Finding Management Module

Step-by-Step Tutorial

Document Version: 01.00.02 | December 2018

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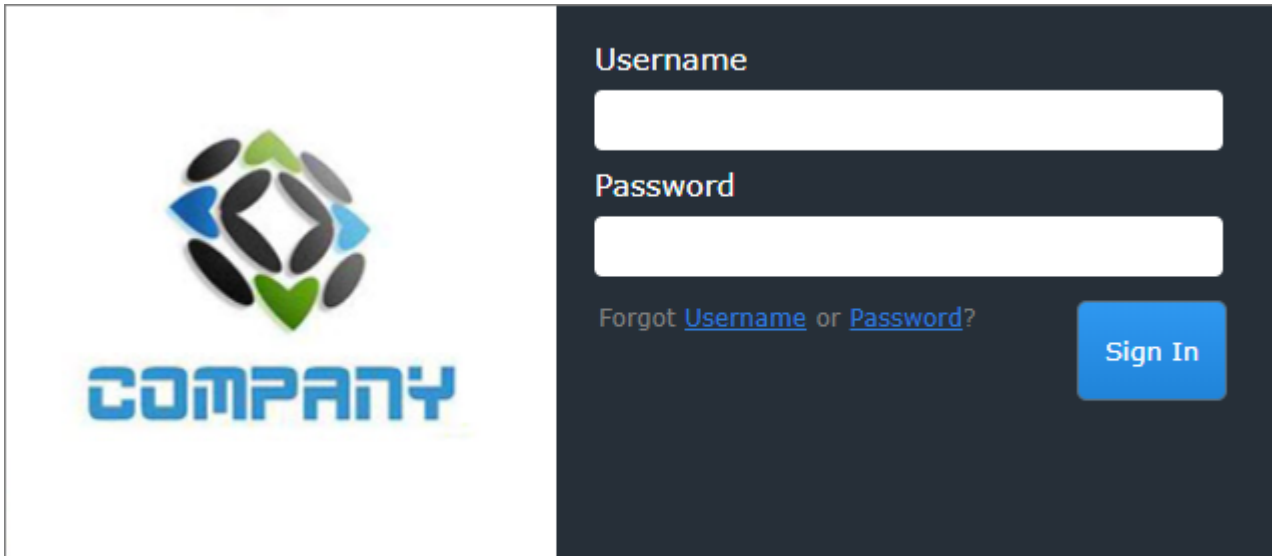
Like most elements in Rsam, the Sign-In page can be configured in a number of ways. Different authentication options such as user self-registration, integration with customer user directories (such as Active Directory), or integration with Single Sign-On products, such as Shibboleth, can be applied.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

Rsam Finding Management

Overview

The Rsam Finding Management module helps businesses to understand the wide spectrum of enterprise findings from a wide variety of sources, such as assessments, audits, issues, and other sources. By using the Rsam Finding module, organizations can leverage automated workflow to effectively prioritize and execute on remediation efforts for findings.
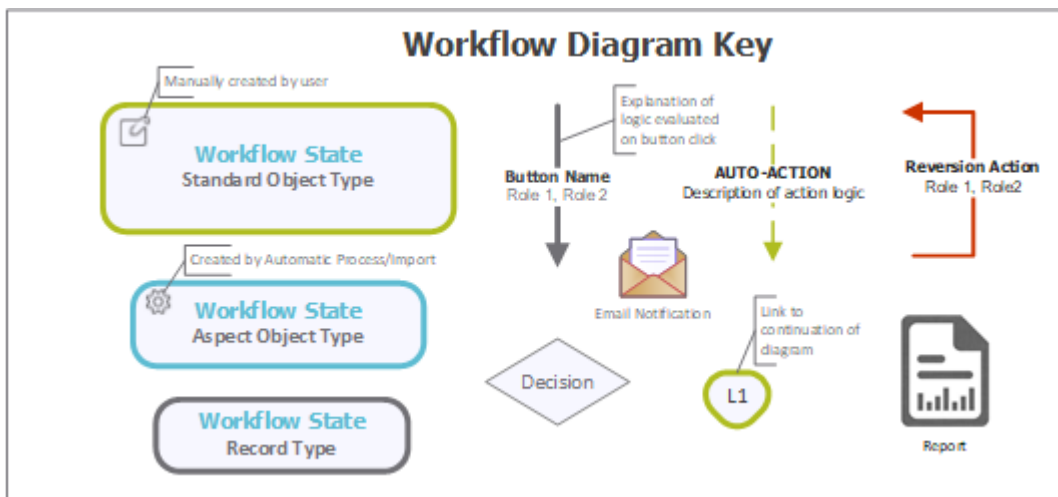
This tutorial provides a step-by-step procedure to walk you through one path of the Finding module workflow.

