Case Management V6 SmartResponse Plugin Guide

September 20, 2021

Introduction

This guide describes the Case SRP V6 SmartResponse Plugin (Case Management), the plugin's available actions, and how to configure the plugin. This plugin uses LogRhythm's Case API to run a variety of Case related actions, including adding Playbooks and collaborators and creating or finding Cases.

Plugin Version History

Version	Release Date	Improvements
V1	January 31, 2018	Initial release
V2	June 29, 2018	Added certification for plugin
V3	March 22, 2019	Bug fix for Add Playbook to Case action
V4	April 26, 2019	Add Create Case Configuration File and Add Collaborators to Case actions
V5	February 5, 2020 (revA) February 7, 2020 (revB)	• Added Add Tags to Case action, along with new functionality in Create a New Case and Add to Existing Case actions • Updated procedure for API token generation in LogRhythm 7.4.9 and later
V5.1	October 22, 2020	Change default value of port number from 8505 to 8501
V6	TBD	Updated to perform multiple case management activities within a single defined action.

Prerequisites

- This SmartResponse Plugin is compatible with LogRhythm Enterprise 7.6.0 and later.
- To use this plugin, you must be running PowerShell v5.1 or later. To determine your PowerShell version, open PowerShell and enter $PSVersionTable.PSVersion at the prompt. If necessary, download a new version from the Microsoft Download Center.

- The PowerShell execution policy on the host where the SmartResponse plugin will be executed must allow the execution of scripts. Set this policy to either RemoteSigned or Unrestricted.
- This plugin requires access to the internet.

Import the Plugin

To import a SmartResponse Plugin:

1. Log in to the Client Console as a Global Administrator.
2. On the main toolbar, click Deployment Manager.
3. On the Tools menu, click Administration, and then click SmartResponse Plugin Manager. The SmartResponse Plugin Manager window appears.
4. On the Actions menu, click Import.
5. Locate and select the SmartResponse Plugin (.lpi file) that you want to import, and then click Open.
6. If you are prompted to accept the terms of the Sample Code License Agreement, read and accept the terms, and then click OK.
   The plugin loads in the SmartResponse Plugin Manager, and the associated actions are now available in the Actions tab of LogRhythm AI Engine Rules and Web Console Inspector.

   > For more information about SmartResponse actions or manual execution from the Client Console, see the LogRhythm Documentation site.

Create the Configuration File

The Case Management SmartResponse Plugin includes a configuration file with fixed-value parameters that store information, such as API key, that does not change frequently and is required for all other plugin actions. This allows you to perform multiple plugin actions without having to enter the same credentials for each one.

> You must execute the Create Config File action before using the plugin's other actions and rerun it whenever the fixed-value parameters change.

Run the Plugin from the Web Console

1. Log in to the LogRhythm Web Console, and then click Dashboards.
2. In the lower-right corner of the screen, click the Logs tab.
3. Click a log entry, and then click the gear symbol that appears in any column. The Inspector panel appears at the right side of the screen.

4. Scroll to the Smart Response section of the Inspector panel.
5. From the Plugin menu, select Case SRP V6.
6. From the Action menu, select Create Case Configuration File.
   For more information on other plugin actions, see SmartResponse Plugin Actions.
7. Configure the following parameters:

Name	Type	Details	Required
IP/Hostname/URL	String	System where the LogRhythm API Gateway is hosted (typically the Platform Manager or Web Console machine).	Yes
Port	String	Port on which the Case API runs. The default value is 8501. For LRCloud set this value to 443.	No
Output Path	String	File path where the plugin creates a folder containing the Case ID for each Alarm. This folder also contains log errors, warnings, and other information. The default value is C:\Program Files\LogRhythm\LogRhythm Alarming and Response Manager\SRP-Case. Do not include a trailing slash ("\") at the end of the file path.	No
Case API Key	String	LogRhythm Case API key obtained from a service account in the LogRhythm Client Console. For more information, see Generate an API Token.	Yes

8. From the Execute from menu, select whether to run this plugin from either the Platform Manager or a designated Agent.
9. Click Run.
   The SRP results open in a new tab.

