RESILIENT SYSTEMS

# Integration Guide for HP ArcSight

Version 1.2


One Alewife Center • Suite 450
Cambridge, MA 02140
Phone 617.206.3900 • Fax 617.206.3825

# Table of Contents

# Overview

The Resilient Systems Application supports integration with HP ArcSight to simplify and streamline the process of escalating and managing incidents.

Resilient is an open system with many integration points, ranging from user-configurable connections, simple scripts, through complex custom workflows. The integration techniques include:

1. Email. Resilient Systems provides an email integration feature that can be used to process emails from the ArcSight server, extract information from each email, and then populate an incident and related information in Resilient. This provides automatic and easily managed integration with every user's familiar tools.

2. "Right-click" or Web URL integration. The user interface of HP ArcSight can be extended to add custom commands and configurations. In these configurations, a simple customization creates a direct link from the ArcSight UI where users can immediately create and enrich incidents in Resilient.

3. Automated escalation. Resilient Systems provides a simple, configurable utility that processes ArcSight "export files" and creates corresponding incidents and related artifacts. ArcSight can be configured to export selected incidents automatically, resulting in automated escalation.

4. Custom integration. The Resilient REST APIs can be used for extensive custom integration. Additionally, the Resilient Actions Module can trigger custom actions when incident status changes in the Resilient system. The Resilient API includes documentation and examples of these patterns in several popular programming languages. The result is a deep and powerful combination of product features, producing a streamlined response workflow.

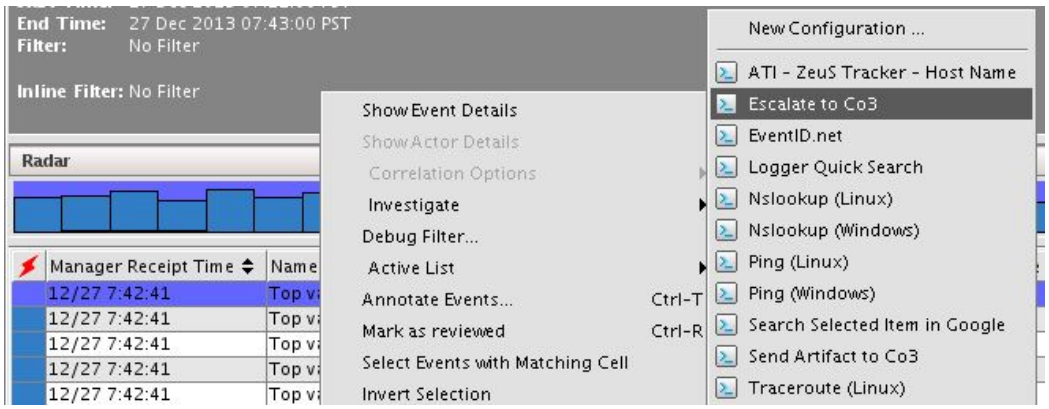
This document describes how to configure "right-click" Web URL integration in ArcSight. It should be read in conjunction with the Resilient Web URL Integration Guide, which contains useful reference material.

## Web URL Integration Overview

By directing a user's browser to specially-constructed Web URLs, the user can be guided through automatic creation of an incident, and other functions.

A typical use case for this integration is in manually creating Resilient incidents from within HP ArcSight. This streamlines the process of escalation to the incident response team.

The ArcSight user interface can be extended to add custom commands and configurations. In these configurations, a simple customization creates a direct link from the ArcSight UI where users can immediately create and enrich incidents in Resilient.




This integration uses ArcSight's **Integration Commands** feature. There are two steps to configure these integrations in ArcSight: the creation of **commands** and then **configurations**. The configuration determines how the command is carried out.

# Manual Escalation of Incidents

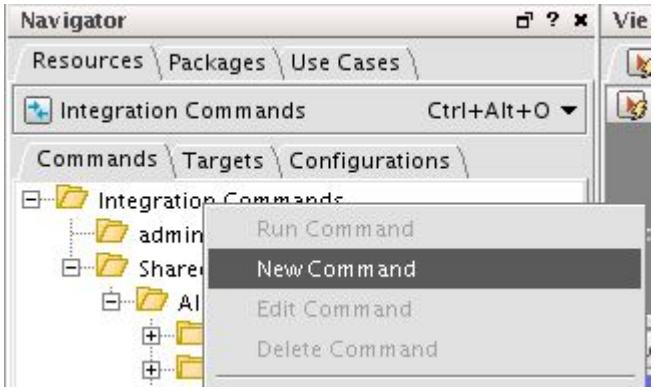
Follow the steps below to configure a manual escalation facility, which creates a new incident in Resilient starting from the ArcSight user interface.

## Creating the Integration Command

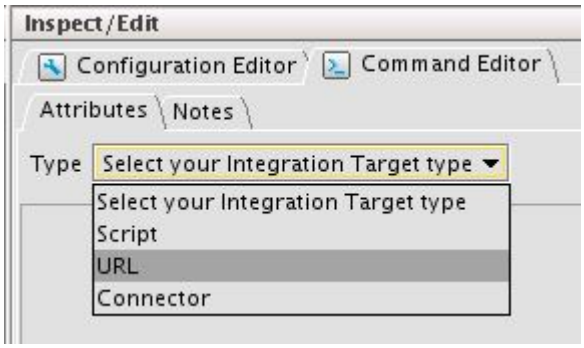
In the drop down menu on the left side of the ArcSight console, choose **Integration Commands**.

Make sure you have the Commands tab selected. Right click on a folder and select New Group to create a new group folder called "Resilient".

