Security Incident Response Module

Baseline Configuration Guide

Document Version: 01.00.02 | December 2018

Contents

About Rsam Baseline Configuration Guides

Rsam Baseline Configuration Guides provide you the information needed to understand the pre-defined configurations for each module. These guides should be referenced to gain a better understanding of how the module is configured and can be used out-of-the-box.

Baseline Configuration Overview

This document describes the baseline configuration and structure for the Rsam Security Incident Response (SIRP) module. The baseline configurations for the Security Incident Response module allow your users to manage a wide variety of events and incidents. The pre-configured activities help streamline your program by leveraging a central repository, allowing for data normalization, workflow, and timely reporting in a more automated fashion.

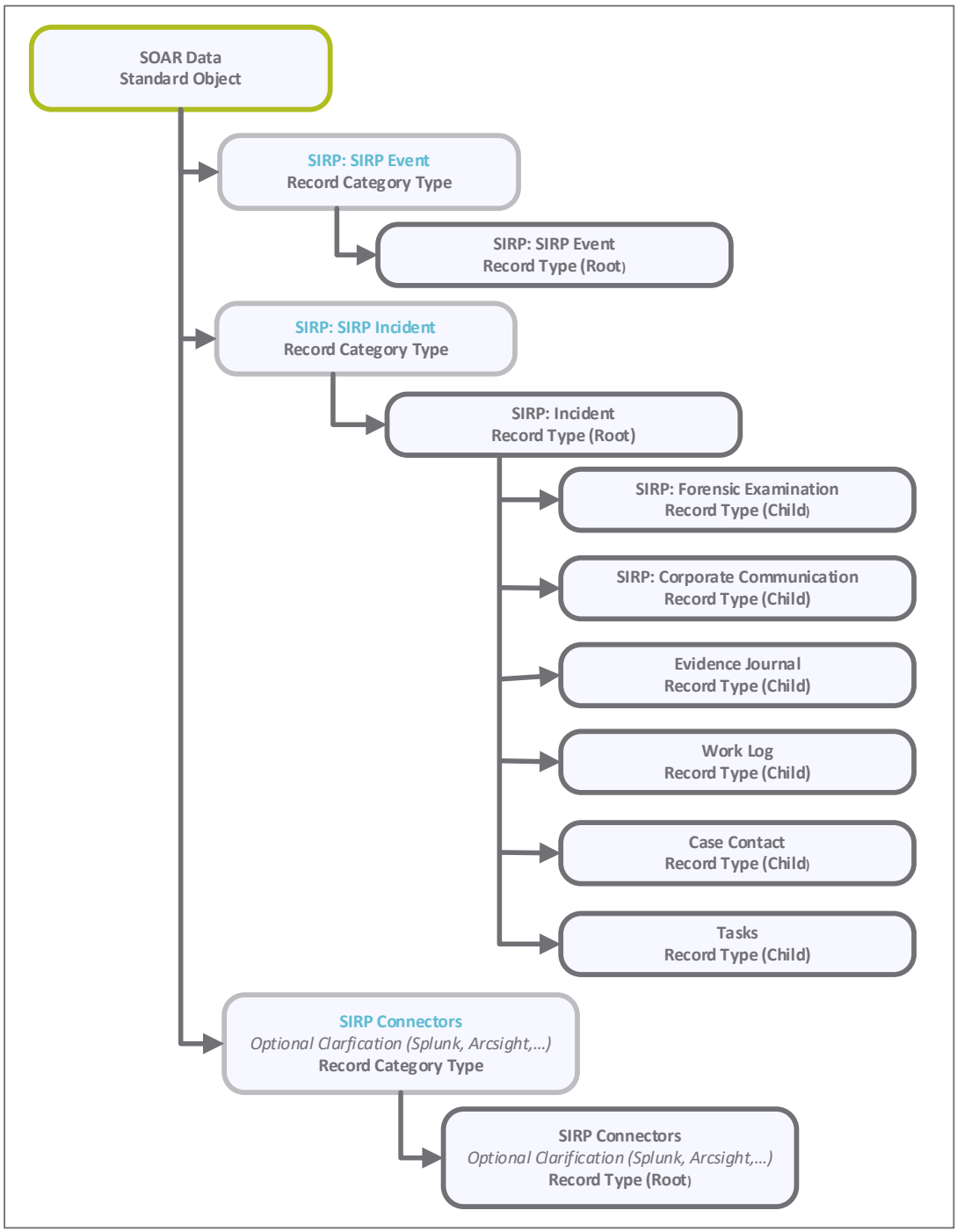
The following is a list of elements that have been configured in the Security Incident Response module:

- Structure
- Home Page Tabs
- Security Incident Response Workflows
- Data Import
- Email Listeners

The information on the elements mentioned above will provide a baseline understanding before you leverage the *Security Incident Response Step by Step Tutorial* or begin to tailor the module to meet your unique requirements.

Security Incident Response Structure

All objects and records in the Security Incident Response module are stored in object type *SOAR Data*.



Object Type

The following object type has been pre-configured in this module.

Object Type	Usage
SOAR Data	A standard library object under which all the event and incident records are stored.

Record Categories

The following record categories have been pre-configured in this module.

Record Categories	Usage
SIRP: SIRP Incident	A category type that includes the Incident record type and all its child record types, such as Forensic Examination, Corporate Communication, Evidence Journal, Work Log, Case Contact, and Tasks.
SIRP: SIRP Event	A category type that includes the Event record type.
SIRP: Event Escalation Rules	A category type that includes the Event Escalation Rule record type.
SIRP: Task Library	A category type that includes the Library Task record type.
SIRP: Playbook Rules	A category type that includes the Playbook Rule record type.

Note: In addition to the above category types, there are other record categories that allow you to get event data into SIRP. These record categories include SIRP: SIRP-ArcSight, SIRP: SIRP – QRadar, SIRP: SIRP – Splunk, SIRP: SIRP – AWS, SIRP: SIRP – Checkpoint, and SIRP: SIRP – Symantec Endpoint Protection.

Record Types

The following record types have been pre-configured in this module.

Record Type	Usage
SIRP: Event	This is a root-level record that contains all the event related information. This record can have multiple child records or record types.
SIRP: Incident	This is a root-level record that contains all the incident related information. This record can have multiple child records or record types.
SIRP: Forensic Examination	This is a child-level record of an incident record (one-to-many). The forensic examination record tracks investigative actions and allows a user to attach supporting documentation.

