IncidentBond

Step-by-Step Tutorials

Rsam Version: 10 | Document Version: 01.00.04

October 2020

www.wegalvanize.com

Contents

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.

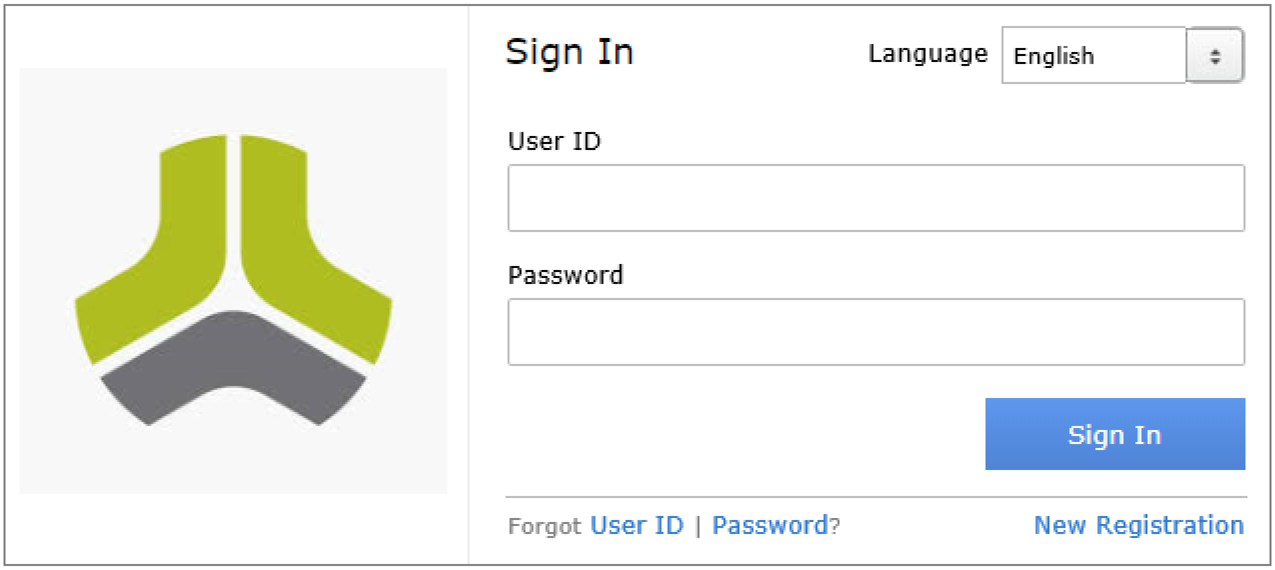
Rsam Sandbox Environment

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.

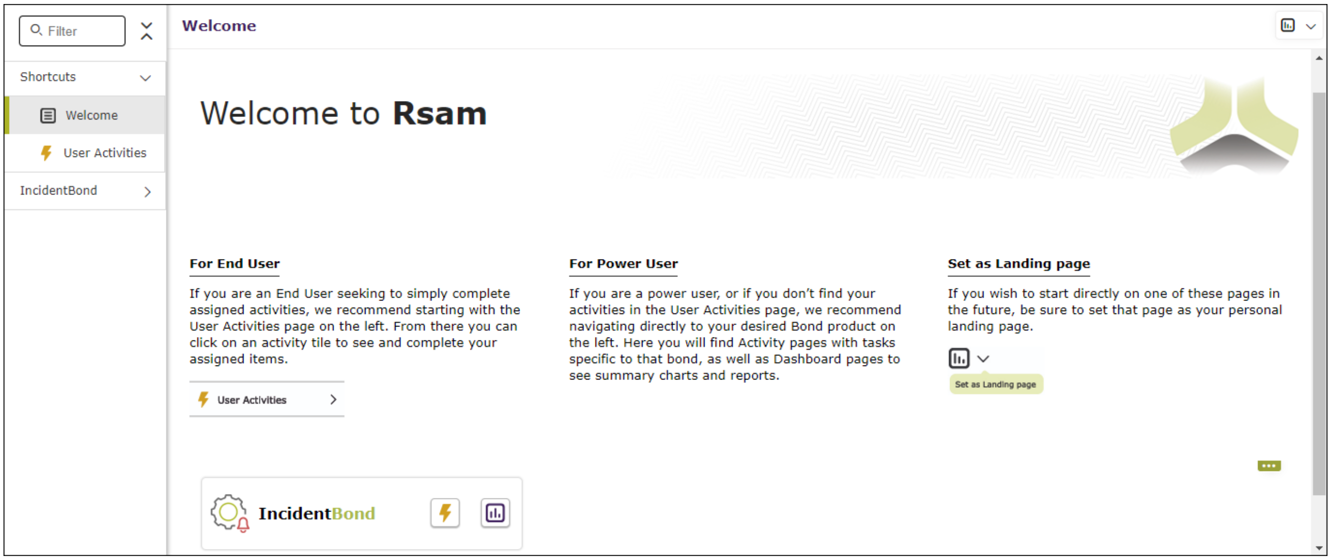


Language English

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.

Welcome Page

The Welcome Page is the first page that appears when you log in to Rsam for the first time. This page provides navigation instructions and shortcuts to access the most commonly used pages from the bonds you have access to.



Welcome to **Rsam**

For End User

If you are an End User seeking to simply complete assigned activities, we recommend starting with the User Activities page on the left. From there you can click on an activity tile to see and complete your assigned items.

For Power User

If you are a power user, or if you don't find your activities in the User Activities page, we recommend navigating directly to your desired Bond product on the left. Here you will find Activity pages with tasks specific to that bond, as well as Dashboard pages to see summary charts and reports.

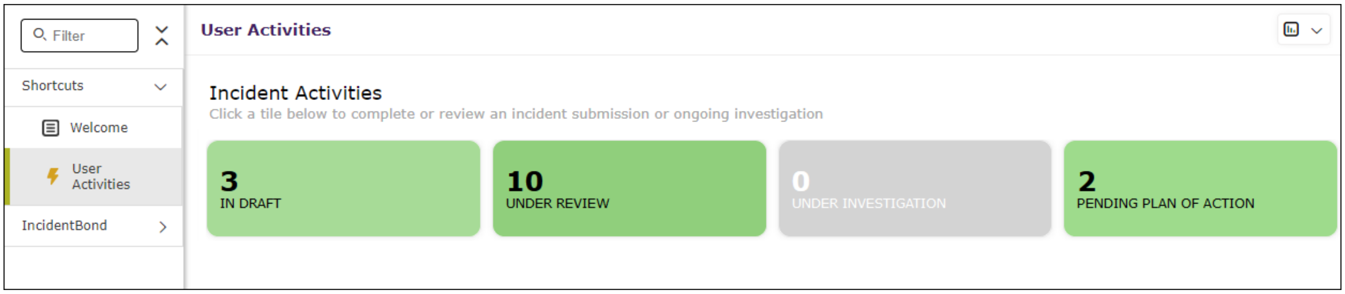
Set as Landing page

If you wish to start directly on one of these pages in the future, be sure to set that page as your personal landing page.

