

# IBM Resilient



## Incident Response Platform

ADD-ON FOR SPLUNK USER GUIDE v1.0

Licensed Materials – Property of IBM

© Copyright IBM Corp. 2010, 2018. All Rights Reserved.

US Government Users Restricted Rights: Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

### **Resilient Incident Response Platform Add-On for Splunk User Guide**

<b>Version</b>	<b>Publication</b>	<b>Notes</b>
1.0	April 2018	Updated Splunk version number.
1.0	January 2018	Initial publication.

## Table of Contents

<b>1. Overview .....</b>	<b>5</b>
<b>2. Installation .....</b>	<b>5</b>
2.1. Requirements.....	5
2.2. Installation and Setup .....	5
2.3. Configuration.....	6
<b>3. Escalating Splunk Alerts .....</b>	<b>7</b>
3.1. Adding a Splunk Alert Action .....	7
3.2. Updating the Default Incident Mapping .....	8
<b>4. Escalating Splunk ES Notable Events .....</b>	<b>8</b>
4.1. Adding an Adaptive Response Action.....	8
4.2. Ad Hoc Invocation.....	10
4.3. Show Escalated Notable Events .....	13
4.4. Mapping Additional Fields .....	13
4.5. Mapping event_id for Notable Events .....	14
4.6. Updating the Default Incident Mapping .....	14
<b>5. Troubleshooting .....</b>	<b>16</b>
5.1. Setup Screen .....	16
5.2. Incident Not Created .....	16
5.3. Ad Hoc Invocation Failure .....	16
<b>6. Support.....</b>	<b>17</b>



# 1. Overview

The Resilient Add-On supports Splunk and Splunk ES. The Add-On provides the capability of escalating a Splunk alert or Splunk ES notable event to a Resilient incident.

The Resilient Add-On features include:

- **Easy Incident Mapping:** Enables mapping of static values or search result tokens into Resilient incident fields. You can map fields parsed from the event in the alert or notable event directly into any incident field. You also have custom incident mapping rules for each saved alert or notable event.
- **Create Artifacts:** Maps result tokens into artifacts at the same time the incident mapping is defined.
- **Custom Field Discovery:** Retrieves the incident definition from the Resilient platform so that all defined fields and field values are catalogued inside Splunk or Splunk ES. This allows you to add custom fields to the Resilient platform, which are then available for mapping in Splunk or Splunk ES.
- **Automatic and manual escalation:** Escalates notable events from a correlation search or alerts from a saved search to Resilient incidents (automatic escalation). For Splunk ES only, you can escalate notable events as an ad hoc action (manual escalation).

## 2. Installation

### 2.1. Requirements

The following lists the system requirements:

- Splunk version 7.0 or later, or Splunk Cloud
- Splunk ES 4.7.2 or later, or Splunk ES Cloud
- Splunk CIM framework is installed
- Resilient platform version 27 or later
- Ability to connect directly from Splunk to your Resilient platform with HTTPS on port 443
- You have a Master Administrator or equivalent account on the Resilient platform

### 2.2. Installation and Setup

For Splunk Cloud and Splunk ES Cloud users, contact Splunk Support to create a ticket for installing the Resilient Add-On.

If you have installed Splunk or Splunk on-premises, you can download and install the add-on from [Splunkbase](#). Alternatively, you can request an installer from IBM Resilient.

After installing the add-on and restarting Splunk, navigate back to the App Manager screen. Click **Set up** in the Resilient row. Fill out the required attributes for your Resilient platform and click **Save**. When you save, the Set Up program performs the following:

- Retrieves the incident definition from the Resilient platform, so that all fields, including custom fields, are catalogued.  
**NOTE:** If a Resilient administrator adds custom fields after you run Set Up, you need to run Set Up again to capture the fields.
- Tests the configuration to verify that the connection is successful. If the configuration saves successfully, you are up and running.

Refer to the [Troubleshooting](#) section if you encounter a problem.