Record Type	Usage
SIRP: Corporate Communication	This is a child-level record of an incident record (one-to-many). The communication record tracks communication actions and allows a user to attach copies of that communication.
SIRP: Evidence Journal	This is a child-level record of an incident record (one-to-many). The evidence record tracks investigative actions and allows a user to attach evidence.
SIRP: Tasks	This is a child-level record of an incident record (one-to-many). The task record allows a task to be assigned to an individual and tracked.
SIRP: Work Log	This is a child-level record of an incident record (one-to-many). The work log record captures and tracks work entries.
SIRP: Case Contact	This is a child-level record of an incident record (one-to-many). The contact record captures details regarding individual related to an incident.
SIRP: Playbook Rule	This is a root-level record that contains playbook rules. These rules are used to build lists of tasks from the task library.
SIRP: Library Task	This is a root-level record that contains tasks. These tasks are used by playbook rules to build lists of tasks.
SIRP: Event Escalation Rule	This is a root-level record that contains escalation rules. These rules define criteria and actions for various events.

Note: In addition to the above record types, there are other record types that allow you to get event data into SIRP. These record types include SIRP: ArcSight Event, SIRP: QRadar Event, SIRP: Splunk Event, SIRP: AWS Event, SIRP: Checkpoint Event, and SIRP: Symantec Endpoint Protection Event.

Home Page Tabs

The baseline configuration of the Security Incident Response module contains several Home Page Tabs. These tabs can be configured for various roles and then can be assigned to users to complete their tasks. The following table lists the Home Page tabs available in the Security Incident Response module.

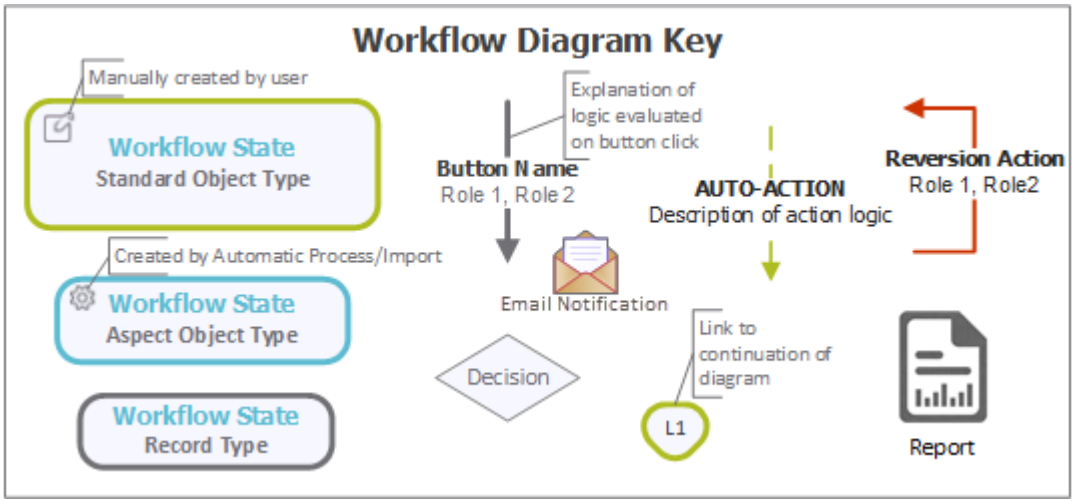
Home Page Tab	Description
SIRP: Security Incident Response (grouping tab)	Allows quick access to the sub-tabs available in this module.
SIRP: SIRP Management Team Home	Provides a quick overview of the SIRP module with overview and rules charts and self-registration links.
SIRP: Events Navigator	This is a record navigator that allows users to navigate to the events.
SIRP: Event Dashboard	This is a standard Home Page tab that displays event data in various charts.
SIRP: Incident Response Navigator	This is a record navigator that allows the users to view incidents grouped by various attributes such as workflow state.
SIRP: Incident Response Dashboard	This is a standard Home Page tab that displays incident data in various charts.
SIRP: Event Rules Management	This is a standard Home Page tab that allows the users to view event rules, activate or deactivate the rules, and create new event rules.
SIRP: Playbook Rules Management	This is a standard Home Page tab that allows the user to view playbook rules, activate or deactivate the rules, and create new playbook rules.
SIRP: Task Library Management	This is a standard Home Page tab that allows the users to view tasks, activate or archive those tasks, and create new tasks.

Security Incident Response Workflows

This section covers various details on the following baseline workflows in the Security Incident Response module:

- Event
- Incident
- Task
- Rule
- Library Task

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

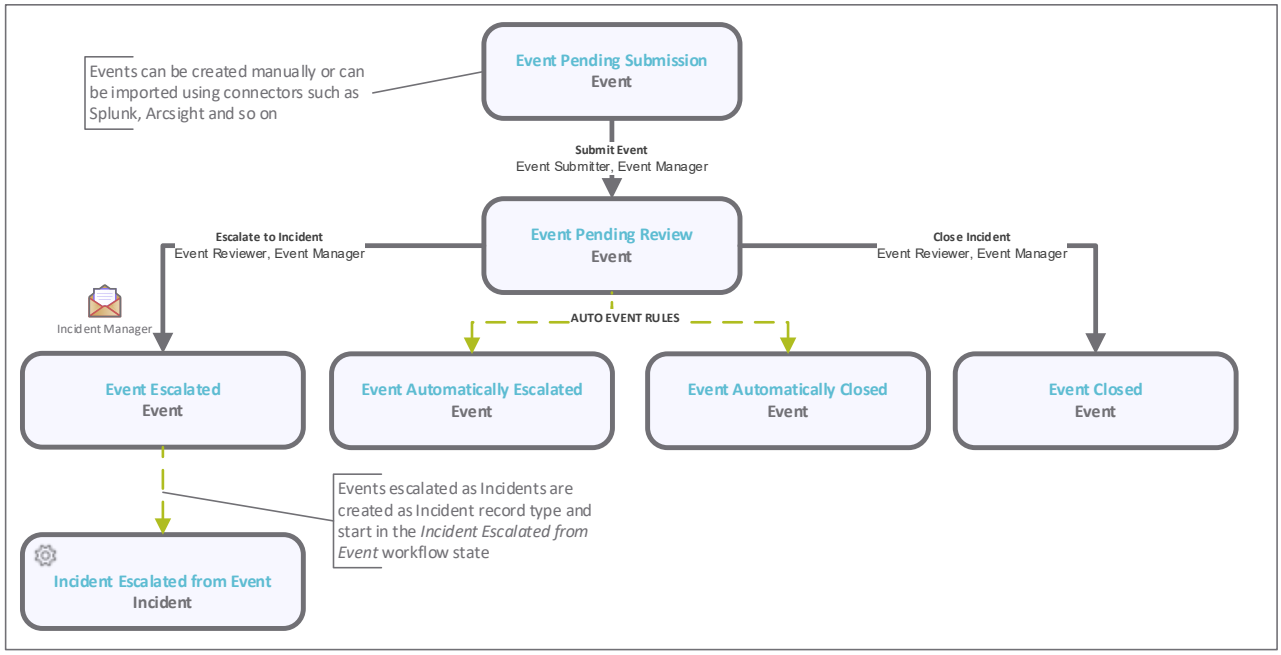


Event Workflow

This section covers the Workflow diagram, states, and buttons of the baseline Event workflow in the Security Incident Response module.