SmartResponse Plugin Actions

Each SmartResponse Plugin has one or more actions. This plugin contains the following actions:

- Create Case Configuration File
- Create Case: Always Create New
- Create Case: Associate Existing or Create
- Add Alarm to Case
- Add Tags to Case
- Add Playbooks
- Add Collaborators to Case

Create Case: Always Create New

Description

This action creates a new Case and performs the following: can assign default case priority, update the case priority based on Alarm risk, assign case owner, assign case collaborators, assign playbooks, set case summary, define group-by fields 1-3, set group-by field tag prefix, create tags, define tag schema, add a case note, add an alarm summary, add threat intelligence summary, add alarm to case, and add alarm drilldown logs to case as evidence.

Use Case

This action has been designed to be assigned to an AIE rule to facilitate consistent behavior for creating a new case. This behavior has not been designed to support manual execution but can be applied and ran manually as needed. This action performs no method of case association and will always generate a new case upon execution.

Parameters

This action expects the following parameters to be configured in the Actions tab of an Alarm.

Name	Type	Details	Required
Alarm Id	String	Alarm ID of the Alarm being added to the Case.	Yes
Alarm Rule Name	String	Alarm Rule Name to be used as the default Case Name and to find Cases containing Alarms with the same name.	Yes
Default Priority (1-5)	String	Initial case priority (1-5).	Yes
Dynamic Priority (Alarm Risk -> Case Priority)	String	Sets the case priority based on the Alarm's risk score. For additional details reference Appendix 1 – Dynamic Priority.	No
Owner	String	Person Display Name or ID. To find a Person ID, in the LogRhythm Client Console, click Deployment Manager, click the People tab, click the user you want to add, and then scroll right to find the Person ID column. The owner is automatically added as a collaborator.	No
Collaborator(s)	String	Option 1: Notification Group Name • Assigns all individual person records assigned to a LogRhythm Notification Group as a case collaborator. Option 2: Pipe delimited • Person Display Names to be added as collaborators to a case. ○ user1, example|user2, example|user3	No

		• Person ID Numbers to be added as collaborators to a case. ○ 22|33|16 To find a Person Name in the LogRhythm Client Console, click Deployment Manager, click the People tab, click the user you want to add, and then copy the Person Name from Name tab.	
Playbook(s)	String	Pipe delimited list of Playbook Names or Playbook GUIDs. • Name: SOC Basic 1|Phishing • GUID: 510C7D5B-F058-4748-A948-233FAECB8348|6D980445-F31D-4FF6-AC67-2F0D992C8D4E	No
Case Summary	String	User defined static case summary to be populated on case creation.	No
Group-by 1: Metadata Field	String	If populated, this parameter defines the created Case's name and optionally can be applied as a Case Tag. If enabled as a Case Tag the Group-by field can be applied in the Case Lookup function of the Case Management SmartResponse plugin.	No
Group-by 1: Enable Tag	String	When set to true defines the Group-by 1 Metadata Field value will be established as a tag on the case.	No
Group-by 1: Tag Prefix	String	Applies a user defined prefix before the Metadata Field value. Example: ○ Metadata Field Value: adm_user1 ○ Enable Tag: true ○ Tag Prefix: user_login- ○ Tag Result: user_login-adm_user1	No
Group-by 2: Metadata Field	String	If populated, this parameter defines the created Case's name and optionally can be applied as a Case Tag. If enabled as a Case Tag the Group-by field can be applied in the Case Lookup function of the Case Management SmartResponse plugin.	No
Group-by 2: Enable Tag	String	When set to true defines the Group-by 2 Metadata Field value will be established as a tag on the case.	No
Group-by 2: Tag Prefix	String	Applies a user defined prefix before the Metadata Field value. Example: ○ Metadata Field Value: win32calc.exe ○ Enable Tag: true ○ Tag Prefix: process-	No

