Monitoring ServiceNow

ScienceLogic: ServiceNow Base Pack PowerPack version 103, rev1

Table of Contents

Introduction to the ServiceNow Base Pack PowerPack 1
What Does the ServiceNow Base Pack PowerPack Monitor? 2
Installing the ServiceNow Base Pack PowerPack 3
Configuring ServiceNow Base Pack Monitoring 4
Creating a SOAP/XML Credential for ServiceNow 5
Enabling the Run Book Automation Policies 8
Enabling and Customizing the Run Book Action Policy 9
Customizing the Snippet Code in the Input Parameters Pane 10
Customizing Logging in the Run Book Action 13
Sending Custom Data to ServiceNow Using the Passthrough Option 13
Passing Custom Data to ServiceNow 14
Snippet Code Example 16
Configuring the "ServiceNow: Click to Create Incident" Automation Policy 17
Creating a Virtual Device for the ServiceNow Base Pack 19
Aligning the ServiceNow Base Pack Dynamic Applications 19
ServiceNow Base Pack Dashboards 21
ServiceNow Open Incidents Dashboard 22

Chapter 1

Introduction to the ServiceNow Base Pack PowerPack

Introduction to the ServiceNow Base Pack PowerPack

This chapter describes how to monitor ServiceNow in SL1 using the *ServiceNow Base Pack* PowerPack. This PowerPack also contains the four Run Book Automation policies and the Run Book Action policy that you use with the Incident Sync Integration with ServiceNow.

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 ( ).

The following topics describe how to use the *ServiceNow Base Pack* PowerPack:

What Does the ServiceNow Base Pack PowerPack Monitor? 2
Installing the ServiceNow Base Pack PowerPack 3

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.

What Does the ServiceNow Base Pack PowerPack Monitor?

To monitor a ServiceNow instance with SL1, you must install the *ServiceNow Base Pack* PowerPack. This PowerPack enables you to model and collect data about ServiceNow Incident and CMDB tables.

The *ServiceNow Base Pack* PowerPack monitors the ServiceNow Incident and CMDB tables, and it returns information about Incident types, priorities, and states, displaying the information in an easy-to-consume dashboard. The PowerPack also returns information about the CI records that are actively being synced between SL1 and ServiceNow via the Integration Service, including basic CI metadata as well as an overall count.

Also, the PowerPack is a critical component of the Incident Sync Integration with ServiceNow, using Run Book Automations to integrate with the ServiceNow Incident Management module.

The *ServiceNow Base Pack* PowerPack includes:

- The "ServiceNow: CMDB Configuration" Dynamic Application, which provides data for Integration Service systems communicating with ServiceNow
- The "ServiceNow: Incident Metrics" Dynamic Application, which collects information about the types, statuses, and properties of ServiceNow incidents
- A Device Class for ServiceNow instances
- The "ServiceNow: Add/Update/Clear Incident" Run Book Action policy, which you can use with the "ServiceNow: Create, Update, Clear Incident" Action Type (also included) to automate adding, updating, and clearing ServiceNow incidents
- The following Run Book Automation policies to automate adding, updating, and clearing incidents, and to automate creating ServiceNow incidents in SL1:
    - ServiceNow: Add/Update Incident
    - ServiceNow: Click to Create Incident
    - ServiceNow: Event Acknowledged
    - ServiceNow: Event Cleared
- Two Sample Credentials: one for connecting to a ServiceNow instance and one for sending event payload information to the Integration Service, which is required for integration with the ServiceNow Incident Management Module
- The "ServiceNow Open Incidents" Dashboard, which displays information about ServiceNow incident statuses and types
- ScienceLogic Libraries that are utilized by this PowerPack:
    - content
    - content_cache
    - silo_core
    - silo_core_rest
    - silo_credentials
    - silo_servicenow

Installing the ServiceNow Base Pack PowerPack

To monitor a ServiceNow instance with SL1, you must import and install the latest version of the *ServiceNow Base Pack* PowerPack.

NOTE: If you are upgrading from SyncServer, you must disable the old SyncServer Run Book Actions and Run Book Automation policies before installing the *ServiceNow Base Pack* PowerPack.

TIP: By default, installing a new version of a PowerPack overwrites 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 new PowerPacks from overwriting local changes for some commonly customized fields. For more information, see the ***System Administration*** manual.

To install the *ServiceNow Base Pack* PowerPack:

1. Download the latest version of the PowerPack from the Customer Portal to a local computer.
2. Log in to SL1 as an administrator, then go to the **PowerPack Manager** page (System > Manage > PowerPacks).
3. Click the **[Actions]** button and select *Import PowerPack*.
4. Click the **[Browse]** button and navigate to the *ServiceNow Base Pack* PowerPack file from step 1.
5. Select the PowerPack file and click **[Import]**. The **PowerPack Installer** modal page displays a list of the PowerPack contents.
6. Click the **[Install]** button. After the installation is complete, the *ServiceNow Base Pack* PowerPack appears on the **PowerPack Manager** page.

Chapter 2

Configuring ServiceNow Base Pack Monitoring

Overview

This chapter describes how to configure ServiceNow for monitoring by SL1 using the *ServiceNow Base Pack* PowerPack.

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 chapter covers the following topics:

Creating a SOAP/XML Credential for ServiceNow 5
Enabling the Run Book Automation Policies 8
Enabling and Customizing the Run Book Action Policy 9
Customizing the Snippet Code in the Input Parameters Pane 10
Customizing Logging in the Run Book Action 13
Sending Custom Data to ServiceNow Using the Passthrough Option 13
Passing Custom Data to ServiceNow 14
Snippet Code Example 16
Configuring the "ServiceNow: Click to Create Incident" Automation Policy 17
Creating a Virtual Device for the ServiceNow Base Pack 19
Aligning the ServiceNow Base Pack Dynamic Applications 19

