

# Release Notes

---

HP Reputation Security Monitor 1.01

ArcSight ESM and ArcSight Express

March 6, 2013



Copyright © 2013 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Follow this link to see a complete statement of copyrights and acknowledgements:

<http://www.hpenterprisesecurity.com/copyright>

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

This document is confidential.

## Contact Information

---

<b>Phone</b>	A list of phone numbers is available on the HP ArcSight Technical Support page: <a href="http://www8.hp.com/us/en/software-solutions/software.html?compURI=1345981#.URitMaVwpWI">http://www8.hp.com/us/en/software-solutions/software.html?compURI=1345981#.URitMaVwpWI</a> .
<b>Support Web Site</b>	<a href="http://support.openview.hp.com">http://support.openview.hp.com</a>
<b>Protect 724 Community</b>	<a href="https://protect724.arcsight.com">https://protect724.arcsight.com</a>

---

## Revision History

---

<b>Date</b>	<b>Product Version</b>	<b>Description</b>
3/6/2013	Reputation Security Monitor Solution 1.01	Final revision for release.

---

# Contents

---

- Reputation Security Monitor 1.01 ..... 5**
- How RepSM Works ..... 5
- Requirements ..... 6
- Release Contents ..... 6
- What's New in RepSM 1.01 ..... 7
- Installing RepSM ..... 7
- Performance Impact of RepSM ..... 7
- Open Issue in this Release ..... 8

---

# Reputation Security Monitor 1.01

---

These release notes discuss the following topics.

- ["How RepSM Works" on page 5](#)
- ["Requirements" on page 6](#)
- ["Release Contents" on page 6](#)
- ["What's New in RepSM 1.01" on page 7](#)
- ["Installing RepSM" on page 7](#)
- ["Performance Impact of RepSM" on page 7](#)
- ["Open Issue in this Release" on page 8](#)

## How RepSM Works

The HP Reputation Security Monitor (RepSM) solution uses internet threat intelligence to detect malware infection, zero day attacks, and dangerous browsing on your network. RepSM consists of the following components:

- The **HP RepSM service**, powered by HP TippingPoint Reputation Digital Vaccine (RepDV), provides reputation data from the comprehensive RepDV database of malicious IP addresses, host names, and domain names. RepDV uses IPv4 and Domain Name System (DNS) security intelligence feeds from multiple sources to provide a broad set of reputation data.
- The **HP Model Import Connector for RepSM** imports the reputation data at regular intervals from the RepSM service to ArcSight ESM or ArcSight Express.
- The **HP RepSM content** running on ArcSight ESM or ArcSight Express, correlates the reputation data and security events to detect and remediate security incidents and issues that would otherwise be undetectable. RepSM content is organized into several use cases, which address specific objectives.

For a complete overview of RepSM, see the *Reputation Security Monitor 1.01 Solution Guide*.

---

## Requirements

RepSM requires the Model Import Connector for RepSM, with an active subscription to the RepSM service.

RepSM 1.01 is supported on:

- ArcSight Express 4.0 with CORR-Engine, or later.  
A trial version of RepSM is available on ArcSight Express 4.0. You will need to contact your HP ArcSight sales representative for an evaluation license. You can use the on-board version of RepSM, or ask your sales representative if there is a newer version available for evaluation. After you get the license, install the solution first, and then the Model Import Connector for RepSM.
- ArcSight ESM 5.2 or later. The following configuration is required:
  - ◆ The ArcSight ESM active lists capacity must be set to 1,000,000 to enable the installation of the RepSM content package (the default capacity is 500,000).
  - ◆ The ArcSight Manager Java heap memory size must be set to at least 4 GB to support RepSM.

For more information about these requirements, see the *Reputation Security Monitor 1.01 Solution Guide*.

For additional connector requirements, see the documentation for the Model Import Connector for RepSM.

## Release Contents

The following files are included in this release.

---

File name	Description
<b>RepSM Solution</b>	
<a href="#">ArcSight-SolutionPackage-ReputationSecurityMonitor.1.0.0.1203.0.arb</a>	For ArcSight ESM, the installation package bundle for all operating systems. Contains all the resources for the RepSM content package. (For ArcSight Express, this package is available on the appliance.)  <b>Note:</b> Internet Explorer sometimes converts the ARB file to a ZIP file during download. If this occurs, rename the ZIP file back to an ARB file before importing into ArcSight ESM.
<a href="#">ESM_RepSM_Solution_RelNotes_1.01.pdf</a>	The <i>Reputation Security Monitor 1.01 Release Notes</i> (this document) provide release contents, and include a list of open issues with workarounds where available.
<a href="#">ESM_RepSM_SolutionGuide_1.01.pdf</a>	The <i>Reputation Security Monitor 1.01 Solution Guide</i> provides product architecture, installation, configuration, and operation instructions with a description of product contents.

---

File name	Description
<b>Model Import Connector for RepSM</b>	
<a href="#">ArcSight-5.2.7.6581.0-RepSMModelConnector-Linux64.bin</a>	The installation executables for the Model Import Connector for RepSM.
<a href="#">ArcSight-5.2.7.6581.0-RepSMModelConnector-Win64.exe</a>	<b>Note:</b> For the location of the Model Import Connector for RepSM in ArcSight Express, see "Post Configuration Steps" in the "Configuring ArcSight Express Appliance" section of the ArcSight Express Configuration Guide.
<a href="#">RepSMModelImportConn_RelNotes_5.2.7.6581.0.pdf</a>	The <i>Model Import Connector for RepSM Release Notes</i> provide a product description and open issues.
<a href="#">RepSMModelImportConn_ConfigGuide_5.2.7.6581.0.pdf</a>	The <i>Model Import Connector for RepSM Configuration Guide</i> provides information about installing and configuring the Model Import Connector for RepSM.

## What's New in RepSM 1.01

The RepSM solution content has not been updated for this release.

The Model Import Connector for RepSM now supports pure 64-bit operating systems, making it compatible with ArcSight Express 4.0, and simplified configuration.

The *Reputation Security Monitor 1.01 Solution Guide* now includes a troubleshooting appendix and information on getting email notifications about RepSM service outages.

## Installing RepSM

For installation and configuration instructions for the RepSM solution, see the *Reputation Security Monitor 1.01 Solution Guide*.

## Performance Impact of RepSM

ArcSight solution packages contain data monitors, trends, and rules that can place an additional load on the ArcSight Manager and impact performance. If your ArcSight system is operating at an average event per second (EPS) rate that has maximized the CPU utilization, you might experience a reduced average EPS rate after installing the RepSM package. If this performance impact occurs, you can disable unneeded data monitors, trends, and rules to reduce the load on the ArcSight Manager.

---

## Open Issue in this Release

This release contains the following open issue.

---

Number	Description
CON-12419	<p>When restarting the Model Import Connector for RepSM after it has been inactive for an extended time, for example, more than a month, the connector retrieves all of the available reputation data deltas at once, instead of retrieving a full update or only the appropriate deltas.</p> <p><b>Workaround:</b> Restart the connector and perform a full import of the reputation data, as described in the <i>Model Import Connector for RepSM Configuration Guide</i>.</p>

---