		○ Tag Result: user_login-adm_user1	
Group-by 3: Metadata Field	String	If populated, this parameter defines the created Case's name and optionally can be applied as a Case Tag. If enabled as a Case Tag the Group-by field can be applied in the Case Lookup function of the Case Management SmartResponse plugin.	No
Group-by 3: Enable Tag	String	When set to true defines the Group-by 3 Metadata Field value will be established as a tag on the case.	No
Group-by 3: Tag Prefix	String	Applies a user defined prefix before the Metadata Field value. Example: ○ Metadata Field Value: usample@exampl.com ○ Enable Tag: true ○ Tag Prefix: sender-usample@exampl.com ○ Tag Result: sender-usample@exampl.com	No
Tagging: Static Tag(s)	String	Pipe-separated tag names to be added to the case. Example: ○ CaseSRPv6|Automation|TECH_UnauthorizedAccess	No
Tagging: Schema	String	Sets the default character case for tags created through this plugin. Can be set to Lower or Upper. Default: Lower	No
Case Enrichment: Static Note	String	Adds a user defined note to the case. The note must be a single consistent string. To apply new lines, add \r\n to add new lines. Example: Input: This note will be added into the case.\r\nThis note will be added only once when the case has been created. Output: This note will be added into the case. This note will be added only once when the case has been created.	No
Case Enrichment: Enable Alarm Summary	String	Adds an alarm summary note to the case.	No
Case Enrichment: Threat Intelligence	String	Adds a Threat Intelligence lookup note to the case.	No

Create Case: Associate Existing or Create

Description

This action performs a case lookup service in attempt to identify a matching existing case for the triggering alarm. In the event an existing case has been identified matching the lookup criteria the triggering alarm will be appended into the case.

When creating a new case, the SmartResponse action can assign default case priority, update the case priority based on Alarm risk, assign case owner, assign case collaborators, assign playbooks, set case summary, define group-by fields 1-3, set group-by field tag prefix, create tags, define tag schema, add a case note, add an alarm summary, add threat intelligence summary, add alarm to case, and add alarm drilldown logs to case as evidence.

When updating an existing case, the SmartResponse can update case priority based on Alarm risk, define group-by fields 1-3, set group-by field tag prefix, append new tags, add an alarm summary, add threat intelligence summary, add alarm to case, and add alarm drilldown logs to case as evidence.

Use Case

This action has been designed to be assigned to an AIE rule to facilitate consistent behavior for creating and associating LogRhythm Alarm's to Cases. This behavior has not been designed to support manual execution but can be applied and ran manually as needed.

Parameters

This action expects the following parameters to be configured in the Actions tab of an Alarm.

Name	Type	Details	Required
Alarm Id	String	Alarm ID of the Alarm being added to the Case.	Yes
Alarm Rule Name	String	Alarm Rule Name to be used as the default Case Name and to find Cases containing Alarms with the same name.	Yes
Default Priority (1-5)	String	Initial case priority (1-5).	Yes
Dynamic Priority (Alarm Risk -> Case Priority)	String	Sets the case priority based on the Alarm's risk score. For additional details reference Appendix 1 – Dynamic Priority.	No
Owner	String	Person Display Name or ID. To find a Person ID, in the LogRhythm Client Console, click Deployment Manager, click the People tab, click the user you want to add, and then scroll right to find the Person ID column. The owner is automatically added as a collaborator.	No

Collaborator(s)	String	Option 1: Notification Group Name
		• Assigns all individual person records assigned to a LogRhythm Notification Group as a case collaborator.
		
		Option 2: Pipe delimited
		• Person Display Names to be added as collaborators to a case.
		  ○ user1, example|user2, example|user3
		• Person ID Numbers to be added as collaborators to a case.
		  ○ 22|33|16
		
		To find a Person Name in the LogRhythm Client Console, click Deployment Manager, click the People tab, click the user you want to add, and then copy the Person Name from Name tab.
			No

Playbook(s)	String	Pipe delimited list of Playbook Names or Playbook GUIDs. • Name: SOC Basic 1|Phishing • GUID: 510C7D5B-F058-4748-A948-233FAECB8348|6D980445-F31D-4FF6-AC67-2F0D992C8D4E	No
Case Summary	String	User defined static case summary to be populated on case creation.	No
Group-by 1: Metadata Field	String	If populated, this parameter defines the created Case's name and optionally can be applied as a Case Tag. If enabled as a Case Tag the Group-by field can be applied in the Case Lookup function of the Case Management SmartResponse plugin.	No
Group-by 1: Enable Tag	String	When set to true defines the Group-by 1 Metadata Field value will be established as a tag on the case.	No

