PowerPack as a template by using the **[Save As]** option.

The automation actions accept the following parameters in JSON:

Parameter	Input type	Description
sl1_credential_id	integer	The ID of the credential to use when running the command. The credential connects to the Restorepoint API to gather data. For more information on finding your SL1 credential ID, see the chapter Configuring Device Credentials .
max_log	integer	The number of log entries to collect from Restorepoint. This parameter only applies to the "get_logs" action setting.
action	string	The data to collect from Restorepoint. There are three support values for this parameter: • get_logs: The most recent logs associated with the Restorepoint device. The number of logs is configurable with the max_log parameter. • last_backup_link: The URL of the last backup performed in Restorepoint for the selected device. • recent_backups_diff: The difference between the last two backups performed in Restorepoint for the selected device.

© 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