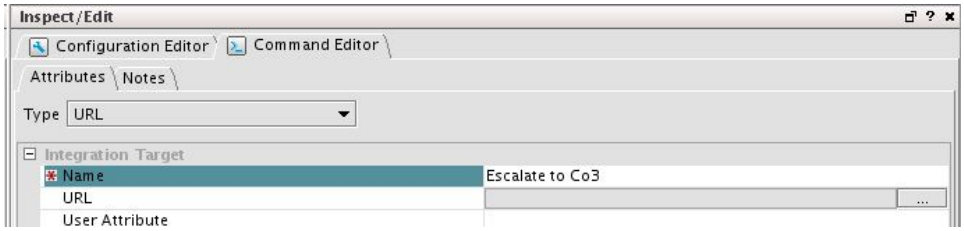
Right click your new folder and choose **New Command**. The command editor opens.



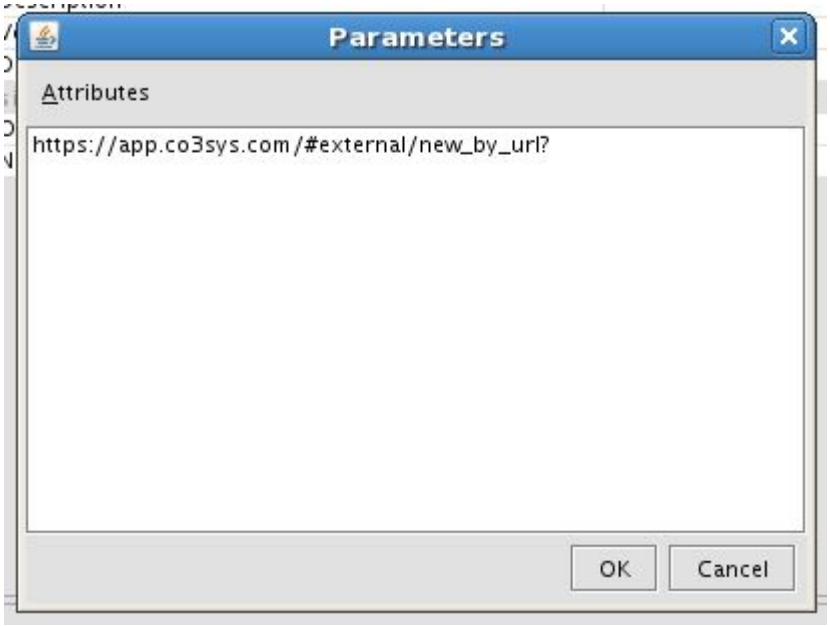

In the command editor box, select "URL" as the Integration Target Type.




Give your command a name, such as "Escalate to Resilient".




In the URL field, click on the ellipsis (…) button to enter the URL to send information to, and the parameters dialog will appear.




In this box you will enter the base URL and configure the fields you wish to map to your Resilient Incident.

The base URL is your normal Resilient application URL, followed by "`#external/new_by_url?`". For example, enter the full URL below:

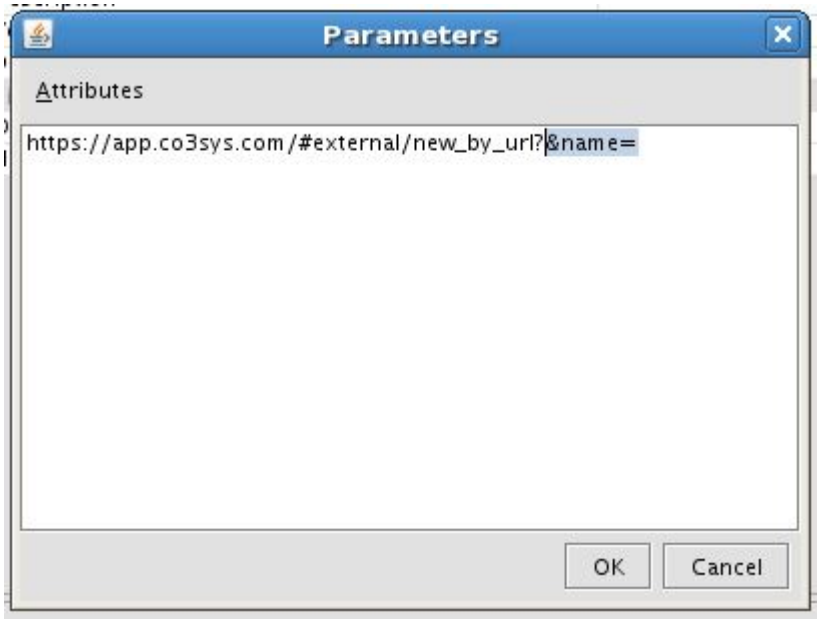
```
https://app.resilientsystems.com/#external/new_by_url?
```

After the '`?`', you specify **parameters** that map ArcSight field values onto fields in the Resilient incident. You can create static parameters that never change, as well as variable parameters that carry values from ArcSight into Resilient. Multiple parameters are separated by the ampersand ("`&`").

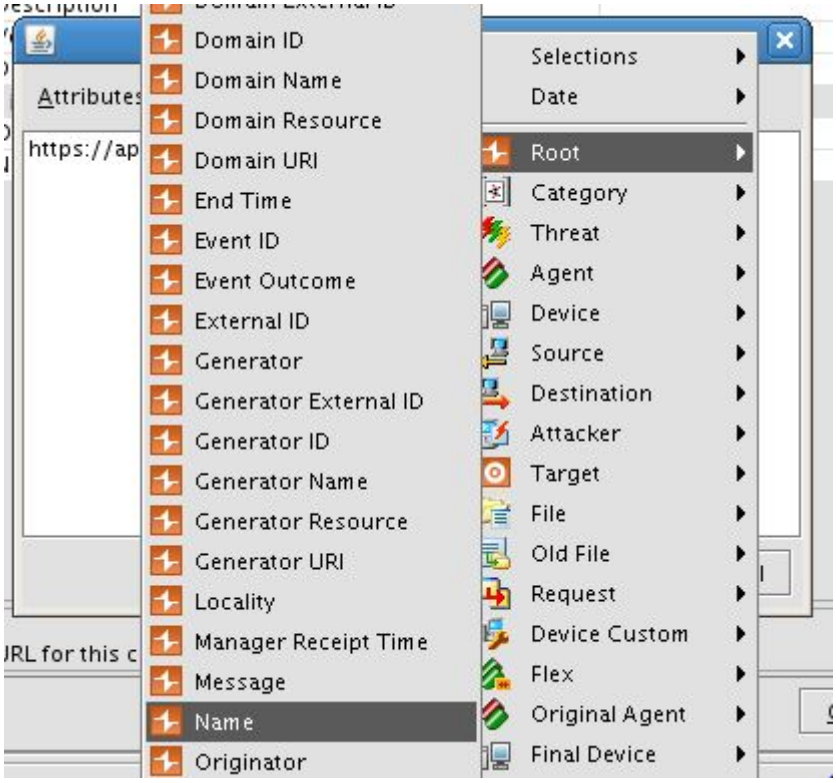
For example, a full URL with parameters to set the name of the new incident to the word "New", and a description of "Incident",

```
https://app.resilientsystems.com/#external/new_by_url?&name=New&descripti
on=Incident
```

