



Incident Management Module

Step-by-Step Tutorial

Document Version: 01.00.03 | April 2019

Rsam © 2019. All rights reserved

[Privacy Policy](#) | [Terms of Service](#)

Contents

About Rsam Tutorials	3
Rsam Sandbox Environment	4
Sign-In Page.....	4
Rsam Incident Management.....	5
Overview	5
Incident Management Workflow.....	6
User Accounts	8
High-Level Steps	9
Step-by-Step Procedure.....	10
Step 1: Submitting an Incident	10
Step 2: Assigning an Owner	11
Step 3: Creating an Investigation	14
Step 4: Closing an Incident	16
Appendix 1: Email Notifications and Offline Decision Making	17
Setting up Email Addresses	17
Offline Decision Making	18
Appendix 2: Rsam Documentation	19
Incident Management Module Baseline Configuration Guide	19
Online Help	19

About Rsam Tutorials

The Rsam module step-by-step tutorials are designed to help you learn about a specific Rsam module and to gain basic familiarity with the user interface. The Rsam platform is highly configurable and is capable of handling both simple and comprehensive applications. The step-by-step tutorials and Rsam sandboxes, however, are specifically designed to quickly deliver a user experience without requiring further training. Each step-by-step tutorial walks you through common, out-of-the-box functionality within a given Rsam module, allowing you to get immediate hands-on familiarity with the module.

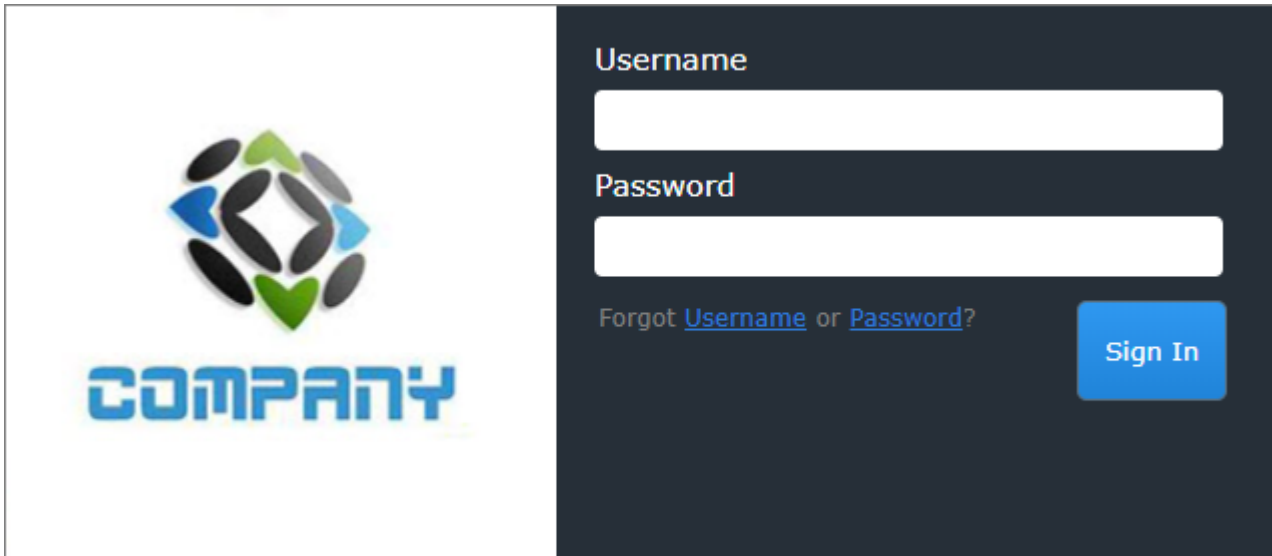
Rsam Sandbox Environment

Rsam module step-by-step tutorials are designed to work with the out-of-the-box Rsam configuration. You may follow this tutorial using an Rsam Sandbox environment or using your own instance of Rsam that you already own. If you are using this tutorial with an Rsam Sandbox environment, the URL to access your Rsam sandbox is delivered through an email. Otherwise, you may contact your Rsam Administrator for the URL to access your Rsam instance.

If you are using an Rsam sandbox environment, you should have provided Rsam with your organization's internet facing IP address. To find this information, open a browser and connect to an IP discovery site such as www.whatismyip.com, or contact your organization's Network Administrator for assistance. You may also contact your Rsam Customer Representative with any questions.

Sign-In Page

Tutorials leverage pre-defined accounts that require manual authentication. While your organization may intend to use SSO authentication, Rsam sandbox environments require manual authentication through the Rsam Sign-In page so that you can easily toggle between various sample accounts used throughout the tutorial.



Like most elements in Rsam, the Sign-In page can be configured in a number of ways. Different authentication options such as user self-registration, integration with customer user directories (such as Active Directory), or integration with Single Sign-On products, such as Shibboleth, can be applied. You can also embed your own branding and logo on the Sign-In page.

