Rsam SSRS Report Installation Requirements and Administration Guide

Vulnerability Status Summary Report

Document Version: 2017.01 | December 2017

Contents

About this Guide

Each Rsam SSRS report has a unique set of steps for installing the report and ensuring that all the required configurations for the report are met. This guide provides a walk through of all the items to consider when installing the **Vulnerability Status Summary Report** and executing it for the first time.

For general information about integrating SSRS with your Rsam environment, refer the document *RSAM Reporting - SSRS Integration*.

For information on building your own SSRS reports, refer the document *Rsam Platform Step-by-Step Tutorial - Building SSRS Reports*.

Overview

This guide provides details around the installation artifacts and configuration dependencies required to run the Vulnerability Summary Report.

Minimum Rsam Version

The minimum version of Rsam required to execute this report is **9.2.2126.2**.

Required Modules

This report requires that you have licensed and installed the **Vulnerability Management** baseline module.

Required SSRS Artifacts

This section provides information about the required SSRS artifacts for the Vulnerability Status Summary report.

Report-Specific SSRS Artifacts

The following Report Definition Language files must be applied in your Rsam environment.

Report Definition Language (RDL) Files

The following Report Definition Language files must be applied in your Rsam environment.

If your Rsam instance is on premise, then add the RDL files to your report server using SSRS Report Manager.

If your Rsam instance is in the Rsam Cloud, then contact support to have the RDL files added to your environment.

RDL File Name	Description
VulnerabilitySummaryReport.rdl	This is the primary RDL file for the Vulnerability Status Summary Report.
VulnerabilityStatusDetail.rdl	This is the RDL File for the drill through Report.
Trend of Average Days Open_Subreport.rdl	This is the RDL file for a sub report.

Configuration Dependencies

Before executing the report, you must ensure that your Rsam environment includes all the configuration elements on which the report depends. This section details the searches, record types, attribute types, and other elements that must be available in the environment before executing the report. New Rsam customers will have these items included in the databases by default, but existing customers who want to add SSRS reports to their existing Rsam environments may need to obtain these items from Rsam in the form of environment migration files.

Attribute Types

The attribute types listed in the following table must be present in your Rsam environment for the report to execute successfully. They are available in optional environment migration script called **Vulnerability Summary Report – Attributes.**

Note: If you are an existing Rsam customer, applying these attribute types to your environment through an environment migration script may overwrite configuration changes that you have made to those attribute types.

Attribute Type Admin Name	Rsam ID
U: Open / Closed	RSAM01-00000861-033032A0D51F4743A243FBA49B4B70C2
U: Universal Severity / Risk	RSAM-00209
VM: Exploitable	RSAM-00628
VM: Port	RSAM-00224
VM: Protocol	RSAM-00225
VM: Vulnerability ID	RSAM-00200
VM: Vulnerability Name	RSAM-00201
MG: Metric Result AVG	RSAM-MT012
MG: Metric Result MAX	RSAM-MT014
MG: Metric Result MIN	RSAM-MT013
MG: Metric Result SUM	RSAM-MT011
U: Date of Entry	RSAM-00126

Attribute Type Admin Name	Rsam ID
VM: Host IP Address	RSAM-00217
VM: Host Name - DNS	RSAM-00219
VM: Host Name - NetBIOS	RSAM-00220
VM: Host OS	RSAM-00222
VM: Host Zone	RSAM01-00000826-7F21288CAE634718A998AA1579E1869D

Searches

A set of searches must be present in your Rsam environment for the report to execute successfully. These searches have been created specifically for use with the SSRS report (note the naming convention). These searches should not be modified for use within other parts of Rsam (navigators, charts, etc.). If you want to use these searches throughout other areas of Rsam, it is recommended that you create copies of these searches and modify the searches for the required purposes.

The following table lists the searches that must be present in your Rsam environment for the Vulnerability Status Summary Report to execute successfully. To add these searches to your environment, import the environment migration script, **Vulnerability Summary Report - Searches**.

Search Name	Rsam ID
VM: SSRS: Open Vulnerabilities (Host-based)	RSAM01-00002128-91B67549255440C6BFF59A87A1D17F0F
VM: SSRS: Vulnerabilities: All Active Assets	RSAM01-00002154-B1664A2C58994D7EB80DE5483E51EFC1
VM: SSRS: Average Days Open by Severity	RSAMR3-00003531-D96880CC7B464A26AD0FDD0D47C6B775

Object Types

The object type listed in the following table is included as part of the Vulnerability Management baseline module in Rsam and for most customers, this serves as the object type presented in the Vulnerability Status Summary report.

