Skylar Compliance Automation PowerPack

Version 200

Table of Contents

Chapter 1

Introduction to the Skylar Compliance Automation PowerPack

Overview

This manual describes how to use the Skylar One automation policies, automation actions, and custom action types found in the "Skylar Compliance Automation" PowerPack. You can use this PowerPack to enrich Skylar One events for Skylar Compliance devices by automatically running diagnostic commands, and the command output is added to the Skylar One event log or associated incident.

This PowerPack requires the "Datacenter Automation Utilities" PowerPack, version 103 or later.

This chapter covers the following topics:

What is the Skylar Compliance Automation PowerPack?

The "Skylar Compliance Automation" PowerPack includes automation policies that enrich Skylar One events for Skylar Compliance devices (for example, from the "Skylar Compliance" PowerPack) by automatically running diagnostic commands. The command output is added to the Skylar One event log or associated incident.

The Skylar Compliance run book actions are executed on the Skylar One All-In-One Appliance or Data Collector.

In addition to using the standard content, you can use the content in the "Skylar Compliance 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.

Contents of the PowerPack

This PowerPack includes the following features:

- The "Restorepoint Connectivity" Dynamic Application, which validates the type of credentials used by Skylar Compliance
- Run book automation policies:
    - Restorepoint Event Enrichment
    - Revert Restorepoint Backup
    - Start Restorepoint Backup
- Run book action policies:
    - Restorepoint: Difference between Last Two Backups
    - Restorepoint: Link to Last Configuration Backup
    - Restorepoint: Recent Logs
    - Restorepoint: Revert Backup
    - Restorepoint: Start Backup
- The "Restorepoint: Generic Action type" run book action type
- The "Restorepoint Automation" credential
- The "Restorepoint Devices" device group, which includes a dynamic rule that matches devices with aligned Dynamic Applications, including the "RestorepointConnectivity" Dynamic Application

Installing the Skylar Compliance Automation PowerPack

Before completing the steps in this manual, you must import and install the latest version of the "Skylar Compliance Automation" PowerPack.

IMPORTANT: You must install the"Datacenter Automation Utilities" PowerPack version 103 before using the "Skylar Compliance Automation" PowerPack.

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

NOTE: For details on upgrading Skylar One, see the relevant *Skylar One Platform Release Notes*.

To download and install the PowerPack:

1. Search for and download the PowerPack from the **PowerPacks** page at the ScienceLogic Support Center (Skylar One > PowerPacks, login required).
2. In Skylar One, go to the **PowerPacks** page (System > Manage > PowerPacks).
3. Click the actions icon and choose *Import PowerPack*. The **Import PowerPack** dialog box appears.
4. Click **[Browse]** and navigate to the PowerPack file from step 1.
5. Select the PowerPack file and click **[Import]**. The **PowerPack Installer** modal displays a list of the PowerPack contents.
6. Click **[Install]**. The PowerPack is added to the **PowerPacks** page.

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

Downloading and Compiling the Skylar Compliance MIB Files

After installing the PowerPack, you will need to download the following MIB files from Skylar Compliance and compile the MIB files in Skylar One:

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

You can access the Skylar Compliance MIB files from your Skylar Compliance system.

To download the MIB files in Skylar Compliance:

1. In your Skylar Compliance 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 Skylar Compliance MIB files in Skylar One:

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 Skylar One can use them. To compile a MIB, click its lightning bolt icon ( ).
5. To enable Skylar Compliance to send trap events to Skylar One, go to **Administration > System Settings > Logs/Alerts** in the Skylar Compliance user interface and change the following:
    - ***SNMP Traps***: Check this checkbox.
    - ***SNMP Server***: Enter the IP address of the Skylar One All-In-One or Data Collector.

Chapter 2

Skylar Compliance Automation Policies

Overview

This chapter describes how to use the automation policies, automation actions, and custom action types found in the "Skylar Compliance Automation" PowerPack.

