



---

## Linux SSH Automations PowerPack

Linux SSH Automations PowerPack version 107

---

# Table of Contents

<b>Introduction to the Linux SSH Automations PowerPack</b> .....	<b>3</b>
What is the Linux SSH Automations PowerPack? .....	4
Installing the Linux SSH Automations PowerPack .....	4
<b>Configuring Linux SSH Automations</b> .....	<b>6</b>
Linux SSH Automation Policies .....	7
User-initiated Automation Policies .....	16
Creating and Customizing Automation Policies .....	17
Prerequisites .....	17
Creating or Customizing an Automation Policy .....	17
Removing an Automation Policy from a PowerPack .....	19
<b>Customizing Linux SSH Run Book Actions</b> .....	<b>20</b>
Linux SSH Run Book Actions .....	21
Creating a Custom Run Book Action Policy .....	23
Creating a Linux SSH Run Book Action .....	23
Configuring Linux Devices .....	25
Configuring Device Credentials .....	25
Creating an SSH/Key Credential .....	26
<b>Run Book Variables</b> .....	<b>27</b>
Run Book Variables .....	28

---

# Chapter

# 1

## Introduction to the Linux SSH Automations PowerPack

---

### Overview

This manual describes how to use the automation policies and run book actions in the "Linux SSH Automations" PowerPack to enrich problematic events with additional diagnostic information for monitored Linux devices.

This PowerPack can retrieve diagnostic data such as CPU, file system, and memory data, as well as interface configurations. Each set of data has its own associated policies and actions that run automatically in response to relevant events.

This PowerPack is intended to be used in conjunction with the "Linux Base Pack" PowerPack.

**NOTE:** ScienceLogic provides this documentation for the convenience of ScienceLogic customers. Some of the configuration information contained herein pertains to third-party vendor software that is subject to change without notice to ScienceLogic. ScienceLogic makes every attempt to maintain accurate technical information and cannot be held responsible for defects or changes in third-party vendor software. There is no written or implied guarantee that information contained herein will work for all third-party variants. See the End User License Agreement (EULA) for more information.

This chapter covers the following topics:

<a href="#">What is the Linux SSH Automations PowerPack?</a> .....	4
<a href="#">Installing the Linux SSH Automations PowerPack</a> .....	4

---

## What is the Linux SSH Automations PowerPack?

The "Linux SSH Automation" PowerPack includes run book automation policies that:

- Enrich SL1 events for Linux devices (for example, from the "Linux Base Pack" PowerPack and native SNMP collection) by automatically running diagnostic commands using a remote SSH connection. The command output is added to the SL1 event log or associated incident. Supported events include CPU, swap, file system, interface, and system process issues.
- Run remediation commands using a remote SSH connection in response to SL1 system process events for Linux devices in the "Linux Automation" device group.

The Linux SSH run book actions are executed on the SL1 All-In-One Appliance or Data Collector.

In addition to using the standard content, you can use the content in the "Linux SSH Automation" PowerPack to:

- Create your own run book automation policies that include the pre-defined actions that run different sets of diagnostic commands.
- Use the supplied "Execute Shell Commands" custom action type to configure your own run book action by supplying a set of commands to be executed via SSH.

The automation policies in this PowerPack can also be used as "User-Initiated" Automations.

---

## Installing the Linux SSH Automations PowerPack

Before completing the steps in this manual, you must import and install the latest version of the "Linux SSH Automations" PowerPack.

**IMPORTANT:** This PowerPack requires version 200 of the "Datacenter Automation Utilities" PowerPack.

**NOTE:** This PowerPack also requires SL1 version 12.1.2 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 section on [Global Settings](#).

To download and install the PowerPack:

1. Search for and download the PowerPack from the **PowerPacks** page (Product Downloads > PowerPacks & SyncPacks) at the [ScienceLogic Support Site](#).
2. In SL1, go to the **PowerPacks** page (System > Manage > PowerPacks).

3. Click the **[Actions]** button 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 in the **PowerPacks** 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

# 2

## Configuring Linux SSH Automations

---

### Overview

This chapter describes how to use the automation policies, run book actions, and the custom action type found in the "Linux SSH Automations" PowerPack.

This chapter covers the following topics:

<i>Linux SSH Automation Policies</i> .....	7
<i>Creating and Customizing Automation Policies</i> .....	17

# Linux SSH Automation Policies

The "Linux SSH Automations" PowerPack includes eight run book automation policies. Each automation policy triggers a run book action that collects diagnostic data or runs a remediation command over SSH for events associated with devices in the "Linux Automation" device group, and an action that formats the output. The "Linux Automation" device group is included in this PowerPack.

All run book actions use the "Execute Shell Commands" custom action type, which is also included in the PowerPack.

The screenshot shows a web interface for editing a PowerPack. The main content area displays a table titled "Embedded Run Book Policies [8]". The table has columns for Automation Policy Name, ID, Policy State, Organization, Devices, Events, Actions, Edited By, and Last Edited. There are 8 rows of data, each representing a different automation policy. Below this table, there is a section for "Available Run Book Policies [0]" which is currently empty, showing "No results to display."