The ArcSight Parameters dialog in ArcSight helps you map ArcSight's values to the URL parameters. This is done by choosing a desired Resilient parameter and adding it to the base URL. You will then right-click in the parameters box and choose the ArcSight field that you wish to map to it. Each parameter will appear as a name like "`${address}`".

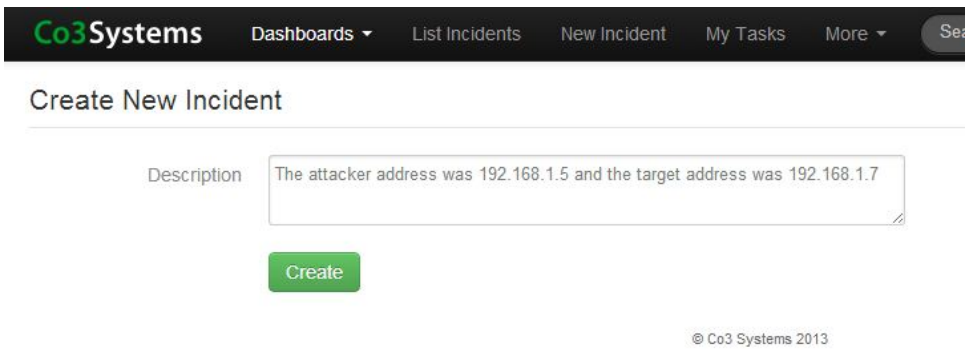


Then, right click to add the ArcSight field Root->Name




You may add many more fields to your URL. You can also add multiple ArcSight field values into the value of a single URL parameter. For example, you could add an attacker address to your description, as well as the target. The URL would then look like this:

```
https://app.resilientsystems.com/#external/new_by_url?&description=The attacker address was ${attackerAddress} and the target address was ${targetAddress}
```




Once your URL is configured, click OK to save your work, then click OK again to save your command in the command editor dialog box.

A Resilient **incident** has an extensive set of fields that can be configured in this way.

Refer to the document "**Web URL Integration Guide**" for a complete guide, including a list of the standard Resilient field names, valid values for the standard set of coded fields (Country, etc.), and additional techniques to specify fields of different types.

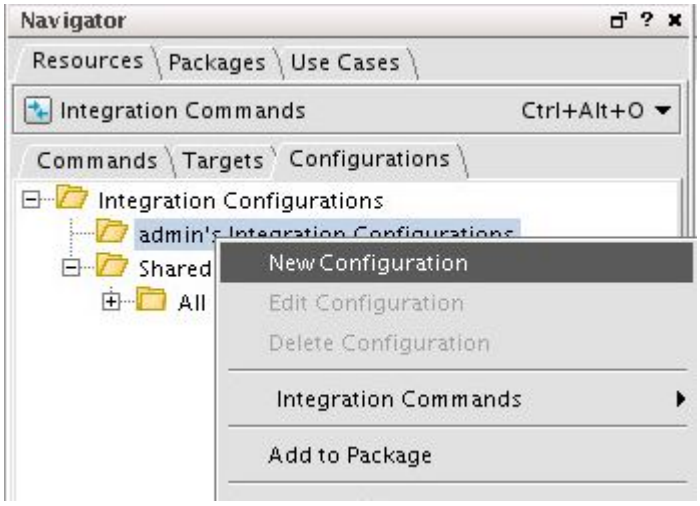
## Creating the Configuration

The Configuration options determine how the Command operates, such as where it is available in your ArcSight console.

On the right side of the screen, you should still be on the Integration Configuration option in the dropdown list. Select the Configurations tab.

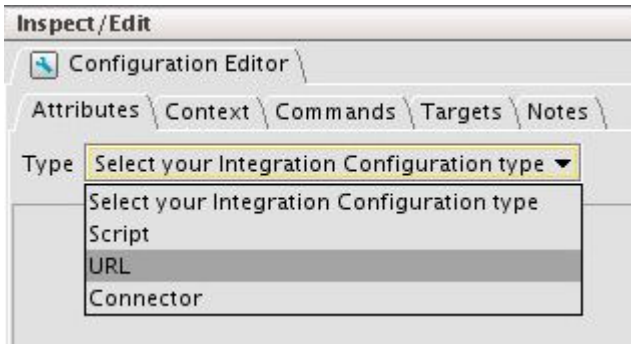
Right click your folder and choose New Group then name your group Resilient.

Right click your new Resilient folder and choose **New Configuration**

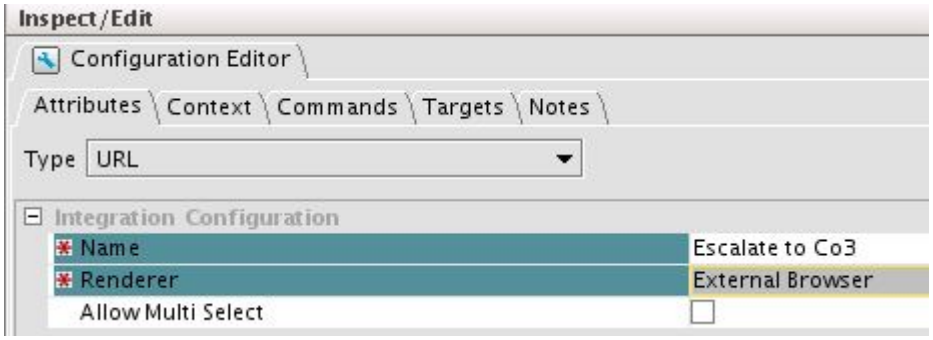



This opens the Configuration Editor on the right side of the screen.

