



Rsam Documentation

Getting Started Guide for SOAR-Vulnerability Management Module

Document Version: 2017.03.01

March 2017



Contents

About this Guide-----	3
Preparing Your Rsam Instance for SOAR-VM Implementation -----	4
Step 1: Get to Know the Baseline-----	4
Step 2: Modify Attributes and Tabs -----	4
Step 3: Confirm Rsam Installation Settings for Importing Large Files-----	4
Step 4: Import Existing Vulnerabilities -----	5
Step 5: Provision Your Users and Groups-----	5
Step 6: Grant Import Ability for Non-Administrative User Accounts -----	6
Step 7: Remove Sample Data and Users-----	6
Step 8: Schedule Events-----	6
Step 9: Go Live Quickly and Prepare for the Future-----	7
Appendix: Rsam Documentation-----	8
Inline Help-----	8



About this Guide

This guide provides a brief overview of steps required prior to implementation of the Security Operations Analytics and Reporting-Vulnerability Management (SOAR-VM) module.

Preparing Your Rsam Instance for SOAR-VM Implementation

This section walks you through the configuration activities that are required for the baseline implementation of the Security Operations Analytics and Reporting-Vulnerability Management (SOAR-VM) module.

Step 1: Get to Know the Baseline

Begin familiarizing yourself and your key stakeholders with the SOAR-VM baseline configuration by walking through it with the help of the document titled “SOAR - Vulnerability Management Module Step-by-Step Tutorial”. This document provides some sample day-in-the-life experiences for key user roles included in the SOAR-VM baseline configuration.

For additional information on what’s included in your SOAR-VM baseline, refer to the document titled *SOAR - Threat and Vulnerability Management Baseline Configuration Guide*.



Rsam’s baseline implementation methodology assumes that you will be leveraging Rsam’s out-of-the-box configuration of industry best practices for vulnerability management. However, as you move through the configuration with the help of these documents, begin to capture notes on minor configuration changes to attributes, tabs, etc. that might be required prior to your organization leveraging this module.

Step 2: Modify Attributes and Tabs

The intent of a baseline implementation is to leverage Rsam’s out-of-the-box configuration in order to get up-and-running quickly. However, the Rsam platform provides many opportunities for configuring modifications to the out-of-the-box attributes, their arrangement on screens, and their behavior (controlled through the use of risk analytic handlers). If your stakeholders require additional attributes or modification to existing ones before going live, implement them early in the baseline implementation process. Other items in this checklist (e.g. importing vulnerabilities) may be affected by your configuration choices.

In the Rsam Basic class, an Rsam administrator will have learned about tasks like creating and modifying attributes. For more information on Rsam administration, refer to Rsam User Help and Rsam Administrator Help.

Step 3: Confirm Rsam Installation Settings for Importing Large Files

If planning to import large files, please ensure your web server administrator has completed all the required configurations specific to importing larger files. These settings are outlined in the “Setting ‘Request Filtering’ if Importing Large Files” section of the *Rsam Installation Guide (Installer Method)*.

Step 4: Import Existing Vulnerabilities

If you have a repository (Excel, database, scanner tool, etc) of existing vulnerabilities that you would like to place into Rsam for your go-live, then you may want to leverage Rsam's import engine to import the vulnerabilities and any desired attributes.

The SOAR-VM baseline configuration comes with several predefined import mappings for vulnerability records, however, if you made modifications to vulnerability attributes in Step 2: Modify Attributes and Tabs, then you may want to modify the provided mappings) to accommodate those changes.

Importing records (like Vulnerabilities) was taught to your Rsam Administrator in Rsam's Basic Administration course. For more information on using Rsam's import engine to import your vulnerabilities, refer to the "Importing Records" section in *Rsam Administrator Help*.