Note: The view of the Welcome Page may be different from the one shown in the image, based on the role of the logged in user.

Navigating to Tasks and Dashboards

If you are an end user and have logged in to complete assigned tasks, you can click User Activities available on the left navigation bar to view the most frequently used Activity Centers *across all bonds assigned for your role*. You can click the relevant activity tile to navigate to your tasks.



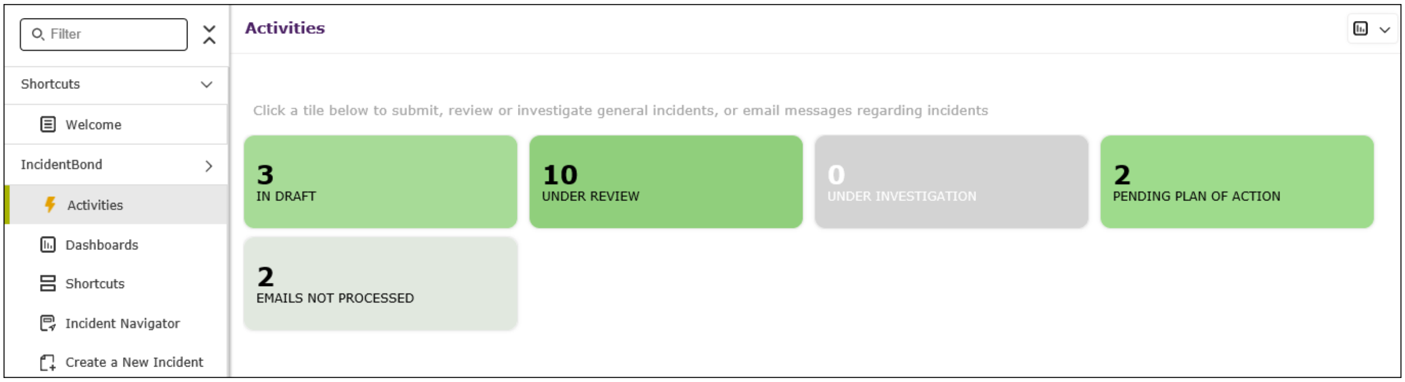
User Activities

Incident Activities

Click a tile below to complete or review an incident submission or ongoing investigation

3 IN DRAFT	10 UNDER REVIEW	0 UNDER INVESTIGATION	2 PENDING PLAN OF ACTION

If you do not find the required activity tiles, you can either click ⚡ corresponding to a bond on the Welcome Page or navigate directly to the bonds from the left navigation bar and select the **Activities** tab to view all related Activity Centers.



Activities

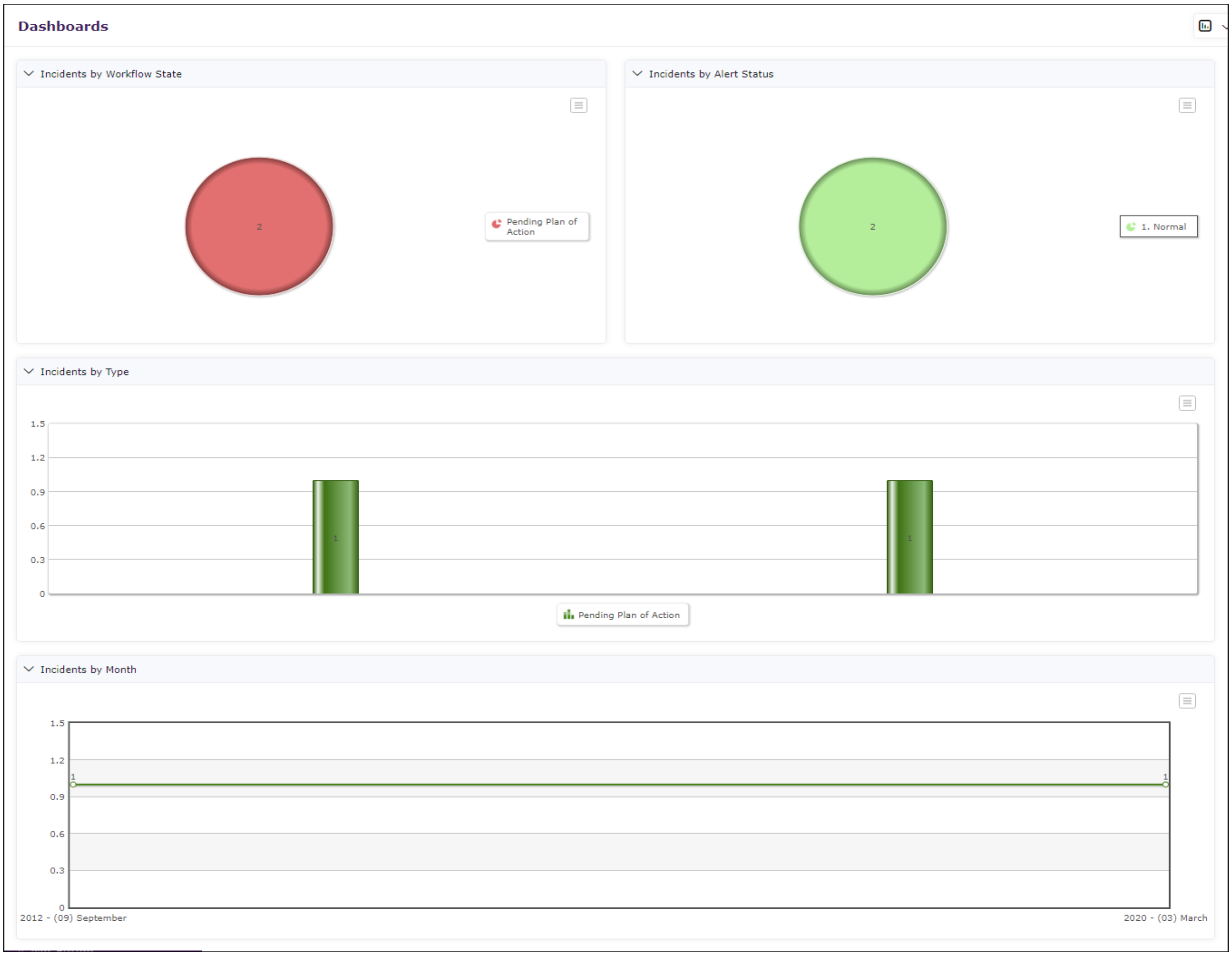
Click a tile below to submit, review or investigate general incidents, or email messages regarding incidents

3 IN DRAFT	10 UNDER REVIEW	0 UNDER INVESTIGATION	2 PENDING PLAN OF ACTION
2 EMAILS NOT PROCESSED			

Click an Activity Center tile to view all related tasks.

Additionally, you can perform the following navigation actions:

- Click 📊 corresponding to a bond on the Welcome page to view all Dashboards configured for the bond.



Alternatively, you can navigate to the required bond from the left navigation bar and select **Dashboards**.

- Expand the required bond from the left navigation bar and use the pages.