Group-by 1: Tag Prefix	String	Applies a user defined prefix before the Metadata Field value. Example:
		  ○ Metadata Field Value: adm_user1
		  ○ Enable Tag: true
		  ○ Tag Prefix: user_login-
		
		  ○ Tag Result: user_login-adm_user1
			No

Group-by 2: Metadata Field	String	If populated, this parameter defines the created Case's name and optionally can be applied as a Case Tag. If enabled as a Case Tag the Group-by field can be applied in the Case Lookup function of the Case Management SmartResponse plugin.	No

Group-by 2: Enable Tag	String	When set to true defines the Group-by 2 Metadata Field value will be established as a tag on the case.	No
Group-by 2: Tag Prefix	String	Applies a user defined prefix before the Metadata Field value. Example: ○ Metadata Field Value: win32calc.exe ○ Enable Tag: true ○ Tag Prefix: process- ○ Tag Result: user_login-adm_user1	No
Group-by 3: Metadata Field	String	If populated, this parameter defines the created Case's name and optionally can be applied as a Case Tag. If enabled as a Case Tag the Group-by field can be applied in the Case Lookup function of the Case Management SmartResponse plugin.	No
Group-by 3: Enable Tag	String	When set to true defines the Group-by 3 Metadata Field value will be established as a tag on the case.	No
Group-by 3: Tag Prefix	String	Applies a user defined prefix before the Metadata Field value. Example: ○ Metadata Field Value: usample@exampl.com ○ Enable Tag: true ○ Tag Prefix: sender-usample@exampl.com ○ Tag Result: sender-usample@exampl.com	No
Tagging: Static Tag(s)	String	Pipe-separated tag names to be added to the case. Example: ○ CaseSRPv6|Automation|TECH_UnauthorizedAccess	No
Tagging: Schema	String	Sets the default character case for tags created through this plugin. Can be set to Lower or Upper. Default: Lower	No
Case Lookup: Previous Days	String	The number of previous days to search for existing cases. The default value is 3.	Yes
Case Lookup: Case Status	String	Pipe-delimited list of statuses (1-5) of existinv cases to search. The default value is 1|3.	Yes
Case Lookup: Exclude Tag	String	Optional capability to exclude associating an alarm to a case based on a Case Tag being assigned to a case manually. Apply this setting with a case tag defined to represent that the case should no longer receive new alarms, even if the case matches all the other defined criteria.	No

Case Lookup: Field Tag Mode	String	This setting defines how case lookup is performed based on the provided Alarm Rule Name and defined Group-by field's that have Enable Tag set to True. Supported values: All, Any, None, Field1, Field2, Field3 For additional details on Field Tag Mode Reference Appendix 2 – Field Tag Modes.	No
Case Enrichment: Static Note	String	Adds a user defined note to the case. The note must be a single consistent string. To apply new lines, add \r\n to add new lines. Example: Input: This note will be added into the case.\r\nThis note will be added only once when the case has been created. Output: This note will be added into the case. This note will be added only once when the case has been created.	No
Case Enrichment: Enable Alarm Summary	String	Adds an alarm summary note to the case.	No
Case Enrichment: Threat Intelligence	String	Adds a Threat Intelligence lookup note to the case.	No

Add Collaborators to Case

Description

This action adds a list of new collaborators to a Case.

Use Case

During an investigation into malicious activity, an analyst quickly adds collaborators and Alarm details to a Case to share information.

Parameters

Name	Type	Details	Required
Alarm ID	String	Optional parameter to indicate which alarm this process is associated to.	No
Case Number	String	Case Number for the target case.	Yes

Collaborator Name(s)	String	Option 1: Notification Group Name
		• Assigns all individual person records assigned to a LogRhythm Notification Group as a case collaborator.
		
		Option 2: Pipe delimited
		• Person Display Names to be added as collaborators to a case.
		  ○ user1, example|user2, example|user3
		• Person ID Numbers to be added as collaborators to a case.
		  ○ 22|33|16
		
		To find a Person Name in the LogRhythm Client Console, click Deployment Manager, click the People tab, click the user you want to add, and then copy the Person Name from Name tab.
			Yes

Add Playbooks

Description

This action adds Playbooks to a Case.