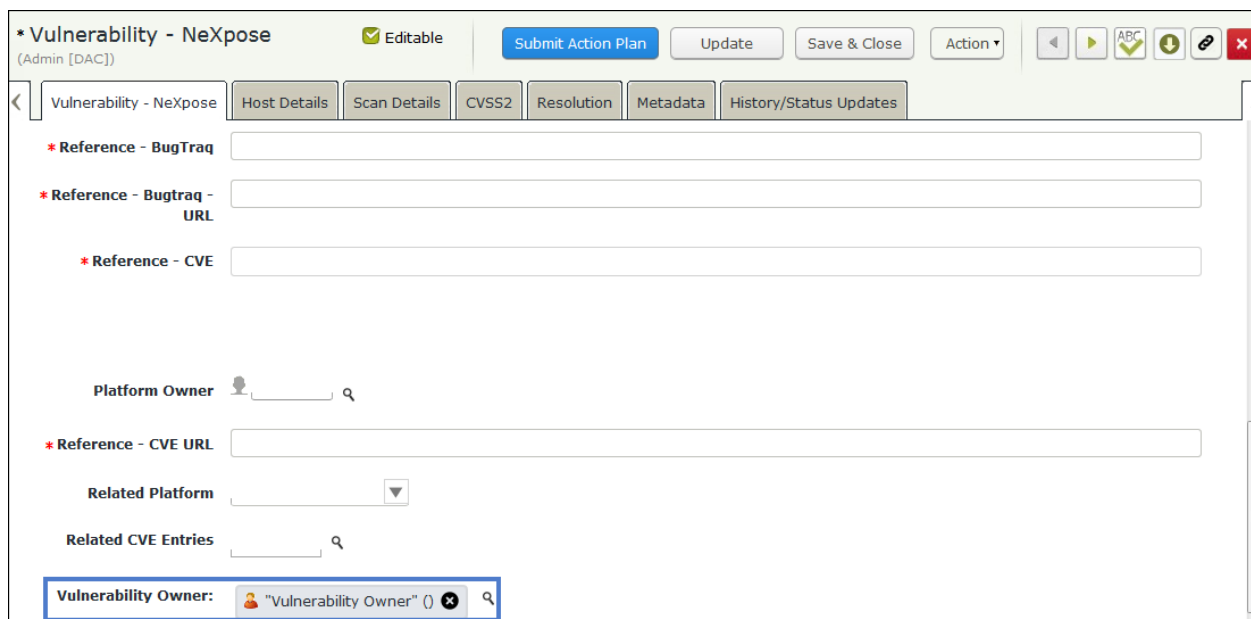
Step 5: Provision Your Users and Groups

Rsam SOAR-VM baseline configuration comes with a number of predefined groups, roles, and test users. Before going live, you'll need to make sure you've created / imported actual user accounts and that you've assigned them to the appropriate groups and roles.

If Rsam is connected to your LDAP / Directory, then Rsam will leverage this directory during the assignment process (no need to create user accounts). However, if you have not connected Rsam to your directory, then you will need to add each individual user by clicking **Manage > Users/Groups** from the top menu.

Roles can be assigned to users in several ways, but the most common ways are via an attribute or via a user group. The SOAR-VM module includes three predefined roles, one of which is assigned by attribute, and two of which are assigned via a group (for more information on these specific roles, refer to the baseline configuration guide).

In order to assign a user a role via an attribute, that user account would need to be selected as the value for that attribute:



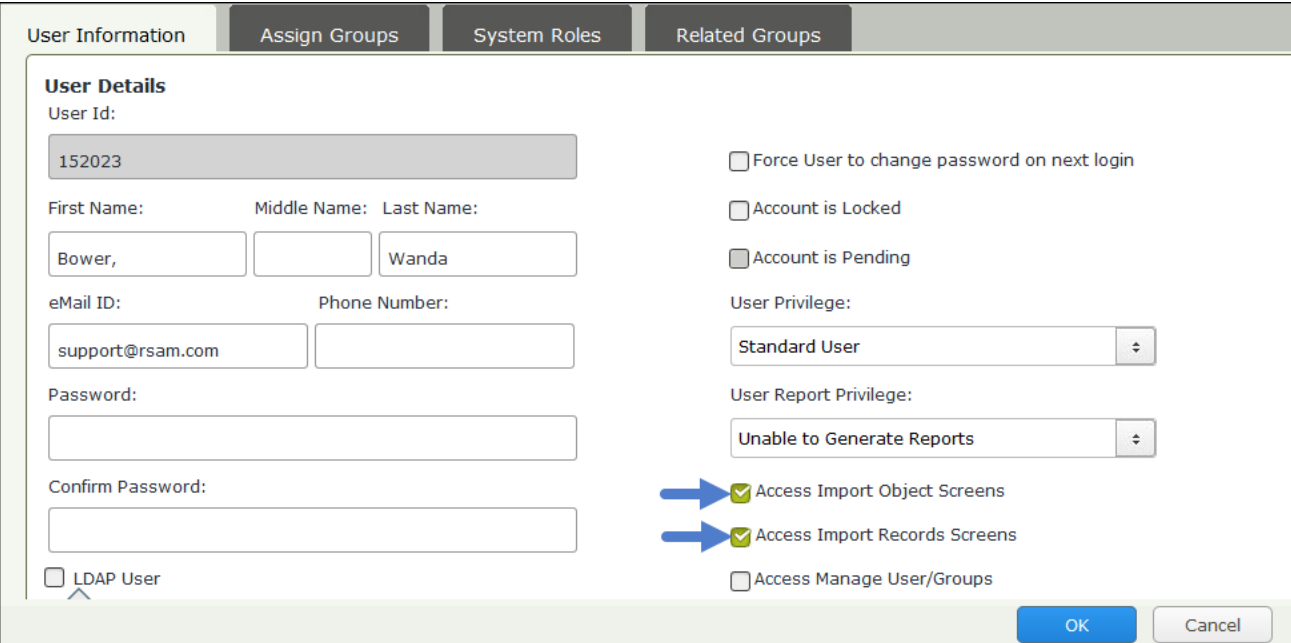
If you plan to import a large number of vulnerabilities prior to go-live, then attribute-level assignments are most easily accomplished across multiple vulnerabilities using the import mapping method described in Step 4: Import Existing V or using Risk Analytics Handlers executed during import. For additional information on creating risk analytics handlers, refer *Rsam Administrator Help*.