Rsam Incident Management

Overview

The Rsam Incident Management module is designed for businesses to detect, monitor, and resolve incidents quickly and efficiently. The automated and streamlined incident management process helps you store, categorize, investigate, resolve, and close incidents. This tutorial provides a step-by-step procedure to walk you through one path of an Incident Management workflow within the module.

The Rsam Incident Management has the following capabilities and benefits:

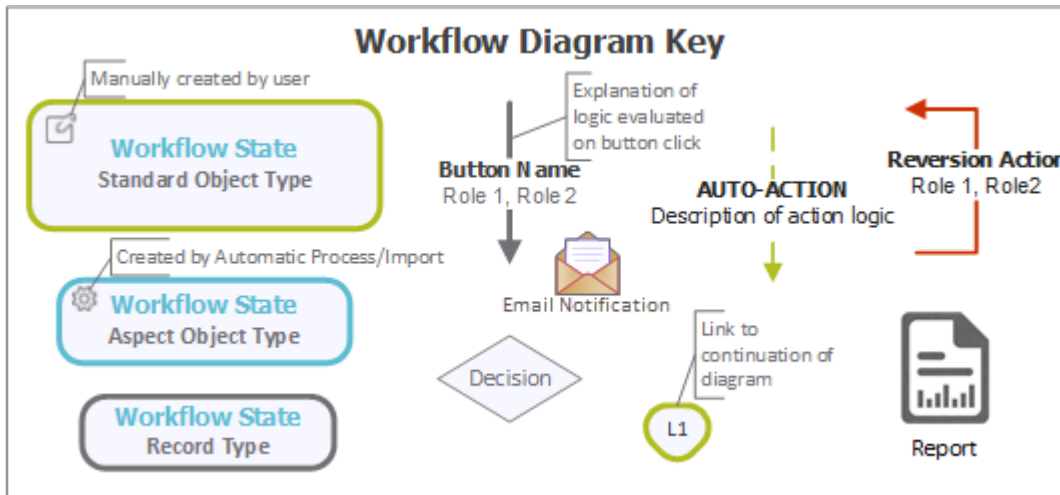
- Increased visibility into incident management process, therefore, all activities in the incident lifecycle are accountable.
- Track incidents by reporters and areas affected.
- Incident impact details.
- Relate incidents and attach evidence.
- Role-based dashboards and charts to track frequently occurring incidents.

This tutorial provides a step-by-step procedure to walk you through one path of workflow within the Incident Management module. To get more insights into the Incident Management module, please refer the *Incident Management Baseline Configuration Guide*.