Automation Policy Name	ID	Policy State	Organization	Devices	Events	Actions	Edited By	Last Edited
1. Linux SSH: Illicit Process Remediation	43	Enabled	System	1 group	1	2	em7admin	2025-01-07 19:01:55
2. Linux SSH: Process Restart Remediation	42	Enabled	System	1 group	2	2	em7admin	2025-01-07 19:01:55
3. Linux SSH: Run CPU Diagnostic Commands	39	Enabled	System	1 group	4	2	em7admin	2025-01-07 19:01:55
4. Linux SSH: Run File System Diagnostic Commands	40	Enabled	System	1 group	2	2	em7admin	2025-01-07 19:01:55
5. Linux SSH: Run Interface Error/Discard Diagnostic Commands	45	Enabled	System	1 group	50	2	em7admin	2025-01-07 19:01:55
6. Linux SSH: Run Interface Utilization Diagnostic Commands	44	Enabled	System	1 group	25	4	em7admin	2025-01-07 19:01:55
7. Linux SSH: Run Memory/Swap Diagnostic Commands	41	Enabled	System	1 group	5	4	em7admin	2025-01-07 19:01:55
8. Linux SSH: Run System-Storage Diagnostic Commands	46	Enabled	System	1 group	1	2	em7admin	2025-01-07 19:01:55

All automation policies are tied to SL1 events generated by:

- Dynamic Applications from the "Host Resources" PowerPack
- Dynamic Applications from the "Net-SNMP" PowerPack
- Dynamic Applications from the "Linux Base" PowerPack
- Interface collection
- File System Collection
- System Process Monitoring Policies

Several of the run book actions use the substitution character feature of the "Execute Shell Commands" custom action type. If an event variable is included in a command, such as %Y for the sub-entity name, the custom action type automatically replaces that variable with the value from the triggering event.

The following table shows the standard automation policies, their aligned events, and the run book actions that runs in response to the events.

**NOTE:** The aligned events are included as part of this PowerPack and are not installed with the SL1 platform. You must install the PowerPack to obtain these events.

Automation Policy Name	Aligned Device Group	Aligned Events	Aligned Run Book Actions
Linux SSH: Illicit Process Remediation	Linux Automation	<ul style="list-style-type: none"> <li>• Poller: Illicit process running</li> </ul>	<ul style="list-style-type: none"> <li>• Linux Illicit Process Remediation</li> <li>• Datacenter Automation: Format Output as HTML</li> </ul>
Linux SSH: Process Restart Remediation	Linux Automation	<ul style="list-style-type: none"> <li>• AKCP: DC Voltage sensor High Critical</li> <li>• Poller: required process not running</li> </ul>	<ul style="list-style-type: none"> <li>• Linux Process Restart Remediation</li> <li>• Datacenter Automation: Format Output as HTML</li> </ul>
Linux SSH: Run CPU Diagnostic Commands	Linux Automation	<ul style="list-style-type: none"> <li>• AKCP: DC Voltage sensor Low Critical</li> <li>• Linux SSH: CPU utilization has Exceeded Threshold</li> <li>• Host Resource: CPU has exceeded threshold</li> <li>• Net-SNMP: CPU has exceeded threshold</li> </ul>	<ul style="list-style-type: none"> <li>• Linux CPU Diagnostic Commands</li> <li>• Datacenter Automation: Format Output as HTML</li> </ul>
Linux SSH: Run File System Diagnostic Commands	Linux Automation	<ul style="list-style-type: none"> <li>• Poller: File system usage exceeded (critical) threshold</li> <li>• Poller: File system usage exceeded (major) threshold</li> </ul>	<ul style="list-style-type: none"> <li>• Linux File System Diagnostic Commands</li> <li>• Datacenter Automation: Format Output as HTML</li> </ul>
Linux SSH: Run Interface Error/Discard Diagnostic Commands	Linux Automation	<ul style="list-style-type: none"> <li>• Interface inbound discards has exceeded the Falling-High threshold</li> <li>• Interface inbound discards has exceeded the Rising-Low threshold</li> <li>• Interface inbound discards percentage has exceeded the Falling-High threshold</li> <li>• Interface inbound discards percentage has exceeded the Rising-High threshold</li> </ul>	<ul style="list-style-type: none"> <li>• Linux Interface Error/Discard Diagnostic Commands</li> <li>• Datacenter Automation: Format Output as HTML</li> </ul>



Automation Policy Name	Aligned Device Group	Aligned Events	Aligned Run Book Actions
		<ul style="list-style-type: none"> <li>• Interface inbound errors has exceeded the Falling-High threshold</li> <li>• Interface inbound errors has exceeded the Rising-High threshold</li> <li>• Interface inbound errors has exceeded Rising-Medium threshold</li> <li>• Interface inbound errors has exceeded the Falling-Low threshold</li> <li>• Interface inbound errors has exceeded the Falling-Medium threshold</li> <li>• Interface inbound errors has exceeded the Rising-Low threshold</li> <li>• Interface inbound discards has exceeded the Rising-Low threshold</li> <li>• Interface inbound discards has exceeded the Rising-Medium threshold</li> <li>• Interface inbound discards percentage has exceeded the Falling-Low threshold</li> <li>• Interface inbound discards percentage has exceeded the Falling-Medium threshold</li> <li>• Interface inbound discards percentage has exceeded the Rising-High threshold</li> <li>• Interface inbound discards percentage has exceeded the Rising-Low threshold</li> <li>• Interface inbound discards percentage has exceeded the Rising-Medium threshold</li> </ul>	