For information on using the home page features and configuring Activity Centers, see the *Rsam Administrator* and *End-User Help*.

IncidentBond

Overview

IncidentBond 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.

IncidentBond has the following capabilities and benefits:

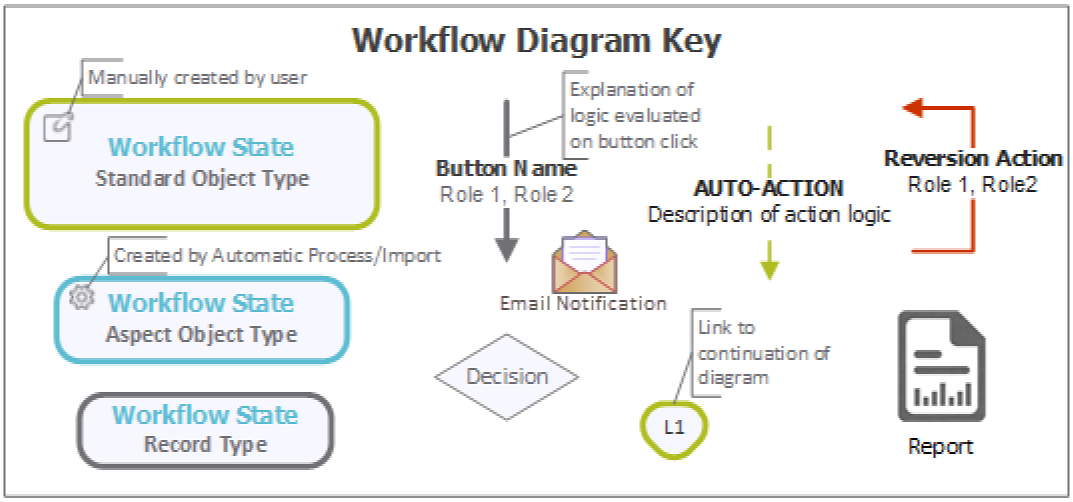
- Increased visibility into incident management process, therefore, all activities in the incident lifecycle are accountable.
- Track incidents by reporters and areas affected.
- Incident impact details.
- Relate incidents and attach evidence.
- Role-based dashboards and charts to track frequently occurring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

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

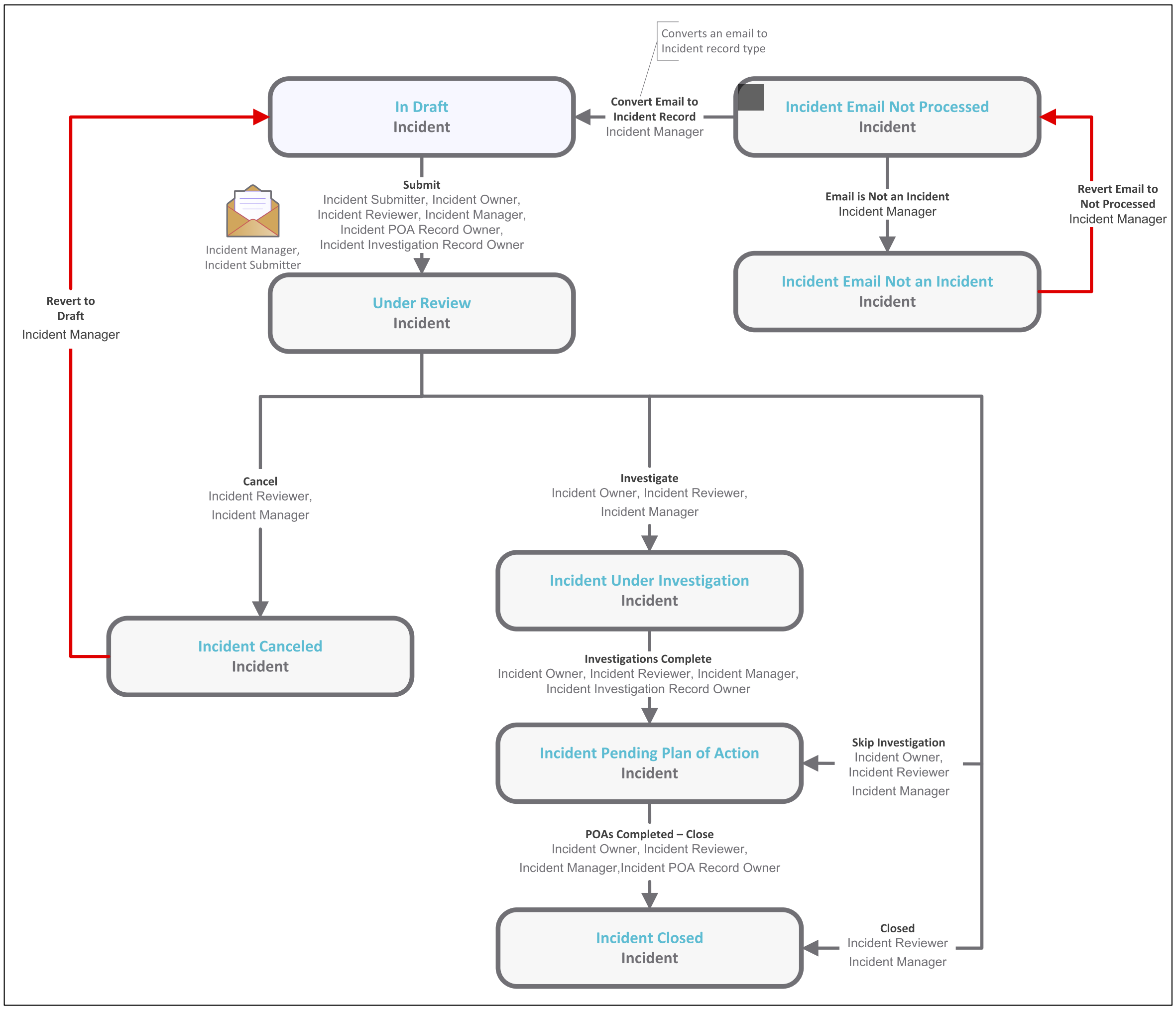
IncidentBond Workflow

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

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



The following diagram shows the IncidentBond workflow.


Converts an email to Incident record type
In Draft
Incident
Convert Email to Incident Record
Incident Manager
Incident Email Not Processed
Incident
Revert Email to Not Processed
Incident Manager
Submit
Incident Submitter, Incident Owner, Incident Reviewer, Incident Manager, Incident POA Record Owner, Incident Investigation Record Owner
Incident Manager, Incident Submitter
Email is Not an Incident
Incident Manager
Incident Email Not an Incident
Incident
Revert to Draft
Incident Manager
Under Review
Incident
Cancel
Incident Reviewer, Incident Manager
Investigate
Incident Owner, Incident Reviewer, Incident Manager
Incident Under Investigation
Incident
Incident Canceled
Incident
Investigations Complete
Incident Owner, Incident Reviewer, Incident Manager, Incident Investigation Record Owner
Incident Pending Plan of Action
Incident
Skip Investigation
Incident Owner, Incident Reviewer
Incident Manager
POAs Completed – Close
Incident Owner, Incident Reviewer, Incident Manager,Incident POA Record Owner
Incident Closed
Incident
Closed
Incident Reviewer
Incident Manager

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. The Rsam sandbox for IncidentBond comes with pre-populated sample accounts as explained in the following table.