Workflow Diagram

The following diagram represents the baseline Event workflow.



Workflow States

The following is a list of states associated with the baseline Event workflow.

Workflow State	Description
SIRP: Event Pending Submission	An event that is created manually enters this state. No further action will be taken on the event until the user submits the event. After submission, the event moves to the **Event Pending Review** state.
SIRP: Event Pending Review	In this state, an event is reviewed and a decision is made on how to handle the event. Depending on the outcome of analysis, the event can be escalated or closed. Escalated events are changed into incident records. Closed events move to the **Event Closed** workflow state.
SIRP: Event Escalated	An event enters this state from the **Event Pending Review** state when it is escalated by an *Event Reviewer*.

Workflow State	Description
SIRP: Event Automatically Escalated	An event enters this state from the **Event Pending Review** state when it is escalated by an Event Escalation Rule.
SIRP: Event Closed	An event enters this state from the **Pending Review** state when it is closed by an *Event Reviewer*. Events are locked in this state.
SIRP: Event Automatically Closed	An event enters this state from the **Event Pending Review** state when it is closed by an Event Escalation Rule. Events are locked in this state.

Workflow Buttons

The following is a list of buttons that are available in the various states of the baseline Event workflow.

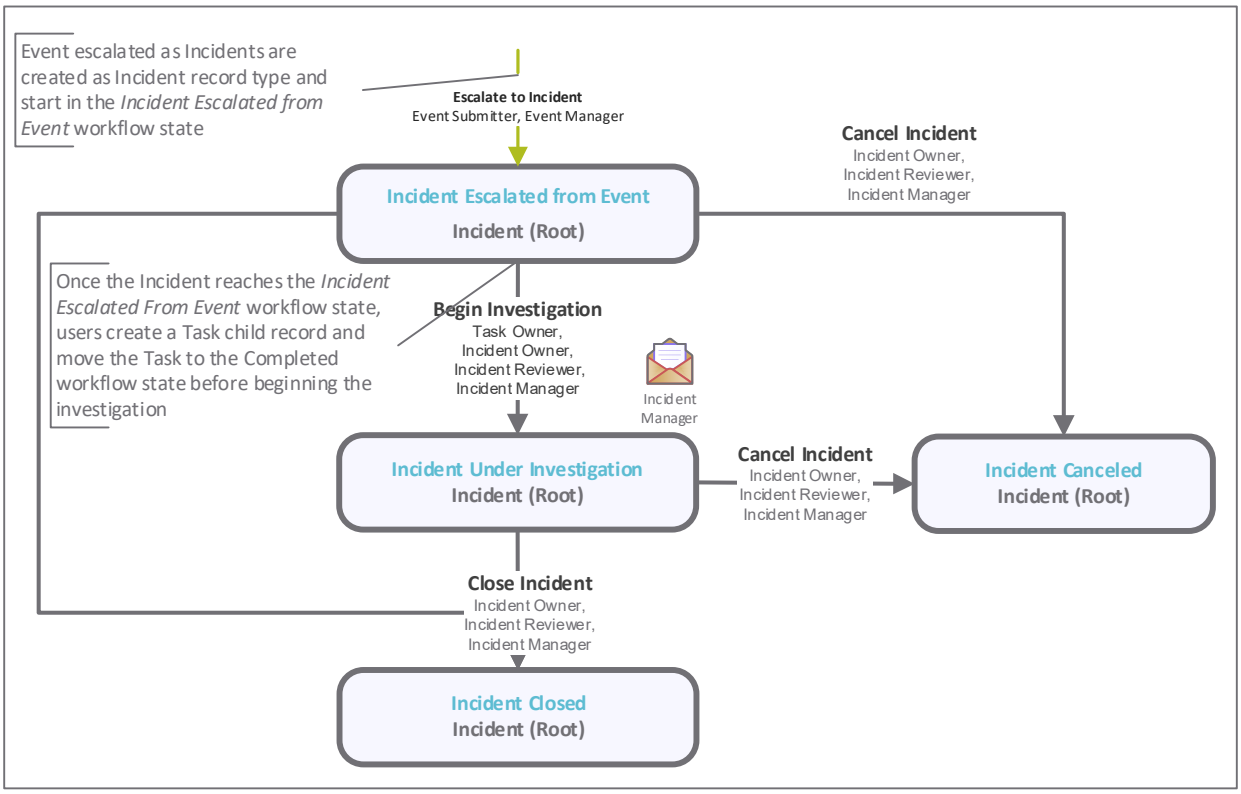
Button	Available to	Notification	Description
SIRP: Submit Event	Event Submitter Event Manager	No	Available in the **Event Pending Submission** state to move the event record workflow to the **Event Pending Review** state.
SIRP: Escalate to Incident	Event Reviewer Event Manager	No	Available in the **Event Pending Review** state to change the event into an incident. The incident is created in the **Incident Escalated from Event** workflow state.
SIRP: Close Event	Event Reviewer Event Manager	No	Available in the **Event Pending Review** state to move the event record workflow to the **Event Closed** state.