Creating a SOAP/XML Credential for ServiceNow

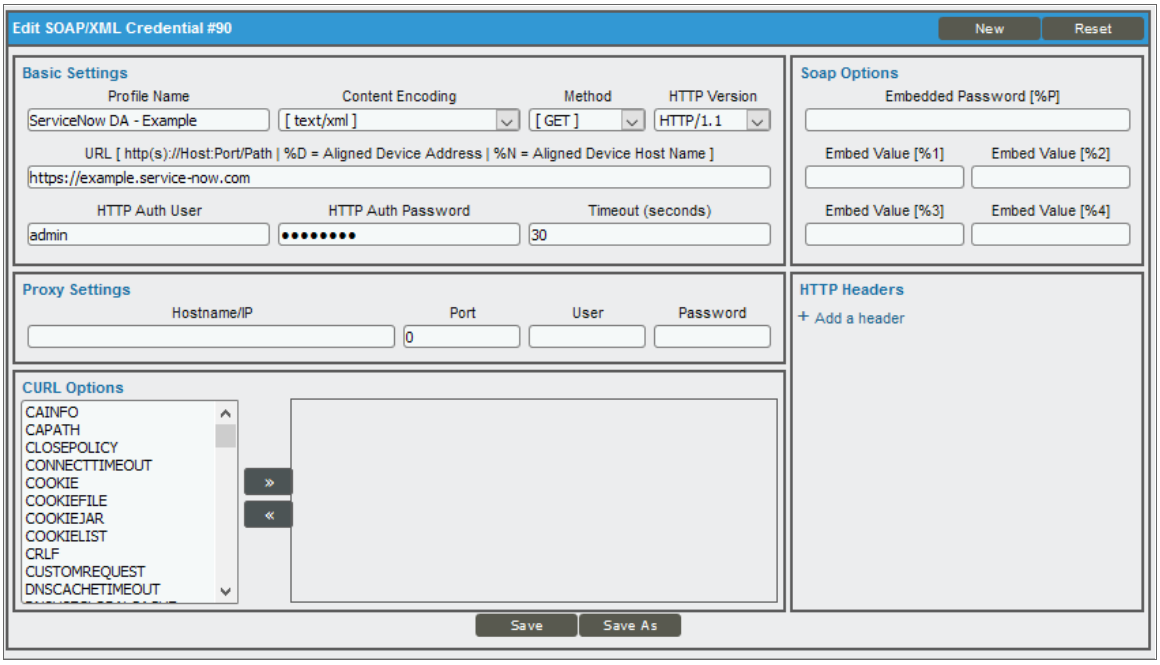
To configure SL1 to monitor a ServiceNow instance, you must first create at least one SOAP/XML credential to enable the Dynamic Applications in the *ServiceNow Base Pack* PowerPack to communicate with ServiceNow and the Integration Service.

The PowerPack includes two sample credentials:

- **ServiceNow DA - Example**. This credential connects the Dynamic Applications in the *ServiceNow Base Pack* PowerPack to a ServiceNow instance. This credential lets you monitor the CMDB and Incident tables in ServiceNow.
- **ServiceNow RBA - Example**. This credential lets you send event payload data from SL1 to the Integration Service and then to ServiceNow. Use this credential if you want to integrate with the ServiceNow Incident Management Module by aligning it with the "ServiceNow: Add/Update/Clear Incident" Run Book Action.

To configure the **ServiceNow DA - Example** credential:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the **ServiceNow DA - Example** credential and then click its wrench icon (). The **Edit SOAP/XML Credential** modal page appears:



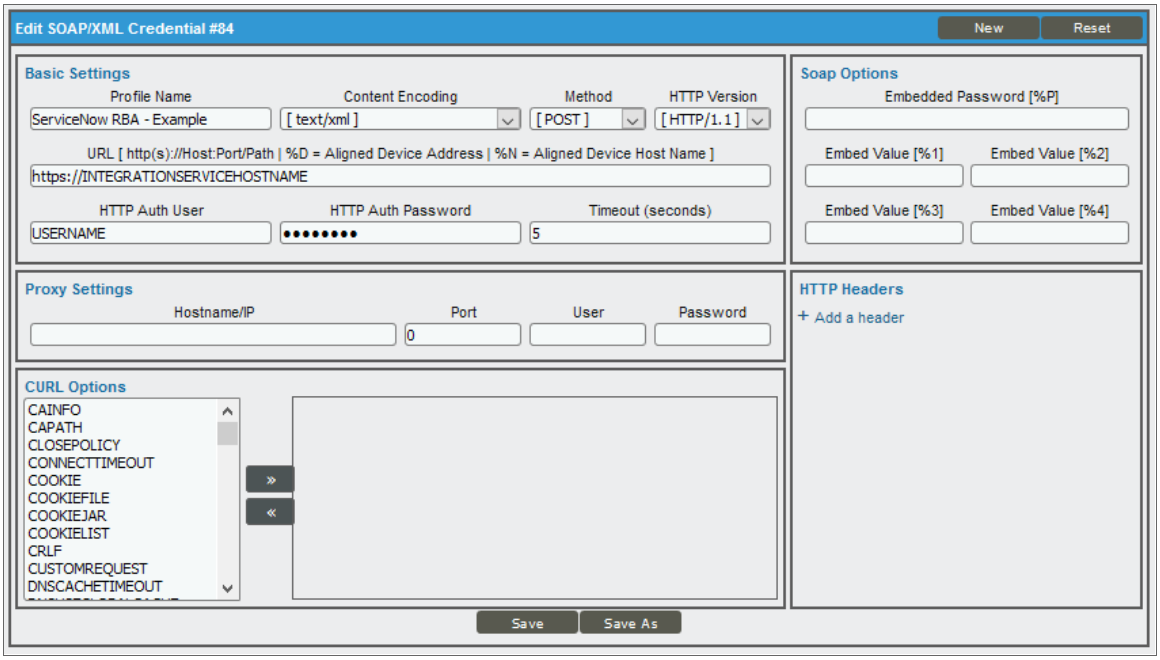
3. Complete the following fields:
   - ***Profile Name***. Type a name for the ServiceNow Dynamic Applications credential.
   - ***Content Encoding***. Select *text/xml*.
   - ***Method***. Select *GET*.

- ***HTTP Version***. Select *HTTP/1.1*.
- ***URL***. Type the URL for your ServiceNow system.
- ***HTTP Auth User***. Type the ServiceNow administrator username.
- ***HTTP Auth Password***. Type the ServiceNow administrator password.
- ***Timeout (seconds)***. Type "30".