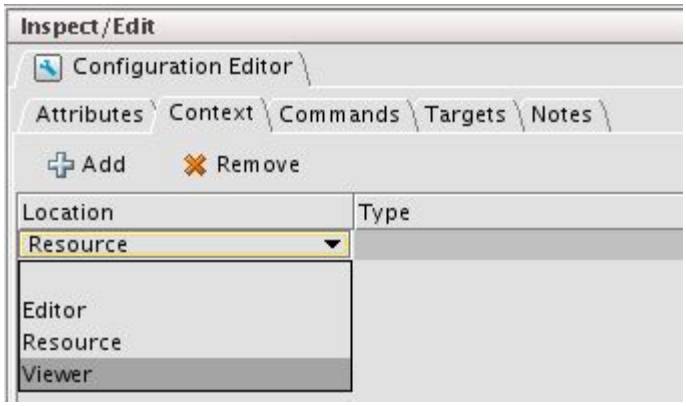
Within the Configuration editor, on the Attributes tab, there is a dropdown menu which allows you to select your Configuration type. Choose URL from the list.



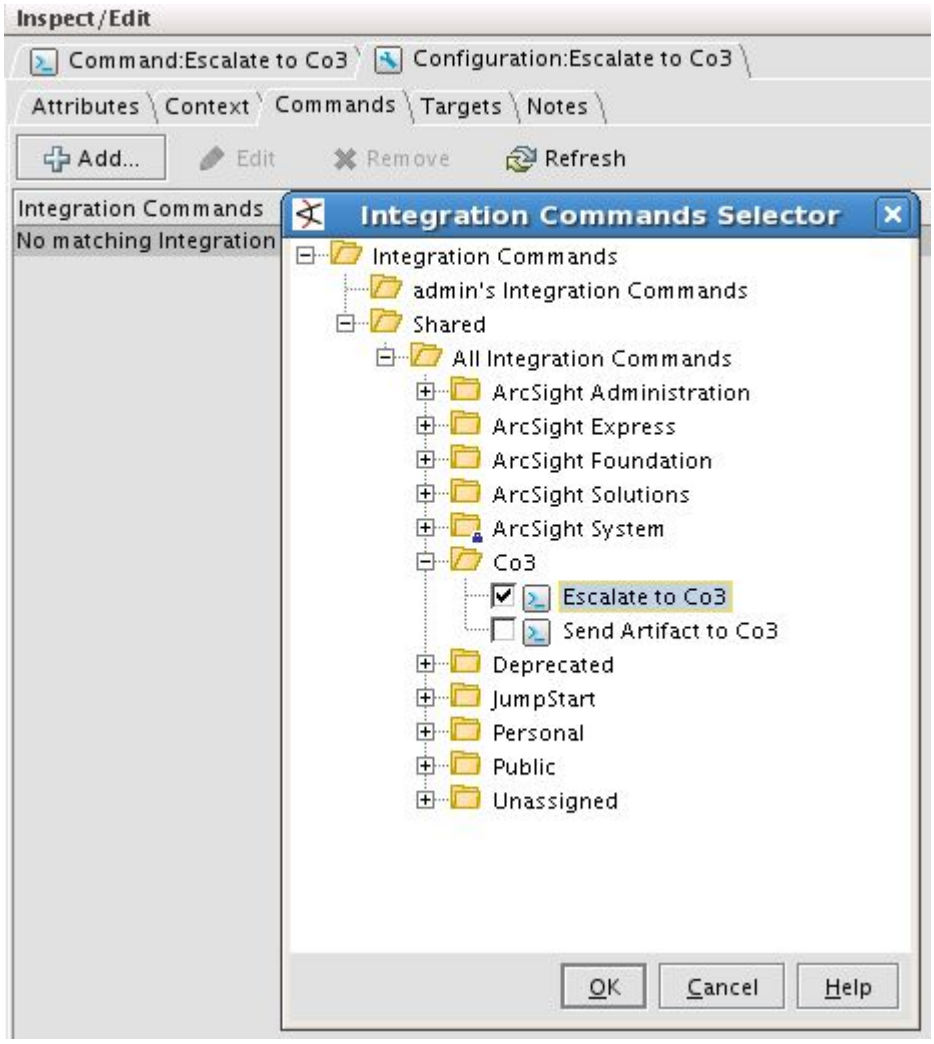

Next, give your Configuration a name, and choose how the URL is launched. Name your configuration (e.g. "**Escalate to Resilient**") and choose **External Browser** for the renderer.




Click on the Context tab and then click on the **Add** button. Click in the cell underneath **Location** and choose **Viewer** from the dropdown list.



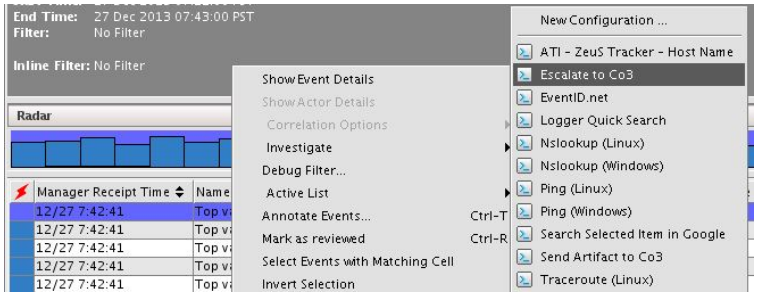

Click on the **Commands** tab, and then click on the **Add** button. A new box will appear. Find your Resilient folder and the Integration Command that you configured previously, then click the checkbox next to it to select this command into the configuration.