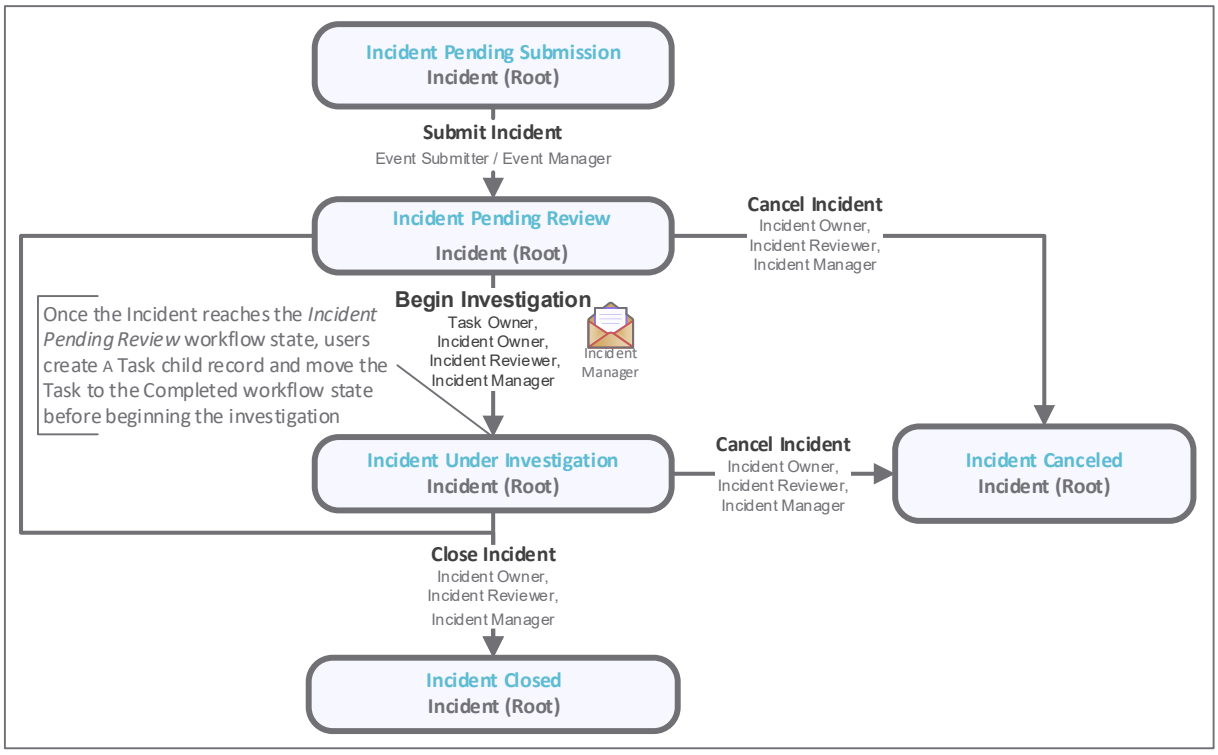
Incident Workflow

This section covers the Workflow diagram, states, and buttons of the baseline Incident workflow in the Security Incident Response module.

Workflow Diagram

The following diagrams represent the baseline Incident workflow.





Workflow States

The following is a list of states associated with the baseline Incident workflow.

Workflow State	Description
SIRP: Incident Pending Submission	An incident that is created manually enters this state. No further action will be taken on the incident until the user submits the incident. After submission, the incident moves to the **Incident Pending Review** workflow state.
SIRP: Incident Pending Review	In this state, an incident is reviewed and a decision is made on how to handle the incident. Depending on the outcome of analysis, the incident can be investigated, closed, or cancelled. Incidents to be investigated move to the **Incident Under Investigation** workflow state. Closed incidents move to the **Incident Closed** workflow state. Cancelled incidents move to the **Incident Cancelled** workflow state.
SIRP: Incident Escalated from Event	This workflow state is similar to the **Incident Pending Submission** state, but it indicates that the incident was created by escalating an event. Child records, such as communications, evidence, and forensic examinations can be created in this workflow state.
SIRP: Incident Under Investigation	This workflow state indicates that the incident is being investigated. Child records, such as communications, evidence, and forensic examinations can be created in this workflow state.

Workflow State	Description
SIRP: Incident Closed	This workflow state contains incidents that have been closed by an analyst. Incidents are locked in this state.
SIRP: Incident Cancelled	This workflow state contains incidents that have been cancelled by an analyst. Incidents are locked in this state.

Workflow Buttons

The following is a list of buttons that are available in the various states of the baseline Incident workflow.

Button	Available to	Notification	Description
SIRP: Escalate to Incident	Event Reviewer Event Manager	No	Available in the **Event Pending Review** state to change the event into an incident. The incident is created in the **Incident Escalated from Event** workflow state.
SIRP: Submit Incident	Incident Submitter Incident Manager	No	Available in the **Incident Pending Submission** state to move the incident record workflow to the **Incident Pending Review** state.
SIRP: Begin Investigation	Incident Reviewer Incident Manager	No	Available in the **Incident Pending Review** and **Incident Escalated from Event** states to move the incident record workflow to the **Incident Under Investigation** state. This workflow button also runs all active Playbook Rules against the Incident and will create related Tasks based on those rules.
SIRP: Close Incident	Incident Reviewer Incident Manager	No	Available in the **Incident Pending Review**, **Incident Escalated from Event**, and **Incident Under Investigation** states to move the incident record workflow to the **Incident Closed** state.
SIRP: Cancel Incident	Incident Reviewer Incident Manager	No	Available in the **Incident Pending Review**, **Incident Escalated from Event**, and **Incident Under Investigation** states to move the incident record workflow to the **Incident Cancelled** state.
SIRP: Build Task List	SIRP Incident Reviewer SIRP: Incident Manager	No	Available in the **Incident Escalated from Event** and **Incident Under Investigation** states. Clicking this button records will create Task records that have been added on the Task Library tab.

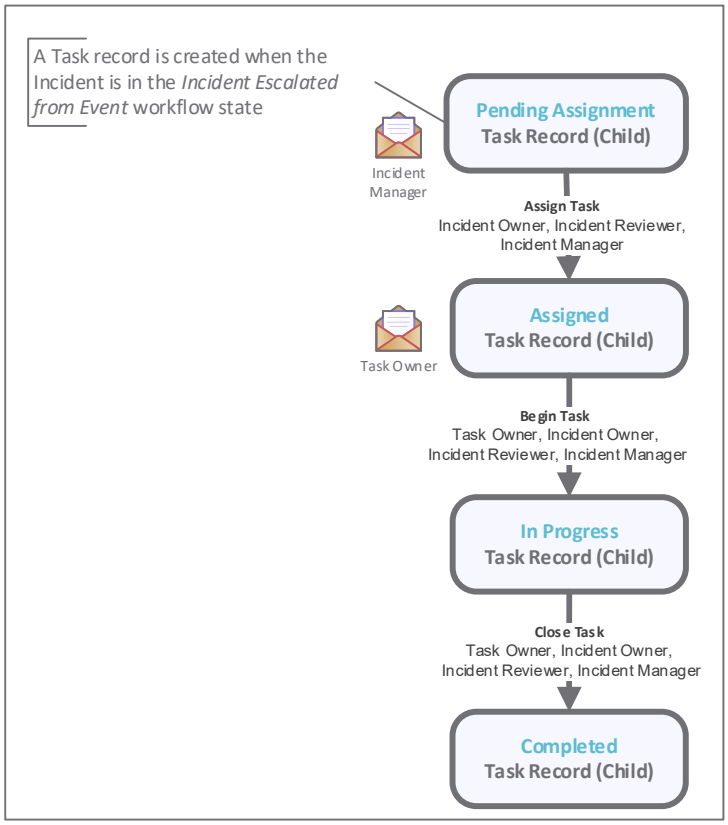
Button	Available to	Notification	Description
SIRP: Create Tasks From Playbook	SIRP Incident Reviewer SIRP: Incident Manager	No	Available in the **Incident Pending Review**, **Incident Escalated from Event**, and **Incident Under Investigation** states. Clicking this button creates Task records based on Playbook Rules.

