SOAR-TVM Module

ServiceNow Integration Guide Using Outbound API

Document Version: 2018.03.02 | March 2018

Contents

Solution Overview

Rsam's universal "outbound connector" has the ability to connect and interact with ServiceNow. This "outbound connector" helps formulate a holistic connection with ServiceNow.

In the latest version of Rsam, it is possible to execute most API commands in ServiceNow. The API commands will allow you to perform tasks such as creating, modifying, deleting of tickets and other records, as well as getting in data from updated records.

High-Level Configurations

To configure the RSAM outbound API to successfully integrate with the inbound REST API of ServiceNow, you must set up the following:

1. Rsam Connector

   This is used to configure the connection details for the Outbound API connectivity.

2. Rsam Risk Analytics Handlers

   This is used to configure the Outbound API calls to create, update, read, and delete incidents or any other application exposed by ServiceNow API.

Set up an Rsam Connector

This section describes the procedural steps to create a new connector. The Rsam connector that you will create to integrate with ServiceNow supports the following modes of authentication.

- Basic
- Token

You may connect to the inbound ServiceNow API through Basic or Token authentication.
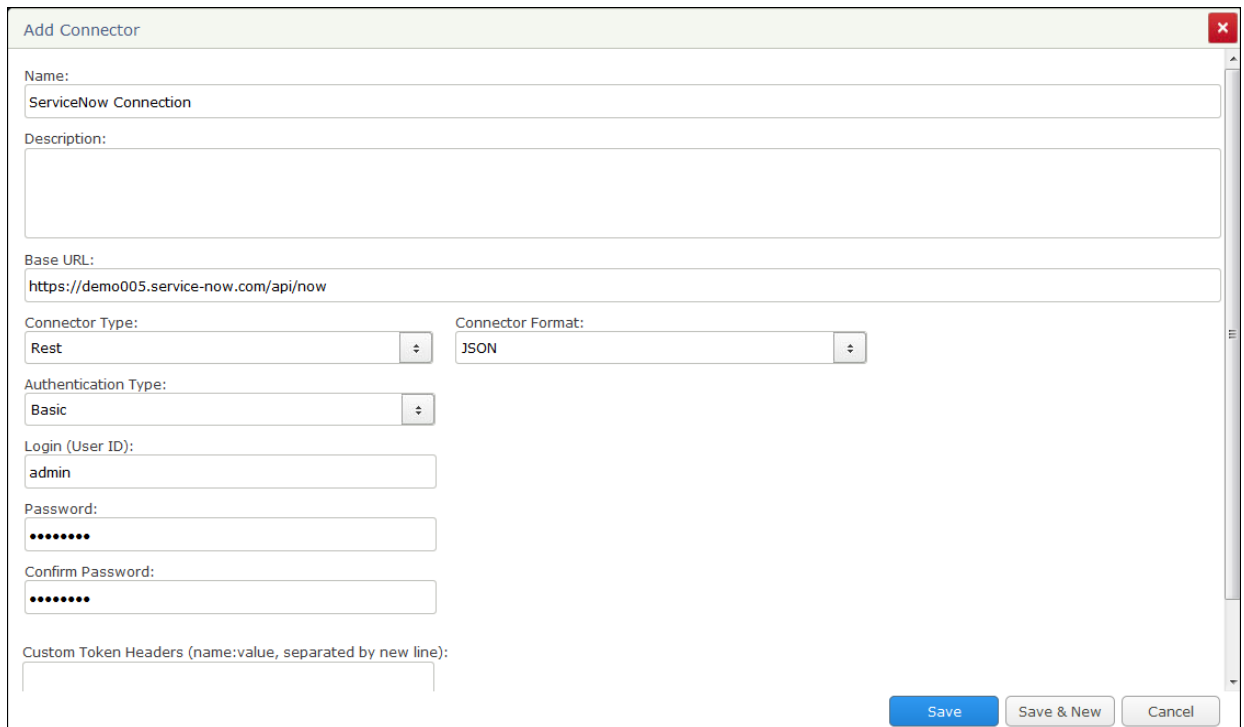
Basic Authentication

This section describes the procedural steps to create a connector that will connect ServiceNow through Basic authentication.