## 2.3. Configuration

**Hostname for Resilient server:** Hostname or IP for your Resilient platform. Do not include the https:// prefix.

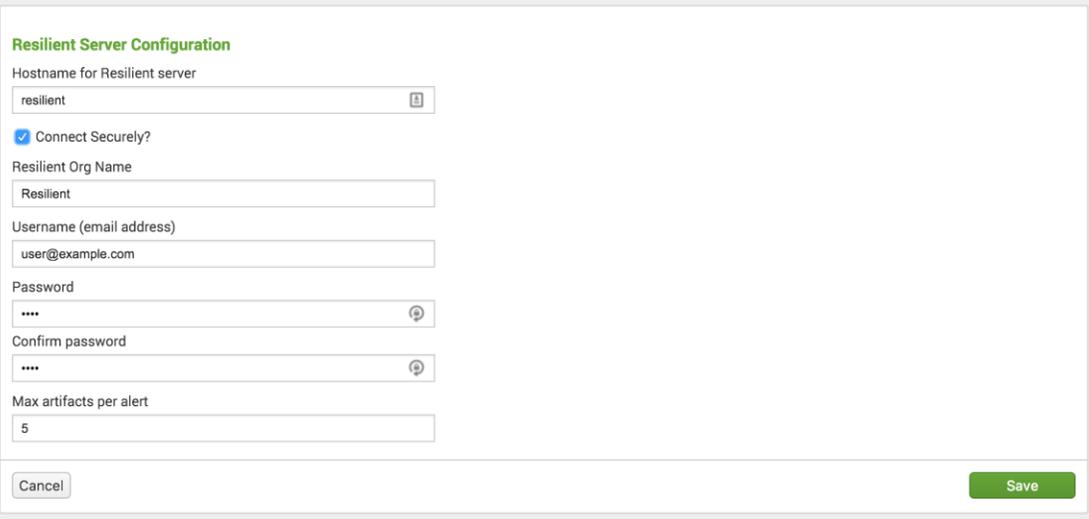
**Connect Securely:** Do not check if using self-signed certificates on your Resilient platform.

**Resilient Org Name:** The name of the Resilient organization.

**Username (email address):** User name of the registered Resilient master administrator or equivalent account.

**Password:** Password for the Resilient account.

**Max Artifacts per alert:** Maximum number of artifacts you may need to map into a single Resilient incident from any given Splunk alert or Splunk ES notable event.



The image shows a configuration form titled "Resilient Server Configuration". It contains the following fields and controls:

- Hostname for Resilient server:** A text input field containing the value "resilient".
- Connect Securely?:** A checked checkbox.
- Resilient Org Name:** A text input field containing the value "Resilient".
- Username (email address):** A text input field containing the value "user@example.com".
- Password:** A password input field with masked characters (dots) and a visibility toggle icon.
- Confirm password:** A password input field with masked characters (dots) and a visibility toggle icon.
- Max artifacts per alert:** A text input field containing the value "5".

At the bottom of the form, there are two buttons: "Cancel" on the left and "Save" on the right.

## 3. Escalating Splunk Alerts

### 3.1. Adding a Splunk Alert Action

To add a Resilient escalation to an alert, go to the **Alerts** tab in the Search & Reporting app and find the alert for which you want to create a Resilient incident. Click **Edit**, and select **Edit Actions**. Click **+ Add Actions** and select **Resilient**. Update the incident fields to indicate how you want them mapped. You can use static values or tokens from the alert data. In addition to the fields parsed in your particular alert search, the [Splunk documentation](#) has a list of the default tokens available in any search.

Be sure to map a valid value for the Date Discovered field, which is always required.

A sample alert, `sa_failed_splunk_login`, is included. If you enable this alert, a Resilient incident is created each time there is a failed login attempt to Splunk. If you have added custom required fields to your Resilient platform, you need to edit the mapping on the alert action screen to include them before triggering the example.



Edit Alert
✕

Run on Cron Schedule ▾

Time Range

Last 5 minutes ▶

Cron Expression

\*/5 \* \* \* \*

e.g. 00 18 \*\*\* (every day at 6PM). [Learn More](#)

**Trigger Conditions**

Trigger alert when

Number of Results ▾

is greater than ▾

0

Trigger

Once

For each result

Throttle?

**Trigger Actions**

+ Add Actions ▾

When triggered

▾

Create Resilient Incident (SA-Resilient)
 Remove

Enter a value to map for each incident field.  
 This text can include tokens that will  
 resolve to text based on search results.  
[Learn More](#)

\* required

Date Discovered

\$result\_time\$ \*

Name

\$result.rule\_title\$ (from Splunk) \*

Cancel

Save

## 3.2. Updating the Default Incident Mapping

You can change the default mapping when you configure the action. If the incident mapping for most of your alerts will be very similar, you may want to override the default mapping where all the alerts start. Create an `alert_actions.conf` in `$(SPLUNK_HOME)/etc/apps/SA-resilient/local` and override the default mappings.