Task Workflow

This section covers the workflow diagram, state, and buttons of the baseline Task workflow in the Security Incident Response module.

Workflow Diagram

The following diagram represents the baseline Task workflow.



Workflow States

The following is a list of states associated with the baseline Task workflow.

Workflow State	Description
SIRP: Task - Pending Assignment	A task is created in this workflow state and will remain in this state until it is assigned.
SIRP: Task - Assigned	A task is moved to this workflow state upon assignment. A notification is sent to the *Task Owner* upon assignment. The *Task Owner* must click **Begin Task** to move the task to the **Task - In Progress** workflow state.
SIRP: Task - In Progress	This workflow state contains tasks that are currently being worked. The Task Owner must click the **Task Completed** button to move the task to the **Task – Completed** workflow state.
SIRP: Task - Completed	This workflow state contains tasks that have been completed by the *Task Owner*. Tasks are locked in this state.

Workflow Buttons

The following is a list of buttons that are available in the various states of the baseline Task workflow.

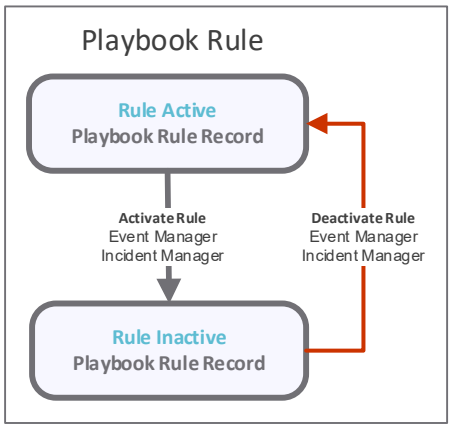
Button	Available to	Notification	Description
SIRP: Assign Task	Incident Reviewer Incident Manager	Yes	Available in the **Task – Pending Assignment** state to move the task to the **Task – Assigned** state. This also sends a notification to the *Task Owner*.
SIRP: Begin Task	Task Owner Incident Reviewer Incident Manager	No	Available in the **Task – Assigned** state to move the task to the **Task – In Progress** state.
SIRP: Close Task	Task Owner Incident Reviewer Incident Manager	No	Available in the **Task – In Progress** state to move the task to the **Task – Completed** state.

Rule Workflow

This section covers the Workflow Diagram, states, and buttons of the baseline Rule workflow in the Security Incident Response module

Workflow Diagram

The following diagram represents the baseline Rule workflow.



Workflow States

The following is a list of states associated with the baseline Rule workflow.

Workflow State	Description
SIRP: Rule Active	A rule in this workflow state is run against new events and/or incidents.
SIRP: Rule Inactive	A rule in this workflow state will not be run against new events and/or incidents.

Workflow Buttons

The following is a list of buttons that are available in the various states of the baseline Rule workflow.

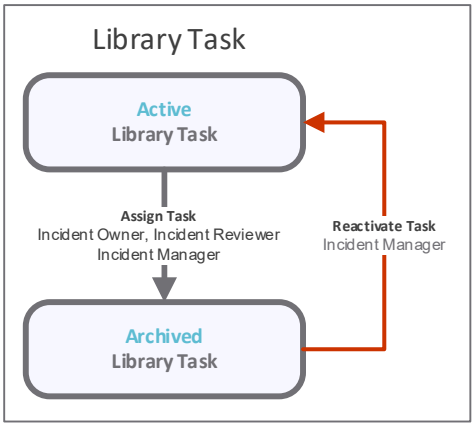
Button	Available to	Notification	Description
SIRP: Activate Rule	Event Manager Incident Manager	No	Available in the **Rule Inactive** state to move the rule to the **Rule Active** state.
SIRP: Deactivate Rule	Event Manager Incident Manager	No	Available in the **Rule Active** state to move the rule to the **Rule Inactive** state.

Library Task Workflow

This section covers the Workflow diagram, states, and buttons of the baseline Rule workflow in the Security Incident Response module.

Workflow Diagram

The following diagram represents the baseline Library Task workflow.



Workflow States

The following is a list of states associated with the baseline Library Task workflow.

Workflow State	Description
SIRP: Library Task - Active	This workflow state contains Library Tasks that can be assigned to incidents.
SIRP: Library Task - Archived	This workflow state contains Library Tasks that cannot be assigned to incidents.

Workflow Buttons

The following is a list of buttons that are available in the various states of the baseline Library Task workflow.

Button	Available to	Notification	Description
SIRP: Archive Task (Library)	Incident Manager	No	Available in the **Library Task - Active** state to move the rule to the **Library Task - Archived** state.
SIRP: Reactivate Task (Library)	Incident Manager	No	Available in the **Library Task - Archived** state to move the rule to the **Library Task - Active** state.

Workflow Roles

The following is a list of workflow roles that perform tasks associated with the states in the baseline Security Incident Response workflows.