Object Type Admin Name	Rsam ID
IT Host	RSAM01-00000279-5E307965AE0A489F89C63BA7F911F6CF

Record Types and Record Category Types

The record types and record category types mentioned in the following tables are included as part of the Vulnerability Management module in Rsam and for most customers. These serve as the record types that are presented in the Vulnerability Status Summary Report.

If you have created vulnerability record types, those will be included in the report if the following criteria are met:

- You have included your custom record category types in the SSRS-specific searches
- You have associated your record types with the required attribute types

Note: If you are an existing Rsam customer, applying these record types to your environment through an environment migration script may overwrite configuration changes that you have made to those record types.

The following table lists the Record Types for the Vulnerability Status Summary report.

Record Type Admin Name	Rsam ID
VM: Metrics - Days Open by Severity	RSAMR3-00000621-8B82043ED95D404BB0992CD2B72DD672
VM: Vulnerability - Qualys VM	RSAM-00204
VM: Vulnerability - Qualys PCM	RSAM-00234
VM: Vulnerability - Qualys VM Summary	RSAM-00243
VM: Vulnerability - Qualys Tickets	RSAM-00245
VM: Vulnerability - McAfee Vulnerability Manager	RSAM-00205
VM: Vulnerability - NetIQ	RSAM01-00000056-334CC51F8A8E437DBC0D9CD25269606A

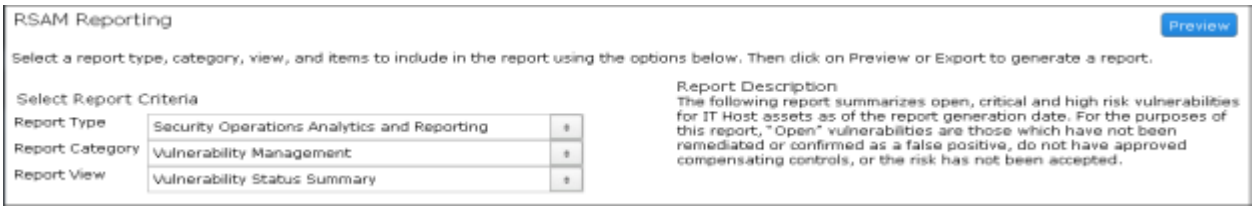
Record Type Admin Name	Rsam ID
VM: Vulnerability - Trustwave	RSAM-00216
VM: Vulnerability - NeXpose	RSAM-00223
VM: Vulnerability - Tenable Security Center	RSAM-00244
VM: Vulnerability - Nessus	RSAM-00203
VM: Vulnerability - Burp Suite	RSAMR3-00000463-A1D133B089794D98A2B639A8F0B77EE6
VM: Vulnerability - ISS	RSAM-00202

The following table lists the Record Category Types for the Vulnerability Status Summary report.

Record Category Type Admin Name	Rsam ID
VM: VM - Nessus	RSAM-00201
VM: VM - ISS	RSAM-00202
VM: VM - NetIQ	RSAM01-00000038-158D146648D04F38BA6ACB4CEDDF4718
VM: VM - Qualys VM	RSAM-00205
VM: VM - McAfee Vulnerability Manager	RSAM-00209
VM: VM - Qualys VM Summary	RSAM-00230
VM: VM - Qualys PCM	RSAM-00226
VM: VM - Qualys Tickets	RSAM-00233
VM: VM - TrustWave	RSAM-00207
VM: VM - NeXpose	RSAM-00220
VM: VM - Tenable Security Center	RSAM-00232
VM: VM - Burp Suite	RSAMR3-00000413-0CF732D31DB04AD789A92B38F22B2EC7

Report

To access the report from the **Report** menu in Rsam, you must apply the report record through the provided migration script - **Vulnerability Summary Report – Report**.



The following table lists the name and ID of the report.

Record Name	Rsam ID
Vulnerability Status Summary Report	RSAMA6-00000238-D79E8020D0994BA9B707BA64043A8B55
Security Operations Analytics and Reporting (Report Type)	RSAMA6-00000236-2560462764F949BFBA6371E575CB0E84
Vulnerability Management (Report Category)	RSAMA6-00000237-A72788F740054F4FA6366DC5522692F4

Home Pages

In addition to the **Report** menu, the Vulnerability Status Summary Report can be accessed also by adding a link to view the report, to any home page. If you want to include a link in your environment, add it to any home page by placing a **Report List widget type** on that home page tab.

The following image shows an example home page tab with a Report List widget type, which includes a link to open the Vulnerability Status Summary report.