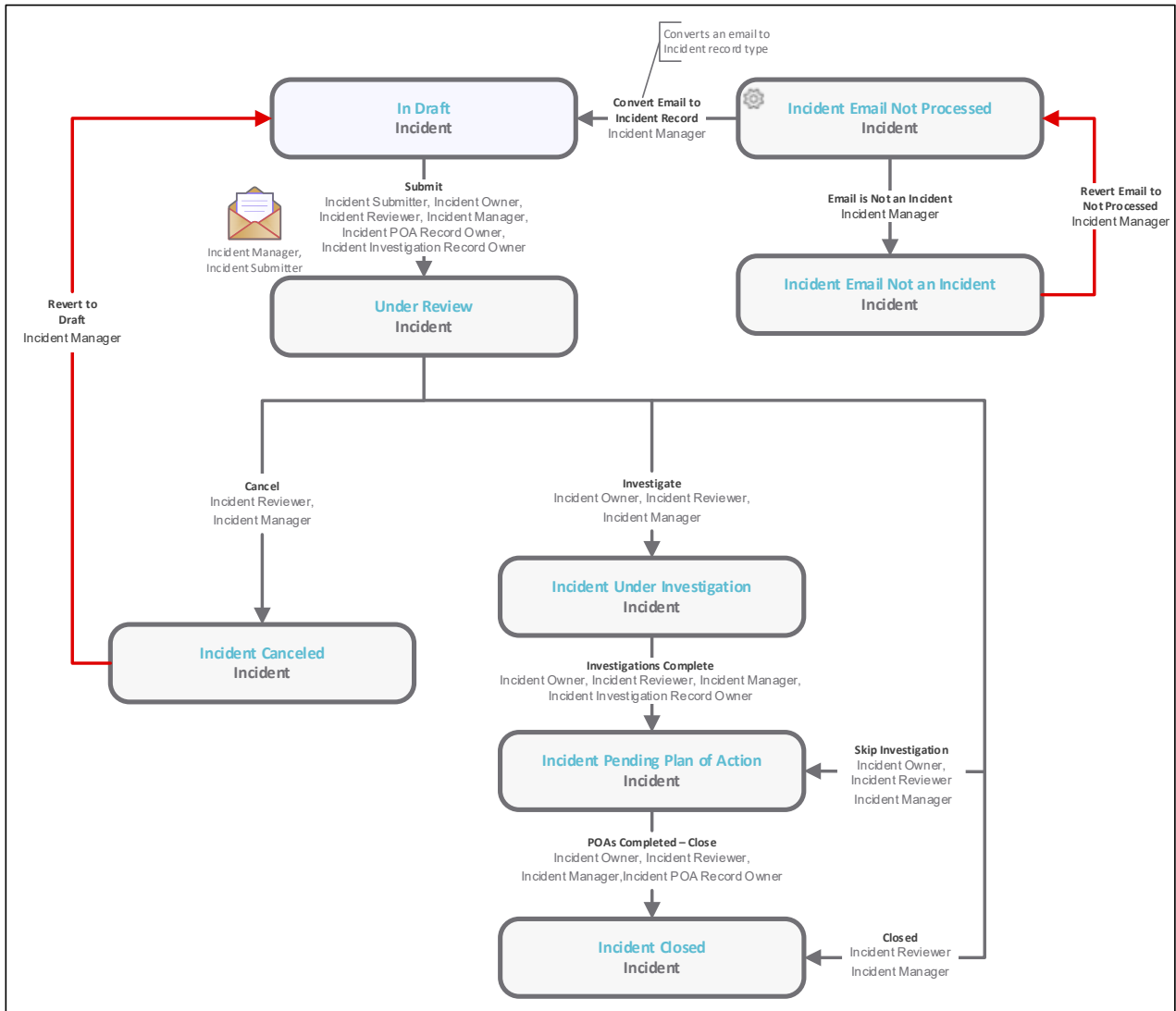
Incident Management Workflow

This section covers the workflow diagram associated with the out-of-the-box Incident Management workflow.

Before proceeding to the workflow, it is recommended that you familiarize yourself with the following Rsam workflow diagram key.



The following diagram shows the Incident Management workflow.



Note: You may create as many variations to this pre-defined workflow configuration as desired to lessen or increase the number of steps and to match your specific business processes.

User Accounts

User Accounts are required for the individuals that are authorized to access a specific Rsam baseline module.

Note: Sample users for each of these roles are optionally provided with the baseline module installation package

The Rsam sandbox for Incident Management comes with the following pre-populated sample accounts.

Account ID	User	Business Responsibilities
r_incident_submitter	Incident Submitter	This user is responsible for creating and submitting incidents manually. Note that this user need not be the same user that reported the incident.
r_incident_owner	Incident Owner	This user is responsible for performing analysis on the assigned incidents and take necessary actions such as creating remediation plans to resolve them. During analysis, the incident owner will also check to see whether the assigned incident has been reported earlier or is related to any incident. This user will respond to the incidents effectively and provide a remediation mechanism to avoid its recurrence in future.
r_incident_manager	Incident Manager	This user has the ability to assign responsibilities for incident management, and performs all functions within the workflow. Typically, this user is assigned at the object level so that the user has access to all the incidents.

The default password for all accounts in the Rsam Incident Management sandbox is *password*. Individual users may change their password once authenticated. Users with administrator permissions may also reset the password of other users.

High-Level Steps

The following is a high-level list of the steps described in this tutorial.

Step	User	Description
Step 1: Submitting an Incident	Incident Submitter	In this step, the <i>Incident Submitter</i> user creates and submits an incident.
Step 2: Assigning an Incident	Incident Manager	In this step, the <i>Incident Manager</i> user reviews the incident submitted by the <i>Incident Submitter</i> and assigns an owner to the incident.
Step 3: Creating an Investigation	Incident Owner	In this step, the <i>Incident Owner</i> user reviews the details and determines the incident resolution method, such as Investigate, Remediation, and more.
Step 4: Closing an Incident	Incident Owner	In this step, the <i>Incident Owner</i> user completes the pending plan of action and closes the incident case.

Step-by-Step Procedure

This section contains the workflow steps we will follow in this tutorial. The path followed in this tutorial resolves an incident using the investigation method and completes the pending plan of action by skipping the investigation in the incident workflow. This path was chosen as is a common path to follow, though you are welcome to explore the other paths as well.

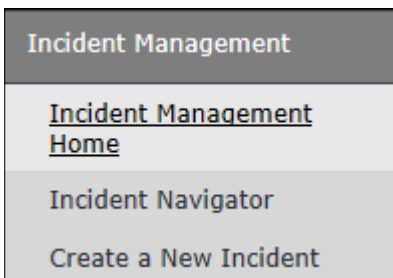
From this point forward, we will provide the steps that are required to complete this tutorial. Before you begin to practice each step, consider following underlying capabilities:

- Practicing each step requires a different user account as mentioned in the [High-Level Steps](#) section. However, you may execute all the steps with the Incident Manager user credentials in one session if desired.
- Workflow state transitions involve sending email notifications to users in the workflow. If you want to ensure that your workflow users receive the notifications while practicing the steps, please see the [Setting up Email Addresses](#) section later in this tutorial.