Procedure:

1. Navigate to **Manage** > **Administration**.

2. From within the left pane, navigate to **Options** > **Connectors**.
   The **Connectors** page appears, in which any previously added connectors are shown.

3. Click **Add** at the top-right corner.
   The **Add Connector** dialog appears.

4. Complete the attributes listed in the table below:

Attribute	Description
Name	Enter a connector name to integrate with ServiceNow.
Base URL	Enter the ServiceNow URL.
Connector Type	Select Rest in the drop-down list.
Connector Format	Select JSON in the drop-down list.
Authentication Type	Select Basic in the drop-down list.
Login (User ID)	Enter a username. This user must own the rest_service role in ServiceNow to make API calls. The <instance-name> is the name of the ServiceNow instance that will be accessed.
Password	Enter the password of the user to authenticate the connection

Attribute	Description
Confirm Password	Re-enter the same password for confirmation purpose.
Custom Token Headers (name:value, separated by new line)	Optional. Passes additional request headers such as cookies and encryption standard for additional security. Specify each request header on a new line in the name:value format. Example: Cookie: Skin=new Content-Length: 348

5. Click **Save**.
   The connector is added.

Token Authentication

This section describes the procedural steps to create a connector that will connect ServiceNow through Token authentication.
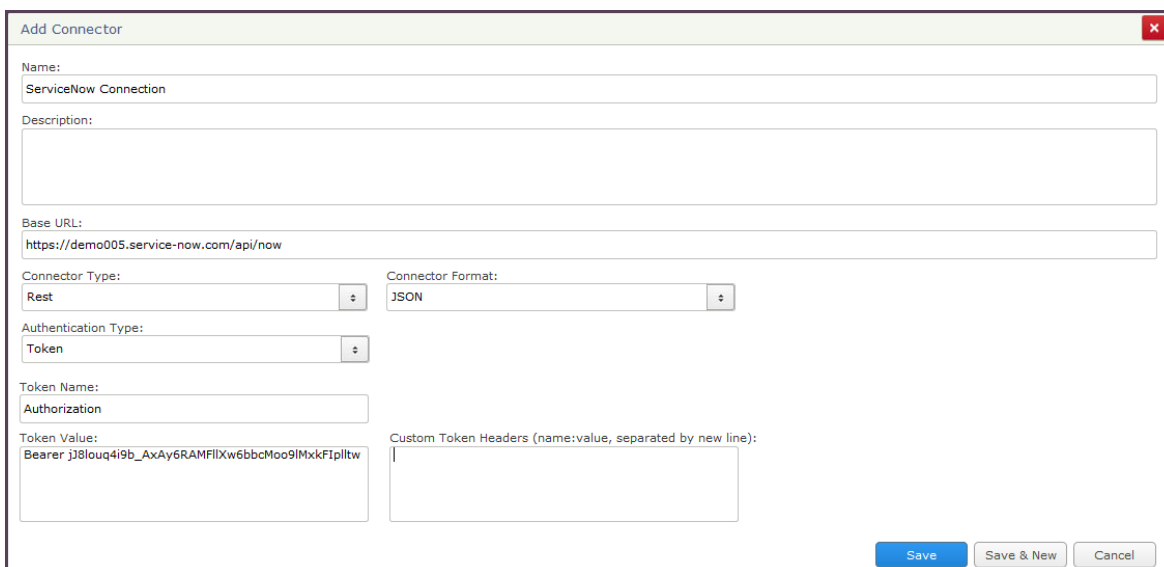
Procedure:

1. Keep the access token handy. On the ServiceNow side, navigate to **Option** > **System OAuth** > **System Registry**, create a client secret key and client ID, and then specify the access

token lifespan. Then, generate the token by submitting a request to the ServiceNow instance URL.