This chapter covers the following topics:

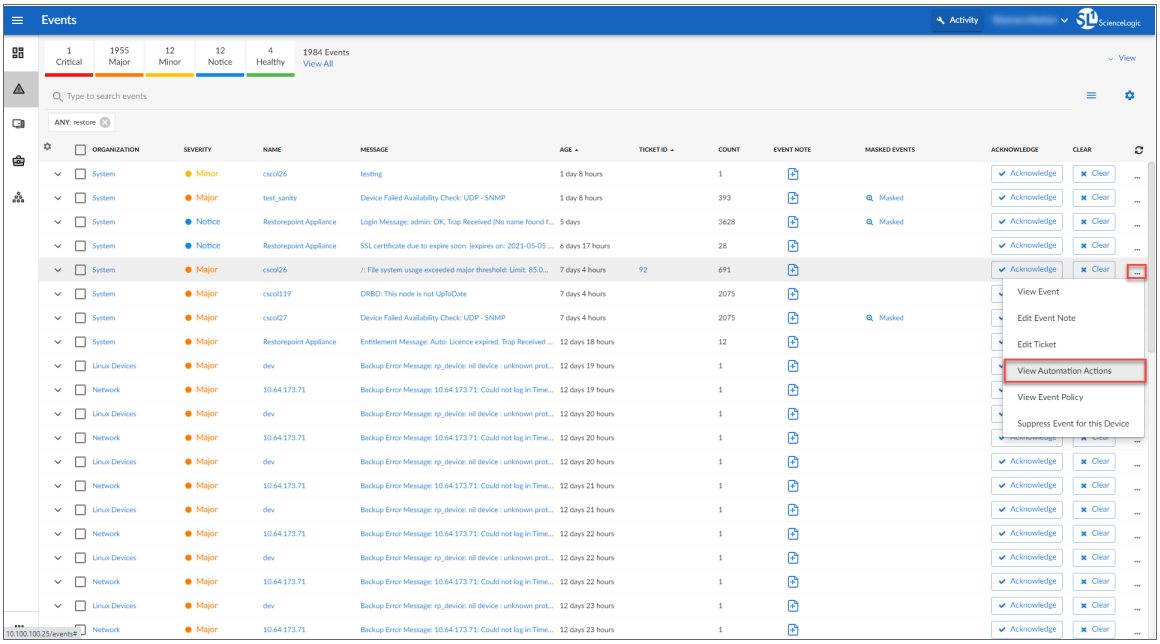
Standard Automation Policies

The "Skylar Compliance Automation" PowerPack includes one standard automation policy. This policy triggers three different automation actions that collect diagnostic data and formats an output. All of the automation actions use the custom action type "Restorepoint: Generic Action type", which is supplied in the PowerPack.

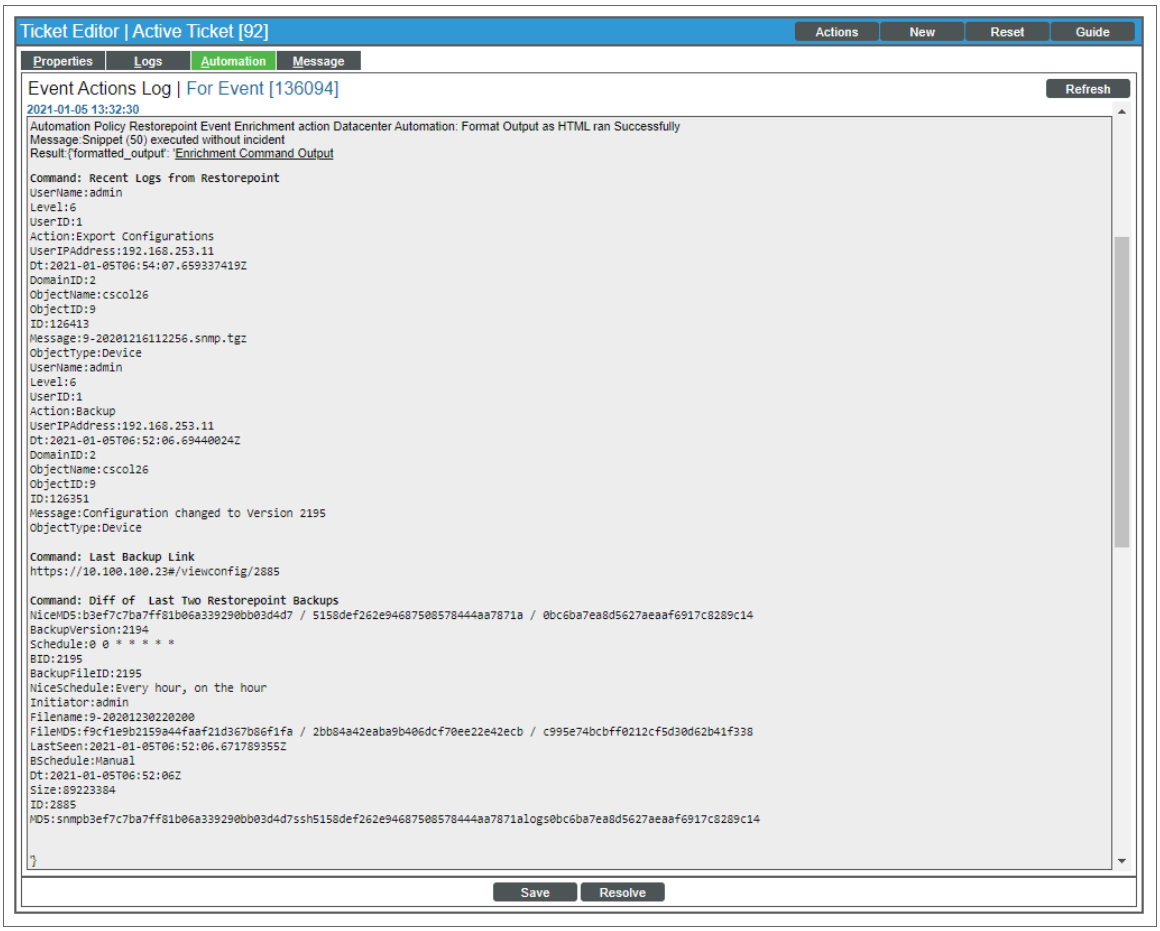
The following table shows the standard automation policy, the aligned events, and the automation actions that run in response to the events:

Automation Policy Name	Aligned Events	Automation Actions
Restorepoint Event Enrichment	All events in your Skylar One system are aligned to this policy	• Restorepoint: Difference Between Last Two Backups • Restorepoint: Link to Last Configuration Backup • Restorepoint: Recent Logs

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.



The results shown for this event, in the **Event Actions Log**, include the 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:



To learn more about which commands are executed by default for a given automation action, see *Customizing Actions*.

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.

Chapter 3

Creating and Customizing Automation Policies

Overview

This chapter describes how to create automation policies using the automation actions in the "Skylar Compliance Automation" PowerPack.

This chapter covers the following topics:

Prerequisites

Before you create an automation policy using the automation actions in the "Skylar Compliance Automation" PowerPack, you must determine:

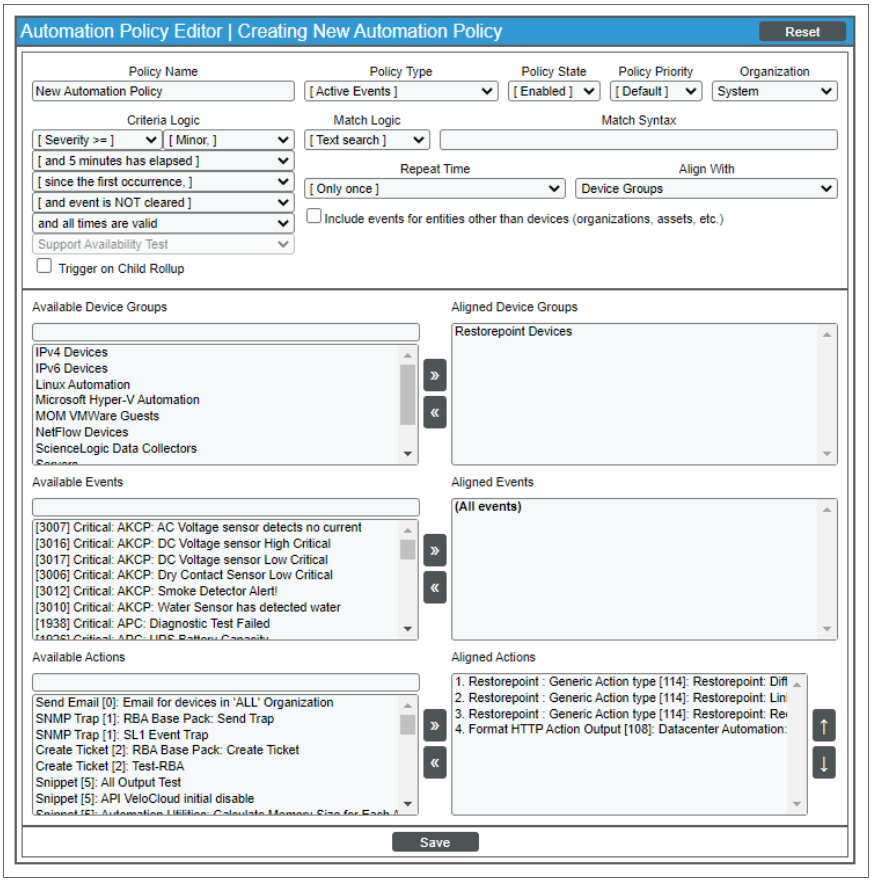
- Which set of commands you want to run on a monitored device when an event occurs. There are three automation actions in the PowerPack that run the "Restorepoint: Generic Action type" action type with different commands and output formats. You can also create your own automation actions using the custom 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 "Skylar Compliance Automation" PowerPack, perform the following steps:

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

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



3. 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 *Skylar Compliance Automation*PowerPack. 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 run book 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.

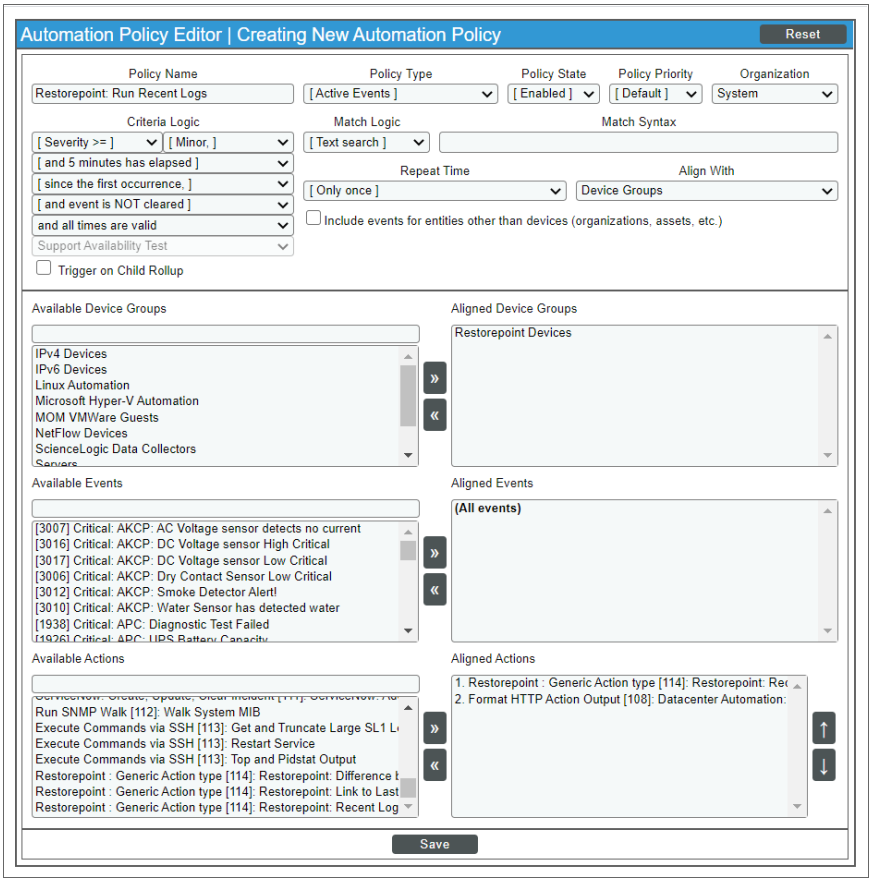
> **NOTE:** If you are selecting the "Difference Between Last Two Logs" or the "Restorepoint Recent Logs" collection actions, you may want to include the “Format Output as HTML” automation action, found in the *Datacenter Automation Utilities* PowerPack, in your automation policy.

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 "Skylar Compliance Automation" PowerPack:



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.