Step 1: Submitting an Incident

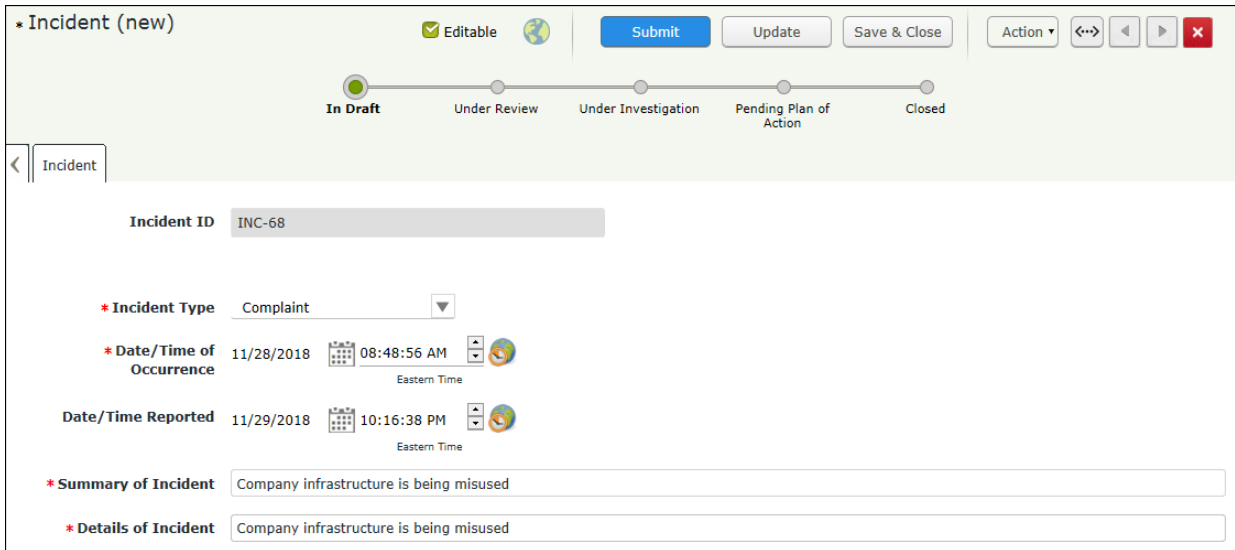
In this step, you will log in to Rsam as the *Incident Submitter* user to create and submit an incident.

1. Open an Rsam supported browser and enter the URL of your Rsam instance containing the Incident Management module.
2. Sign in as the *Incident Submitter* user. Enter **Username** as *r_incident_submitter* and **Password** as *password*.
3. In the navigation panel on the left, navigate to **Incident Management > Create a New Incident**.



The **Incident (new)** record opens with the **Incident** tab selected appears.

- Complete all the attributes as necessary, and then click **Submit**.



The screenshot shows the 'Incident (new)' form in the R.sam system. At the top, there is a progress bar with five stages: 'In Draft' (selected), 'Under Review', 'Under Investigation', 'Pending Plan of Action', and 'Closed'. Below the progress bar, the form fields are as follows:

- Incident ID:** INC-68
- * Incident Type:** Complaint
- * Date/Time of Occurrence:** 11/28/2018 08:48:56 AM Eastern Time
- Date/Time Reported:** 11/29/2018 10:16:38 PM Eastern Time
- * Summary of Incident:** Company infrastructure is being misused
- * Details of Incident:** Company infrastructure is being misused

- Click **Submit**.

You are navigated to the Incident Management grid. The incident record enters the **Under Review** workflow state, and an email notification is sent to the *Incident Manager* user.


Note: The user creating an incident will automatically inherit the Incident Submitter role on the incident record. This role provides access to the necessary screens including the Home Page Tabs in the Incident Management module so that the users can view their submitted incidents.

- Move the mouse pointer over the username at the top-right corner and select **Logout**. You have successfully logged out of the Rsam Incident Management module.

Step 2: Assigning an Owner

In this step, you will log in to Rsam as the *Incident Manager* user to review the incident submitted by the Incident Submitter user in [Step 1: Submitting an Incident](#) and assign an owner.

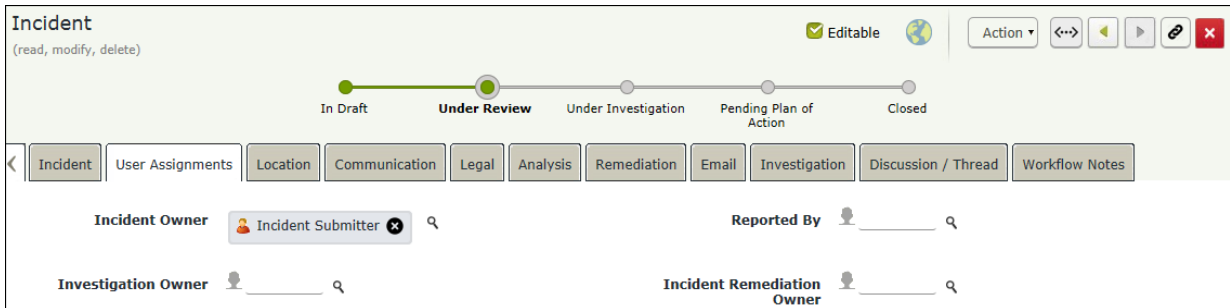
- Open an Rsam supported browser and enter the URL of your Rsam instance containing the Incident Management module.
- Sign in as the *Incident Manager* user. Enter **Username** as *r_incident_manager* and **Password** as *password*.
- In the navigation panel on the left, navigate to **Incident Management > Incident Navigator**. The incident navigator appears.