2. Navigate to **Manage** > **Administration**.

3. From within the left pane, navigate to **Options** > **Connectors**.
   The **Connectors** page appears in which any previously added connectors are shown.

4. Click **Add** at the top-right corner.
   The **Add Connector** dialog appears.

5. Complete the attributes listed in the table below:

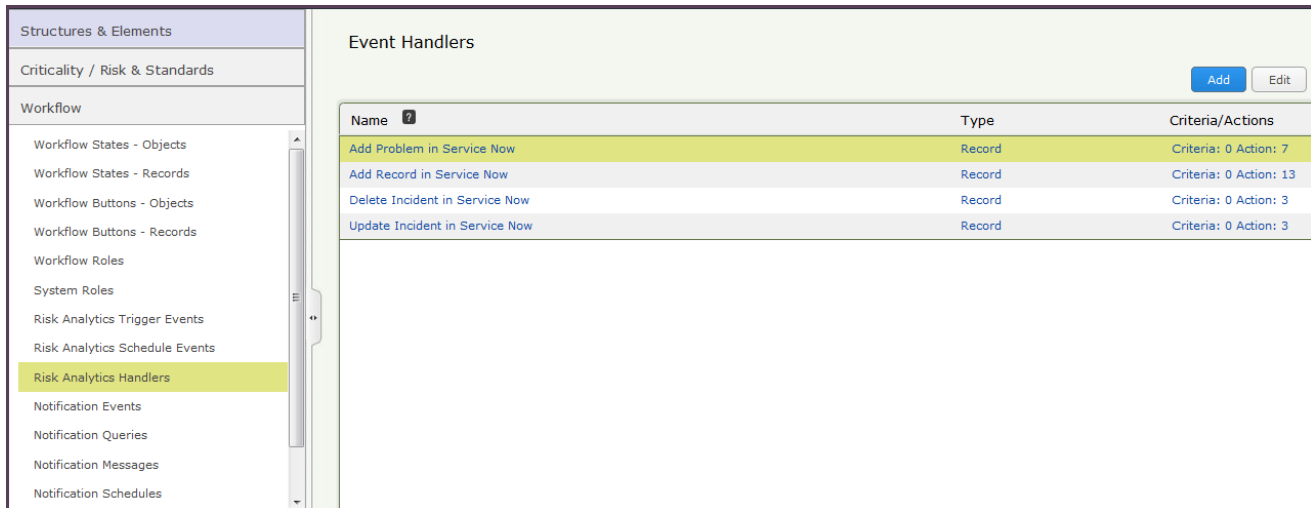| Attribute	Description
Name	Enter a connector name to integrate with ServiceNow.
Base URL	Enter the ServiceNow URL.
Connector Type	Select Rest in the drop-down list.
Connector Format	Select JSON in the drop-down list.
Authentication Type	Select Token in the drop-down list.
Token Name	Enter Authorization.
Token Value	Enter Bearer followed by the token.
Custom Token Headers	Optional. Passes additional request headers such as cookies and encryption standard for additional security. Specify each request header on a new line in the name:value format. Example: Cookie: Skin=new Content-Length: 348

6. Click **Save**.
   The connector is added.

Set up Risk Analytics Handlers

This section describes the Risk Analytics Handlers used in various API calls.

To add a Risk Analytics Handler, navigate to **Manage** > **Administration**, then navigate to **Workflow** > **Risk Analytics Handlers**, and click **Add** at the top-right corner.

The "Execute External API Command" Action Type used in the Risk Analytics Handlers for ServiceNow supports the following HTTP verbs:

- GET
- POST
- PUT
- DELETE

These HTTP verbs allow you to manage ServiceNow data from within Rsam.

Configuring the HTTP GET Verb

The HTTP GET verb can be used to read the details of a ServiceNow incident such as sys_user. The following example screenshot displays the command with the HTTP GET verb.