4. Click the **[Save As]** button.

To configure the **ServiceNow RBA - Example** credential to use with the "ServiceNow: Add/Update/Clear Incident" Run Book Action:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the **ServiceNow RBA - Example** credential and then click its wrench icon (). The **Edit SOAP/XML Credential** modal page appears:

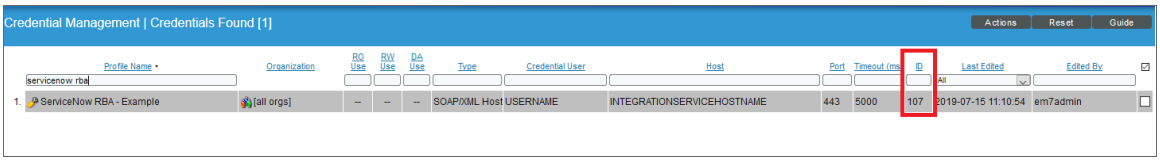


3. Complete the following fields:

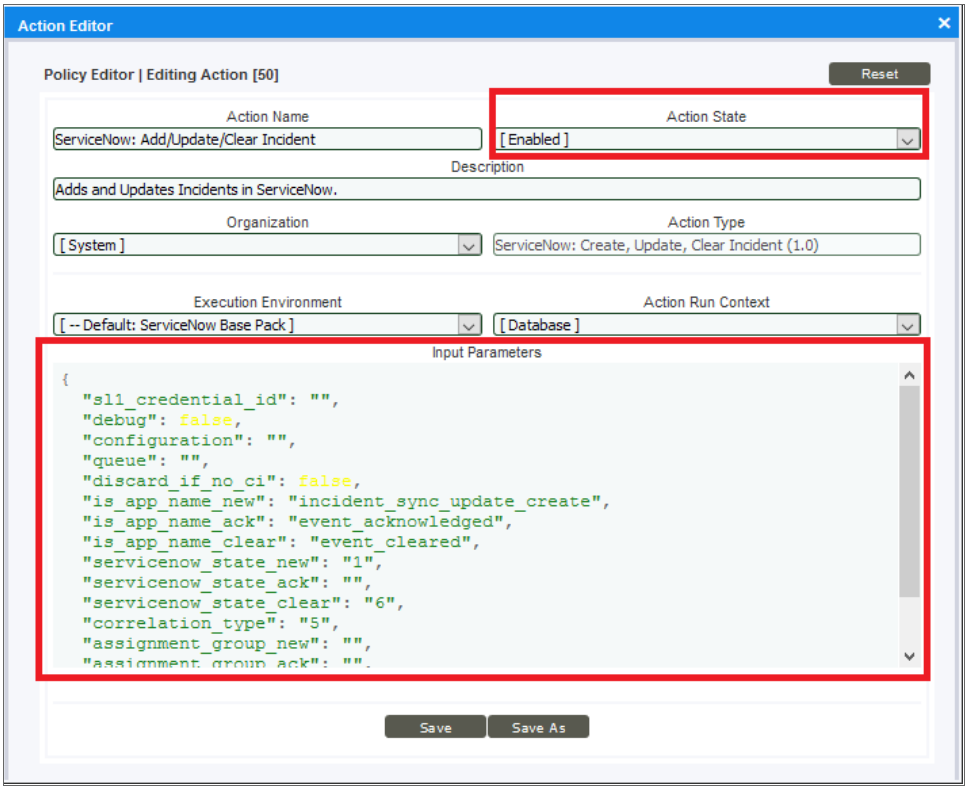
- ***Profile Name***. Type a name for the ServiceNow Run Book Action credential.
- ***Content Encoding***. Select *text/xml*.
- ***Method***. Select *POST*.
- ***HTTP Version***. Select *HTTP/1.1*.
- ***URL***. Type the host name for the Integration Service.
- ***HTTP Auth User***. Type the Integration Service administrator username.

- ***HTTP Auth Password***. Type the Integration Service administrator password.
- ***Timeout (seconds)***. Type "5".

4. Click **[Save As]**.
5. When the confirmation message appears, click **[OK]**.
6. On the **Credential Management** page (System > Manage > Credentials), make a note of the value in the **ID** column for the credential you just created:



You will use this value with the "sl1_credential_id" parameter when you enable and customize the snippet code of the "ServiceNow: Add/Update/Clear Incident" Run Book Action policy:



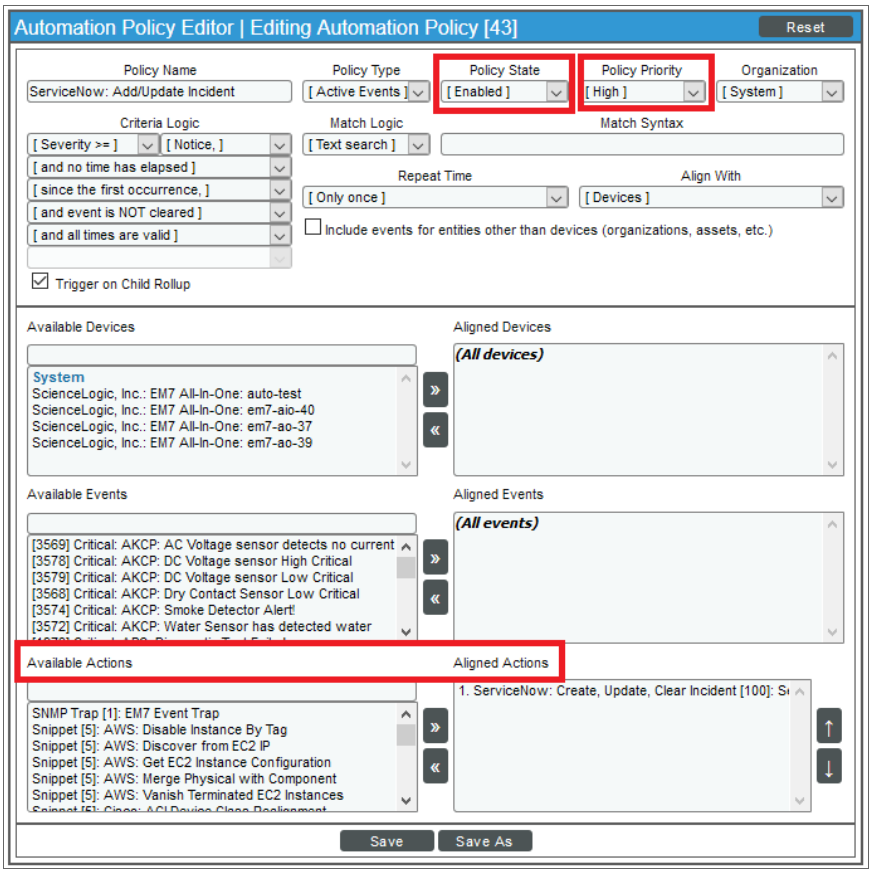
Enabling the Run Book Automation Policies