Automation Policy Name	Aligned Device Group	Aligned Events	Aligned Run Book Actions
		<ul style="list-style-type: none"> <li>• Interface outbound discards has exceeded the Falling-High threshold</li> <li>• Interface outbound discards has exceeded the Falling-Low threshold</li> <li>• Interface outbound discards has exceeded the Falling-Medium threshold</li> <li>• Interface outbound discards has exceeded the Rising-High threshold</li> <li>• Interface outbound discards has exceeded the Rising-Low threshold</li> <li>• Interface outbound discards has exceeded the Rising-Medium threshold</li> <li>• Interface outbound discards percentage has exceeded the Falling-High threshold</li> <li>• Interface outbound discards percentage has exceeded the Falling-Low threshold</li> <li>• Interface outbound discards percentage has exceeded the Falling-Medium threshold</li> <li>• Interface outbound discards percentage has exceeded the Rising-High threshold</li> <li>• Interface outbound discards percentage has exceeded the Rising-Low threshold</li> <li>• Interface outbound discards percentage has exceeded the Rising-Medium threshold</li> <li>• Interface inbound errors percentage has exceeded the Falling-High threshold</li> </ul>	

Automation Policy Name	Aligned Device Group	Aligned Events	Aligned Run Book Actions
		<ul style="list-style-type: none"> <li>• Interface inbound errors percentage has exceeded the Falling-Low threshold</li> <li>• Interface inbound errors percentage has exceeded the Falling-Medium threshold</li> <li>• Interface inbound errors percentage has exceeded the Rising-High threshold</li> <li>• Interface inbound errors percentage has exceeded the Rising-Low threshold</li> <li>• Interface inbound errors percentage has exceeded the Rising-Medium threshold</li> <li>• Interface outbound errors has exceeded the Falling-High threshold</li> <li>• Interface outbound errors has exceeded the Falling-Low threshold</li> <li>• Interface outbound errors has exceeded the Falling-Medium threshold</li> <li>• Interface outbound errors has exceeded the Rising-High threshold</li> <li>• Interface outbound errors has exceeded the Rising-Low threshold</li> <li>• Interface outbound errors has exceeded the Rising-Medium threshold</li> <li>• Interface outbound errors percentage has exceeded the Falling-High threshold</li> <li>• Interface outbound errors percentage has exceeded the Falling-Low threshold</li> </ul>	

Automation Policy Name	Aligned Device Group	Aligned Events	Aligned Run Book Actions
		<ul style="list-style-type: none"> <li>• Interface outbound errors percentage has exceeded the Falling-Medium threshold</li> <li>• Interface outbound errors percentage has exceeded the Rising-High threshold</li> <li>• Interface outbound errors percentage has exceeded the Rising-Low threshold</li> <li>• Interface outbound errors percentage has exceeded the Rising-Medium threshold</li> <li>• Poller: Interface reporting discards</li> <li>• Poller: Interface reporting packet errors</li> </ul>	
Linux SSH: Run Interface Utilization Diagnostic Commands	Linux Automation	<ul style="list-style-type: none"> <li>• Interface inbound usage percentage has exceeded the Falling-High threshold</li> <li>• Interface inbound usage percentage has exceeded the Rising-High threshold</li> <li>• Interface inbound usage percentage has exceeded the Falling-Low threshold</li> <li>• Interface inbound usage percentage has exceeded the Falling-Medium threshold</li> <li>• Interface inbound usage percentage has exceeded the Rising-Low threshold</li> <li>• Interface inbound usage percentage has exceeded the Rising-Medium threshold</li> <li>• Interface inbound usage rate has exceeded the Falling-High threshold</li> <li>• Interface inbound usage rate has exceeded the Falling-Low threshold</li> </ul>	<ul style="list-style-type: none"> <li>• Automation Utilities: Calculate Memory Size for Each Action (from the <i>Datacenter Automation Utilities</i> PowerPack)</li> <li>• Linux Interface Utilization Diagnostic Commands</li> <li>• Linux Tcpdump Command</li> <li>• Datacenter Automation: Format Output as HTML</li> </ul>

Automation Policy Name	Aligned Device Group	Aligned Events	Aligned Run Book Actions
		<ul style="list-style-type: none"> <li>• Interface inbound usage rate has exceeded the Falling-Medium threshold</li> <li>• Interface inbound usage rate has exceeded the Rising-High threshold</li> <li>• Interface inbound usage rate has exceeded the Rising-Low threshold</li> <li>• Interface inbound usage rate has exceeded the Rising-Medium threshold</li> <li>• Interface outbound usage percentage has exceeded the Falling-High threshold</li> <li>• Interface outbound usage percentage has exceeded the Falling-Low threshold</li> <li>• Interface outbound usage percentage has exceeded the Falling-Medium threshold</li> <li>• Interface outbound usage percentage has exceeded the Rising-High threshold</li> <li>• Interface outbound usage percentage has exceeded the Rising-Low threshold</li> <li>• Interface outbound usage percentage has exceeded the Rising-Medium threshold</li> <li>• Interface outbound usage rate has exceeded the Falling-High threshold</li> <li>• Interface outbound usage rate has exceeded the Falling-Low threshold</li> <li>• Interface outbound usage rate has exceeded the Falling-Medium threshold</li> <li>• Interface outbound usage rate has exceeded the Rising-High threshold</li> </ul>	

