

# Release Notes

---

Microsoft Windows Monitoring 1.0

for ArcSight™ ESM and  
ArcSight Express™ with CORR-Engine

June 28, 2012



## Release Notes - Microsoft Windows Monitoring 1.0

Copyright © 2012 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.arcsight.com/copyrightnotice>

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

This document is confidential.

## Revision History

---

Date	Product Version	Description
06/28/2012	Microsoft Windows Monitoring 1.0	Release of Microsoft Windows Monitoring 1.0.

---

Release Notes template version: 1.0.5

## Contact Information

---

<b>Phone</b>	1-866-535-3285 (North America) +44 (0)870 141 7487 (EMEA)
<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>

---

# Contents

---

- Microsoft Windows Monitoring 1.0 ..... 5**
- Minimum Requirements ..... 5
- Release Contents ..... 6
- Installing Microsoft Windows Monitoring 1.0 ..... 6
- Open Issues in this Release ..... 6



# Microsoft Windows Monitoring 1.0

---

Microsoft Windows Monitoring is a content package that provides additional support for monitoring network activity specific to Microsoft Windows operating systems. The package eliminates the need to modify parsers, categorizations, and existing content to accommodate changes to the Microsoft Windows platform.

The Microsoft Windows Monitoring content is designed for events supported in the Microsoft Windows Event Log – Unified SmartConnector parser version 1.

[“Minimum Requirements” on page 5](#)

[“Release Contents” on page 6](#)

[“Installing Microsoft Windows Monitoring 1.0” on page 6](#)

[“Open Issues in this Release” on page 6](#)

## Minimum Requirements

The Microsoft Windows Monitoring content requires the following products and later versions of these products:

- ArcSight™ ESM 5.0 Patch 1 or ArcSight Express 3.0 with CORR-Engine
- Microsoft Windows Event Log – Unified SmartConnector version 5.2.4.6326 with parser version 1.



**Note**

Microsoft Windows Monitoring on ESM supports events that are forwarded from Logger 5.2 Patch 1 and later.

---

---

## Release Contents

The following files are included in this release.

File name	Description
<a href="#">HP-ArcSight-StandardContent-WindowsMonitoring.1.0.0.&lt;0628&gt;.0.arb</a>	Installable package bundle for all operating systems. Contains all the resources for Microsoft Windows Monitoring.
<a href="#">ESM_Windows_Content_ReleaseNotes_1.0.pdf</a>	Product description and open issues (this document).
<a href="#">ESM_SCG_Windows_1.0.pdf</a>	The <i>Microsoft Windows Monitoring 1.0 Standard Content Guide</i> provides product architecture, installation, configuration, and operation instructions with a description of product contents.
<a href="#">MSWindowsEventLogUnifiedMappingsParserVersion1.pdf</a>	The <i>Security Event Mappings, SmartConnector for Microsoft Windows Event Log - Unified with Parser Version 1</i> document provides security event mappings for the Microsoft Windows Event Log - Unified SmartConnector.

## Installing Microsoft Windows Monitoring 1.0

Complete installation and configuration instructions for the Microsoft Windows Monitoring content are located in the *Microsoft Windows Monitoring 1.0 Standard Content Guide* ([ESM\\_SCG\\_Windows\\_1.0.pdf](#)).

## Open Issues in this Release

This release contains the following open issue.

Number	Description
CONT-358	Content related to changes in Windows services might not work on localized systems. This content is part of the System Services and Auditing use case.