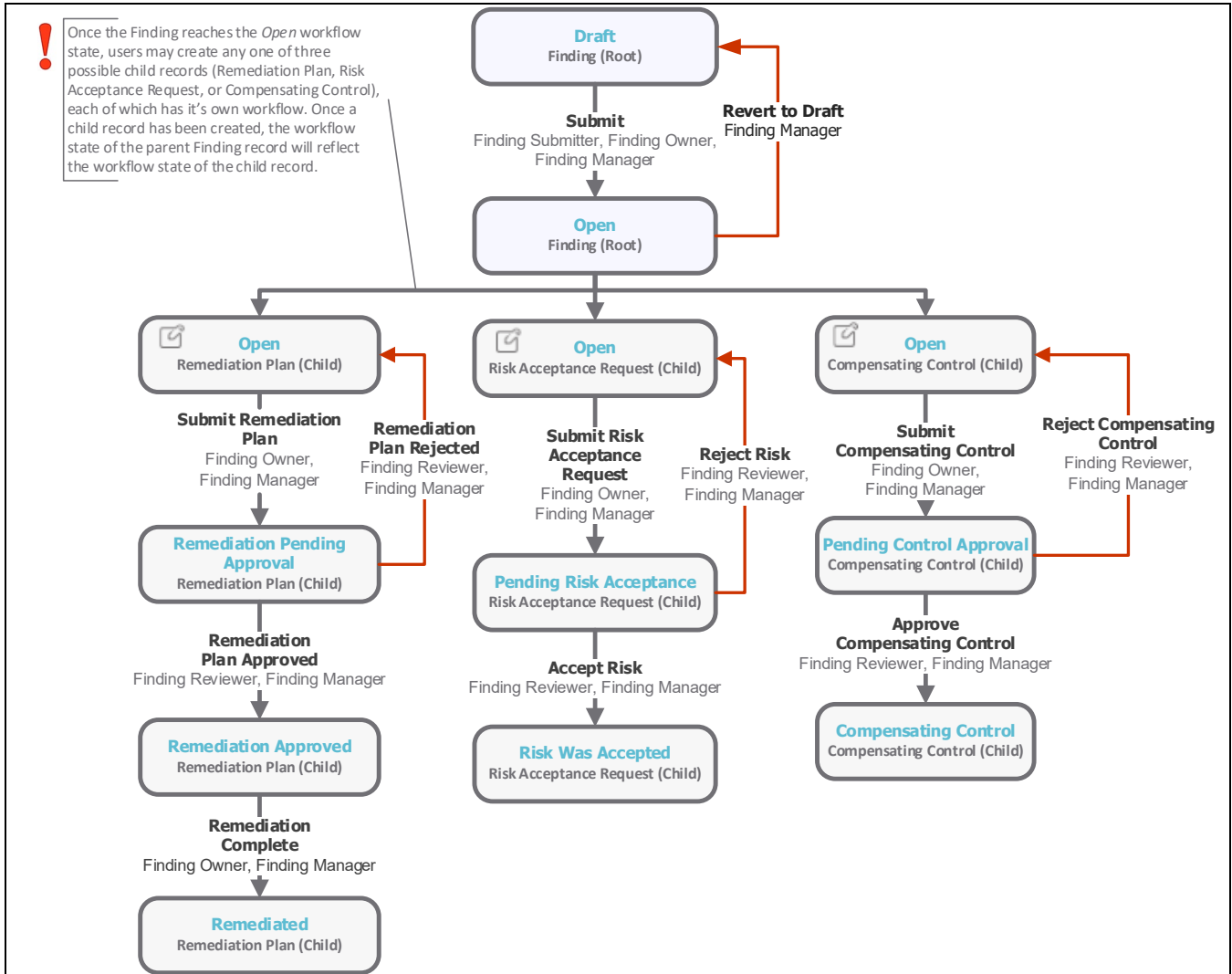The Rsam Finding Management module provides the following capabilities and benefits:

- Track individuals involved, and associate related risks and business areas

- Role-based access control and LDAP authentication

- Integrated and dynamic workflow

- Built-in customizable dashboards

Finding Workflow

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

The following diagram depicts the out-of-the-box Finding module 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. The Rsam sandbox for Finding module comes with pre-populated sample accounts that include the following:

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

Account ID	User	Business Responsibilities
r_finding_owner	Finding Owner	This user studies the assigned findings, checks and follows special instructions from management and audit. Determines and creates a remediation method, and then submits the remediation method for review and approval.
r_finding_reviewer	Finding Reviewer	This user reviews the finding and remediation plan, and then approves the remediation plan.
r_finding_manager	Finding Manager	This user is a power user, having full set of permissions to manage findings.

The default password for all accounts in the Rsam Finding module 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: Creating a Finding	Finding Owner	In this step, a finding is created
Step 2: Studying the Finding	Finding Owner	In this step, the finding is analyzed to determine related domains, business areas, related risks, etc.
Step 3: Creating a Remediation Plan	Finding Owner	In this step, a remediation method is determined and a remediation plan is created, and then it is submitted for review and approval.
Step 4: Reviewing and Approving the Remediation Plan	Finding Reviewer	In this step, the remediation plan is reviewed and approved.
Step 5: Flagging Completion of the Remediation Plan	Finding Owner	In this step, the approved remediation plan is flagged as completed.

Step-by-Step Procedure

This section contains steps we will follow in this tutorial. The path followed in this tutorial walks you through the steps to track and remediate a finding. In this tutorial, you will learn how to create a finding and how to create a remediation plan to mitigate the finding. This particular workflow path was chosen as it is the most 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:

a. 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 Finding Manager user credentials in one session if desired.

b. 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.
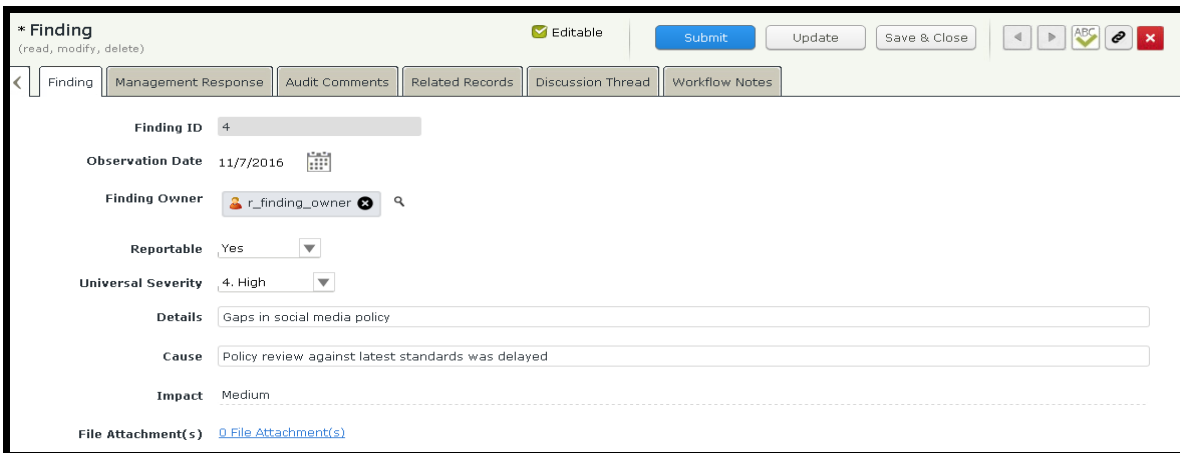
Step 1: Creating a Finding

In this step, you will log in to Rsam as the *Finding Submitter* user to create a finding and assign an owner to that finding.

