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

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

Phone	1-866-535-3285 (North America) +44 (0)870 141 7487 (EMEA)
Support Web Site	http://support.openview.hp.com
Protect 724 Community	https://protect724.arcsight.com

Contents

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

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.

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
HP-ArcSight-StandardContent-WindowsMonitoring.1.0.0.<0628>.0.arb	Installable package bundle for all operating systems. Contains all the resources for Microsoft Windows Monitoring.
ESM_Windows_Content_ReleaseNotes_1.0.pdf	Product description and open issues (this document).
ESM_SCG_Windows_1.0.pdf	The *Microsoft Windows Monitoring 1.0 Standard Content Guide* provides product architecture, installation, configuration, and operation instructions with a description of product contents.
MSWindowsEventLogUnifiedMappingsParserVersion1.pdf	The *Security Event Mappings, SmartConnector for Microsoft Windows Event Log - Unified with Parser Version 1* 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.