Before you can run the "ServiceNow: Add/Update/Clear Incident" Run Book Action, you must enable the three related Run Book Automation policies in SL1:

- ServiceNow: Add/Update Incident
- ServiceNow: Event Acknowledged
- ServiceNow: Event Cleared

To enable the three ServiceNow Run Book Automation policies:

1. In SL1, go to the **Automation Policy Manager** page (Registry > Run Book > Automation).
2. Locate the "ServiceNow: Add/Update Incident" automation policy and click its wrench icon (). The **Automation Policy Editor** page appears:



3. Update the following fields:
    - ***Policy State***. Select *Enabled*.
    - ***Policy Priority***. Select *High* to ensure that this Integration Service automation policy is added to the top of the queue.
    - ***Available Actions***. If it is not already selected, select the corresponding ServiceNow Run Book Action policy.

TIP: By default, the "ServiceNow: Add/Update Incident" automation policy will create ServiceNow incidents for ***all*** devices. You can limit the devices affected by making changes to the ***Organization***, ***Severity***, ***Match Logic***, ***Aligned Devices***, and/or ***Aligned Events*** fields.

WARNING: ScienceLogic highly recommends that you do not make changes to the ***Policy Type***, ***Repeat Time***, or ***Align With*** fields or the *And event is NOT acknowledged* setting.

4. Click **[Save]**.
5. Repeat steps 2-4 for the "ServiceNow: Event Acknowledged" and "ServiceNow: Event Cleared" Run Book Automation policies.

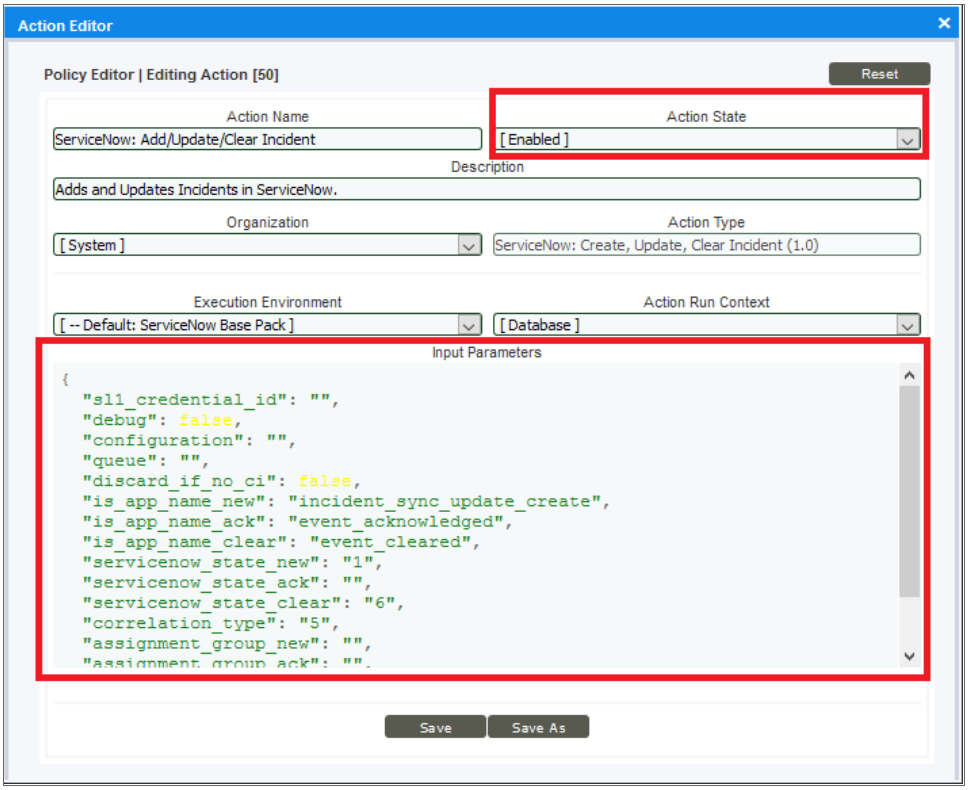
Enabling and Customizing the Run Book Action Policy

The "ServiceNow: Add/Update/Clear Incident" Run Book Action policy contains several default values in the snippet code for the policy that you can customize for Incident Sync. You can edit these values in the **Input Parameters** pane of the **Action Policy Editor** page for this policy.

For example, the ***Correlation Type*** is a value that you can use to correlate an SL1 event with a ServiceNow incident. For the Correlation Type, which is also called the "Correlation ID", you can choose a number of different ways in which an incident can be created. The default setting is `"correlation_type": "5"`, which means that this Run Book Action correlates all events by device ID and event policy ID, and if the event matches and the state is active, the Action updates the existing incident. The Action creates a *new* incident if the event does *not* match by device ID and event policy ID. As a result, the Correlation Type helps determine which events get rolled up under an incident. All Run Book Action scripts should use the same Correlation Type value, otherwise correlation will fail.

To enable and customize the Run Book Automation policies:

1. In SL1, go to the **Action Policy Manager** page (Registry > Run Book > Actions).
2. Locate the **ServiceNow: Add/Update/Clear Incident** policy and click its wrench icon (). The **Action Policy Editor** page appears:



3. For the ***Action State*** filed select *Enabled*.
4. In the **Input Parameters** pane, edit the snippet code as necessary, using the information in the ***Customizing the Snippet Code in the Input Parameters Pane*** section, below. When you are finished, click **[Save]**.

