Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for Microsoft Windows Event Log – Native: Microsoft Forefront Protection 2010

Supplemental Configuration Guide

August 30, 2016

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise 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. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

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

HPE Security ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise 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.

Copyright Notice

Revision History

Date	Description
08/30/2016	Updated versions supported.
02/16/2015	First edition of this configuration guide, for initial support of Microsoft Forefront Protection.

Support

Contact Information

Phone	A list of phone numbers is available on the HPE Security ArcSight Technical Support Page: https://softwaresupport.hp.com/documents/10180/14684/esp-support-contact-list
Support Web Site	https://softwaresupport.hp.com
Protect 724 Community	https://www.protect724.hpe.com

Contents

SmartConnector for Microsoft Windows Event Log – Native: Microsoft Forefront Protection 2010

This guide provides information about the SmartConnector for Microsoft Windows Event Log – Native: Microsoft Forefront Protection and its event mappings to ArcSight data fields. This connector supports Microsoft Forefront Protection 2010 events for Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012 Standard with Exchange 2010.

The *ArcSight SmartConnector 2008/2012 Mappings to Windows Security Events* document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this document are specifically for the SmartConnector for Windows Event Log – Native: Microsoft Forefront Protection.

Product Overview

Microsoft Forefront Protection 2010 for Exchange Server (FPE) provides protection against malware and spam by including multiple scanning engines in a single solution. FPE provides customers with an administration console that includes customizable configuration settings, filtering options, monitoring features and reports, anti-spam protection, and integration with the Forefront Online Protection for Exchange (FOPE) product.

Forefront Protection Configuration

To enable writing events to the Windows Event Log from Forefront Protection:

1. In the Forefront Protection 2010 for Exchange Server Administrator Console, click **Policy Management**, and under **Global Settings**, click **Advanced Options**.
2. In the **Global Settings - Advanced Options** pane, under the **Logging Options** section, select the **Enable event logging** check box. When checked (the default), you can use the associated check boxes to individually enable or disable the following options (which are enabled by default):
   - **Incidents**—Enables or disables event logging for incidents.
   - **Engines**—Enables or disables event logging for engines.
   - **Operational**—Enables or disables logging for all other events, such as system information and health events.

   When the **Enable event logging** check box is cleared, incidents logging is suspended for incidents, engines, and operational events.
3. Click **Save**.

Note: The relevant Microsoft Exchange and Microsoft Forefront Server protection services must be restarted in order for any changes to these settings to take effect. This typically includes the Microsoft Exchange Transport, Microsoft Exchange Information Store, and Microsoft Forefront Server Protection Controller services.

See **Microsoft TechNet → Microsoft Forefront TechCenter Library → Forefront Protection 2010 for Exchange Server → Operations → Configuring logging options** for more information.

Connector Installation and Configuration

Follow the installation and configuration procedures in the *SmartConnector Configuration Guide for Microsoft Windows Event Log – Native*, selecting **Microsoft Windows Event Log – Native** as the connector to be configured.

Collect Events from the Event Log

To set up the connector to collect application events:

1. From $ARCSIGHT_HOME\current\bin, double-click **runagentsetup.bat**.
2. Select **Modify Connector** on the window displayed and click **Next**.
3. Select **Modify connector parameters** and click **Next**.
4. Select Navigate to the **Modify table parameters** window.
5. To collect events from an application log, modify the **Application** field by selecting **true** for event collection in the Application field and enter **Forefront Protection** in the **Custom Log Names** field.
   You can specify multiple Custom Log Names in a comma-separated format; for example:
   ```
   Directory Service, Forefront Protection
   ```
6. Click **Next** to update the parameters; when you receive the successful update message, click **Next**.
7. Select **Exit** and click **Next** to exit the configuration wizard.
8. Restart the connector for your changes to take effect.

For more information about application event support, see the *SmartConnector Configuration Guide for Microsoft Windows Event Log – Native*.

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See *ArcSight 101* for more information about the ArcSight data fields.