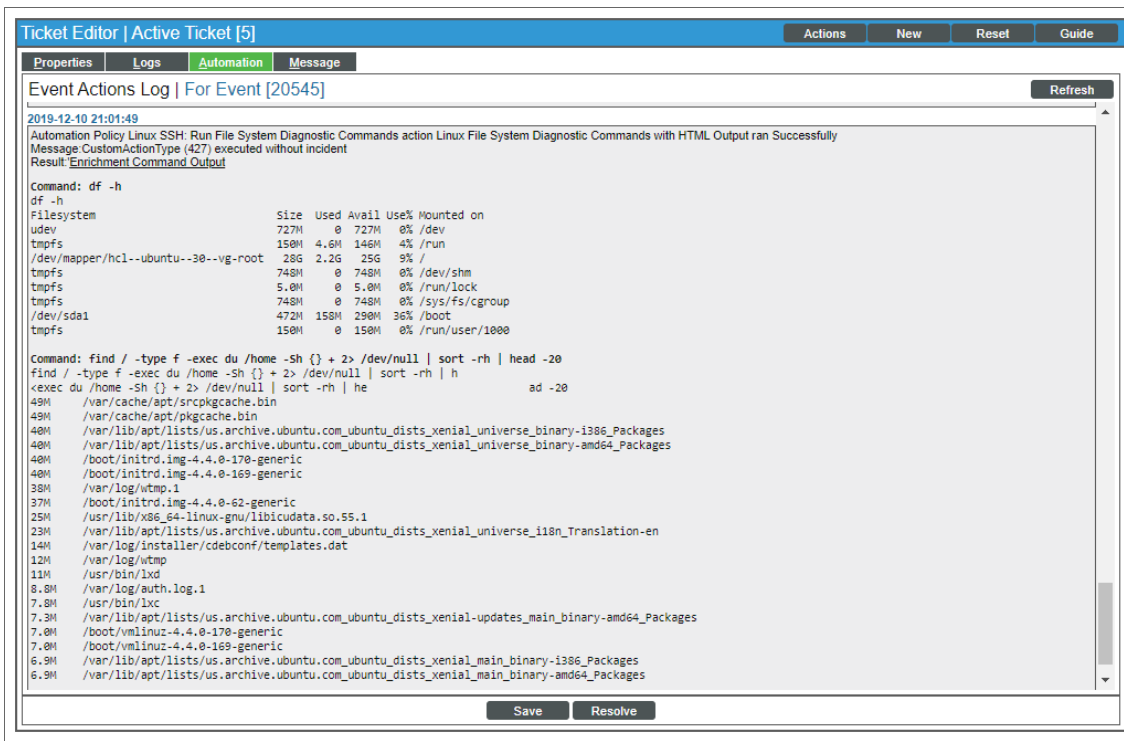
Automation Policy Name	Aligned Device Group	Aligned Events	Aligned Run Book Actions
		<ul style="list-style-type: none"> <li>Interface outbound usage rate has exceeded the Rising-Low threshold</li> <li>Interface outbound usage rate has exceeded the Rising-Medium threshold</li> </ul>	
Linux SSH: Run Memory/Swap Diagnostic Commands	Linux Automation	<ul style="list-style-type: none"> <li>Host Resource: Swap Memory has exceeded threshold</li> <li>Linux SSH: Swap usage has Exceeded Threshold</li> <li>Net-SNMP: Swap has exceeded threshold</li> <li>Host Resource: Physical Memory has exceeded threshold</li> <li>Net-SNMP: Physical Memory exceeded threshold</li> </ul>	<ul style="list-style-type: none"> <li>Automation Utilities: Calculate Memory Size for Each Action (from the "Datacenter Automation Utilities" PowerPack)</li> <li>Linux Memory/Swap Diagnostic Commands</li> <li>Linux Memory Dmidecode Command</li> <li>Datacenter Automation: Format Output as HTML</li> </ul>
Linux SSH: Run System-Storage Diagnostic Commands	Linux Automation	<ul style="list-style-type: none"> <li>Linux SSH: File System over usage threshold</li> </ul>	<ul style="list-style-type: none"> <li>Linux System-Storage Diagnostic Commands</li> <li>Datacenter Automation: Format Output as HTML</li> </ul>

The following figure shows a file system usage threshold exceeded event with a Severity of Major on the **Events** page. Click the **[Actions]** button (⋮) for an event and select *View Automation Actions* to see the run book actions triggered by the events.

The screenshot shows the ScienceLogic Events page. At the top, there are filters for severity levels: 1 Critical, 19 Major, 7 Minor, 0 Notice, and 2 Healthy. A search bar contains 'ANY: linux'. Below is a table of events with columns for Organization, Severity, Name, Message, Age, Ticket ID, CO, Event No., Masked Events, Acknowledge, and Clear. The third event is highlighted in grey. Its actions menu is open, showing options like 'View Event', 'Edit Event Note', 'Create External Ticket', 'Align External Ticket', 'View Automation Actions' (highlighted with a red box), 'View Event Policy', and 'Suppress Event for this Device'.

ORGANIZATION	SEVERIT...	NAME	MESSAGE	AGE	TICKET I...	CO...	EVENT NO...	MASKED EVENTS	ACKNOWLEDGE	CLEAR
System	Major	ec2-18-217-1	Linux File System /dev/loop1 : /sn...	12 days 1			3172	Masked	Acknowledge	Clear
Linux Devices	Major	10.2.24.31	Linux File System /dev/mapper/ce...	12 days 1			3179	Masked	Acknowledge	Clear
Linux Devices	Major	10.2.24.30	/: File system usage exceeded maj...	6 days 18   5			647		Acknowledge	Clear
System	Major	ec2-18-217-1	Linux File System /dev/loop0 : /sn...	6 days			1546			
Linux Devices	Minor	10.2.24.30	App: 1551, Snippet: 1939 reporte...	1 hour 49			3			
Linux Devices	Health	10.2.24.30	Network Latency below threshold	6 minutes			1			

The results shown for this event, in the **Event Actions Log**, include the automation policy that ran (shown at the top of the following figure), along with the run book actions (commands) that ran. 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 run book action, see [Configuring Linux SSH Run Book 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.

## User-initiated Automation Policies

All Linux SSH automation policies have a **Policy Type** of *Active Events/User Initiated*, which enables all of the features of the "Active Events" and the "User Initiated" policy types. As a result, these automation policies can be triggered by active events that meet the criteria in the policy, or you can manually trigger the automation.