Customizing the Snippet Code in the Input Parameters Pane

SL1 Run Book Action snippets are written in Python. In the event of a syntax error, the policies will no longer run. As a result, you must ensure that all edits adhere to Python standards. True and False options are case-sensitive and must not contain quotes.

> **NOTE:** Previous SyncServer users had three separate Run Book Action scripts for add/update, acknowledge, and clear. These have been rolled into a single Run Book Action in the Integration Service, but there are still three Automation policies.

You can customize the following values in the "ServiceNow: Add/Update/Clear Incident" Run Book Action snippet code:

- ***sl1_credential_id***. Specifies the ID of the credential object. You can find this value in the **ID** column of the **Credentials** page (System > Manage > Credentials of SL1.
- ***debug***. A true/false value that determines if the action is logged in SL1 and if the application is run in Debug Mode on the Integration Service. Troubleshooting logs are written to **/data/tmp/servicenow_rba.log**.
- ***configuration***. Specifies the ID of the configuration object used on the Integration Service. The configuration ID is all lower-case, with spaces in the configuration object "friendly" name replaced by underscores. For example: `"configuration": "servicenow_syncpack_configs"`

NOTE: To find the configuration ID with the API, make a GET request on this endpoint: `https://<Integration_Service_hostname>/api/v1/configurations`.

- ***queue***. Specifies the worker queue on which the application runs. Leave this as default.
- ***discard_if_no_ci***. Specifies whether the Integration Service should create incidents in ServiceNow for devices that do not have a matching CI record. The default is *false*. Your options include:
  - *true*. If a device is not mapped to a CI, the Integration Service will *not* create an incident in ServiceNow, and SL1 is not updated. The following log message appears: "No CI found".
  - *false*. If a device is not mapped to a CI, the Integration Service *will* create an incident in ServiceNow and update SL1.
- ***servicenow_state_new***:
  - *1*. Incident state is "New". This is the default value.
  - *2*. Incident state is "In Progress".
  - *3*. Incident state is "On Hold".
  - *6*. Incident state is "Resolved".
  - *7*. Incident state is "Closed".
  - *8*. Incident state is "Canceled".
- ***servicenow_state_ack***:
  - *1*. Incident state is "New". There is no default value.
  - *2*. Incident state is "In Progress".
  - *3*. Incident state is "On Hold".
  - *6*. Incident state is "Resolved".
  - *7*. Incident state is "Closed".
  - *8*. Incident state is "Canceled".

- ***servicenow_state_clear***:
    - *1*. Incident state is "New".
    - *2*. Incident state is "In Progress".
    - *3*. Incident state is "On Hold".
    - *6*. Incident state is "Resolved". This is the default value.
    - *7*. Incident state is "Closed".
    - *8*. Incident state is "Canceled".
- ***correlation_type***. Correlates an SL1 event with a ServiceNow incident. For this value, which is also called the "Correlation ID", you can choose a number of different ways in which an incident can be created. The default setting is `"correlation_type": "5"`, which means that this Run Book Action correlates all events by device ID and event policy ID, and if the event matches and the state is active, the Action updates the existing incident. The Action creates a *new* incident if the event does *not* match by device ID and event policy ID. As a result, the Correlation Type helps determine which events get rolled up under an incident. All Run Book Action scripts should use the same Correlation Type value, otherwise correlation will fail.

  The possible Correlation Type values include the following:

    - *1*. Correlate all duplicate incidents by SL1 ID only.
    - *2*. Correlate all duplicate incidents by event policy ID only.
    - *3*. Correlate all duplicate incidents by device ID only.
    - *4*. Correlate all duplicate incidents by Interface ID only. This correlation requires that the SL1 event has an interface aligned. If there is no interface aligned to the event, the returned Interface ID will be 0.
    - *5*. Correlate all duplicate incidents by device ID and event policy ID. This is the default Correlation Type value.
    - *6*. Correlate all duplicate incidents by device ID, event policy ID, and event sub entity ID.
    - *7*. Correlate all duplicate incidents by device ID, event policy ID, region, and event ID. Please note that using this correlation type will result in all events triggering new incidents.
    - *8*. Correlate all events to the root device ID of the component device into one incident. Please note that using this correlation type might lead to undesirable behavior, as not all events generated on a child device indicate a problem on the root device. As a result, ScienceLogic recommends that you only use this correlation type against specific event policies.
- You can assign the assignment group to one of the new, acknowledged, or cleared incidents that are mapped. To disable this feature, ensure that no values are set. After an incident is created, the assignment group value will not be changed by the Run Book Action. To assign an assignment group, set the variable value to the ***sys_id*** of the ServiceNow Assignment Group. In the following example, the assignment group is assigned to incidents that are *cleared*:

```
"assignment_group_new": "",
"assignment_group_ack": "",
"assignment_group_clear": "sys_id"
```

Customizing Logging in the Run Book Action

You can customize the following logging-related items in the "ServiceNow: Add/Update/Clear Incident" Run Book Action snippet code:

- `logfile = /data/tmp/ServiceNow_add_update_clear_incident.log`
    - Location for logging output.
    - Will be created if it does not exist.
    - Will be appended with each Run Book job.
    - Is case-sensitive.
- `do_debug_logging = True`
    - True is on, False is off.
    - Is case-sensitive.
    - For troubleshooting, these can be enabled or changed.
    - Writes logs to **/data/tmp/servicenow_rba.log**.

Sending Custom Data to ServiceNow Using the Passthrough Option

You can use the "ServiceNow: Add/Update Incident" Run Book Automation and the "ServiceNow: Add/Update/Clear Incident" Run Book Action to "pass through" custom data to ServiceNow. For example, you might want to use the passthrough functionality to overwrite the impact and urgency of a ServiceNow Incident, which is the only way to change the priority of the Incident.