# 4. Escalating Splunk ES Notable Events

## 4.1. Adding an Adaptive Response Action

To add a Resilient escalation to a correlation search, go to the **Configure** tab in the Enterprise Security App, and select **Content Management**. Click the correlation search for which you want to create a Resilient incident and scroll down to the **Adaptive Response Actions** section. Click **+ Add New Response Action** and select **Create Resilient Incident (SA-Resilient)**. Update the incident fields to indicate how you want them mapped.

To create a new correlation search, go to the **Configure** tab in the Enterprise Security App and select **Content Management**. Click **Create New Content** and select **Correlation Search**. Create a new correlation. A sample correlation search, `failed_splunk_login_cs`, is included, which you can find in **Content Management**.

### Correlation Search

Search Name \*

Application Context \*

UI Dispatch Context \*

Set an app to use for links such as the drill-down search in a notable event or links in an email adaptive response action. If None, uses the Application Context.

Description

Describes what kind of issues this search is intended to detect.

Mode  Guided  Manual

Search \*

### Time Range

Earliest Time

Set a time range of events to search. Type an earliest time using relative time modifiers.

Scroll down to the Adaptive Response Actions section and view that the Resilient Add-On has been added as a response in this sample correlation search. You can change the default configuration.

**Trigger Conditions**

Trigger alert when

**Throttling**

Window duration

How much time to ignore other events that match the field values specified in Fields to group by.

Fields to group by   
Type the fields to consider for matching events for throttling. [Learn More](#)

**Adaptive Response Actions**

[+ Add New Response Action](#)

▼ **Create Resilient Incident (SA-Resilient)** ✕

Enter a value to map for each incident field. This text can include tokens that will resolve to text based on search results. [Learn More](#)

**\* required**

Date Discovered  \*

Name  \*

Description

Simulation

Splunk Notable Event ID

## 4.2. Ad Hoc Invocation

You can dispatch Resilient Add-On as an ad hoc invocation. To escalate a notable event, go to the Incident Review tab of Enterprise Security. Locate the notable event that you wish to escalate and select **Run Adaptive Response Actions** in the Actions column.

The screenshot displays the Splunk Enterprise Security 'Incident Review' interface. On the left, there are filters for Urgency (CRITICAL: 0, HIGH: 0, MEDIUM: 0, LOW: 12, INFO: 0), Status (All), Correlation Search Name, Owner (All), Security Domain (All), and Tag. A bar chart shows 12 events from 12/1/17 to 1/1/18. The main table lists 12 events, all with 'Urgency: Low' and 'Status: New'. The 'Run Adaptive Response Actions' option is highlighted in the Actions column for the selected event.

i	Time	Security Domain	Title	Urgency	Status	Owner	Actions
>	12/26/17 9:35:33.000 AM	Threat	Manual Notable Event - Rule	Low	New	unassigned	<ul style="list-style-type: none"> <li>Add Event to Investigation</li> <li>Create notable event</li> <li>Build Event Type</li> <li>Extract Fields</li> <li>Run Adaptive Response Actions</li> <li>Share Notable Event</li> <li>Suppress Notable Events</li> <li>Show Source</li> </ul>
>	12/20/17 11:20:29.000 AM	Threat	Manual Notable Event - Rule	Low	New		
>	12/20/17 11:14:26.000 AM	Threat	Manual Notable Event - Rule	Low	New		
>	12/20/17 11:14:06.000 AM	Threat	Manual Notable Event - Rule	Low	New		
>	12/20/17 10:13:24.000 AM	Threat	Manual Notable Event - Rule	Low	New		
>	12/6/17 3:30:33.000 PM	Threat	Manual Notable Event - Rule	Low	New		
>	12/6/17 3:27:24.000 PM	Threat	Manual Notable Event - Rule	Low	New		
>	12/6/17 3:27:14.000 PM	Threat	Manual Notable Event - Rule	Low	New		
>	12/6/17 3:25:36.000 PM	Threat	Manual Notable Event - Rule	Low	New		
>	12/6/17 3:23:04.000 PM	Threat	Manual Notable Event - Rule	Low	New		

Click **+ Add New Response Action**, and select **Create Resilient Incident (SA-Resilient)**. Update the incident fields to indicate how you want them mapped.