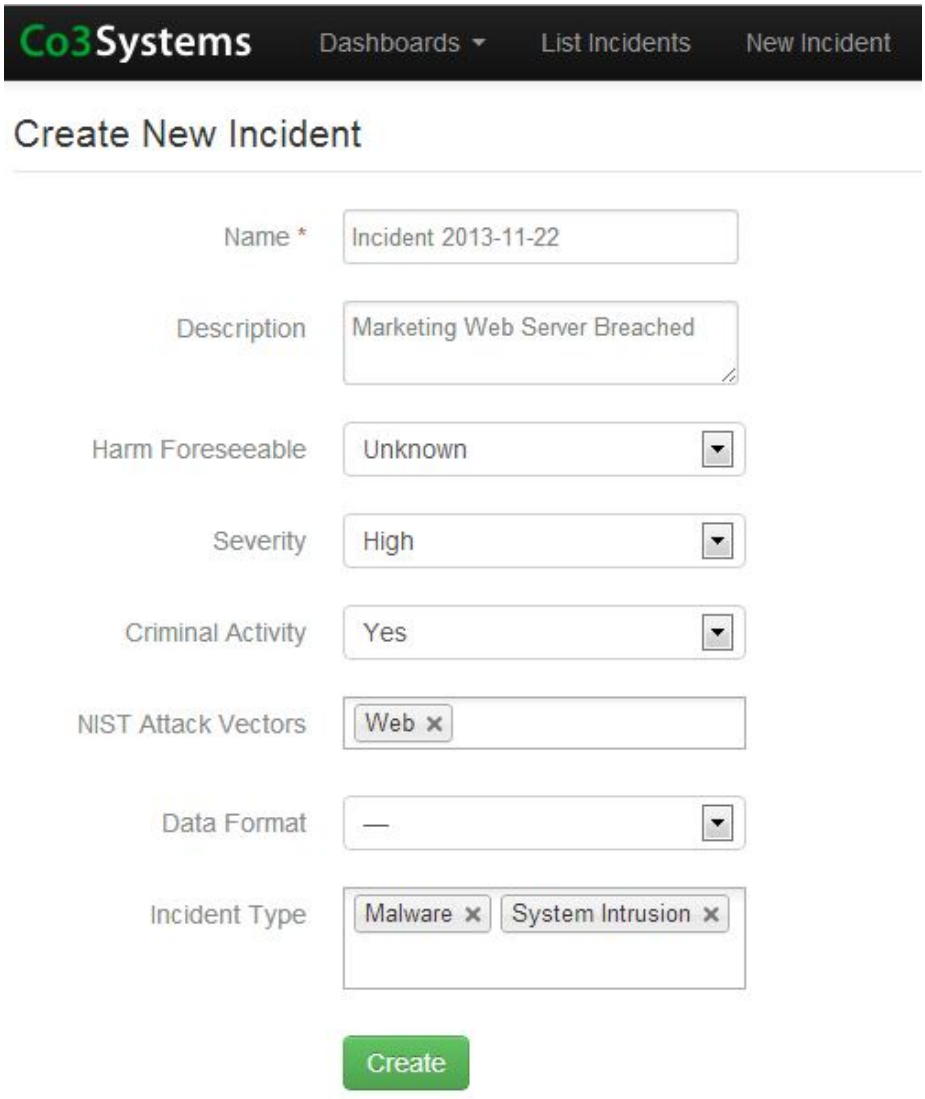

Click OK to save your selection, then click OK again at the bottom of the Configuration editor to save your work.

## Testing the Integration

You can now test your integration command by right clicking an event in the ArcSight Viewer panel, navigating to Integration Commands, and choosing **Escalate to Resilient**.



This will open an external browser providing a login prompt for Resilient if you're not already logged in. Once logged in, you will see the details of the incident being created including the values being mapped from the ArcSight fields. From here you can approve or change your selections and click the **Create** button to create your new incident in Resilient.



# Adding Threat Information to Existing Incidents

Follow the steps below to configure enrichment, which adds threat information from ArcSight to an existing incident in Resilient starting from the ArcSight user interface.

This process is very similar to the manual escalation steps previously detailed. The main differences are,

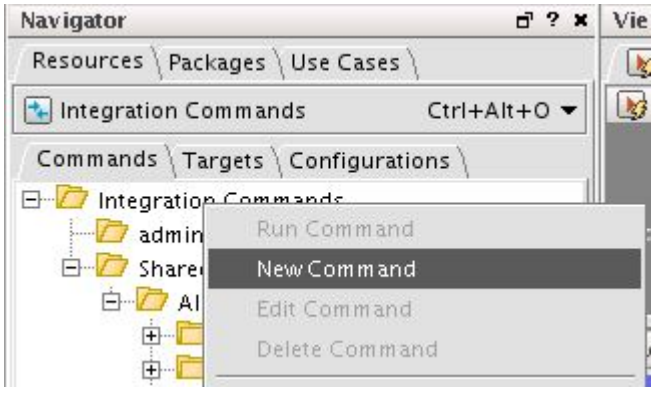
- The incident must already exist, and
- The threat information is stored as Artifacts in the incident, and each artifact has a fixed and structured set of fields.

## Creating the Integration Command

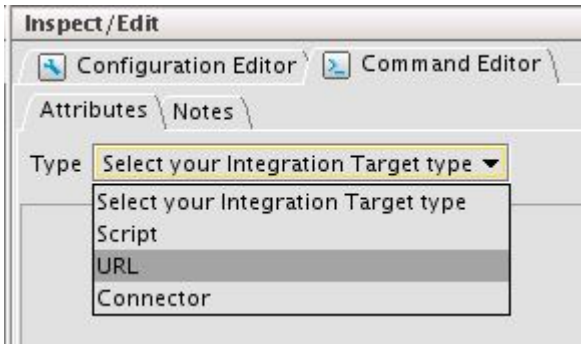
In the drop down menu on the left side of the ArcSight console, choose the **Integration Commands** option.