According to the HTTP protocol definition, the Data field must be blank for a GET call to work successfully. Otherwise, you will encounter an HTTP error when the handler is executed.
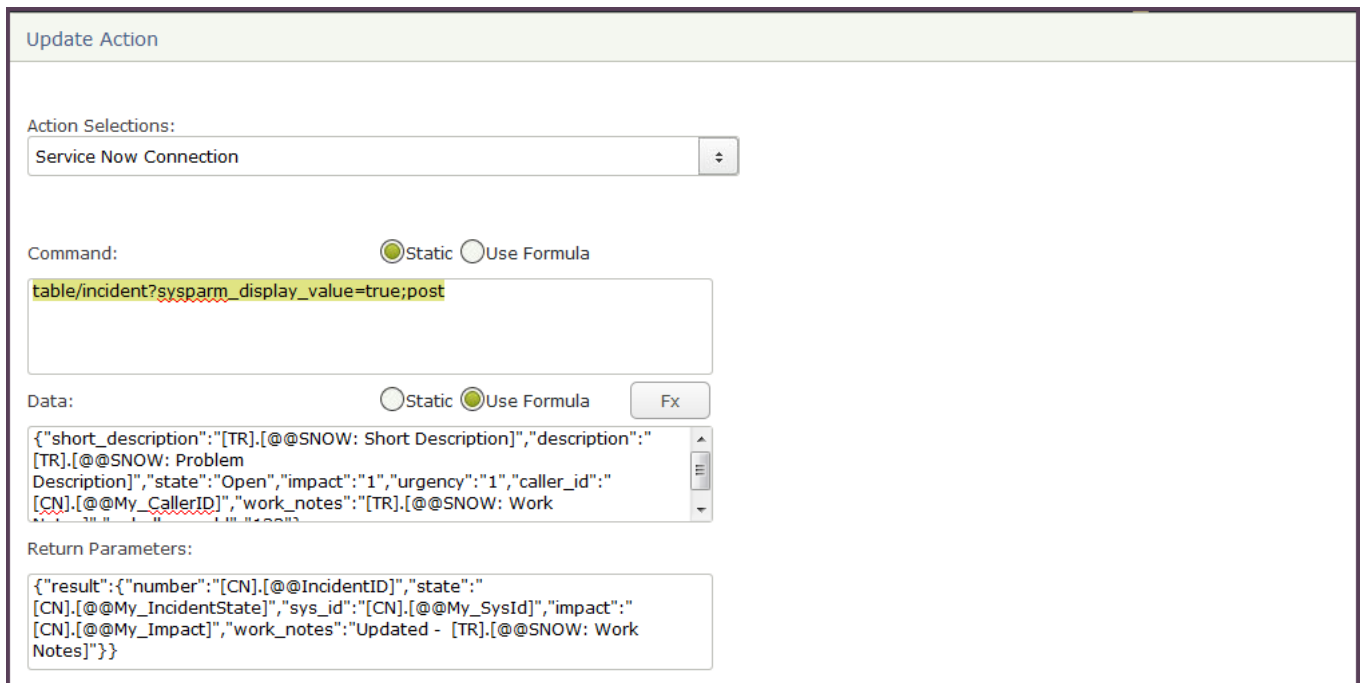
Upon the execution of handler, the result of the API call will be stored in the Return Parameters field in the [CN].[@@variable] format and populated as an attribute through a subsequent action in the same handler.

Configuring the HTTP POST Verb

The HTTP POST verb can be used to create a ServiceNow incident in your Rsam instance. The data specified in the Data field can be dynamically populated from an Rsam record or object.

In the Command field, the string sysparm_display_value = true can be included as a query string parameter in the URL to obtain text values (display values) in a proper format from ServiceNow (for example, the value for Impact would be obtained as "1-High" instead of "1."). It is used mainly for better readability of data received from ServiceNow.

The string ;Post as part of the URL in the Command field is optional, because the default action is POST for an Outbound API call from Rsam.