Adaptive Response Actions ×

Select actions to run.

[+ Add New Response Action](#) ▾

▾ **Create Resilient Incident (SA-Resilient)** ×

Enter a value to map for each incident field. This text can include tokens that will resolve to text based on search results. [Learn More](#) 🔗

**\* required**

Date Discovered  \*

Name  \*

Description

Simulation

Splunk Notable Event ID

Reporting Individual

Address

City

Incident Disposition

Country

Criminal Activity

Click **Run** to escalate. Once completed, refresh the page to see the updated notable event. The comment contains the Incident ID for the incident created. The **Adaptive Responses** field, shown below, displays a success status for **Create Resilient Incident**.

12/26/17 9:35:33.000 AM
Threat

Manual Notable Event  
- Rule

●
Low

New

unassigned

**Description:**  
manually generated using makeresults

Additional Fields	Value	Action
Resilient Test	Success	▼

**Related Investigations:**  
Currently not investigated.

**Correlation Search:**  
None (manually created)

**History:**

2017 Dec 26 10:00:23 AM admin  
Resilient Incident ID: 14008

[View all review activity for this Notable Event](#)

**Adaptive Responses:** 🔄

Response	Mode	Time	User	Status
<a href="#">Create Resilient Incident</a>	adhoc	2017-12-26T10:00:21-0500	system	✓ success
Notable	adhoc	2017-12-26T09:35:30-0500	system	✓ success

[View Adaptive Response Invocations](#)

**Next Steps:**

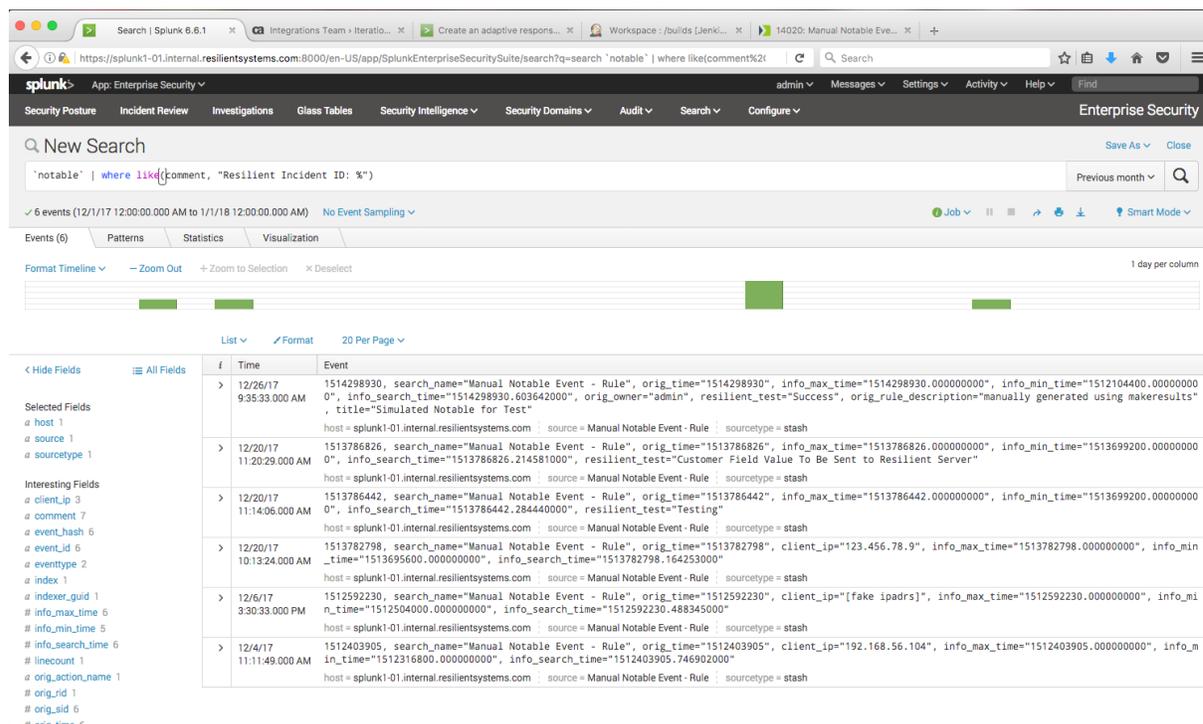
🔔 No Next Steps defined.