Make sure you have the Commands tab selected. You can add this new command to the folder you already created ("Resilient").

Right click your new folder and choose **New Command.** The command editor opens.

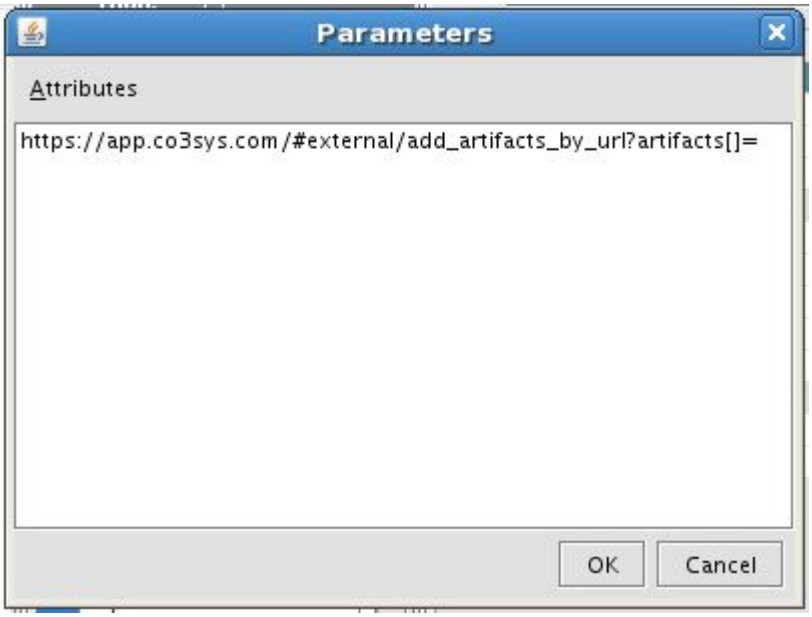



In the command editor box, select "URL" as the Integration Target Type.




Give your command a name, such as "Add Threat Intel to Resilient".

In the URL field, click on the ellipsis (…) button to enter the URL to send information to, and the Parameters dialog will appear. In this dialog box you will enter the base URL and configure the fields you wish to map to artifacts in your Resilient Incident.




The base URL is your normal Resilient application URL, followed by "`#external/add_artifacts_by_url?artifacts[]=`". For example, enter the full URL below:

```
https://app.resilientsystems.com/#external/add_artifacts_by_url?artifacts
[]=
```

After this base URL you will configure a list of artifacts. Each is specified with a number signifying the artifact type, and then the artifact itself, separated by a comma. For example, if the number 1 is used to indicate an IP address, and the IP address is 192.168.1.2, then the resulting URL would be:

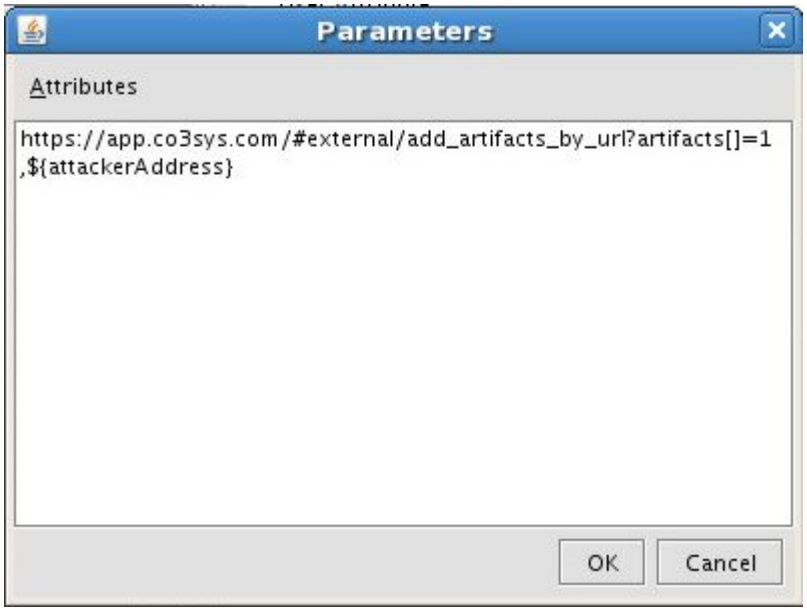
```
https://app.resilientsystems.com/#external/add_artifacts_by_url?artifacts
[]=1,192.168.1.2
```

You may add many more artifacts to the list in your URL, separated with commas.

Typical artifact types include IP addresses, DNS names, URLs. You can also add Email subject, body, attachment name and sender. Refer to the document "**Web URL Integration Guide**" for a complete guide.

For each artifact, you must map fields from ArcSight to Resilient. This is done by choosing a Resilient artifact type ID, and adding it to the base URL. Then right-click the parameters box and choose an ArcSight field that you wish to map to it. Each parameter will appear as a name like "`${address}`".

The following example adds the Attacker Address.




Once your URL is configured, click OK to save your work, then click OK again to save your command in the command editor dialog box.

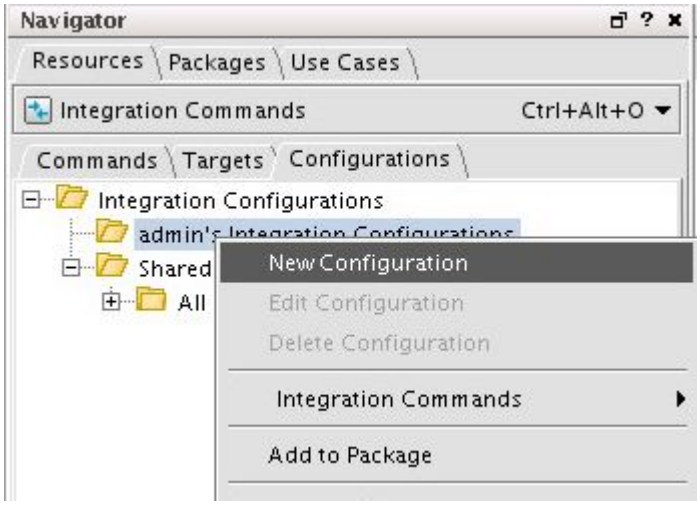
## Step 2. Create your Configuration

The Configuration options determine how the Command operates, such as where it is available in your ArcSight console.