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

User 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. All in all, 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.

Users can contact Rsam Administrator to obtain passwords for assigned accounts. 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 *Incident Submitter* user creates and submits an incident.
Step 2: Assigning an Incident	Incident Manager	In this step, the *Incident Manager* user reviews the incident submitted by the *Incident Submitter* and assigns an owner to the incident.
Step 3: Creating an Investigation	Incident Owner	In this step, the *Incident Owner* 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 *Incident Owner* 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:

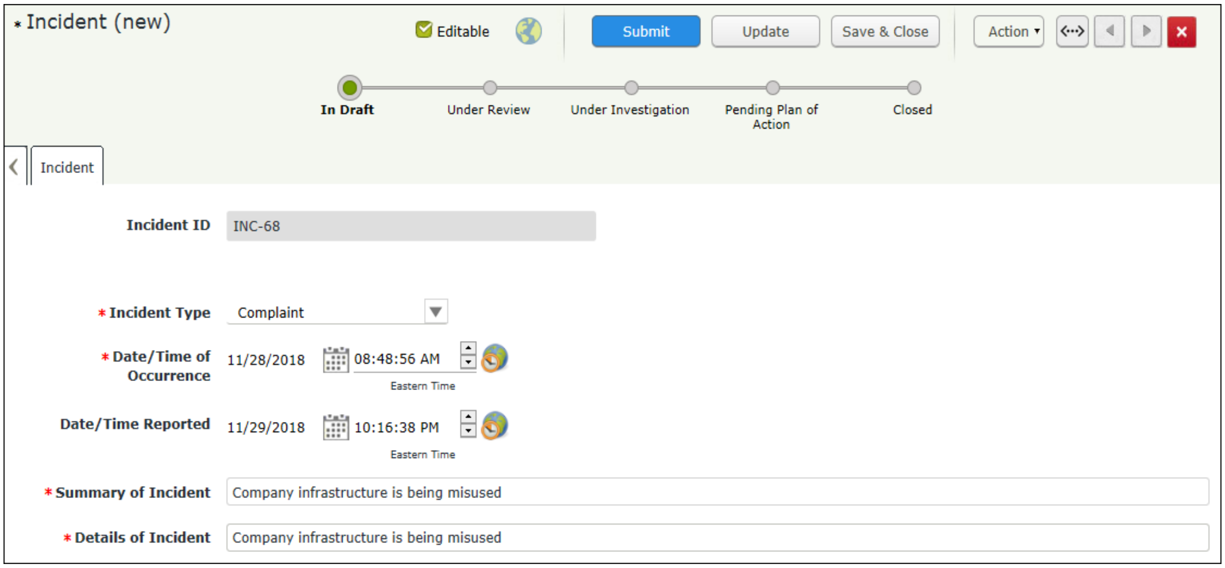
- Practicing each step requires a different user account as mentioned in the High-Level Steps section. However, you may execute all the steps with the Incident Manager user credentials in one session if desired.
- Workflow state transitions involve sending email notifications to users in the workflow. 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 IncidentBond.
2. Sign in as the *Incident Submitter* user. Enter **User ID** as ***r_incident_submitter*** and provide the **Password**.
3. In the navigation panel on the left, navigate to **IncidentBond** > **Create a new Incident**.

   The **Incident (new)** record opens with the **Incident** tab selected appears.
4. Complete all the mandatory attributes, and then click **Submit**.



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

5. Click **Submit**.

   You are directed to the Incident Navigator. 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 IncidentBond so that the users can view their submitted incidents.

6. Move the mouse pointer over the username at the top-right corner and select **Logout**.

   You have successfully logged out of the IncidentBond.

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.

1. Sign in as the *Incident Manager* user. Enter **User ID** as ***r_incident_manager*** and provide the **Password**.

2. In the navigation panel on the left, navigate to **IncidentBond** > **Incident Navigator**.

   The incident navigator appears.

> **Note**: This step can also be accomplished through the Activity Centers when there are a small number of incidents to be reviewed.

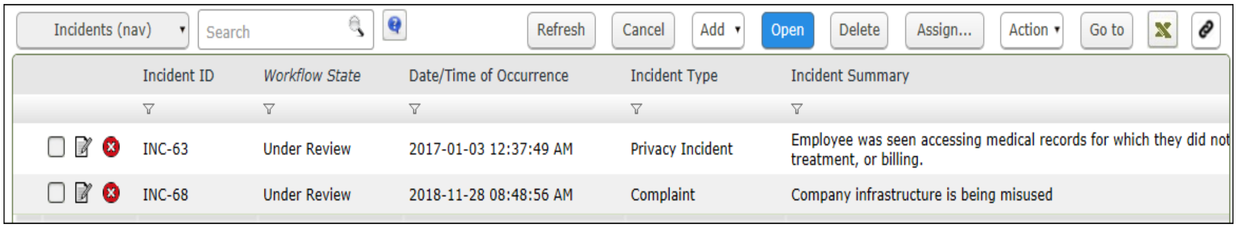
3. Locate the incident record created by the *Incident Submitter* user in Step 1: Submitted an Incident.

4. Use one of the following 3 methods to open the incident record:

   - Double-click the incident record.

   - Select the incident record, and then click **Open**.

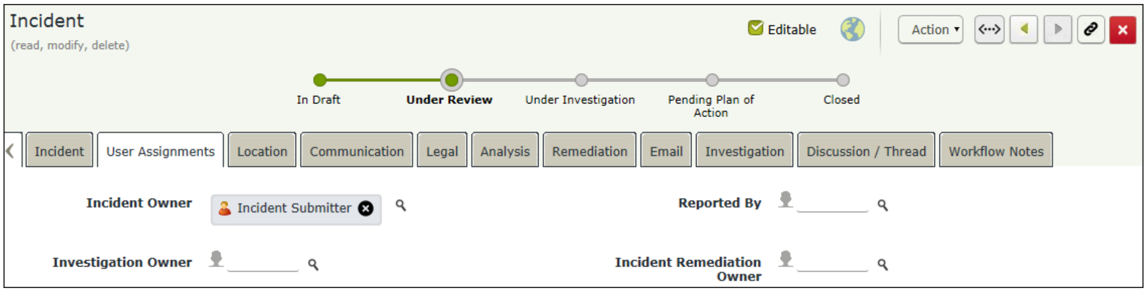
   - Click the ✎ icon in the incident record row.



	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.