To pass custom data to ServiceNow:

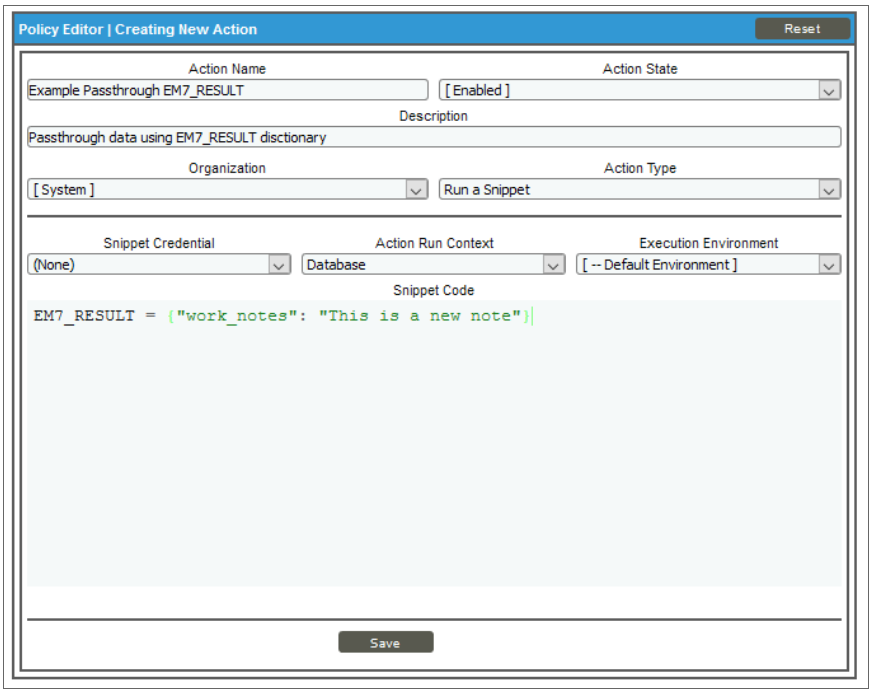
- Create a new Run Book Action that pulls the relevant data and adds it to a dictionary called EM7_RESULT.
- Add the new Run Book Action to the "ServiceNow: Add/Update Incident" Run Book Automation Policy, ahead of the "ServiceNow: Add/Update/Clear Incident" Run Book Action so that the new Action runs first, and then is consumed by the ServiceNow Action.

The following procedure describes how to configure the passthrough functionality.

Passing Custom Data to ServiceNow

To pass custom data to ServiceNow:

1. Go to the **Action Policy Manager** page (Registry > Run Book > Actions) and click **[Create]** to create a new Run Book Action policy:



2. Complete the following fields:

   - ***Action Name***. Type a unique name for the Action.
   - ***Action State***. Select *Enabled*.
   - ***Action Type***. Select *Run a Snippet*.
   - ***Execution Environment***. Select *ServiceNow Base Pack*.
   - Complete the other fields as needed.

3. In the **Snippet Code** pane, add the code for the EM7_RESULT dictionary. For example, the following snippet code lets you override the ServiceNow Incident work notes with a hardcoded note:

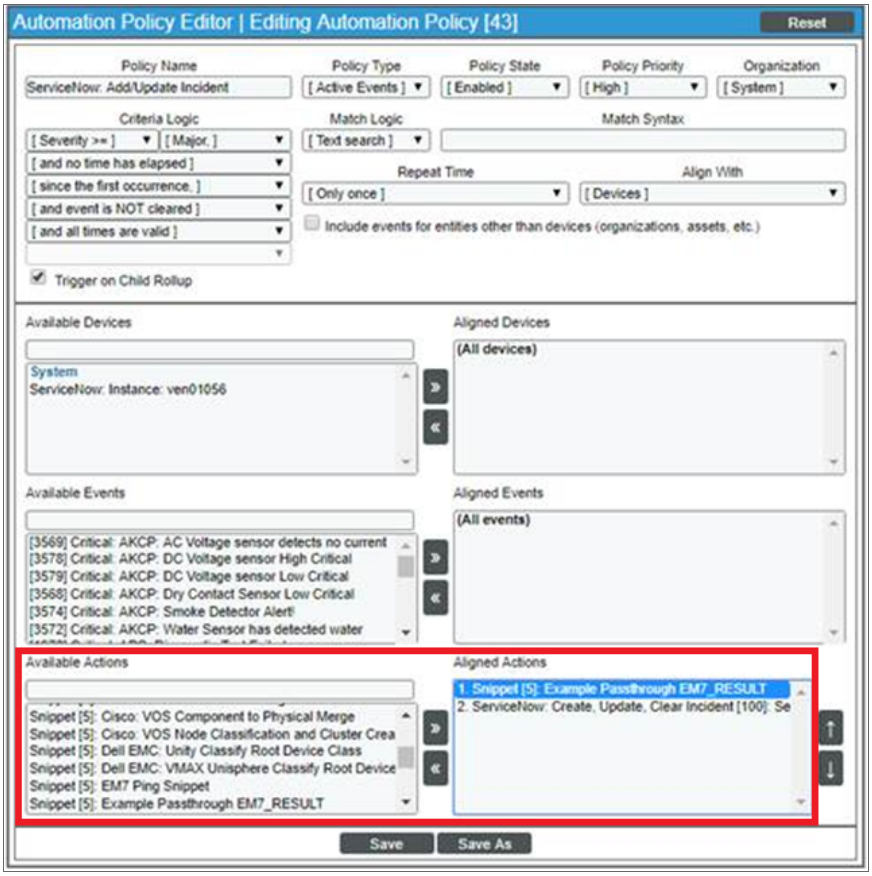
```
EM7_RESULT = {"work_notes": "This is a new note"}
```

Additional notes about the structure of the EM7_RESULT dictionary:

- `EM7_RESULT =` is required for the dictionary, and the formatting of the keys should match the example above.
- All keys defined in the EM7_RESULT dictionary need to map to field IDs on the **ScienceLogic Events** table in ServiceNow.
- You can hard-code the values in the EM7_RESULT dictionary, or you can use variables and functions, like the "Snippet Code Example", below.
- As a best practice, avoid sending null passthrough values to ServiceNow. If you must send 'null' or 'NULL' values to ServiceNow, pass through that value as an empty string, such as `"location":""`. Also, only pass through values that you need. For example, instead of sending `{"location": "", "work_notes": "stuff"}`, simply send `{"work_notes": "stuff"}`.
- A long snippet might delay the ticket being created

4. Click **[Save]**.
5. Go to the **Automation Policy Manager** page (Registry > Run Book > Automation) and open the "ServiceNow: Add/Update Incident" Run Book Automation Policy.