1. Open an Rsam supported browser and enter the URL of your Rsam instance containing the Finding Management module.

2. Sign in as the *Finding Owner* user. Enter **Username** as *r_finding_owner* and **Password** as *password*.

3. From within the left navigation panel at the left-hand side, navigate click on **Start** > **Create a new Finding** record.
   The **Finding (new)** record opens with the **Finding** tab selected.

4. On the **Finding** tab, at a minimum complete all the required attributes (note that the read-only **Finding ID** attribute will populate automatically once the new finding is saved).
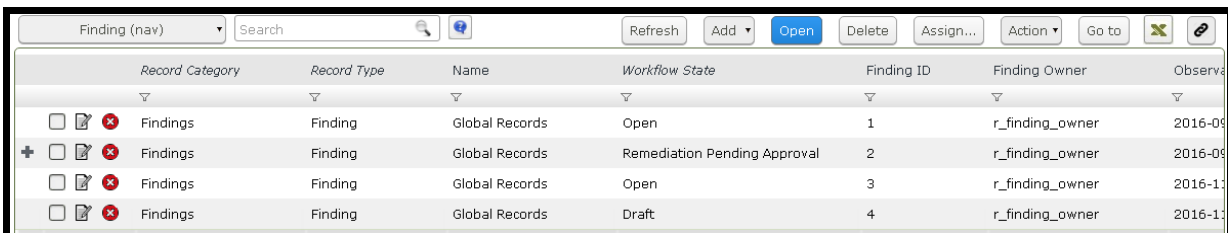

5. Click **Submit** from the buttons that appear at the top of the record form.

Step 2: Analyzing the Finding

In this step, you will log in to Rsam as the *Finding Owner* user to analyze the finding assigned by the *Finding Submitter* user by associating it with related domains, business areas, and risks.

1. Stay logged in as *r_finding_owner*. From within the navigation panel on the left-hand side, navigate to **Finding Management** > **Finding Navigator**.

   The finding navigator appears.

2. From within the finding navigator with **Finding (nav)** selected, locate the finding submitted by the *Finding Submitter* user in Step 1: Creating a Finding.

3. Use one of the following methods to open the finding:

   - Double-click the finding record.

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

   - Click the ![icon] icon in the finding record row.

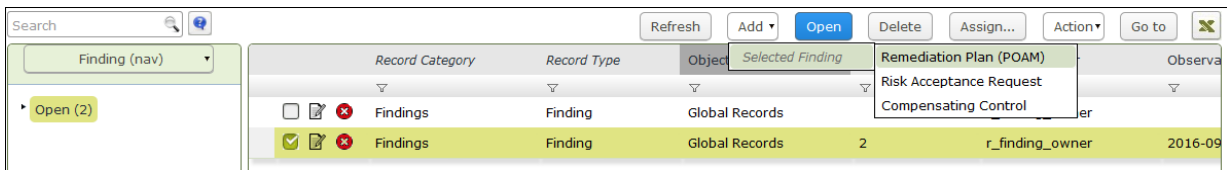   The **Finding** record opens with the **Finding** tab selected.

Next, in Step 3: Creating a Remediation Method, you will create a remediation method to mitigate the finding.

Step 3: Creating a Remediation Plan

In this step, by staying logged in to Rsam as the *Finding Owner* user, you will determine a remediation method for mitigating the finding. As part of this tutorial, you will create and submit a remediation plan to the *Finding Reviewer* user for review.

Note: You can remediate a finding by using the Remediation Plan (POAM), Risk Acceptance Request, or Compensating Control method. However, this tutorial will only walk you through the steps for the Remediation Plan (POAM) method only. You may explore other remediation methods to enhance your learning, if desired.

1. From within the navigation panel at the left-hand side, navigate to **Finding Management** > **Finding Navigator** and locate your finding.

2. Select the finding record, click **Add**, and select **Remediation Plan (POAM)** from the options that appear.

   The **Remediation Plan (POAM) (new)** record opens with the **Remediation Plan (POAM)** tab selected.