5. Click the **User Assignments** tab.



Incident Owner Incident Submitter ⊗

Reported By

Investigation Owner

Incident Remediation Owner

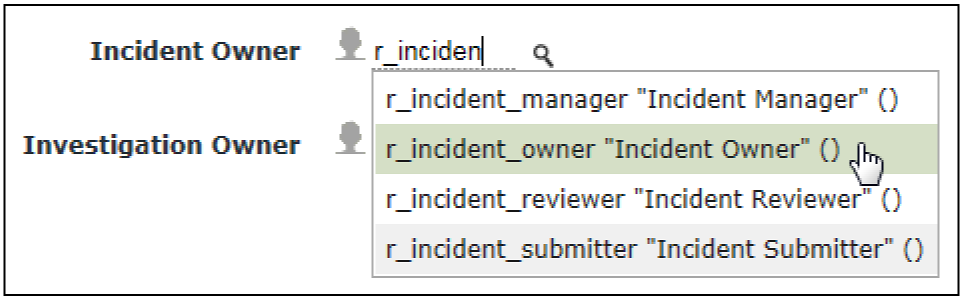
6. To assign or replace the incident owner, use one of the following 2 methods:

   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.



Incident Owner r_inciden

Investigation Owner

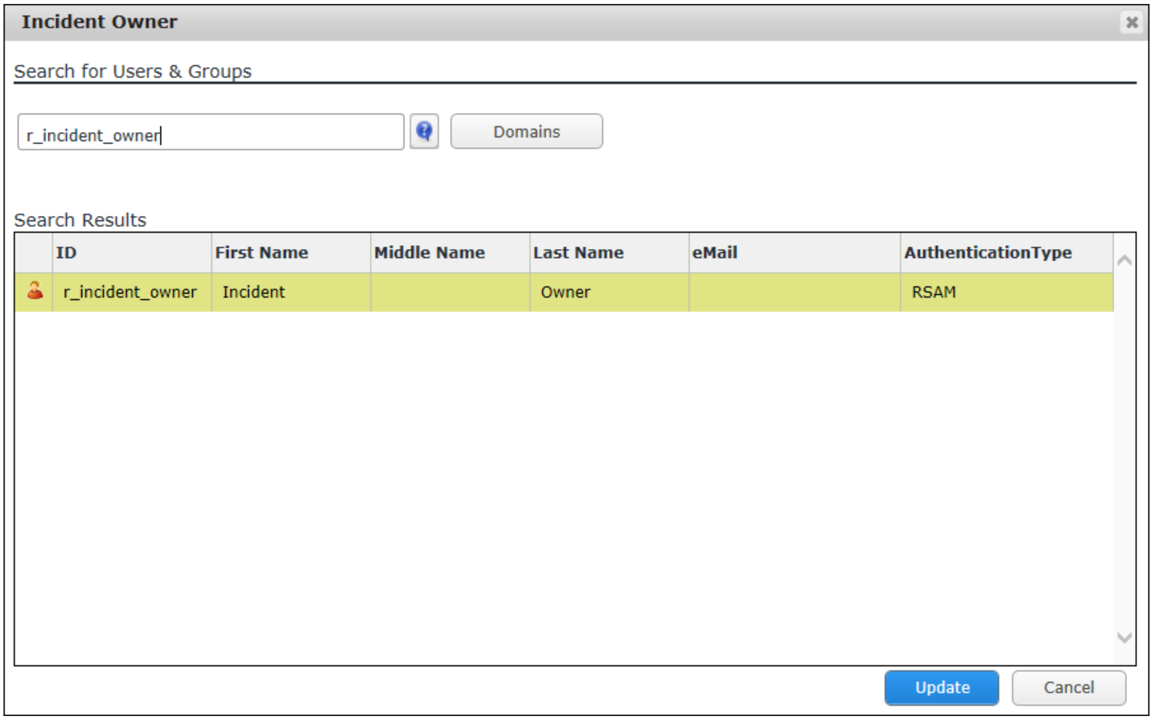
r_incident_manager "Incident Manager" ()
r_incident_owner "Incident Owner" ()
r_incident_reviewer "Incident Reviewer" ()
r_incident_submitter "Incident Submitter" ()

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.



Incident Owner

Search for Users & Groups

r_incident_owner

Search Results

	ID	First Name	Middle Name	Last Name	eMail	AuthenticationType
	r_incident_owner	Incident		Owner		RSAM

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**.

7. Click **Save & Close**.

8. Move the mouse pointer over the username at the top-right corner and select **Logout**.

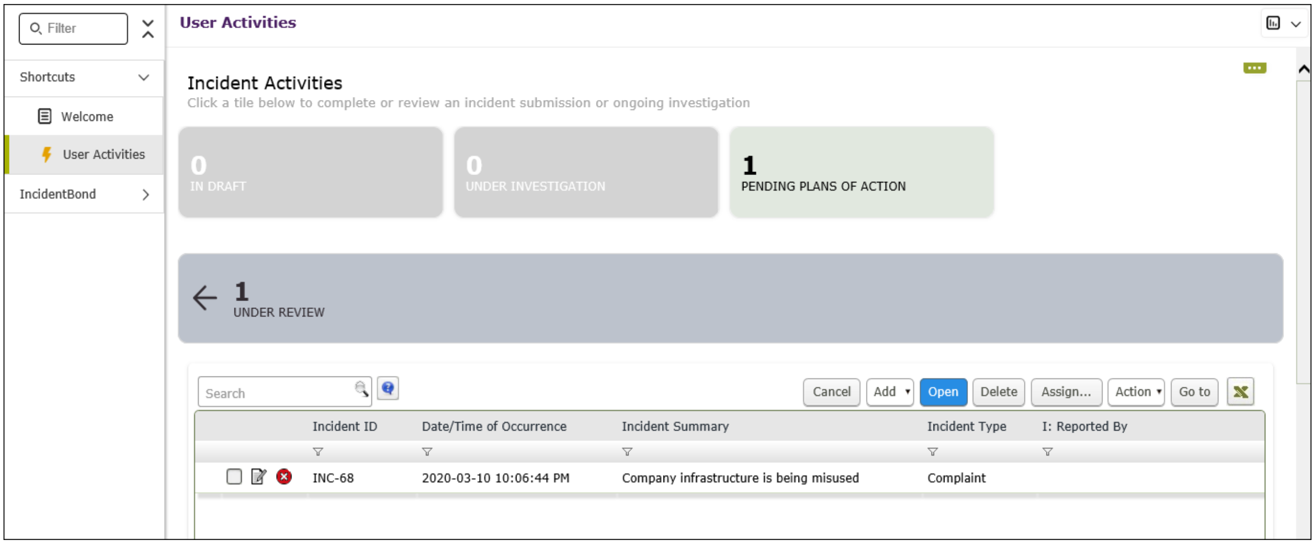
   You have successfully logged out of the IncidentBond.

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. Sign in as the *Incident owner* user. Enter **User ID** as ***r_incident_owner*** and provide the **Password**.