6. In the **Available Actions** section, add the new Run Book Action *before* the "ServiceNow: Create, Update, Clear Incident" Run Book Action:



NOTE: The output of this new Run Book Action will be consumed by the "ServiceNow: Create, Update, Clear Incident" Run Book Action, ensuring that the EM7_RESULT dictionary is passed through to ServiceNow. The "ServiceNow: Create, Update, Clear Incident" Run Book Action automatically populates the passthrough values with any values from EM7_LAST_RESULT. The passthrough overwrites any other previously defined fields, such as assignment group.

7. You can add additional Run Book Actions to the Run Book Automation Policy for any additional workflows that you might want to run. The Automation Policy execute these Actions in a sequential, top-down order. However, the "ServiceNow: Create, Update, Clear Incident" Run Book Action only consumes the EM7_RESULT dictionary from the Run Book Action directly above it.

Snippet Code Example

The following snippet code example shows how to pull additional information and make it available for passthrough. All of the additional information that is going to be sent is contained in a dictionary variable called EM7_RESULT. You can pass through multiple items through in a single Run Book Action by adding additional keys to the EM7_RESULT dictionary.

This example lets you assign assignment groups to an Incident based on certain criteria, such as event policy IDs:

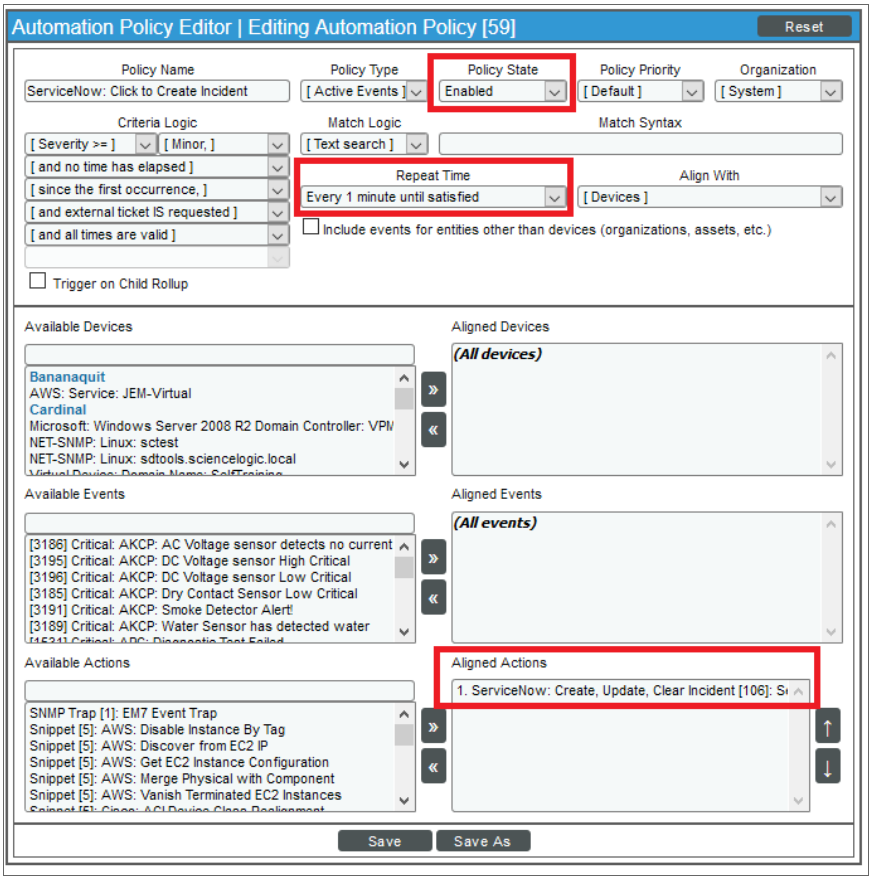
```
from future.utils import iteritems


def invert_mappings(mappings):
    """
    Invert received one-to-many mappings and converts it into a one-to-one
    mapping.

    Args:
        mappings (dict): Dictionary of mapped values

    Returns:
        dict: inverted dictionary.

    """
    inverted_mappings = dict()
    for key, values in iteritems(mappings):
        for sub_value in values:
            invert_mappings[sub_value] = key
    return inverted_mappings


# Example of assignment group to list of event policy ids mapping.
assignment_groups_to_event_policies = {
    "sys_id_1": [1, 2, 3, 4, 5],
    "sys_id_2": [6, 7, 8, 9, 10],
}
# which sys_id to use if the current event_policy_id isn't mapped
default_sys_id = "sys_id_3"

# invert the mappings
event_policy_to_assignment_group = invert_mappings(assignment_groups_to_event_
policies)

# Send assignment group sys_id to IS RBA
EM7_RESULT = {
    "assignment_group": event_policy_to_assignment_group.get(
        EM7_VALUES["%3"], default_sys_id
    )
}
```

Configuring the "ServiceNow: Click to Create Incident" Automation Policy

The "ServiceNow: Click to Create Incident" Run Book Automation policy lets you manually create an incident in ServiceNow by clicking the life-preserver icon ( ) in SL1. This policy is available in the *ServiceNow Base Pack* PowerPack.