Windows 2008

General

ArcSight ESM Field	Device-Specific Field
Device Product	'Forefront Protection'
Device Vendor	'Microsoft'

Event ID 7000

ArcSight ESM Field	Device-Specific Field
Message	'All the antimalware engines selected in the Forefront Administration Console for scanning have been enabled for updates.'
Name	‘All the antimalware engines selected in the Forefront Administration Console’

Event ID 7001

ArcSight ESM Field	Device-Specific Field
Message	'Not all the antimalware engines selected in the Forefront Administration Console for scanning have been enabled for updates.'
Name	‘Not all the antimalware engines selected in the Forefront Administration Console’

Event ID 7002

ArcSight ESM Field	Device-Specific Field
Name	'All the antimalware engines enabled for updates have been updated successfully at the last attempt'

Event ID 7003

ArcSight ESM Field	Device-Specific Field
Name	'Not all of the antimalware engines enabled for updates have successfully updated at the last attempt’

Event ID 7004

ArcSight ESM Field	Device-Specific Field
Name	'Less than half of the antimalware engines enabled for updates have updated successfully at the last attempt.'

Event ID 7005

ArcSight ESM Field	Device-Specific Field
Name	‘All the antimalware engines enabled for updates have updated successfully in the last five days’

Event ID 7006

ArcSight ESM Field	Device-Specific Field
Name	‘At least one of the antimalware engines enabled for updates has not been updated in the last five days.’

Event ID 7007

ArcSight ESM Field	Device-Specific Field
Name	'None of the antimalware engines enabled for updates have been updated in the last five days.'

Event ID 7008

ArcSight ESM Field	Device-Specific Field
Name	'The antimalware engines selected for transport scanning have been initialized.'

Event ID 7010

ArcSight ESM Field	Device-Specific Field
Name	The antimalware engines selected for realtime scanning have been initialized.'

Event ID 7012

ArcSight ESM Field	Device-Specific Field
Name	'The transport scan job is enabled’

Event ID 7015

ArcSight ESM Field	Device-Specific Field
Name	'The realtime scan job is enabled.'

Event ID 7018

ArcSight ESM Field	Device-Specific Field
Name	'The realtime scanning processes are running normally with no issues.'

Event ID 7021

ArcSight ESM Field	Device-Specific Field
Name	'The transport scanning processes are running normally with no issues.'

Event ID 7024

ArcSight ESM Field	Device-Specific Field
Name	'The MS Exchange Transport Service is running and the Forefront Agent is registered.'
Destination Service Name	'MS Exchange Transport Service'

Event ID 7025

ArcSight ESM Field	Device-Specific Field
Name	'The MS Exchange Transport Service is running but the Forefront Agent is not registered'
Destination Service Name	'MS Exchange Transport Service'

Event ID 7026

ArcSight ESM Field	Device-Specific Field
Name	'The MS Information Store is running and the Forefront VSAPI Library is registered.'

Event ID 7028

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection Product is within the license period.'

Event ID 7033

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection Product is within the license period'

Event ID 7035

ArcSight ESM Field	Device-Specific Field
Name	'There is at least amount of disk space available.'

Event ID 7040

ArcSight ESM Field	Device-Specific Field
Name	'The Eventing Service (FSCEventing) is functioning.'
Destination Service Name	'FSC Eventing'

Event ID 7044

ArcSight ESM Field	Device-Specific Field
Name	'The Mail Pickup Service (FSEMailPickup) is functioning.'
Destination Service Name	'FSEMailPickup'

Event ID 7046

ArcSight ESM Field	Device-Specific Field
Name	'Content Filter is enabled and definitions have been updated in the last one hour'

Event ID 7048

ArcSight ESM Field	Device-Specific Field
Name	'Content Filter is enabled and the last definition update was over 12 hours ago.'

Event ID 7051

ArcSight ESM Field	Device-Specific Field
Name	'The Monitor Service (FSCMonitor) is functioning.'
Destination Service Name	'FSCMonitor'

Event ID 7064

ArcSight ESM Field	Device-Specific Field
Name	'No archived undeliverable items exist'

FSC Controller

Event ID 1000

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection service is running.'
Destination Service Name	'Forefront Protection'

Event ID 1001

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection service has stopped.'
Destination Service Name	'Forefront Protection'

Event ID 1020

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection service is starting.'
Destination Service Name	'Forefront Protection'

Event ID 1021

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection service is stopping.'
Destination Service Name	'Forefront Protection'

Event ID 1022

ArcSight ESM Field	Device-Specific Field
Name	'Forefront Protection Version'
Device Version	%1 (version)
Additional data	%2 (Virus Protection Feature)

Event ID 1023

ArcSight ESM Field	Device-Specific Field
Name	'Forefront Protection Service Pack'
Additional data	%1 (ServicePack)
Message	Both ('Forefront Protection Service Pack:',%1)