You can run these automation policies as needed from the **Devices** page, the **Events** page, and the **Service Investigator** page. If there is an event policy specified in the automation policy, that event must be active for the policy to be run manually, and the policy can only be run on that event type. The same applies for the device groups list.

For these automation policies to be visible from the **Tools** panel in the **Device Summary** modal, the following three bullets must be true between the event and the automation policy configuration:



- **Organization.** The organization associated with the event must match the organization configured in the automation policy. Policies in the "System" organization match all organizations.
- **Aligned Devices.** The device for which the event is triggered must be configured as an Aligned Device in the automation policy.
- **Aligned Event.** The event must match one of the Aligned Events configured in the automation policy.

In most situations, you would run a user-initiated automation in response to an event that just occurred. If you have Automation PowerPacks installed on your SL1 system, the **Event Actions Log** window for that event might contain diagnostic information from other automations that have already run, including information that helps you determine which user-initiated automation you should run next to address the cause of the event.

To run a user-initiated automation policy, click the open icon (↗) to open the **Device Summary** modal for the event and click in the **Tools** section. Any available user-initiated automation policy will be listed there, available to run on-demand.

---

## Creating and Customizing Automation Policies

You can use the default run book automation policies in this PowerPack, or you can create and customize the policies as needed.

**TIP:** You might need to configure a run book action policy before you can add it to the automation policy. For more information, see [Customizing Linux SSH Run Book Actions](#).

### Prerequisites

Before you create an automation policy using the run book actions in the "Linux SSH Automations" PowerPack, you must determine:

- Which set of commands you want to run on a monitored device when an event occurs. The run book actions in this PowerPack can run the "Execute Shell Commands" action type with different commands and output formats. You can also create your own run book actions using the custom action type supplied in the PowerPack.
- What event criteria you want to use to determine when the run book 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 the automation policies, see the **Run Book Automation** manual.

### Creating or Customizing an Automation Policy

**IMPORTANT:** In this PowerPack, the automation policies are disabled by default, so at the minimum you will need to set the **Policy State** to *Enabled* before you can run a policy.

To create or customize an automation policy that uses the run book actions in the "Linux SSH Automations" PowerPack:

1. Go to the **Automation Policy Manager** page (Registry > Run Book > Automation).
2. Click the **[Create]** button to create an automation policy, or search for an existing automation policy that you want to edit and click the wrench icon (🔧) for that policy. The **Automation Policy Editor** page appears:

3. Complete the following 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*. The default is *Disabled*.
  - **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 "Linux Automation" device group needs to be aligned. To add the device group to the **Aligned Device Groups** field, select the "Linux Automation" device group in the **Available Device Groups** field and click the right arrow (> >).
- **Aligned Actions.** This field includes the actions from the "Linux SSH Automations" 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 multiple collection actions that use the "Execute Shell Commands" action type, you may want to include the "Calculate Memory Size for Each Action" run book 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]** for a new policy, or click **[Save As]** if you are customizing an existing policy. If you modify one of the included automation policies and save it with the original name, any customizations you made to that policy will be overwritten when you upgrade the PowerPack.

## Removing an Automation Policy from a PowerPack

If you have customized an automation policy from the 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 "Linux SSH 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.

## Customizing Linux SSH Run Book Actions

---

### Overview

This chapter describes how to customize the run book actions embedded in the "Linux SSH Automations" PowerPack to create run book actions to meet your organization's specific requirements.

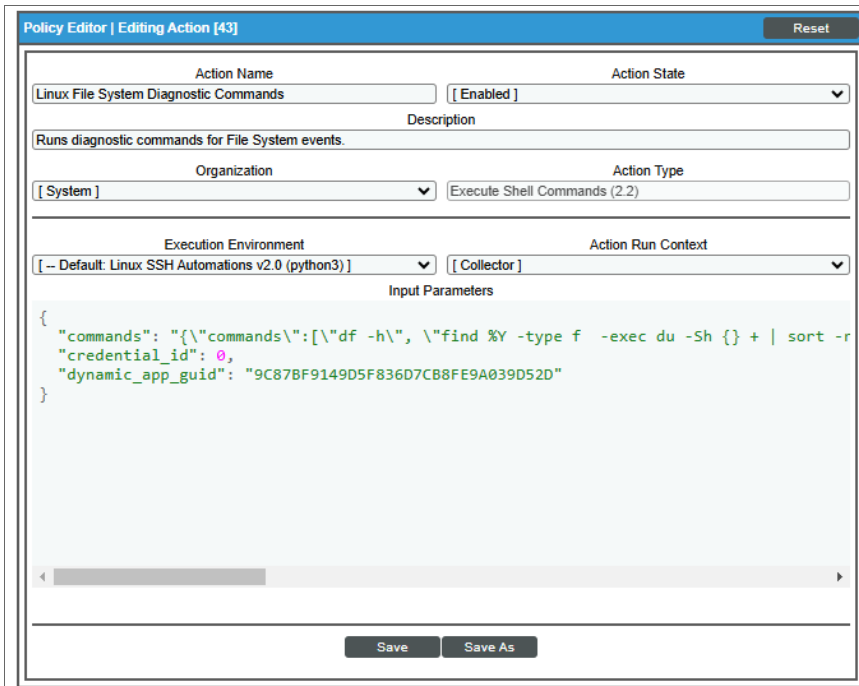
This chapter covers the following topics:

<i>Linux SSH Run Book Actions</i> .....	21
<i>Creating a Custom Run Book Action Policy</i> .....	23
<i>Configuring Linux Devices</i> .....	25
<i>Configuring Device Credentials</i> .....	25

# Linux SSH Run Book Actions

The "Linux SSH Automations" PowerPack includes run book actions that use the "Execute Shell Commands" action type to retrieve diagnostic information or remediate an issue.