4. Locate the incident record created by the *Incident Submitter* user in [Step 1: Submitted an Incident](#).
5. Use one of the following methods to open the incident record:
 - Double-click the incident record.
 - Select the incident record, and then click **Open**.
 - Click the  icon in the incident record row.

Incident ID	Workflow State	Date/Time of Occurrence	Incident Type	Incident Summary
INC-63	Under Review	2017-01-03 12:37:49 AM	Privacy Incident	Employee was seen accessing medical records for which they did not treatment, or billing.
INC-68	Under Review	2018-11-28 08:48:56 AM	Complaint	Company infrastructure is being misused

The incident record details appear.


6. Click the **User Assignments** tab.



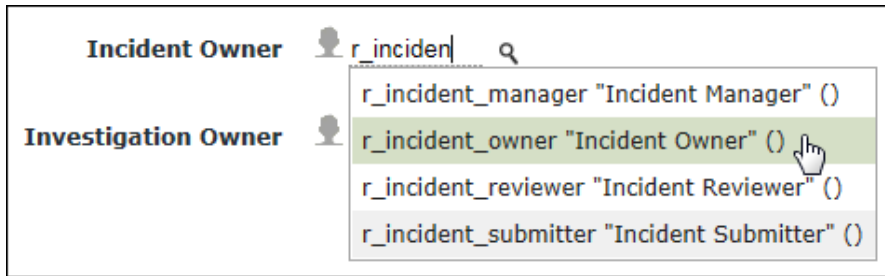
The screenshot shows the 'Incident' details page. At the top, there is a workflow progress bar with stages: In Draft, Under Review (current), Under Investigation, Pending Plan of Action, and Closed. Below the progress bar is a navigation menu with tabs: Incident, User Assignments (selected), Location, Communication, Legal, Analysis, Remediation, Email, Investigation, Discussion / Thread, and Workflow Notes. Underneath, there are fields for Incident Owner (Incident Submitter), Reported By, Investigation Owner, and Incident Remediation Owner, each with a search icon.

7. To assign or replace the incident owner, use one of the following methods:


Method I:

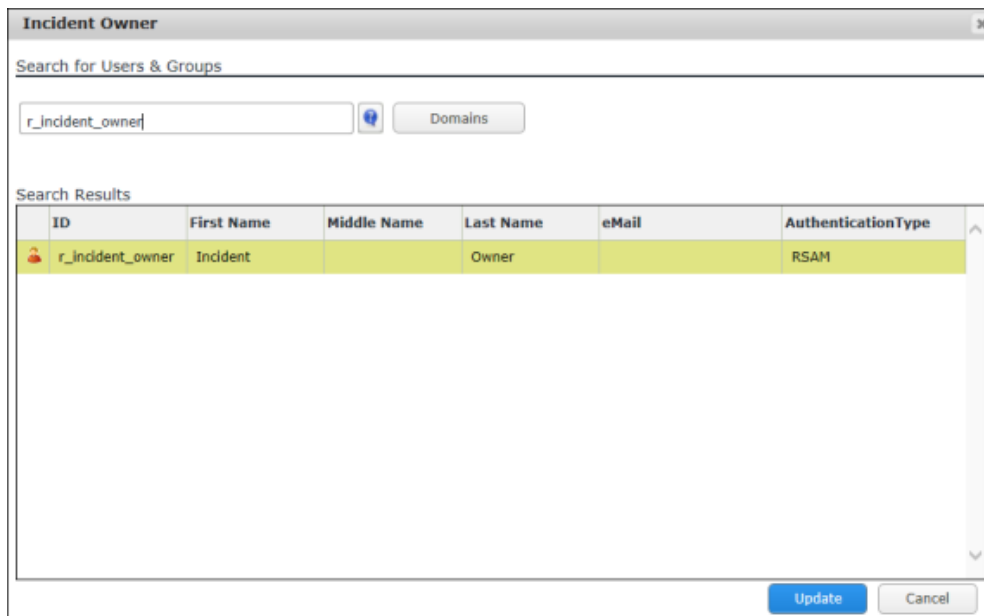
- a. Click the  icon to delete the existing incident owner, *Incident Submitter* in this case.
- b. Enter *r_incident_owner* in the **Incident Owner** attribute. While typing, the users that match the string appear.

- c. Select **r_incident_owner** from the list.



Method II:

- a. Click the  icon next to the **Incident Owner** attribute.
The **Incident Owner** dialog appears.
- b. Enter *r_incident_owner* in the search box.




The **Search Results** display the *r_incident_owner* user.