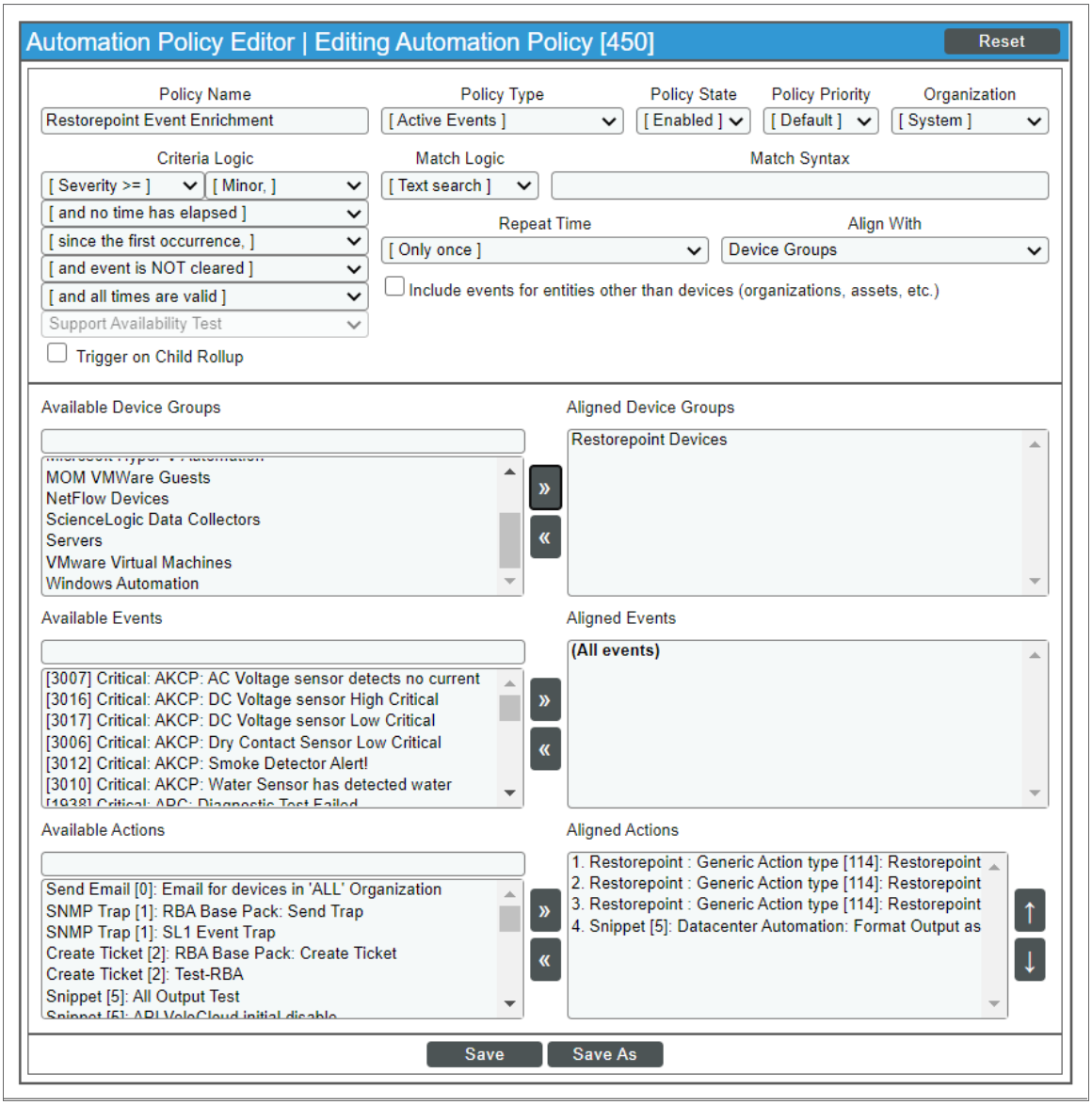
- ***Aligned Actions***. The automation includes the following actions. This action allows you to view the output of the diagnostic commands in the Automation Log, accessed through the Skylar One**Events** page:
    - Restorepoint: Generic Action type [114]: Restorepoint: Recent Logs
    - Format HTTP 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).

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



3. 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 Skylar Compliance 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.

> **NOTE:** 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 the "Skylar Compliance 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 Automations" 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 4

Configuring Device Credentials

Overview

This chapter describes how to configure the credentials required by the automation actions in the "Skylar Compliance Automation" PowerPack.

This chapter 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 Skylar Compliance credential that includes the hostname/IP address, and API token for your Skylar Compliance system. The "Skylar Compliance Automation" PowerPack includes a "Restorepoint Automation" credential template that you can use to create your own credential to communicate with your Skylar Compliance devices.

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

The "Restorepoint Automation" credential requires a Restorepoint API token:

1. In the Skylar Compliance user interface, go to the **Users API Tokens** page (Administration > API Tokens).
2. Click the **[Add Token]** button.
3. Copy the token so you can use it in the next procedure.