**Event Details:**

event_id	1A2BE372-D353-46D3-A775-E577A7AA1068@@notable@@7f3d7632b7660edbdec44daa404a6a39	▼
event_hash	7f3d7632b7660edbdec44daa404a6a39	▼
eventtype	modnotable_results	▼
	notable	▼
Short ID	<a href="#">Create Short ID</a>	

## 4.3. Show Escalated Notable Events

Each time a notable event is escalated successfully, the corresponding Resilient ID is added to the comment field of the notable event. This allows Splunk ES users to easily search for all the notable events escalated successfully. To perform a search, enter the search parameter, such as ``notable` | where like(comment, "Resilient Incident ID: %")`, in the **Search** tab of **Enterprise Security**. For example:



The screenshot shows the Splunk Enterprise Security interface. The search bar contains the query: ``notable` | where like(comment, "Resilient Incident ID: %")`. The search results are displayed in a table format with columns for Time and Event. The table shows several notable events with their respective timestamps and details.

Time	Event
12/26/17 9:35:33.000 AM	1514298930, search_name="Manual Notable Event - Rule", orig_time="1514298930", info_max_time="1514298930.000000000", info_min_time="1512104400.000000000", info_search_time="1514298930.603642000", orig_owner="admin", resilient_test="Success", orig_rule_description="manually generated using makeresults", title="Simulated Notable for Test" host = splunk1-01.internal.resilientsystems.com   source = Manual Notable Event - Rule   sourcetype = stash
12/20/17 11:20:29.000 AM	1513786826, search_name="Manual Notable Event - Rule", orig_time="1513786826", info_max_time="1513786826.000000000", info_min_time="1513699200.000000000", info_search_time="1513786826.214581000", resilient_test="Customer Field Value To Be Sent to Resilient Server" host = splunk1-01.internal.resilientsystems.com   source = Manual Notable Event - Rule   sourcetype = stash
12/20/17 11:14:06.000 AM	1513786442, search_name="Manual Notable Event - Rule", orig_time="1513786442", info_max_time="1513786442.000000000", info_min_time="1513699200.000000000", info_search_time="1513786442.284440000", resilient_test="Testing" host = splunk1-01.internal.resilientsystems.com   source = Manual Notable Event - Rule   sourcetype = stash
12/20/17 10:13:24.000 AM	1513782798, search_name="Manual Notable Event - Rule", orig_time="1513782798", client_ip="123.456.78.9", info_max_time="1513782798.000000000", info_min_time="1513695600.000000000", info_search_time="1513782798.164253000" host = splunk1-01.internal.resilientsystems.com   source = Manual Notable Event - Rule   sourcetype = stash
12/6/17 3:30:33.000 PM	1512592230, search_name="Manual Notable Event - Rule", orig_time="1512592230", client_ip="[fake ipadrs]", info_max_time="1512592230.000000000", info_min_time="1512504000.000000000", info_search_time="1512592230.488345000" host = splunk1-01.internal.resilientsystems.com   source = Manual Notable Event - Rule   sourcetype = stash
12/4/17 11:11:49.000 AM	1512403905, search_name="Manual Notable Event - Rule", orig_time="1512403905", client_ip="192.168.56.104", info_max_time="1512403905.000000000", info_min_time="1512316800.000000000", info_search_time="1512403905.746902000" host = splunk1-01.internal.resilientsystems.com   source = Manual Notable Event - Rule   sourcetype = stash

## 4.4. Mapping Additional Fields

You can customize Splunk ES notable events by adding additional fields, as described in the [Splunk documentation](#). The additional fields can be used in mapping as the following token:

```
$.result.additional_field_label$
```

The `additional_field_label` is the label used for the additional field.

## 4.5. Mapping event\_id for Notable Events

In the Resilient platform, it is recommended that you create a customized field for the Resilient incident for notable event\_id. In the following example, the event\_id of a notable event is mapped to the customized field. Refer to the *Resilient Incident Response Platform Master Administrator Guide* for details.