- c. Select the user row, and then click **Update**.
The **Incident Owner** attribute is set to **r_incident_owner**.
8. Click **Save & Close**.
 9. Move the mouse pointer over the username at the top-right corner and select **Logout**.
You have successfully logged out of the Rsam Incident Management module.

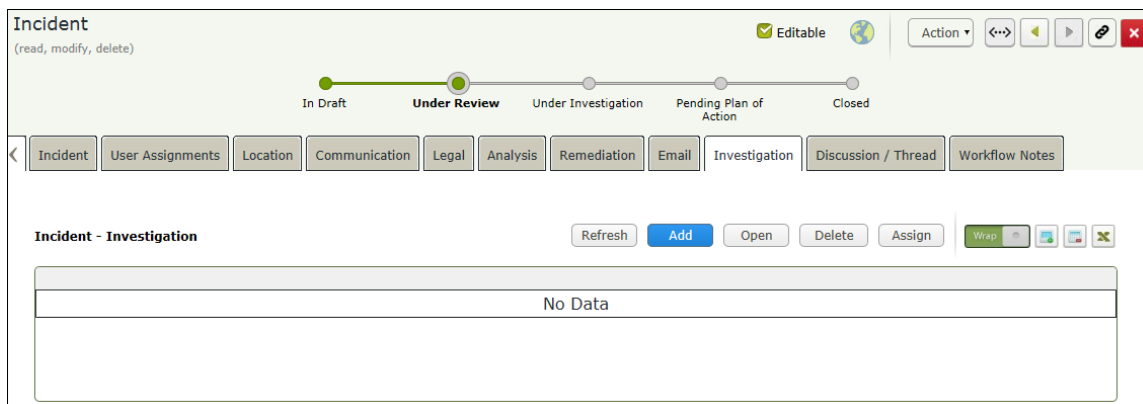
Step 3: Creating an Investigation

In this step, you will log in to Rsam as the *Incident Owner* user to create an investigation record. As part of the path covered by this tutorial, you will bypass the investigation in the incident workflow and take the remediation path in the incident workflow.

1. Open an Rsam supported browser and enter the URL of your Rsam instance containing the Incident Management module.
2. Sign in as the *Incident owner* user. Enter **Username** as *r_incident_owner* and **Password** as *password*.
3. In the navigation panel on the left, navigate to **Incident Management > Incident Navigator**.
The incident navigator appears.
4. Locate the incident that the **Incident Manager** user had assigned an owner in [Step 2: Assigning an Owner](#).
5. Use one of the following methods to open the incident record:
 - Double-click the incident record.
 - Select the incident record, and then click **Open**.
 - Click the  icon in the incident record row.

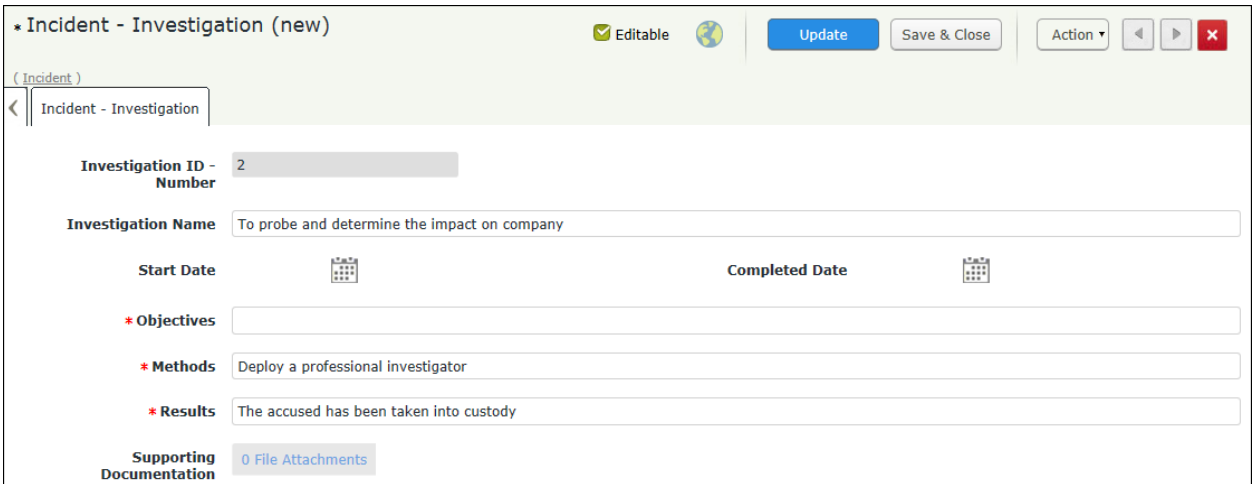
The incident record details appear.