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

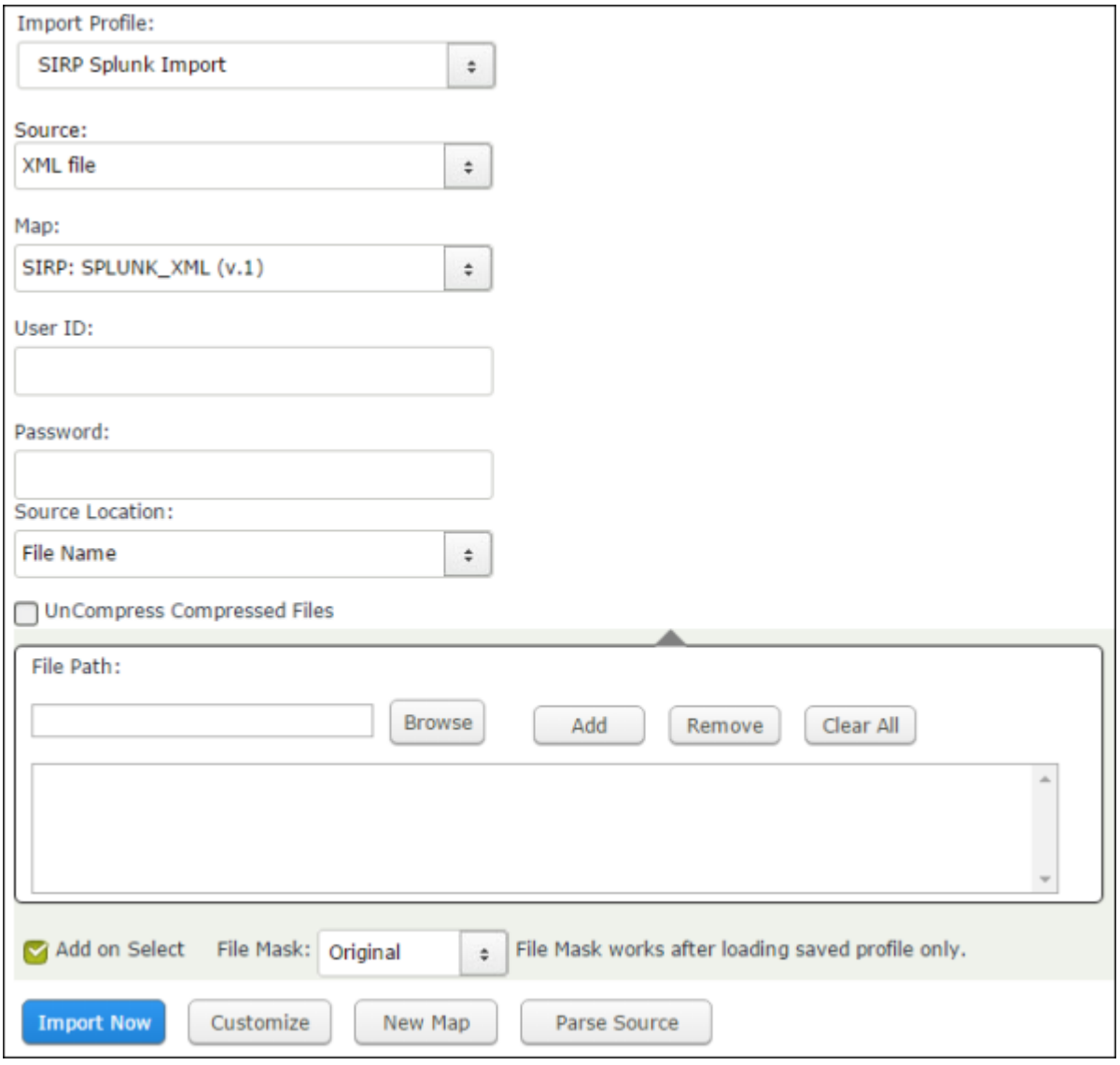
User ID	Role	Description
NA	SIRP: Event Submitter	This role is automatically assigned to the users that submit events.
r_sirp_event_reviewer	SIRP: Event Reviewer	This role is assigned to the users that own the responsibility to review event records. A user with this role reviews events and can escalate or close the event.
r_sirp_event_manager	SIRP: Event Manager	This role is assigned to the users that own the responsibility to manage the event workflow. A user with this role can create, view, update, and delete event records. These users can also create, view, update and delete Event Escalation Rules.
r_incident_submitter	SIRP: Incident Submitter	This role is automatically assigned to the users that submit incidents.
r_sirp_incident_reviewer	SIRP: Incident Reviewer	This role is assigned to the users that own the responsibility to review incident records. A user with this role reviews incidents and can initiate an investigation, close or cancel the investigation. This role allows a user to create, view and update incident records and to create, view and update child records of the incident.
r_sirp_incident_manager	SIRP: Incident Manager	This role is assigned to the users that own the responsibility to manage the incident workflow. A user with this role can create, view, update, and delete incident records, and create, view, and update child records of the incident. Users with this role can also manage Playbook Rules and the Task Library.
r_sirp_task_owner	SIRP: Task Owner	This role is assigned to a user to whom you want to work on a specific portion of an incident. This role has read-only access to the incident record and read and update access to the tasks that are assigned to them.
NA	SIRP: Task Owner Parent Permission	A user with this role has read-only access the parent incident records.

In addition to the above roles, the Rsam installation package includes an administrative role, **U: Object Administrator**, as well as a sample user for that role, **r_admin**. This user has access to all record types, object types, workflow states, and workflow buttons across all Rsam baseline modules. Rsam Administrators should take necessary precautions to restrict standard users from accessing Rsam with this administrative role.

Importing Event Data

Event data can be imported into the Security Incident Response module through several methods. Several import profiles, maps, and email listeners have been predefined for some of the more prevalent SIEM tools, such as Splunk, ArcSight, and QRadar. Additional profiles, maps, and email listeners can be configured as needed. Integration guides created for tools, such as Splunk and QRadar, and are available in the *Rsam Community* portal.

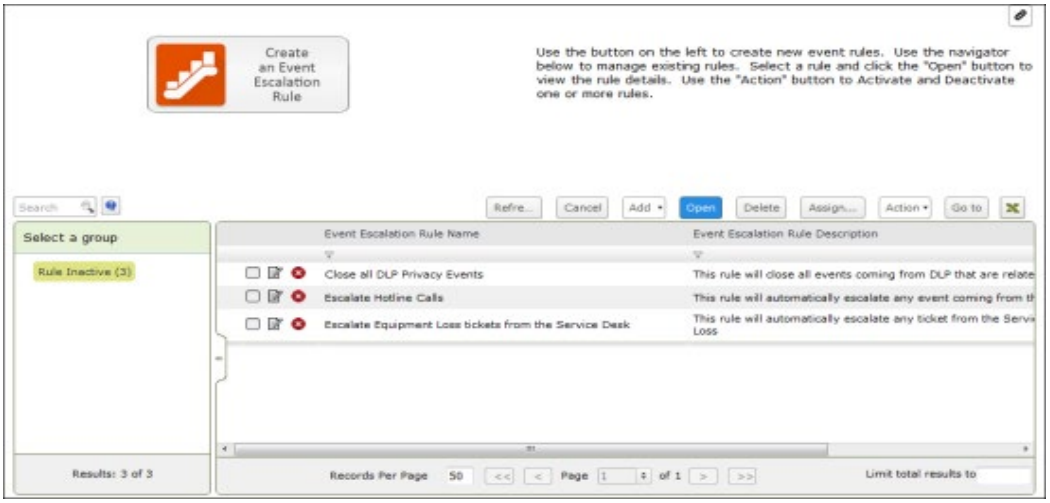
The following images show the Rsam Import pages.