In the **Input Parameters** field for the "Execute Shell Commands" action type, you can specify the list of commands to run and their individual options. These can include the ID of an SSH/Key credential to use. The credential itself can have a specific host assigned to it, but a common configuration is for the action to run on the device or host where the triggering event occurred.



The following run book actions that use the "Execute Shell Commands" action type are included in the "Linux SSH Automations" PowerPack. For more information about the input parameter fields, see the table in [Creating a Linux SSH Run Book Action](#).

Action Name	Description	Commands Run
Linux CPU Diagnostic Commands	Runs diagnostic commands for CPU events.	<ul style="list-style-type: none"> <li>top -b -n 1</li> <li>ps -eo pid,ppid,%cpu,%mem,args --sort=-%cpu   head</li> <li>pidstat</li> <li>iostat -x 2 5</li> <li>dmesg   tail</li> </ul>
Linux File System Diagnostic Commands	Runs diagnostic commands for File System events.	<ul style="list-style-type: none"> <li>df -h</li> </ul>

Action Name	Description	Commands Run
		<ul style="list-style-type: none"> <li><code>find / -type f -exec du /home -Sh {} + 2&gt; /dev/null   sort -rh   head -20</code></li> </ul>
Linux Illicit Process Remediation	Collects a list of users logged in to the system and sends a term signal to a Linux process.	<ul style="list-style-type: none"> <li><code>sudo -S who</code></li> <li><code>sudo -S kill %y</code></li> </ul>
Linux Interface Error/Discard Diagnostic Commands	Runs diagnostic commands for Interface Error/Discard events.	<ul style="list-style-type: none"> <li><code>ifconfig</code></li> <li><code>ethtool %Y</code></li> <li><code>dmesg   tail</code></li> <li><code>netstat -i</code></li> </ul>
Linux Interface Utilization Diagnostic Commands	Runs diagnostic commands for Interface Utilization events.	<ul style="list-style-type: none"> <li><code>ethtool %Y</code></li> <li><code>netstat -plunt</code></li> <li><code>tcpdump -i %Y -c 100</code></li> </ul>
Linux Memory Dmidecode Command	Runs the <code>dmidecode</code> command with the memory option using sudo.	<ul style="list-style-type: none"> <li><code>sudo -S dmidecode --type memory</code></li> </ul>
Linux Memory/Swap Diagnostic Commands	Runs diagnostic commands for Memory/Swap events.	<ul style="list-style-type: none"> <li><code>top -b -n 1</code></li> <li><code>ps -eo pid,ppid,%cpu,%mem,args --sort=-%mem   head</code></li> <li><code>swapon -summary</code></li> <li><code>vmstat 2 5</code></li> <li><code>dmidecode --type memory</code></li> <li><code>dmesg   tail</code></li> </ul>
Linux Process Restart Remediation	Restarts a Linux service and collects service status before and after the restart command.	<ul style="list-style-type: none"> <li><code>sudo -S service %Y status</code></li> <li><code>sudo -S service %Y start</code></li> <li><code>sudo -S service %Y status</code></li> </ul>
Linux System-Storage Diagnostic Commands	Runs diagnostic commands for File System events.	<ul style="list-style-type: none"> <li><code>df -h</code></li> <li><code>find / -type f -exec du -Sh {} +   sort -rh   head -n 20</code></li> <li><code>find / -type f -mmin -10 -exec du -Sh {} +   sort -rh   head -n 20</code></li> </ul>

Action Name	Description	Commands Run
		<ul style="list-style-type: none"> <li><code>find / -type d -exec du -Sh {} +   sort -rh   head -n 20</code></li> <li><code>find / -type d -mmin -10 -exec du -Sh {} +   sort -rh   head -n 20</code></li> </ul>
Linux Tcpdump Command	Runs the tcpdump command using sudo.	<ul style="list-style-type: none"> <li><code>sudo -S tcpdump -i %Y -c 100</code></li> </ul>

## Creating a Custom Run Book Action Policy

You can use the "Execute Shell Commands" action type included with the "Linux SSH Automations" PowerPack to create custom run book actions that you can then use to build custom automation policies.

To create a custom action policy using the "Execute Shell Commands (2.2)" action type:

1. Go to the **Action Policy Manager** page (Registry > Run Book > Actions).
2. Click the **[Create]** button. The **Action Editor** page appears.
3. 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 "Execute Shell Commands (2.2)" action type.
  - **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 input parameter fields, see the table in [Creating a Linux SSH Run Book Action](#).
4. 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.

## Creating a Linux SSH Run Book Action

You can create a new run book action that runs SSH commands using the "Execute Shell Commands" custom action type. To do this, select "Execute Shell Commands (2.2)" in the **Action Type** drop-down list when you create a new run book action.

You can also use the existing run book actions in this PowerPack as a template by using the **[Save As]** option.