6. Click the **Investigation** tab.

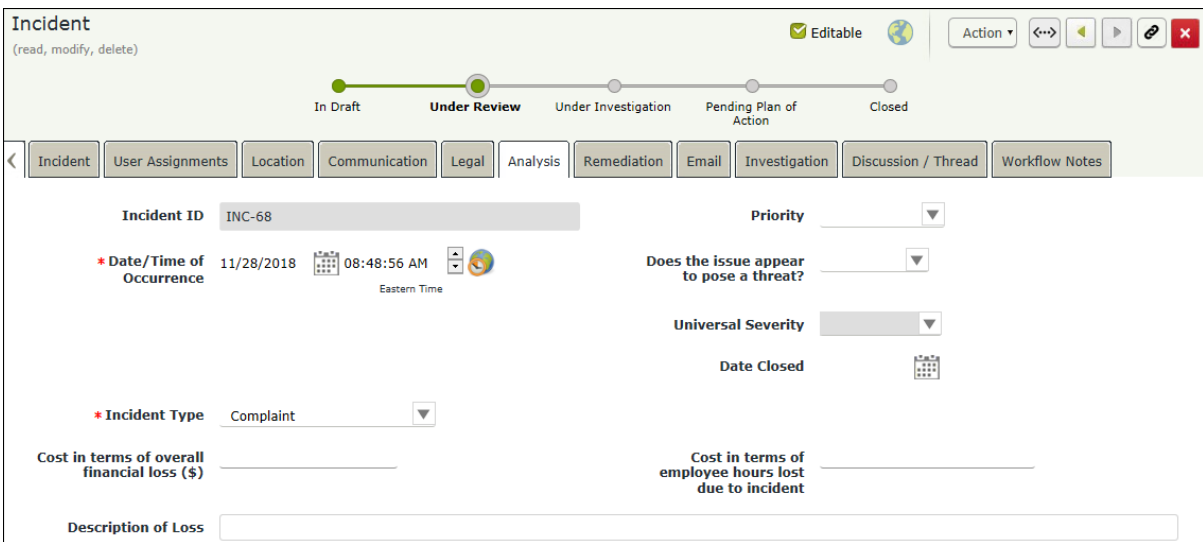


7. Click **Add**. The **Incident - Investigation (new)** record opens with the **Incident - Investigation** tab selected.

8. Complete all the attributes as necessary, and then click **Save & Close**.



9. Click the **Analysis** tab, and then complete attributes as necessary.




10. Click **Action** and select **Skip Investigation** from the actions that appear.

The analysis is completed. The users having the Incident Record Owner and Incident POA Record Owner roles receive the email notification about the incident that has skipped the investigation. The incident record workflow state is moved to the **Pending Plan of Action** state.

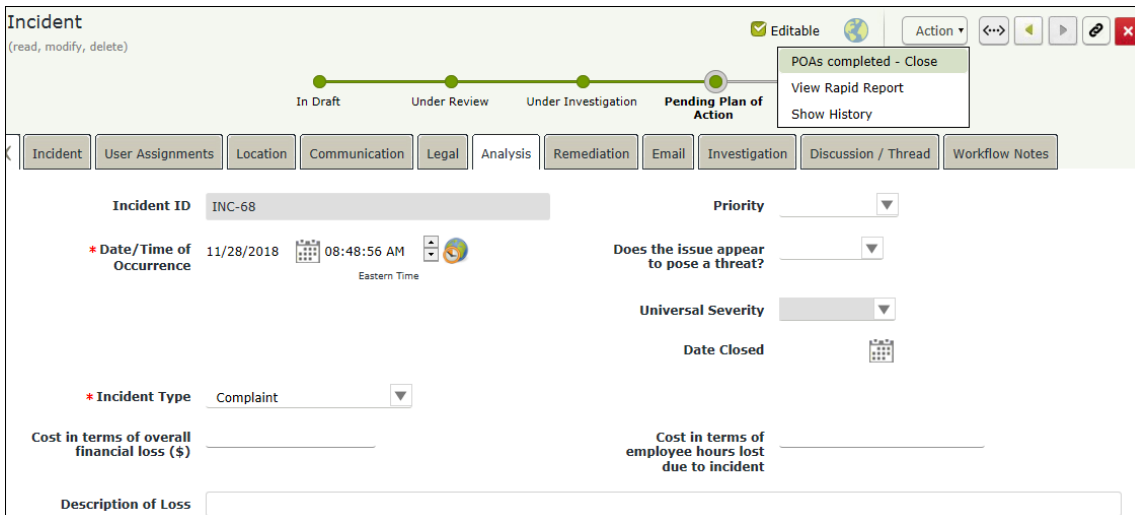
Step 4: Closing an Incident

In this step, you will log in to Rsam as the *Incident Owner* user to keep a track on the incident remediation effort and close the resolved incident.

1. Stay signed in as the *Incident Owner* user.
2. In the navigation panel at the left-hand side, navigate to **Incident Management > Incident Navigator**.
3. Locate the incident record that skipped the investigation in [Step 3: Creating an Investigation](#).
4. Use one of the following methods to open the incident record:
 - Double-click the incident record.
 - Select the incident record, and then click **Open**.
 - Click the  icon in the incident record row.

The incident record details are displayed.