On the right side of the screen, you should still be on the Integration Configuration option in the dropdown list. Select the Configurations tab.

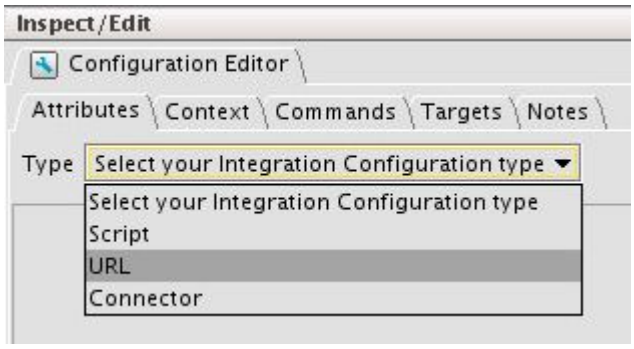
Right click your folder and choose New Group if necessary, then name your group Resilient.

Right click your new Resilient folder and choose **New Configuration**

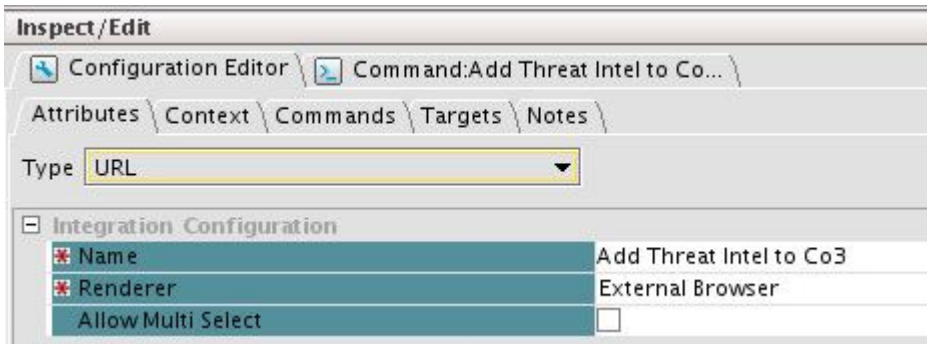



This opens the Configuration Editor on the right side of the screen.

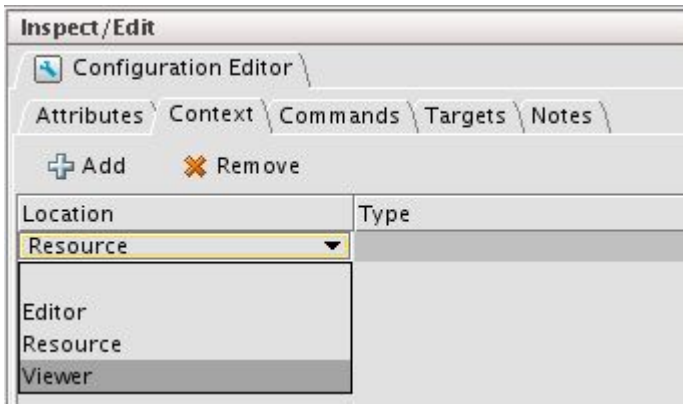
Within the Configuration editor, on the Attributes tab, there is a dropdown menu which allows you to select your Configuration type. Choose URL from the list.



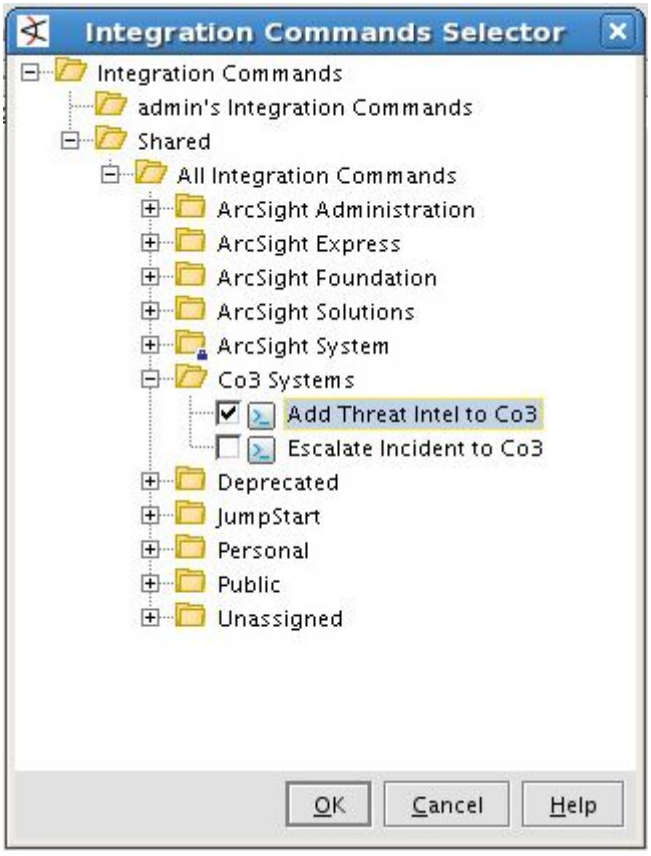

Next, give your Configuration a name, and choose how the URL is launched. Name your configuration (e.g. "**Add Threat Intel to Resilient**") and chose **External Browser** for the renderer.




Click on the Context tab and then click on the **Add** button. Click in the cell underneath **Location** and choose **Viewer** from the dropdown list.