3. Complete all the necessary attributes on the **Remediation Plan (POAM)** and **Supplemental Data** tabs.
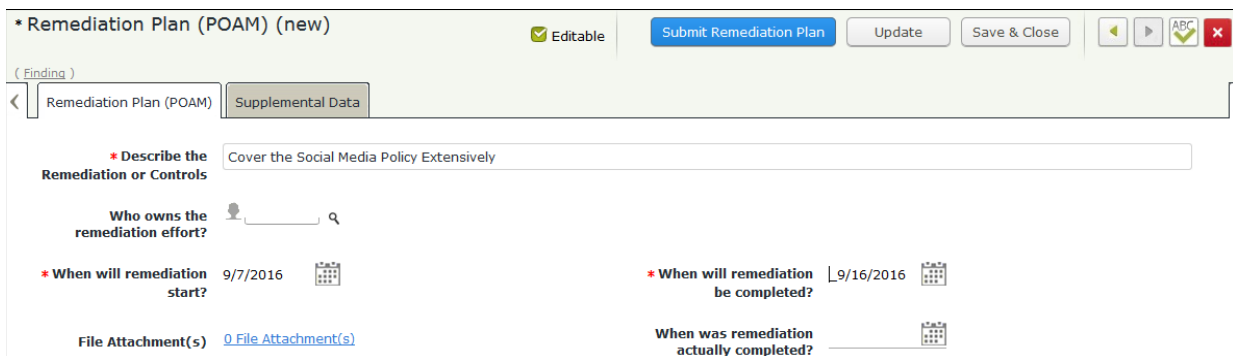
4. Click **Submit Remediation Plan**.
   The finding now has the remediation plan child record. Both the finding and the remediation plan record workflows enter the **Remediation Pending Approval** state.

5. Hover the cursor over the username at the right-hand corner and select **Logout** from the options that appear.
   You have been successfully logged out from the Rsam Finding Management module.

Step 4: Reviewing and Approving the Remediation Plan

In this step, you will log in to Rsam as the *Finding Reviewer* user to review the finding details and the remediation plan. As part of the path taken by this tutorial, the *Finding Reviewer* user will approve the remediation plan.

1. Open an Rsam supported browser and enter the URL of your Rsam instance containing the Finding Management module.

2. Sign in as the *Finding Reviewer* user. Enter **Username** as *r_finding_reviewer* and **Password** as *password*.

3. From within the navigation panel at the left-hand side, navigate to **Finding Management** > **Finding Navigator**.

4. Locate the finding that the *Finding Owner* user had created a remediation plan in Step 3: Creating a Remediation Plan.

5. Click **+** in the finding record row to display the remediation plan you want to approve.

6. Select the remediation plan record.

7. Click **Action** and select **Remediation Plan Approved** from the options that appear.

The finding record and the remediation plan child record enters the **Remediation Approved** workflow state.

8. Hover the cursor over the username at the right-hand corner and select **Logout** from the options that appear.

You have been successfully logged out from the Rsam Finding module.

Step 5: Flagging Completion of the Remediation Plan

In this step, you will log in to Rsam as the *Finding Owner* user to flag the completion of remediation plan which was approved by the *Finding Reviewer* user. This time, rather than using the **Finding** navigator to locate the finding record, we will use dashboard charts to drill-through to the finding record we want to locate.
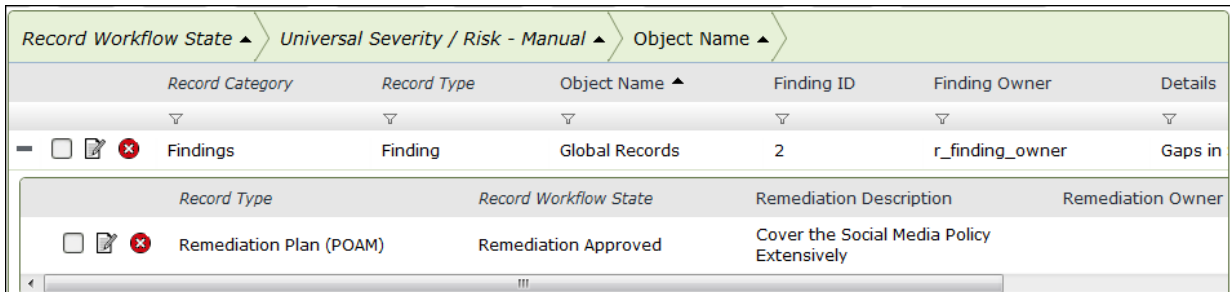
1. Open an Rsam supported browser and enter the URL of your Rsam instance containing the Finding Management module.