2. In the navigation panel on the left, go to **Shortcuts** > **User Activities** and click the **Under Review** tile



Incident Activities

Click a tile below to complete or review an incident submission or ongoing investigation

	Incident ID	Date/Time of Occurrence	Incident Summary	Incident Type	I: Reported By
□	INC-68	2020-03-10 10:06:44 PM	Company infrastructure is being misused	Complaint	

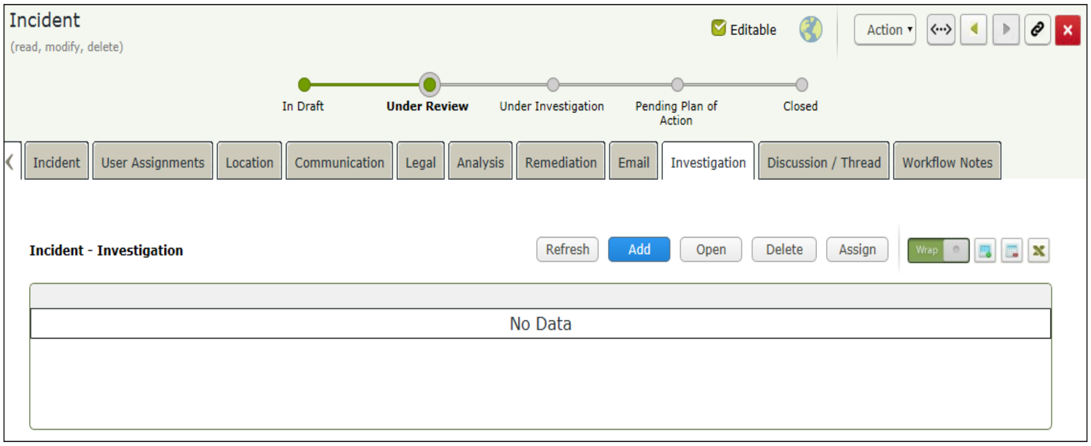
3. Locate the incident that the **Incident Manager** user had assigned an owner in [Step 2: Assigning an Owner](#).

4. Use one of the following 3 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.

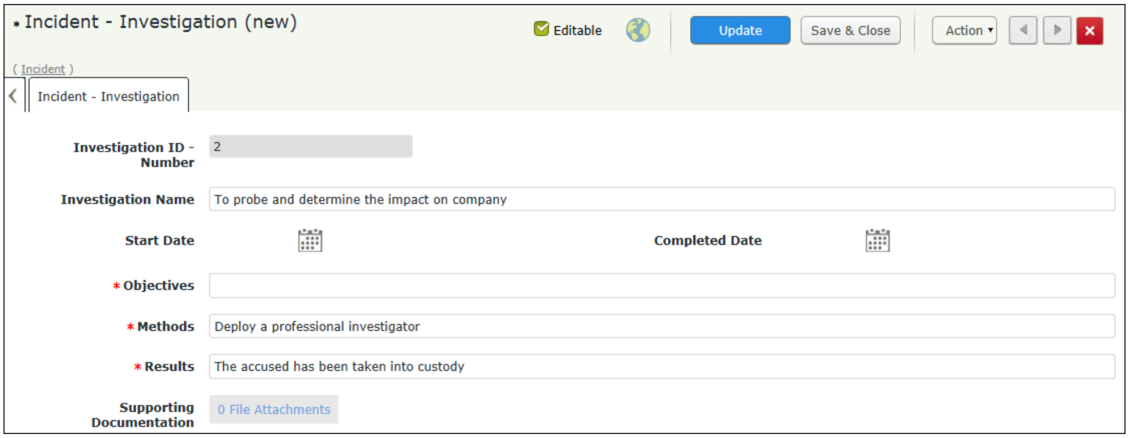
   The incident record details appear.

5. Click the **Investigation** tab.



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

7. Complete all the mandatory attributes, and then click **Save & Close**.



Investigation ID - Number: 2

Investigation Name: To probe and determine the impact on company

Start Date:

Completed Date:

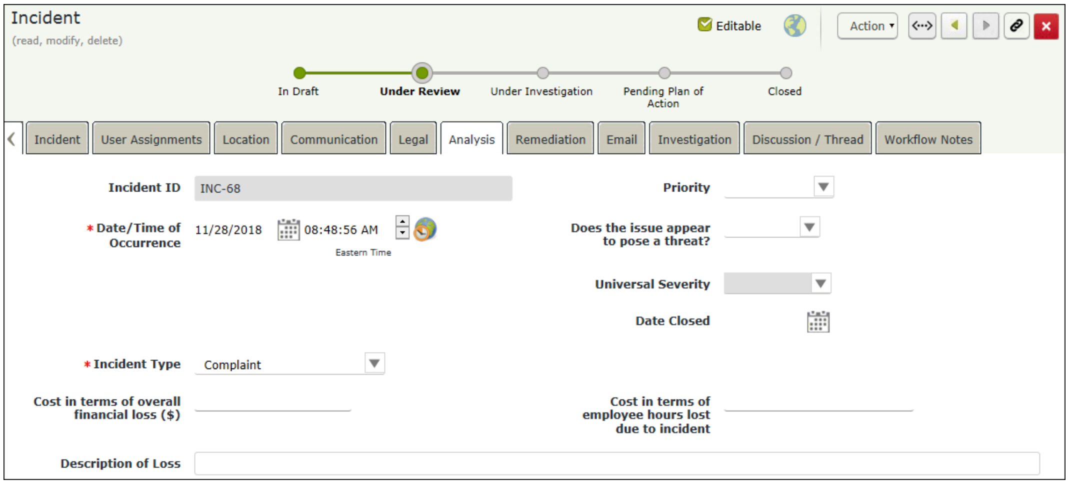
* Objectives:

* Methods: Deploy a professional investigator

* Results: The accused has been taken into custody

Supporting Documentation: 0 File Attachments

8. Click the **Analysis** tab, and then complete all the mandatory attributes.



Incident
(read, modify, delete)

Incident ID: INC-68

* Date/Time of Occurrence: 11/28/2018 08:48:56 AM Eastern Time

Priority:

Does the issue appear to pose a threat?:

Universal Severity:

Date Closed:

* Incident Type: Complaint

Cost in terms of overall financial loss ($):

Cost in terms of employee hours lost due to incident:

Description of Loss:

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

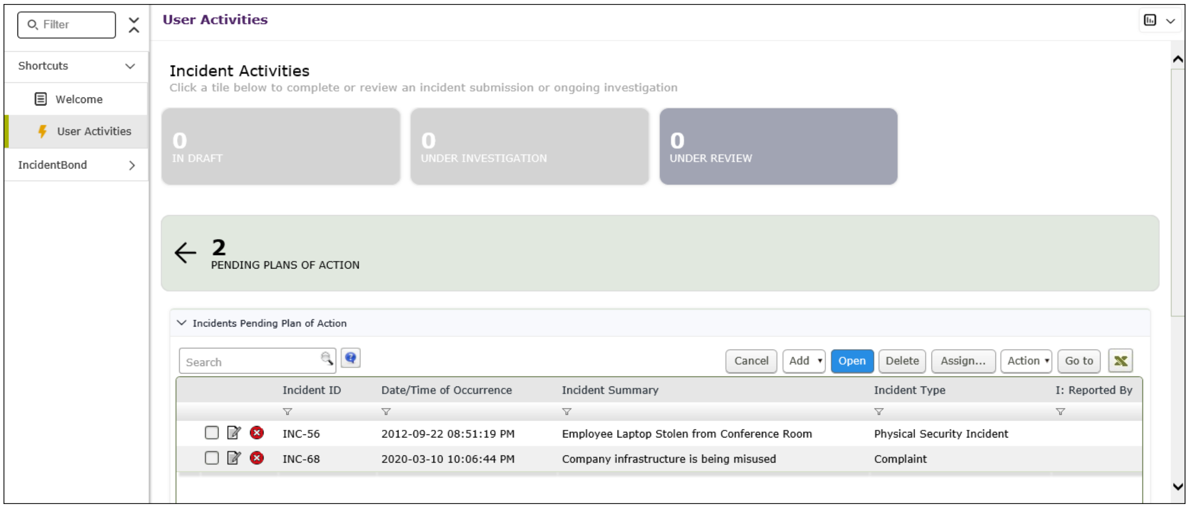
   The analysis is completed. The users having the *Incident Record Owner* and *Incident POA Record Owner* roles receive the email notification about the incident that has skipped the investigation. The incident record workflow state is moved to the **Pending Plan of Action** state.

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 on the left, go to **Shortcuts** > **User Activities** and click the **Pending Plans of Action** tile



User Activities

Incident Activities

Click a tile below to complete or review an incident submission or ongoing investigation

0 IN DRAFT

0 UNDER INVESTIGATION

0 UNDER REVIEW

2 PENDING PLANS OF ACTION

Incidents Pending Plan of Action

Incident ID	Date/Time of Occurrence	Incident Summary	Incident Type	I: Reported By
INC-56	2012-09-22 08:51:19 PM	Employee Laptop Stolen from Conference Room	Physical Security Incident	
INC-68	2020-03-10 10:06:44 PM	Company infrastructure is being misused	Complaint	

3. Locate the incident record that skipped the investigation in Step 3: Creating an Investigation.

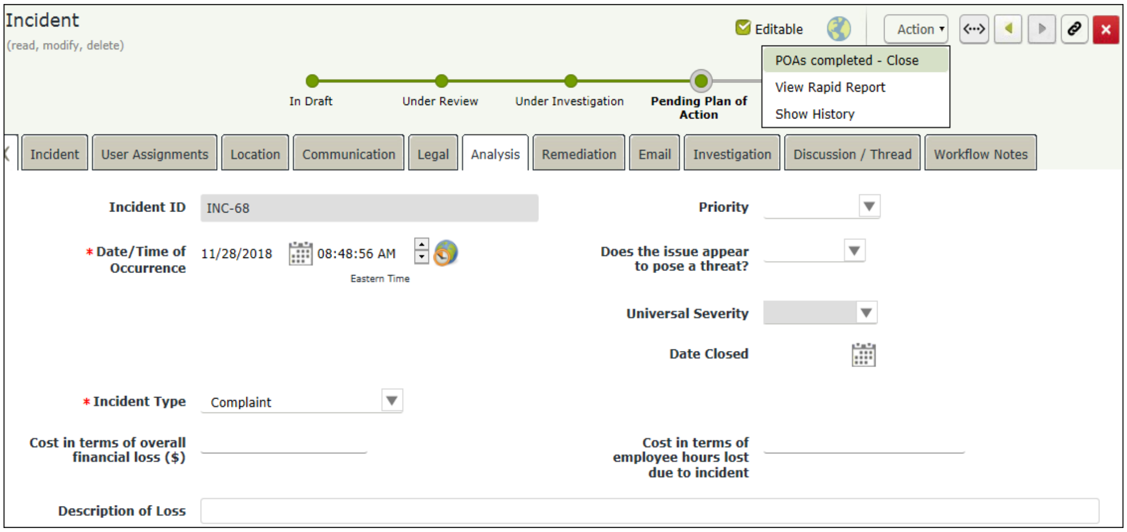
4. Use one of the following 3 methods to open the incident record:

   - 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 mandatory attributes.

6. Click **Action** and select **POAs Completed - Close** from the options that appear.



Incident ID: INC-68

* Date/Time of Occurrence: 11/28/2018 08:48:56 AM Eastern Time

Priority:

Does the issue appear to pose a threat?:

Universal Severity:

Date Closed:

* Incident Type: Complaint

Cost in terms of overall financial loss ($):

Cost in terms of employee hours lost due to incident:

Description of Loss:

The incident record workflow enters 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 IncidentBond.

Appendix 1: Email Notifications and Offline Decision Making

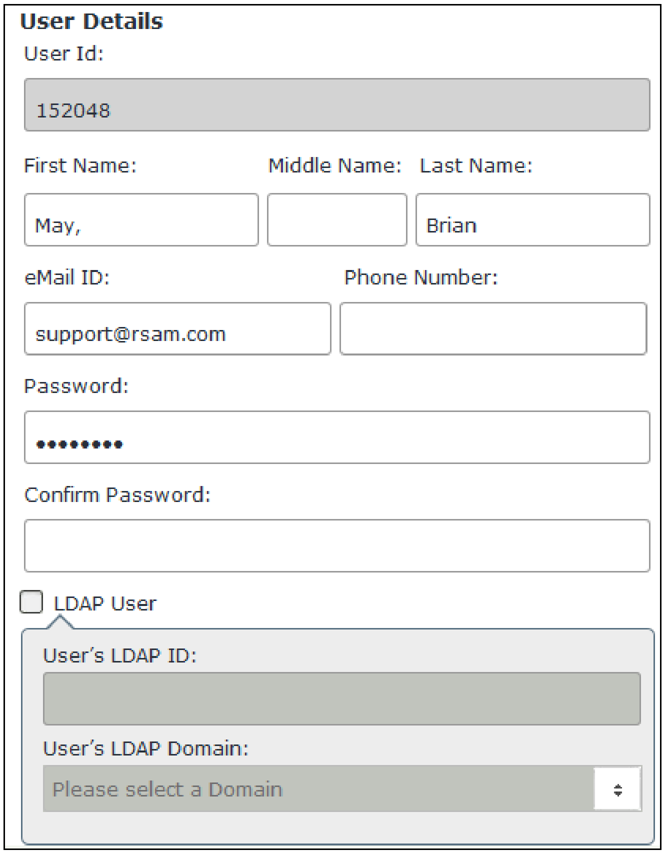
Setting up Email Addresses

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 IncidentBond module.
2. Sign in as *r_admin* user. Enter **User ID** as ***r_admin*** and provide the **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: May,

Middle Name:

Last Name: Brian

eMail ID: support@rsam.com

Phone Number:

Password: ••••••••

Confirm Password:

□ LDAP User

User's LDAP ID:

User's LDAP Domain: Please select a Domain

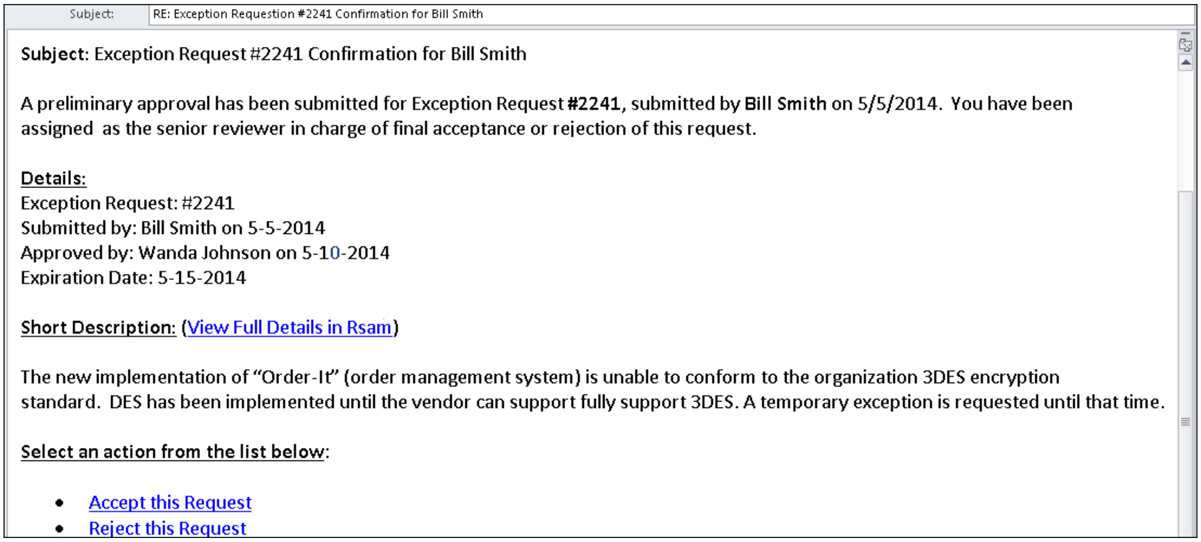
6. Click **OK**.

   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.



RE: Exception Requestion #2241 Confirmation for Bill Smith

Subject: Exception Request #2241 Confirmation for Bill Smith

A preliminary approval has been submitted for Exception Request **#2241**, submitted by **Bill Smith** on 5/5/2014. You have been assigned as the senior reviewer in charge of final acceptance or rejection of this request.

Details:
Exception Request: #2241
Submitted by: Bill Smith on 5-5-2014
Approved by: Wanda Johnson on 5-10-2014
Expiration Date: 5-15-2014

Short Description: (View Full Details in Rsam)

The new implementation of "Order-It" (order management system) is unable to conform to the organization 3DES encryption standard. DES has been implemented until the vendor can support fully support 3DES. A temporary exception is requested until that time.

Select an action from the list below:

- Accept this Request
- Reject this Request

Appendix 2: Rsam Documentation

IncidentBond Baseline Configuration Guide

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

Online Help

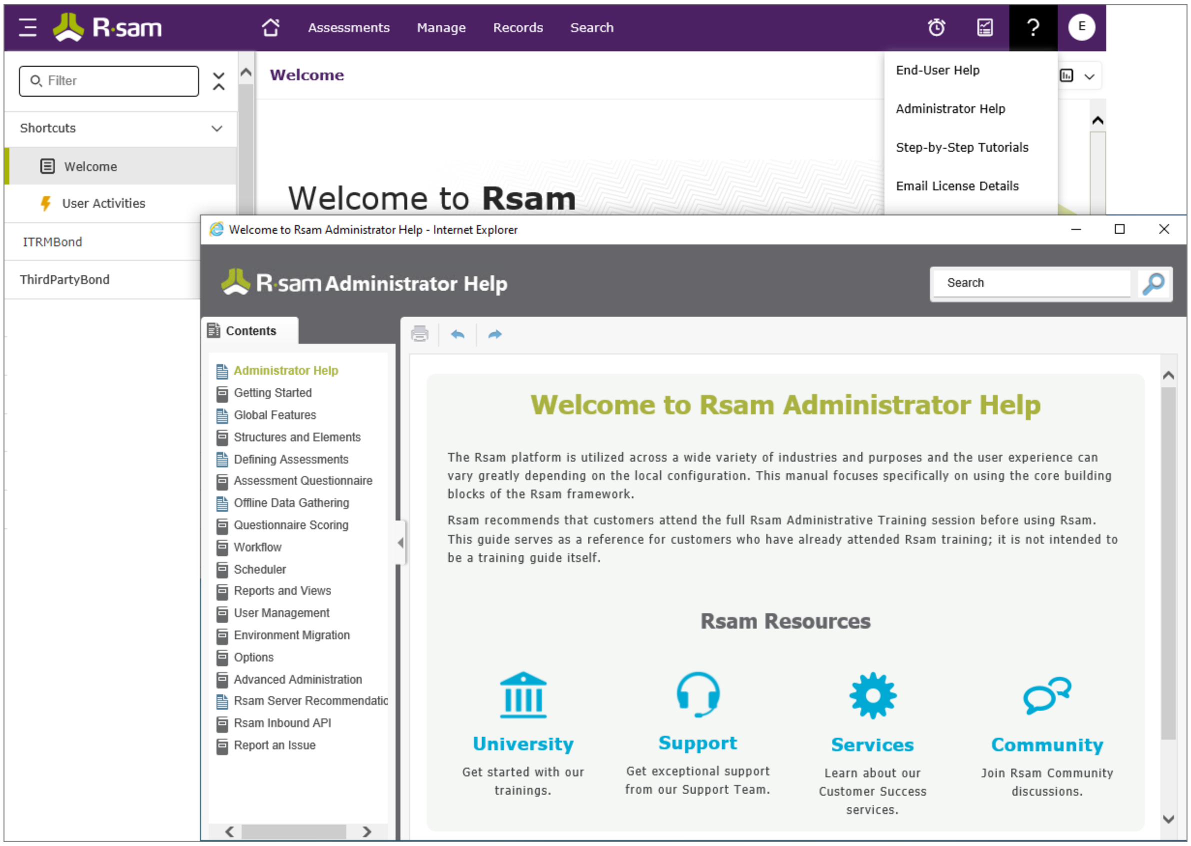
This tutorial provides the step-by-step instructions for the Rsam IncidentBond module. To get familiar with the specific Rsam features used in this configuration, refer the *Rsam End-User Help*, *Rsam Administrator Help*, or both. The Online help you can access depends on your user permissions.

To access the Online Help, perform the following steps:

1. Sign in to your Rsam instance. For example, sign in as *Example Administrator* user. Provide the **User ID** as ***r_admin*** and provide the **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.



Welcome to Rsam Administrator Help

The Rsam platform is utilized across a wide variety of industries and purposes and the user experience can vary greatly depending on the local configuration. This manual focuses specifically on using the core building blocks of the Rsam framework.

Rsam recommends that customers attend the full Rsam Administrative Training session before using Rsam. This guide serves as a reference for customers who have already attended Rsam training; it is not intended to be a training guide itself.

Rsam Resources

University
Get started with our trainings.

Support
Get exceptional support from our Support Team.

Services
Learn about our Customer Success services.

Community
Join Rsam Community discussions.