For group-based assignments, simply add your users to the appropriate group by navigating to **Manage > Users/Groups** from the main Rsam menu. For more information on managing users and groups, refer *Rsam Administrator Help*.

Step 6: Grant Import Ability for Non-Administrative User Accounts

For any non-administrative user accounts that will require the ability to import objects and/or records into Rsam, a flag must be enabled in the user's account. These users can only import using existing import profiles and maps; they will not be able to update the import maps or create new maps.

To provision this access, open the user account, and select **Access Import Object Screens** and **Access Import Records Screens**.



The screenshot shows the 'User Details' tab in the Rsam user management interface. The user being edited is 'Wanda Bower' with User ID '152023'. The interface includes fields for First Name, Middle Name, Last Name, eMail ID, and Phone Number. On the right side, there are several checkboxes and dropdown menus for user privileges. Two checkboxes, 'Access Import Object Screens' and 'Access Import Records Screens', are checked and highlighted with blue arrows. Other options like 'Force User to change password on next login', 'Account is Locked', 'Account is Pending', and 'Access Manage User/Groups' are unchecked. The 'User Privilege' is set to 'Standard User' and 'User Report Privilege' is set to 'Unable to Generate Reports'. At the bottom, there are 'OK' and 'Cancel' buttons.

Step 7: Remove Sample Data and Users

In order to allow you to execute the step-by-step tutorial with no prior configuration, the SOAR-VM baseline configuration comes with a number of sample users and sample vulnerabilities. Be sure to remove these items before you go live. Vulnerabilities can be deleted from most of the searches and navigators shown in the step-by-step tutorial, and users can be deleted by navigating to **Manage > Users/Groups** from the main Rsam menu.

Step 8: Schedule Events



Certain events, including imports, metrics and risk analytics scheduled events, need to be scheduled to occur on a regular basis. You can use existing schedules or configure your own. For more information on scheduling events, refer *Rsam Administrator Help*.

Step 9: Go Live Quickly and Prepare for the Future

Not only are the SOAR-VM baseline configuration product and implementation methodology invaluable tools for getting a SOAR-VM solution up and running quickly and with minimal effort, but they are also built on the most flexible GRC platform in the market. In order to get the most out of your investment in Rsam, plan on your SOAR-VM implementation being an evolution.

Over time, that evolution will likely include not only continued configuration and enhancement of your SOAR-VM solution, but also the addition and integration of additional Rsam baseline modules, configuration of Rsam “build-your-own” use cases, and building out integrations with other systems in your enterprise. So go live with this module to start getting value out of the tool, but plan to spend more time in the future to take advantage of the great configuration opportunities in Rsam.

Appendix: Rsam Documentation

Inline Help

While this guide provides instructions on the SOAR-VM Module, you should refer to the Rsam Help, Rsam Administrator Help, or both when you want to get familiar with the Rsam features covered in this guide. Please keep in mind that the help you can access depends on your user permissions.

Procedure:

1. Sign in to your Rsam instance. For example, sign in as the **r_admin** user; enter Username as **r_admin** and Password as **password**.
1. Mouse hover over **Help** and select the desired help in the menu that appears. Depending on your user permissions, you will be able to access the Rsam Help, Rsam Administrator Help, or both.

The screenshot below illustrates the Example Administrator user account in which the user has opened the Rsam Administrator Help.