Configuring the HTTP PUT Verb

The HTTP PUT verb can be used to update a ServiceNow incident from Rsam.

In the following screenshot, the string [TR].[@@SNOWSysID] of the record or object refers to the auto-generated unique ID from ServiceNow, populated from an existing incident.

Configuring the HTTP DELETE Verb

The HTTP DELETE verb can be used to delete an application in ServiceNow from Rsam.

Notes: ServiceNow fields can be pulled into any Rsam attribute response type by configuring Risk Analytics Handlers**.**

If you add a new custom field in ServiceNow, then it will be automatically exposed by the table API.
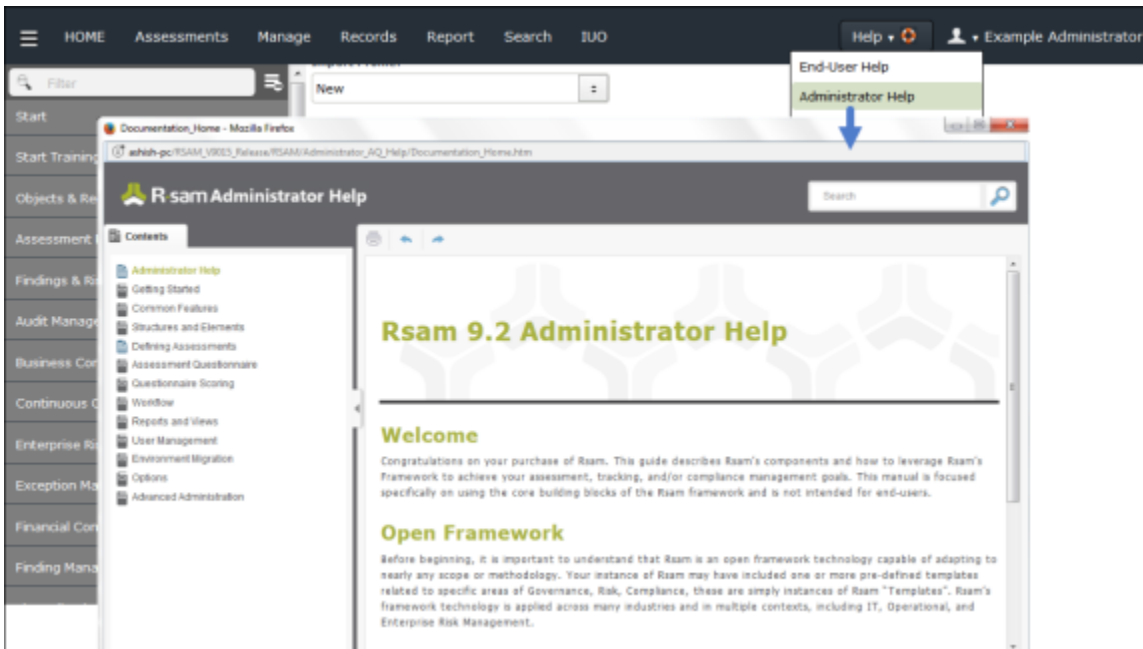
Appendix: Documentation

Rsam

While this guide provides information on how to integrate ServiceNow with Rsam, you should refer to the Rsam Help or Rsam Administrator Help when you want to get familiar with the specific Rsam features used in this guide. Please keep in mind that the help you can access depends on your user permissions.

Procedure:

1. Sign in to your Rsam instance.

2. Mouse hover over Help and select a help in the menu that appears. Depending on your user permissions, you will be able to access the Rsam Help, Rsam Administrator Help, or both.

    The screenshot below illustrates the Example Administrator user account in which the user has opened the Rsam Administrator Help.

ServiceNow

To get more familiar with the ServiceNow REST API, visit the following link: http://wiki.servicenow.com/index.php?title=REST_API

For more information on Rsam's outbound API, refer to the Admininstration Help.