The Linux SSH run book actions accept the following parameters in JSON:

Parameter	Input type	Description
<code>commands</code>	string	<p>Specifies a single command or a list of commands, in JSON format, to execute. You can use substitution variables in the commands.</p> <p>Example:</p> <pre>"commands": "{ \"commands\": [\"top -b -n 1\", \"ps -eo pid,ppid,%cpu,%mem,args --sort=-%cpu   head\", \"pidstat\", \"iostat -x 2 5\", \"dmesg   tail\"] }",</pre> <p>ScienceLogic recommends that you make a copy of a run book action with the "Save As" button, and then rename the copy if you are modifying the list of commands in an existing run book action.</p>
<code>credential_id</code>	integer	<p><b>Default value:</b> 0</p> <p>Specifies the <code>credential_id</code> to use for the connection.</p> <ul style="list-style-type: none"> <li>If set to <code>"credential_id": 0</code> (false), the custom action type will dynamically determine the credential from specific "Linux Base Pack" Dynamic Applications that are aligned to the device. For more information, see <a href="#">Configuring Device Credentials</a>.</li> <li>If set to an ID number, it maps to the credential ID specified. You can find credential IDs by going to the <b>Credentials</b> page (Manage &gt; Credentials).</li> </ul> <p><b>Example:</b> <code>"credential_id": 11</code></p>
<code>dynamic_app_guid</code>	string	<p><b>Default value:</b> The default value for this parameter corresponds to the globally unique ID number (GUID) value in the "Linux: Configuration Discovery" Dynamic Application.</p> <p>Specifies the GUID assigned to the Dynamic Application by SL1. You can specify multiple Dynamic Application IDs, separated by commas.</p> <p>If the <code>credential_id</code> parameter is not specified, SL1 will use the <code>dynamic_app_guid</code> parameter to determine the credential. If this value is not specified, or if it is an empty string, SL1 runs a query against the database to get the credential details.</p>

**Using Substitution Values.** The commands input can contain substitution values that match the keys in EM7\_VALUES.

**TIP:** For more information about substitution variables, see [Appendix A](#).

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



---

## Configuring Linux Devices

If you have run book actions that use `sudo` in their commands, you will need to set up your user with passwordless sudo access on the Linux device being monitored.

For example, if your user is `em7admin`:

1. SSH to the Linux device.
2. Use the following format to create a new file for your user:

```
/etc/sudoers.d/<username>-user
```

For example:

```
sudo vi /etc/sudoers.d/em7admin-user
```

3. Add the following setting to the new file from step 2:

```
<username> ALL=(ALL) NOPASSWD:ALL
```

For example:

```
em7admin ALL=(ALL) NOPASSWD:ALL
```

4. Save the new file. New SSH logins will not ask for the sudo password, and the command and run books automations will run successfully.

---

## Configuring Device Credentials

The "Execute Shell Commands" custom action type supports hard-coded credentials, where you specify the ID of a credential in the run book action. Alternately, the custom action type can dynamically determine the credential to use.

By default, the run book actions use the dynamic method by specifying credential ID 0 in the **Input Parameters** section. The dynamic method uses the first credential that matches the following rules:

- If the "Linux: Configuration Discovery" Dynamic Application from the "Linux Base Pack" PowerPack is aligned to the device associated with the triggering event, the credential aligned to that Dynamic Application is used.
- If none of the Dynamic Application GUIDs provided in the `dynamic_app_guid` list are aligned to the device associated with the triggering event, the first available SSH/Key credential aligned to the device as a secondary credential is used.

**NOTE:** An SSH key is not required for an SSH/Key credential to work, and using a user/password pair in the credential is sufficient. You can set up the SSH key to suit your specific security requirements if needed.

## Creating an SSH/Key Credential

**NOTE:** If you already have the "Linux Base Pack" PowerPack installed and monitoring your Linux devices, you do not need to configure an additional credential.

If you do not have the "Linux Base Pack" PowerPack installed, you must create an SSH credential that includes the username and password, or username and private key, combination to communicate with your Linux devices.

To create a credential:

1. Go to the **Credentials** page (Manage > Credentials).
2. Click **[Create New]** and select *SSH/Key credential*. The **Create New SSH/Key Credential** page appears.
3. Supply values in the following fields:
  - **Name**. Enter a name for the credential.
  - **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 **Select the organizations** drop-down field to align the credential with those specific organizations. This field is required.
  - **Timeout(ms)**. Enter a timeout, in milliseconds, for the connection.
  - **Hostname/IP**. Hostname or IP address of the device from which you want to retrieve data.
    - 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**. To use SSH to connect to the device, enter "22" in this field.
  - **Username**. Enter the username for an SSH user or user account on the device to be monitored.
  - **Password**. Enter the password for the user you entered in the **Username** field.
  - **Private Key (PEM Format)**. Enter the SSH private key that you want SL1 to use, in PEM format.
4. Click **[Save & Close]**.

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

---

# Appendix

# A



## Run Book Variables

---

### Overview

This appendix defines the different variables you can use when creating an action policy.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon ().
- To view a page containing all of the menu options, click the Advanced menu icon (  ).

This appendix covers the following topics:

This chapter covers the following topics:

<i>Run Book Variables</i> .....	28
---------------------------------	----

## Run Book Variables

You can include variables when creating an action policy. These variables are listed in the table below.

- In an action policy of type **Send an Email Notification**, you can include one or more of these variables in the fields **Email Subject** and **Email Body**.
- In an action policy of type **Send an SNMP Trap**, you can include one or more of these variables in the **Trap OID** field, **Varbind OID** field, and the **Varbind Value** field.
- In an action policy of type **Create a New Ticket**, you can include one or more of these variables in the **Description** field or the **Note** field of the related Ticket Template.
- In an action policy of type **Send an SNMP Set**, you can include one or more of these variables in the **SNMP OID** field and the **SNMP Value** field.
- In an action policy of type **Run A Snippet**, you can access variables from the global dictionary **EM7\_VALUES**.
- In a policy of type **Execute an SQL Query**, you can include one or more of these variables in the **SQL Query** field.