To configure the "ServiceNow: Click to Create Incident" policy:

1. In SL1, go to the Behavior Settings page (System > Settings > Behavior) and set the ***Event Console Ticket Life Ring Button Behavior*** option to *Create/View External Ticket*.
2. Click **[Save]** to save your changes.
3. Go to the **Automation Policy Manager** page (Registry > Run Book > Automation).
4. Locate the **ServiceNow: Click to Create Incident** policy and click its wrench icon (). The **Automation Policy Editor** page appears:



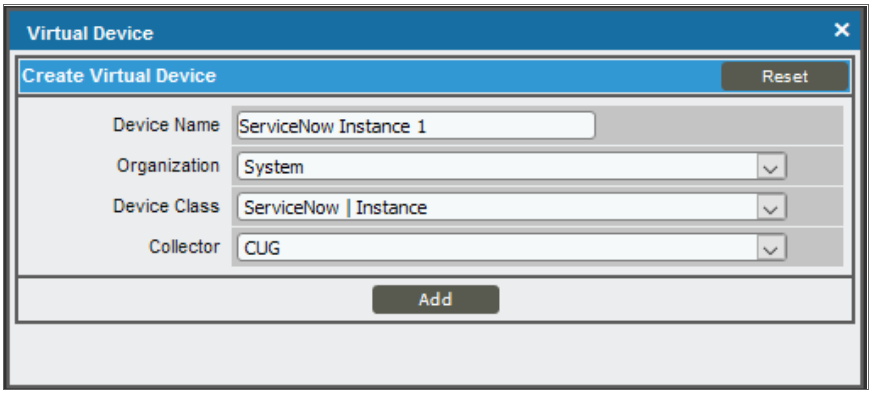
5. Update the following fields:
   - ***Policy State***. Select *Enabled*.
   - ***Repeat Time***. Specify the frequency at which SL1 should execute the automation policy while the conditions are still met. The choices range from "every 30 seconds until satisfied" to "every 2 hours until satisfied", or "only once". By default, the policy only runs once.
   - ***Available Actions***. If it is not already selected, select the corresponding ServiceNow Run Book Action policy to add it to the ***Aligned Actions*** field.
6. Click **[Save]**.

Creating a Virtual Device for the ServiceNow Base Pack

To monitor ServiceNow, you must create a ***virtual device*** that represents the root device for ServiceNow. You can use the virtual device to store information gathered by policies or Dynamic Applications.

To create a virtual device that represents your ServiceNow instance:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
2. Click the **[Actions]** button and select *Create Virtual Device* from the menu. The **Virtual Device** modal page appears:



3. Complete the following fields:
   - ***Device Name***. Type a name for the device.
   - ***Organization***. Select the organization for this device. The organization you associate with the device limits the users that will be able to view and edit the device. Typically, only members of the organization will be able to view and edit the device.
   - ***Device Class***. Select *ServiceNow | Instance*.
   - ***Collector***. Select the collector group that will monitor the device.
4. Click the **[Add]** button to create the virtual device.

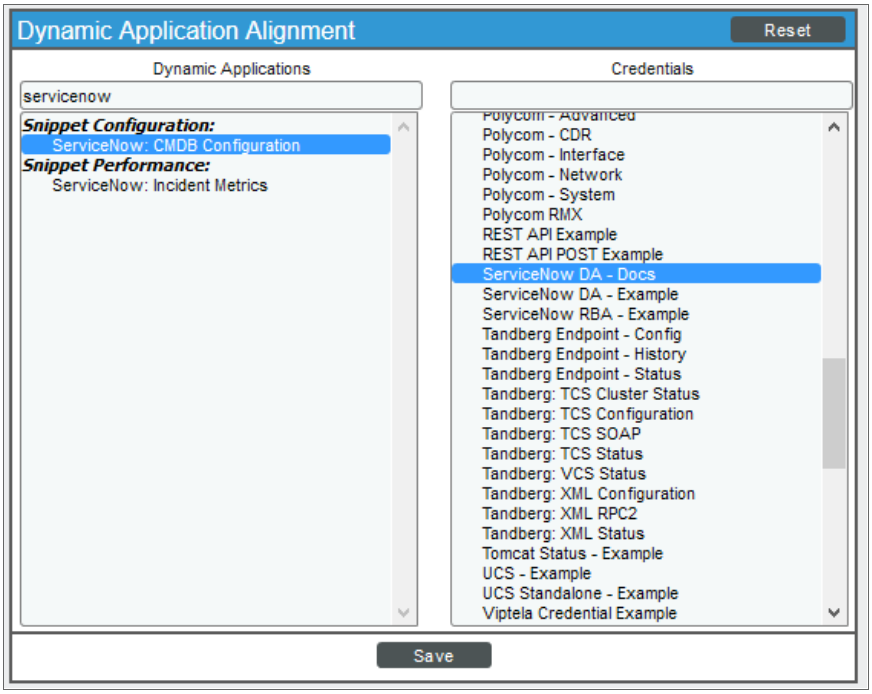
Aligning the ServiceNow Base Pack Dynamic Applications

Before you can run the Dynamic Applications in the ServiceNow Base Pack, you must manually align each Dynamic Application to the virtual device you created in the previous step. When you align the Dynamic Applications, you should use the ServiceNow credential that you created from the **ServiceNow DA - Example** credential.

To align the ServiceNow Base Pack Dynamic Applications with the ServiceNow virtual device:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).

2. Click the wrench icon ( ) for the virtual device you created in the previous section. The **Device Properties** page appears.
3. Click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
4. Click the **[Actions]** button and select *Add Dynamic Application*. The **Dynamic Application Alignment** modal page appears:



5. In the ***Dynamic Applications*** field, select the first of the ServiceNow Dynamic Applications.
6. In the ***Credentials*** field, select the credential you created based on the **ServiceNow DA - Example** credential.
7. Click the **[Save]** button.
8. Repeat steps 4-7 for each remaining Dynamic Application.

Chapter 3

ServiceNow Base Pack Dashboards

Overview

This chapter describes the system dashboard that is included in the *ServiceNow Base Pack* PowerPack.

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 chapter covers the following topics:

ServiceNow Open Incidents Dashboard *22*

ServiceNow Open Incidents Dashboard

The ServiceNow Open Incidents system dashboard displays the following information:

- Open incidents by state
- Open incidents by priority
- Unassigned incidents
- High priority incidents
- Critical priority incidents
- Assigned incidents
- Active incidents
- Resolved incidents
- Incidents unassigned or assigned by percentage
- Incidents source by percentage
- Total open incidents

TIP: If you are using the new user interface for SL1, you can download the *ServiceNow: BasePack SL1 Dashboards PowerPack* to add this dashboard to the new user interface.

© 2003 - 2020, 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

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

International: +1-703-354-1010