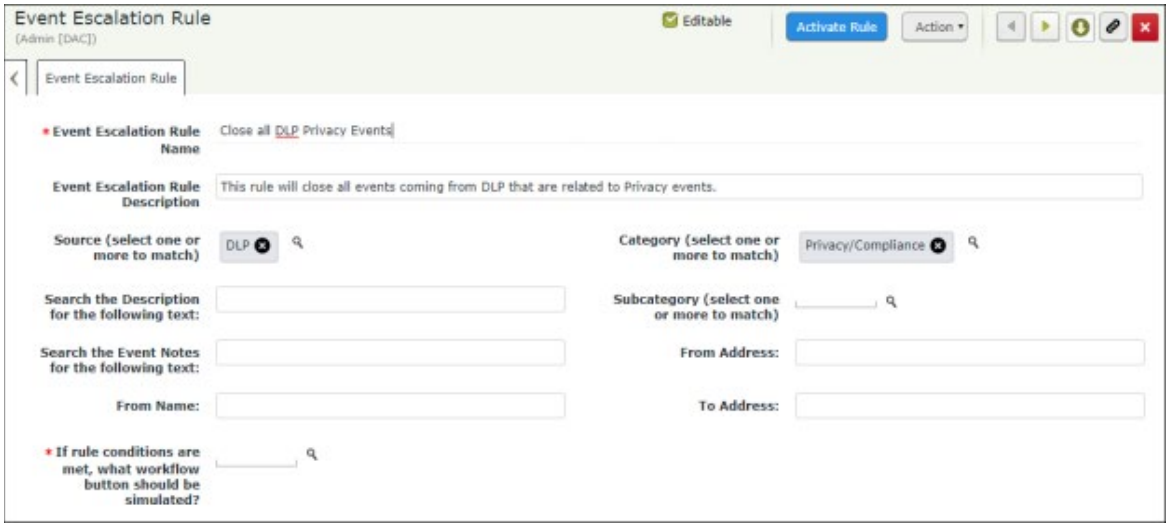
Appendix 1: Automatic Event Analysis

In addition to escalating and closing events manually, Rsam also provides the ability to implement Event Escalation Rules. Event Escalation Rules allow users with the Event Manager role to configure automatic actions based on the criteria included in the Event record. For example, to escalate DLP events automatically and close Privacy events automatically.

Event Escalation Rules can be managed from the **Event Rules** Home Page tab with the *Event Manager* role. Rules can be created, edited, deleted, and made active or inactive.



Event Escalation criteria can be based on several attributes, such as Source, Category, Description and Event Notes. The From Address, To Address, and From Name attributes allow the rule to trigger based on the same attributes available on the Email Info tab of Event record type (this is useful if the event was created from an email).

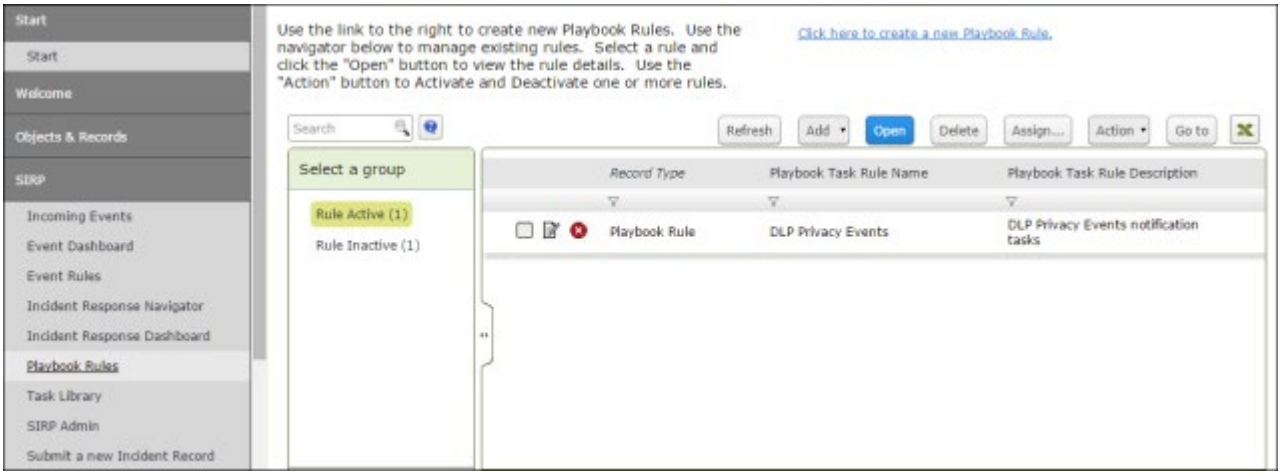


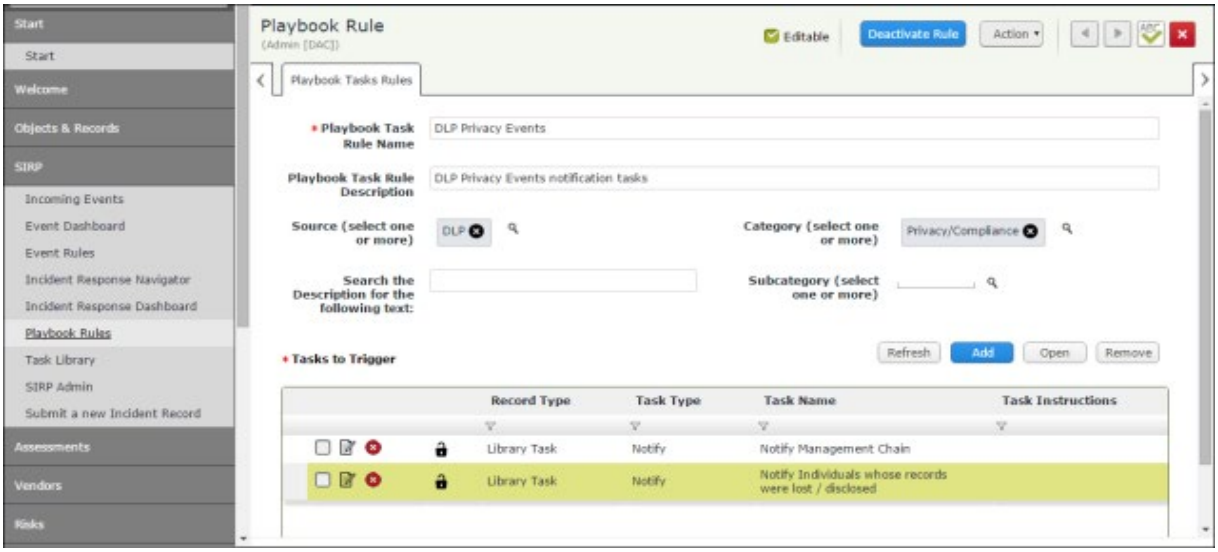
Appendix 2: Automatic Task Generation from Playbook

In addition to manually creating tasks for incidents, Rsam also provides the ability to automatically generate incident handling tasks based on Playbook Rules. Playbook Rules allow users with the *Incident Manager* role to configure automatic task creation based on the criteria included in the Playbook Rule record. The Playbook Rule references one or more tasks from the Task Library that will be generated if the criteria are met.