To create a Skylar Compliance automation credential:

1. In Skylar One, 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 Skylar Compliance credential.
    - ***Hostname/IP***. Enter the URL for the Skylar Compliance device.
    - ***Port***. Enter the port number associated with the data you want to retrieve. The default TCP port for SSH servers is 22.
    - ***Timeout(ms)***. Enter a timeout, in milliseconds, for the connection.
    - ***Username***. Enter any kind of meaningful name in this field, such as "API credential".
    - ***Password***. Enter the Restorepoint API token in this field.
4. Click **[Save As]**.

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

Chapter 5

Customizing Skylar Compliance Actions

Overview

This manual describes how to customize the automation actions embedded in the "Skylar Compliance 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 chapter covers the following topics:

Creating a Custom Action Policy

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

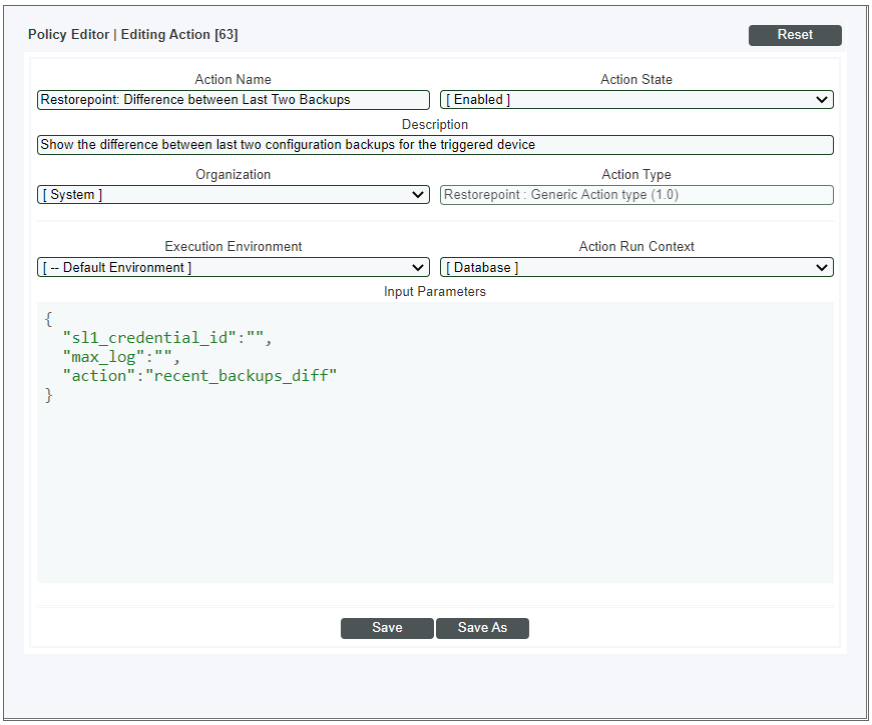
To create a custom action policy using the "Restorepoint: Generic Action type" action type:

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.
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. 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 "Skylar Compliance Automation" PowerPack includes 3 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 Skylar One 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.



The following automation actions that use the "Restorepoint: Generic Action type" action type are included in the PowerPack. Compare the commands run with the example in the image above.

Action Name	Description	Commands Run
Restorepoint Recent Logs	Collects the last number of logs for the device associated with the triggering event. The number of logs is configurable.	• `sl1_credential_id` • `max_log` • `action`
Link to Configuration Backup	Creates a link to the Skylar Compliance user interface that displays the last configuration backup from the device associated with the triggering event.	• `sl1_credential_id` • `action`
Difference between Last Two Backups	Collects the difference between the last two configuration backups for the device associated with the triggering event.	• `sl1_credential_id` • `action`

TIP: For more information about substitution variables, see the section on *Run Book Variables*.

Creating a New Skylar Compliance 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 Skylar Compliance API to gather data.
max_log	integer	The number of log entries to collect from Restorepoint.
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 Skylar Compliancedevice. The number of logs is configurable with the **max_log** parameter. • **last_backup_link**: The URL of the last backup performed in Skylar Compliance for the selected device. • **recent_backups_diff**: The difference between the last two backups performed in Skylar Compliance for the selected device.

Using Substitution Values. The command input can contain substitution values that match the keys in EM7_VALUES.

TIP: For more information about substitution variables, see the section on *Run Book Variables*.

For a description of all options that are available in Automation Policies, see the ***Run Book Automation*** manual.

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

International: +1-703-354-1010