**Editing Field** [X]

What type of field is this? ⓘ Text

What is the label for this field? \* ⓘ

Requirement ⓘ Optional

API Access Name \* ⓘ

Tooltip ⓘ

Placeholder ⓘ

 Cancel Save

## 4.6. Updating the Default Incident Mapping

Default mapping is provided in:

```

$SPLUNK_HOME/etc/apps/SA-Resilient/default/alert_actions.conf

```

This default mapping includes the following tokens. The mapping also includes a hyperlink to the notable event from Splunk ES.

Field	Token
Title of the notable	\$result.rule_title\$
Urgency	\$result.urgency\$
Owner	\$result.owner\$
Notable description	\$result.rule_description\$
Status	\$result.status\$

The following is an example of an incident created in the Resilient platform from the mapping.

**Manual Notable Event - Rule (from Splunk)** SIM Actions

Summary	Description
ID 14020	Manual Notable Event - Rule
Phase Respond	manually generated using makeresults
Severity -	Urgency: low
Date Created 01/02/2018	Owner: unassigned
Date Occurr... -	Status:1
Date Discov... 01/18/1970	Link to Splunk ES <a href="#">notable event</a>
Data Compr... Unknown	
Incident Type -	

Tasks Details Breach Notes Members News Feed Attachments Stats Timeline Artifacts **Custom**

**Custom** Edit

Splunk Notable Event ID	1A2BE372-D353-46D3-A775-E577A7AA1068@@notable@@7f3d7632b7660edbdec44daa404a6a39
-------------------------	---

You can change the default mapping when you configure the action.

## 5. Troubleshooting

### 5.1. Setup Screen

When you click **Save** on the Resilient Setup screen in Splunk, the app attempts to make a connection to your Resilient platform to verify that everything is configured correctly and to update the stored incident definition. If this connection fails, you see an error that looks like this:

resilient

Encountered the following error while trying to update: In handler 'localapps': Error while posting to url=/servicesNS/nobody/resilient/admin/resilientconfig/config

After a few seconds, the Splunk messages tab updates with detailed information about the cause of the failure.

Further information is logged to the following locations in Splunk:

- `$(SPLUNK_HOME)/var/log/splunk/splunkd.log`
- `$(SPLUNK_HOME)/var/log/splunk/python.log`

Some common causes of these issues include:

- Forgot to uncheck the “Connect securely?” box for self-signed certificate.
- Port 443 is blocked.

### 5.2. Incident Not Created

If an alert or automatic escalation for correlation search fails to create an incident, a message should be logged into the Splunk messages tab informing you of the issue. Further information is logged to the following location in Splunk: `$(SPLUNK_HOME)/var/log/splunk/resilient_modalert.log`

Some common causes of these issues include:

- Missing mappings for required fields.
- Fields mapped with invalid values.
- Connection unavailable.

### 5.3. Ad Hoc Invocation Failure

You can view the status of an ad hoc invocation when you refresh the Adaptive Response page. If it fails, click **View Adaptive Response Invocations**. In the search result, you should see a message, “See resilient\_modalert.log for details.”

The screenshot shows the Splunk Enterprise Security interface. The search bar contains the query: `tag=modaction (sid=1514298930.63153 rid=0) OR (dbrig_sid=1514298930.63153 orig_rid=0)`. The search results show 9 events from 1/26/17 9:30:30.000 AM to 1/2/18 1:22:14.000 PM. The event details are as follows:

Time	Event
1/2/18 1:17:14.752 PM	2018-01-02 18:17:14.752+0000 INFO sendmodaction - signature="Adaptive Response Action failed to create Resilient Incident! See resilient_modalert.log for details" action_name="resilient" sid="1514917027.1616" orig_sid="1514298930.63153" rid="0" orig_rid="0" app="SplunkEnterpriseSecuritySuite" user="system" action_mode="adhoc" action_status="failure"
	host = splunk1-01.internal.resilientsystems.com   source = /home/yfeng/Splunk/splunk/var/log/splunk/resilient_modalert.log   sourcetype = modular_alerts:resilient

You can then open `$(SPLUNK_HOME)/var/log/resilient_modalert.log` to look for details about the failure.

## 6. Support

For additional support, contact [support@resilientsystems.com](mailto:support@resilientsystems.com).

Including relevant information from the log files will help us resolve your issue.