Playbook Rules can be managed from the **Playbook Rules** Home Page tab with the *Incident Manager* role. Rules can be created, edited, deleted, and made active or inactive.

The following images show accessing the tab and the **Playbook Rule** page.

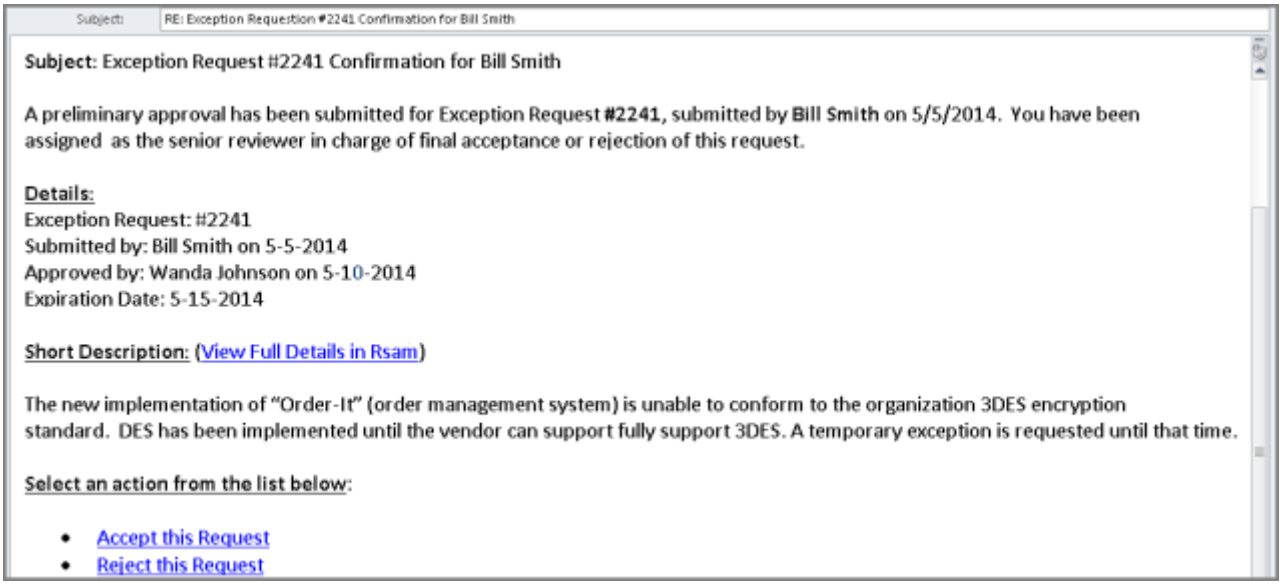




Appendix 3: Offline Decision Making

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 follow image illustrates an example notification template that has custom text, data from the record, embedded links to the application, and Offline Decision Making actions.

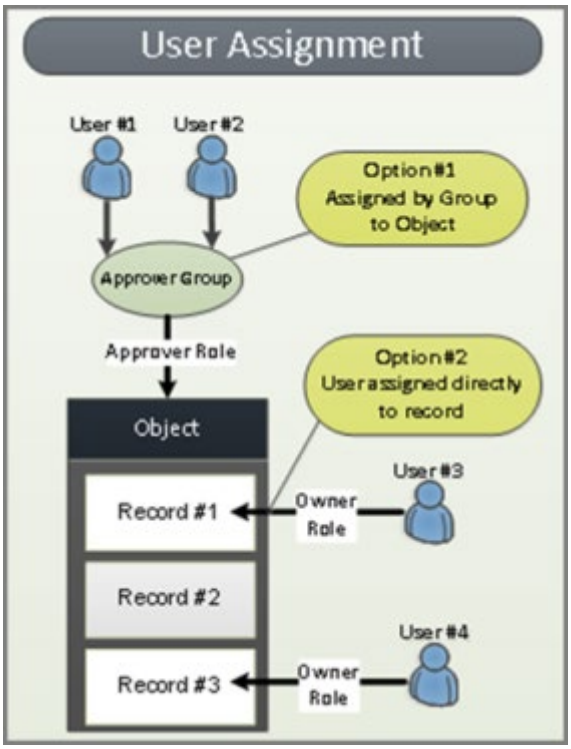


Appendix 4: User Assignment Options

Rsam allows organizations to customize configurations and workflows to their specific business practices. There are many methods by which users can be assigned roles (such as, who is responsible for reviewing and approving exceptions). The following are the most common assignment methods:

- Individual users are assigned to a group. The group is then assigned to the object under which the records are saved. When assigned to the object, the group is also given a specific role. This accomplishes the following:
    - All users in that group inherit the role assigned to the group in the context of the object and all the records under that object.
    - All users in that group have the functionality allocated to that role in the context of the object and all of the records under that object.
- Individual users are assigned a specific role directly in a record. This provides the same result as above – granting the user the functionality with the allocated role. However, it is only in the context of that specific record. No other permissions are granted to the parent object or any other record under that object.

The method for implementing the assignment can also be customizable. The assignment can be manually made through an attribute, assigned when the records are created or imported, or automatically made at different points in the workflow.



Appendix 5: Rsam Documentation

Security Incident Response Module Tutorial

For a detailed walk-through of the Security Incident Response Module user experience, refer the *Security Incident Response Module Step-by-Step Tutorial*. You should have received the *Security Incident Response Module Step-by-Step Tutorial* along with the Security Incident Response Module instance. If not, contact your Rsam Customer Representative to obtain an electronic copy of the *Security Incident Response Module Step-by-Step Tutorial*.

Online Help

This document provides an overview of the Security Incident Response Module configuration. 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 **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.