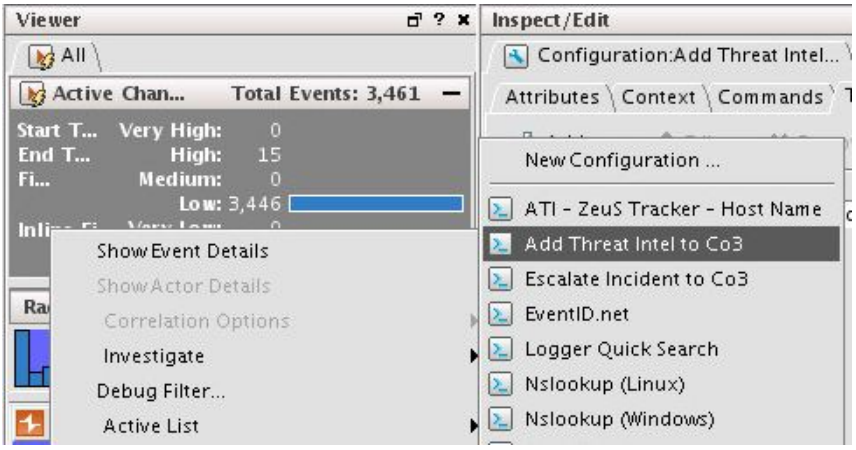

Click on the **Commands** tab, and then click on the **Add** button. A new box will appear. Find your Resilient folder and the Integration Command that you configured previously, then click the checkbox next to it to select this command into the configuration.



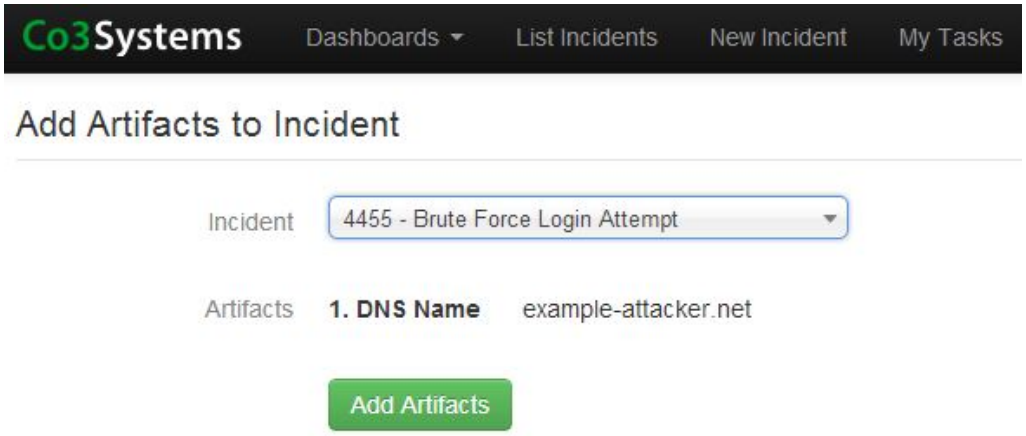

Click OK to save your selection, then click OK again at the bottom of the Configuration editor to save your work.

## Testing the Integration

You can now test your integration command by right-clicking an event in the ArcSight Viewer panel, navigating to Integration Commands, and choosing **Add Threat Intel to Resilient**.

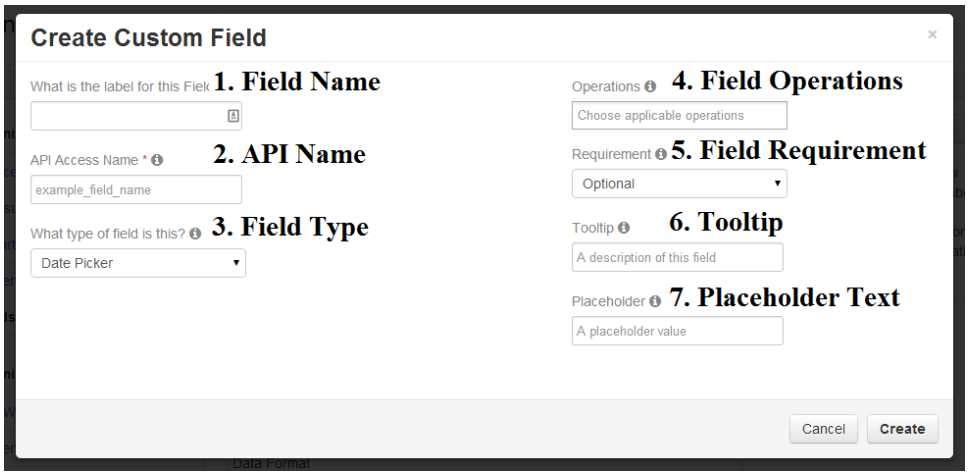


This will open an external browser providing a login prompt. Once logged in, you can add your Artifact by selecting the appropriate Incident from the dropdown list and clicking on the **Add Artifacts** button.



The ArcSight integration can be further extended by the use of custom fields in Resilient. Custom fields could potentially be created to consume the contents of any fieldset data in ArcSight.

To create a custom field in Resilient,




1. Field name – This is the name that will appear in the interface next to your custom field
2. API Name – An automatically generated name for this field in the database for use with the API. This field can be modified if necessary.
3. Field type – This is the type of custom field. Options include:
    a. Data picker – to select a date
    b. Text – a single line text box
    c. Number – An integer only field
    d. Text area – Free form text input
    e. Select – Dropdown with user-defined menu and options to define the type of scrolling, blank options, and default values
    f. Boolean – A dropdown with selections for Yes, No, and Unknown
    g. Multiple Select – Like Select, but with options to multi-select answers.
4. Field operations – This option is used for the **Notifications** engine. Here you decide what operations would cause a notification to trigger, such as your custom field being selected. In such an instance the **equals** option would be selected
5. Field requirements – Here you'll decide if selecting your field is optional, required, or required upon close. The **on close**
6. Field Tooltip – Decide if your field needs a pop up Tooltip and its contents.
7. Field placeholder – The example text that appears inside a custom field box

To address a custom field via the URL, use its **API name** in the integration.