5. Click the **Analysis** tab, and then complete all the attributes as necessary.
6. Click **Actions > POAs Completed - Close**.



The incident record moves to the **Closed workflow** state.

7. Move the mouse pointer over the username at the top-right corner and select **Logout**. You have successfully logged out of the Rsam Incident Management module.

Appendix 1: Email Notifications and Offline Decision Making

Setting up Email Addresses

This module is configured to send automated email notifications at specific points in the workflow. In a production system, email addresses are usually gathered automatically using an LDAP server or a directory service. However, the email addresses in your Rsam instance can be manually provided for testing purposes.

To manually provide the email addresses, perform the following steps:

1. Open an Rsam supported browser and enter the URL of your Rsam instance containing the Incident Management Module.
2. Sign in as *r_admin* user. Enter **Username** as *r_admin* and **Password** as *password*.
3. Navigate to **Manage > Users/Groups**.
4. Double-click a user row to open the details.
5. Provide an email address in the **eMail ID** attribute.



User Details

User Id:
152048

First Name: Middle Name: Last Name:
May, Brian

eMail ID: Phone Number:
support@rsam.com

Password:

Confirm Password:

LDAP User

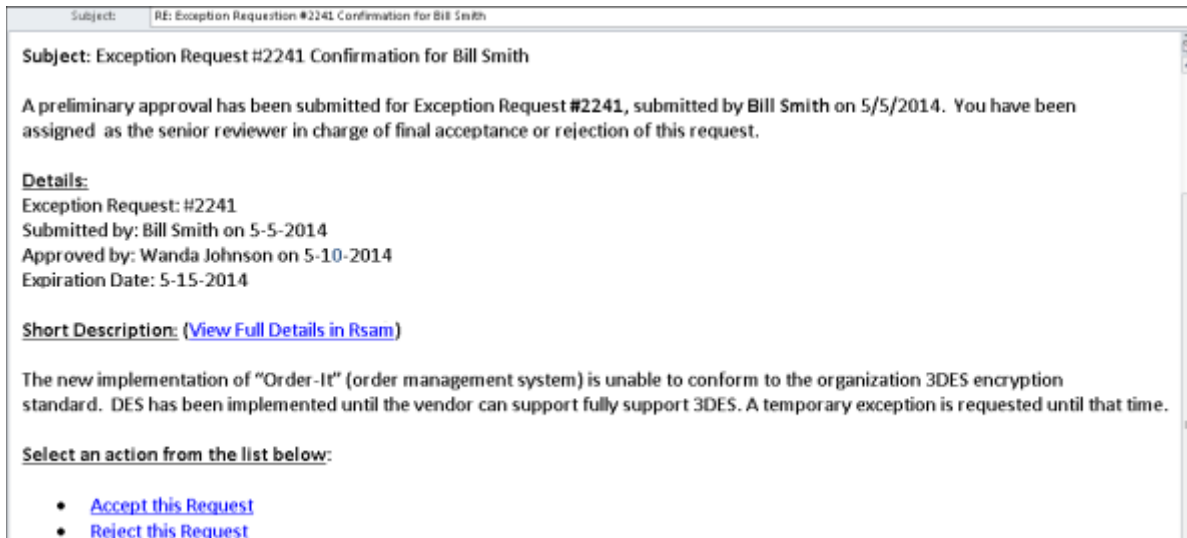
User's LDAP ID:
User's LDAP Domain:
Please select a Domain

6. Click **OK**.
The email address of the user account is saved.

Offline Decision Making

Rsam email notifications are configurable including what notification should be sent, what users or roles will receive the notifications, and the content in the notifications.

Offline Decision Making is a powerful and popular feature of Rsam. It provides the Rsam platform directly to the users to perform workflow actions without connecting to the Rsam module. The following image illustrates an example notification template that has custom text, data from the record, embedded links to the application, and Offline Decision Making actions.



Appendix 2: Rsam Documentation

Incident Management Module Baseline Configuration Guide

To learn more about the pre-configurations in the Incident Management Module, refer the *Incident Management Module Baseline Configuration Guide*. You should have received the *Incident Management Module Baseline Configuration Guide* along with the Incident Management Module sandbox. If not, please contact your Rsam Customer Representative to obtain an electronic copy of the *Incident Management Module Baseline Configuration Guide*.

Online Help

This tutorial provides the step-by-step instructions on the Rsam Incident Management Module. To get familiar with the specific Rsam features used in this configuration, refer the *Rsam End-User Help*, *Rsam Administrator Help*, or both. The online help you can access depends on your user permissions.

To access the online help, perform the following steps:

1. Sign in to your Rsam instance. For example, sign in as *Example Administrator* user. Enter **Username** as *r_admin* and **Password** as *password*.
2. Hover the cursor over **Help** and select an Online help from the menu that appears. Depending on your user permissions, you will be able to access the Rsam End-User Help, Rsam Administrator Help, Step-by-Step Tutorials, or all.

The following image shows the *Rsam Administrator Help*, opened from the *Example Administrator* user account.