2. Sign in as the *Finding Owner* user. Enter **Username** as *r_finding_owner* and **Password** as *password*.

3. From within the navigation panel at the left-hand side, navigate to **Finding Management** > **Findings Management Home**.
   The findings home page containing self-registration links and dashboards appears.

4. Under **Finding by Workflow and Severity** dashboard, click on the data bar representing **Remediation Approved**.
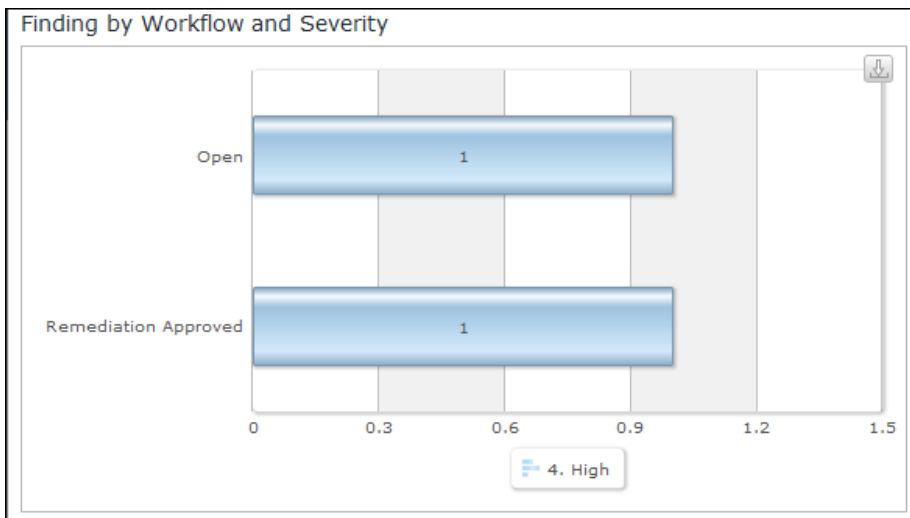
The **FI: Findings by Workflow State and Severity** chart opens with findings in the **Remediation Approved** state.
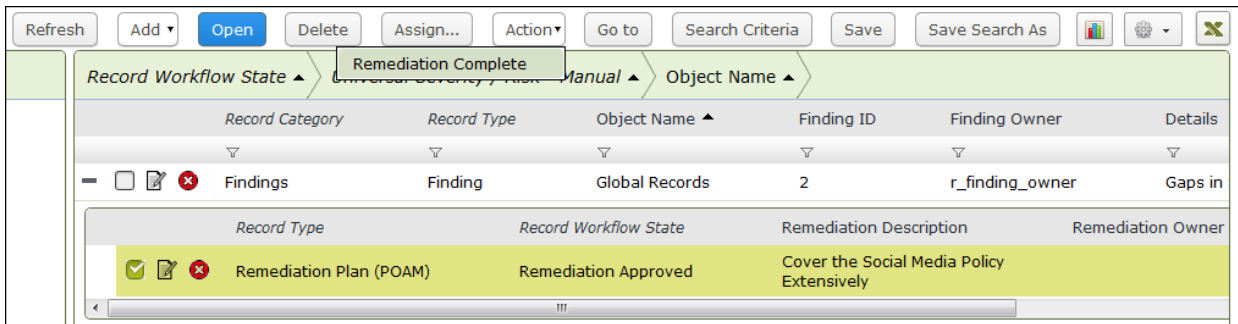
5. Locate the finding that the *Finding Reviewer* approved the remediation plan in Step 4: Approving a Remediation Plan.

6. Click **+** in the finding record row to find the remediation plan you want to flag as complete.

7. Select the remediation plan record.

8. Click **Action** and select **Remediation Complete** from the options that appear.

The finding record and the remediation plan child record enters the Remediated workflow state.

9. Hover the cursor over the username at the right-hand corner and select **Logout** from the options that appear.

You have been successfully logged out from the Rsam Finding Management module.