Use Case

During the course of an investigation, an analyst can easily add multiple Playbooks to a Case for reference and task assignment management.

This action has been designed to be leveraged by Analyst's from within the Web Console directly.

Parameters

Name	Type	Details	Required
Alarm ID	String	Optional parameter to indicate which alarm this process is associated to.	No
Case Number	String	Case Number for the target case.	Yes
Playbook(s)	String	Pipe delimited list of Playbook Names or Playbook GUIDs. • Name: SOC Basic 1|Phishing • GUID: 510C7D5B-F058-4748-A948-233FAECB8348| 6D980445-F31D-4FF6-AC67-2F0D992C8D4E	Yes

Add Tags to Case

Description

This action adds a list of new tags to a Case.

Use Case

During the course of an investigation, an analyst can easily add multiple tags to a Case for quicker searching and reporting.

This action has been designed to be leveraged by Analyst's from within the Web Console directly.

Parameters

Name	Type	Details	Required
Alarm ID	String	Optional parameter to indicate which alarm this process is associated to.	No
Case Number	String	Case Number for the target case.	Yes
Static Tag(s)	String	Pipe-delimited list of tags to add to the target case. Example: Tag1|Tag2|Tag3	Yes

Create Case Configuration File

You must execute this action before using the plugin's other available actions and rerun it whenever the fixed-value parameters change. For more information, see Create the Configuration File.

Generate an API Token

A user account must be given access to the Case API in order to access Case files. Access is given by assigning an API token to the user account. There are two ways to do this: Creating an API token from a person record and using a third-party application.

Create an API Token with a Third-Party Application

1. On the main toolbar, click Deployment Manager.
2. Click the Third Party Applications tab.
3. Right-click the third-party application, and then click Properties.

   > It may be necessary to create a new third-party application record to use as a Case API account. For more information, see "Register Third Party Applications to Use the Admin API" in the *LogRhythm Help*, available on the LogRhythm Community.

4. *(Optional)* Change the number of days you want the token to be valid. The default value is 365 days.
5. Click Generate Token.
   The Credentials dialog box appears.
6. Enter the user name and password associated with the Case API account, and then click OK. The API token is now associated with the application.
7. Click OK to close the Third Party Application Properties window.

Appendix 1 – Dynamic Priority Table

Dynamic Priority is an optional capability of the Case Management v6. If enabled, this sets the Case Management SmartResponse to set and/or update a Case's priority based on the triggering alarm's risk value. The Dynamic Priority can only lower a case's priority when it has initially been created. Any subsequent alarm's that trigger that match the case lookup to an existing open case can only increase a case priority above its current priority.

Alarm Risk	Case Priority
0-59	5
60-69	4
70-79	3
80-89	2
90-100	1

Appendix 2 – Field Tag Mode

Field Tag Mode presents the capability to define and control the Alarm to Case mapping behavior.

Field Tag Mode is one aspect of the Case Lookup mechanism of the Create Case: Associate Existing or Create SmartResponse Action. This mechanism is leveraged in conjunction with all other defined aspects of the Case Lookup criteria: Alarm Rule Name, Case Status, Previous Days, and Exclude Tag.

Field Tag mode is applied only when Group-by fields have been defined with the Tag Mode set to true. Tag prefixes are optional and are applied as a part of the tag lookup for all notated modes. The default behavior for the Case Management SmartResponse Plugin when no Group-by fields have been provided is to perform Alarm to Case association based on the Alarm Rule Name.

Mode	Behavior
All	Requires all configured Group-by fields where Tag Mode is set to true to be present on a case. In the event of multiple case result matches the most recent case will be the case selected. If a case contains some but not all Group-by defined tags a new case will be created.
Any	Requires any configured Group-by fields where Tag Mode is set to true to be present on a case. If a case contains some but not all Group-by defined tags a new case will not be created. The most recent created case returned will have the generating alarm appended into the existing case.
Field1 Field2 Field3	Requires the Group-by: Field # to be defined and tagging enabled for Group-by: Field #. If the Group-by: Field # is not provided by the AIE Alarm the Case Management SmartResponse will generate a new case.
None	Performs Alarm to Case association based on most recent returned case that corresponds to the Alarm Rule Name.