Variable	Source	Description
%A	Account	Username
%a	Entity	IP address
%F	Dynamic Alert	Alert ID for a Dynamic Application Alert
%g	Asset	Asset serial
%h	Asset	Device ID associated with the asset
%l (uppercase "eye")	Dynamic Alert	For events with a source of "dynamic", this variable contains the index value from SNMP. For events with a source of "syslog" or "trap", this variable contains the value that matches the <b>Identifier Pattern</b> field in the event definition.
%i (lowercase "eye")	Asset	Asset Location
%K	Asset	Asset Floor
%k	Asset	Asset Room
%L	Dynamic Alert	Value returned by the label variable in a Dynamic Application Alert.
%m	Automation	Automation policy note
%N	Action	Automation action name
%n	Automation	Automation policy name
%P	Asset	Asset plate
%p	Asset	Asset panel
%Q	Asset	Asset punch
%q	Asset	Asset zone
%T	Dynamic Alert	Value returned by the Threshold function in a Dynamic Application Alert.

Variable	Source	Description
%U	Asset	Asset rack
%u	Asset	Asset shelf
%v	Asset	Asset tag
%W	Asset	Asset make
%w	Asset	Asset model
%V	Dynamic Alert	Value returned by the Result function in a Dynamic Application Alert.
_%category_id	Entity	Device category ID associated with the entity in the event.
_%category_name	Entity	Device category name associated with the entity in the event.
_%class_id	Entity	Device class ID associated with the entity in the event.
_%class_name	Entity	Device class description associated with the entity in the event.
_%parent_id	Entity	For component devices, the device ID of the parent device.
_%parent_name	Entity	For component devices, the name of the parent device.
_%root_id	Entity	For component devices, the device ID of the root device.
_%root_name	Entity	For component devices, the name of the root device.
_%service_investigator_url	Entity	The URL of the Business Service Investigator page for the event that triggered the automation (for run book actions that run against events aligned with business services).
%1 (one)	Event	Entity type. Possible values are: <ul style="list-style-type: none"> <li>• 0. Organization</li> <li>• 1. Device</li> <li>• 2. Asset</li> <li>• 4. IP Network</li> <li>• 5. Interface</li> <li>• 6. Vendor</li> <li>• 7. Account</li> <li>• 8. Virtual Interface</li> <li>• 9. Device Group</li> <li>• 10. IT Service</li> <li>• 11. Ticket</li> </ul>
%2	Event	Sub-entity type. <p>Possible values for organizations are:</p> <ul style="list-style-type: none"> <li>• 9. News feed</li> </ul> <p>Possible values for devices are:</p>

Variable	Source	Description
		<ul style="list-style-type: none"> <li>• 1. CPU</li> <li>• 2. Disk</li> <li>• 3. File System</li> <li>• 4. Memory</li> <li>• 5. Swap</li> <li>• 6. Component</li> <li>• 7. Interface</li> <li>• 9. Process</li> <li>• 10. Port</li> <li>• 11. Service</li> <li>• 12. Content</li> <li>• 13. Email</li> </ul>
%4	Event	Text string of the user name that cleared the event.
%5	Event	Date/time when event was deleted.
%6	Event	Date/time when event became active.
%7	Event	<p>Event severity (1-5), for compatibility with previous versions of SL1 . 1 =critical, 2=major, 3=minor, 4=notify, 5=healthy.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>NOTE:</b> When referring to an event, %7 represents severity (for previous versions of SL1). When referring to a ticket, %7 represents the subject line of an email used to create a ticket.</p> </div>
%c	Event	Event counter
%d	Event	Date/time when last event occurred.
%D	Event	Date/time of first event occurrence.
%e	Event	Event ID
%H	Event	URL link to event
%M	Event	Event message
%s	Event	severity (0 - 4). 0=healthy, 1=notify, 2=minor, 3=major, 4=critical.
%S	Event	Severity (HEALTHY - CRITICAL)
%_user_note	Event	Current note about the event that is displayed on the <b>Events</b> page.
%x	Event	Entity ID
%X	Event	Entity name
%y	Event	Sub-entity ID
%Y	Event	Sub-entity name
%Z	Event	Event source (Syslog - Group)

Variable	Source	Description
%z	Event	Event source (1 - 8)
%_ext_ticket_ref	Event	For events associated with an external Ticket ID, this variable contains the external Ticket ID.
%3	Event Policy	Event policy ID
%E	Event Policy	External ID from event policy
%f	Event Policy	Specifies whether event is stateful, that is, has an associated event that will clear the current event. 1 (one)=stateful; 0 (zero)=not stateful.
%G	Event Policy	External Category
%R	Event Policy	Event policy cause/action text
%_event_policy_name	Event Policy	Name of the event policy that triggered the event.
%B	Organization	Organization billing ID
%b	Organization	Impacted organization
%C	Organization	Organization CRM ID
%o (lowercase "oh")	Organization	Organization ID
%O (uppercase "oh")	Organization	Organization name
%r	System	Unique ID / name for the current SL1 system
%7	Ticket	Subject of email used to create a ticket. If you specify this variable in a ticket template, SL1 will use the subject line of the email in the ticket description or note text when SL1 creates the ticket.  <b>NOTE:</b> When referring to a ticket, %7 represents the subject line of an Email used to create a ticket. When referring to an event, %7 represents severity (for previous versions of SL1).
%t	Ticket	Ticket ID
%J	Ticket	Description field from the SL1 ticket.

© 2003 - 2025, 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](mailto:legal@sciencelogic.com). For more information, see <https://sciencelogic.com/company/legal>.



ScienceLogic

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

International: +1-703-354-1010