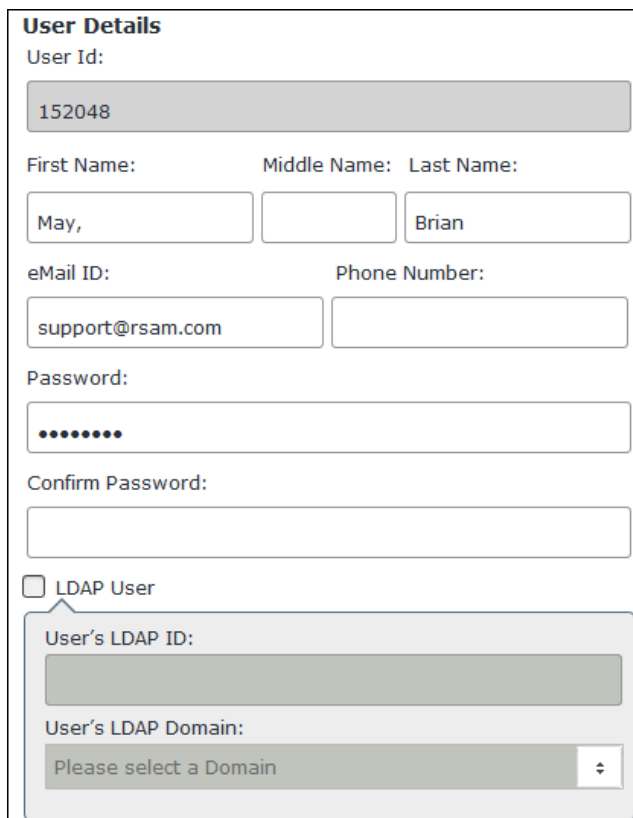# Appendix 1: Email Notifications and Offline Decision Making

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 Finding Management Module 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.

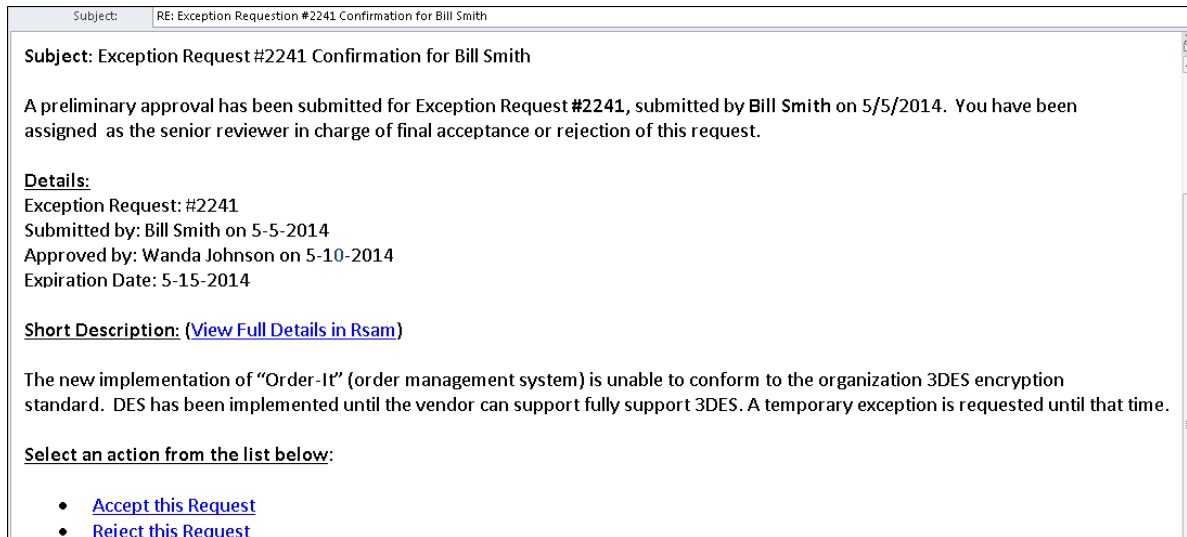5. Provide an email address in the **eMail ID** attribute.

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

Finding Management Module Baseline Configuration Guide

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

Online Help

This tutorial provides the step-by-step instructions for the Rsam Finding 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. 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.