Event ID 1024

ArcSight ESM Field	Device-Specific Field
Name	'Product ID'
Additional data	%1 (ProductID)
Message	Both ('Product ID:', %1)

Event ID 1025

ArcSight ESM Field	Device-Specific Field
Name	'Licensed Components'
Message	All of (Licensed Components: Component, License Type, Expiration Date)

Event ID 1026

ArcSight ESM Field	Device-Specific Field
Name	'Licensed Engines'
Additional data	%1 (LicensedEngines)
Message	Both ('Licensed Engines:', %1)

Event ID 1028

ArcSight ESM Field	Device-Specific Field
Name	'System Information'
Additional data	%1 (System Information)
Message	Both ('System Information:', %1)

Event ID 1037

ArcSight ESM Field	Device-Specific Field
Name	'Event Tracing session has been started.'
Device Severity	'Information'

Event ID 1041

ArcSight ESM Field	Device-Specific Field
Name	'Scheduled Scan has been started'

Event ID 1043

ArcSight ESM Field	Device-Specific Field
Name	'Scheduled Scan has stopped'

Event ID 1044

ArcSight ESM Field	Device-Specific Field
Name	'Scheduled Scan has completed'

Event ID 2102

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection application is still within the license period'

Event ID 5167

ArcSight ESM Field	Device-Specific Field
Name	'Microsoft Forefront Protection Monitor detected abnormal process shutdown'
Source Process Name	%1 (process name)
Message	Both ('Microsoft Forefront Protection Monitor detected abnormal' %1,' shutdown')

Event ID 5183

ArcSight ESM Field	Device-Specific Field
Name	'Scheduled scan exceeded the allowed scan time limit'

Event ID 8046

ArcSight ESM Field	Device-Specific Field
Name	'AD Mark Created'

Event ID 8055

ArcSight ESM Field	Device-Specific Field
Name	'Ad Mark Removed'
Message	'Failed to Delete Reg Key'

FSC Eventing

Event ID 1075

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection Eventing Service has started.'
Destination Service Name	'Forefront Protection Eventing'

Event ID 1076

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection Eventing Service has stopped.'
Destination Service Name	'Forefront Protection Eventing'

FSC Manual Scanner

Event ID 1045

ArcSight ESM Field	Device-Specific Field
Name	'On-Demand Scan started.'
Request Client Operation	%1 (Request Client Operation)

Event ID 1048

ArcSight ESM Field	Device-Specific Field
Name	'On-Demand Scan stopped.'
Request Client Operation	%1 (Request Client Operation)

Event ID 1052

ArcSight ESM Field	Device-Specific Field
Name	'On-Demand Scan has been completed.'
Request Client Operation	%1 (Request Client Operation)

FSC Scheduled Scanner

Event ID 2080

ArcSight ESM Field	Device-Specific Field
Name	'Scheduled scan enabled.'

Event ID 2081

ArcSight ESM Field	Device-Specific Field
Name	'Scheduled scan disabled.'

Event ID 3009

ArcSight ESM Field	Device-Specific Field
Name	'Scheduled scan found virus.'
Device Custom String 4	mailbox name
Message	%2 (Message)
Device Custom String 1	virus name
Device Custom String 6	incident
Additional data	%4 (scan engine)
Device Action	%5 (Device Action)
File Name	%3 (File Name)

FSC Realtime Scanner

Event ID 2000

ArcSight ESM Field	Device-Specific Field
Name	'Realtime scan enabled.'

Event ID 2001

ArcSight ESM Field	Device-Specific Field
Name	'Realtime scan disabled.'

FSC Transport Scanner

Event ID 2007

ArcSight ESM Field	Device-Specific Field
Name	'Transport scan enabled.'

Event ID 2008

ArcSight ESM Field	Device-Specific Field
Name	'Transport scan disabled.'

Event ID 3002

ArcSight ESM Field	Device-Specific Field
Name	'Internet scan found virus'
File Path	%1 (folder)
Message	%2 (Message)
File Name	%4 (file name)
Device Custom String 6	Incident
Device Action	%6 (Device Action or State)
Device Custom String 1	virus name
Additional data	%3 (message ID)
Additional data	%5 (scan engine)

FSC Monitor

Event ID 1007

ArcSight ESM Field	Device-Specific Field
Name	'Forefront Protection Monitor detected Information Store process started.'
Destination Process Name	'Information Store'

Event ID 1008

ArcSight ESM Field	Device-Specific Field
Name	'Forefront Protection Monitor detected Information Store shutdown.'
Destination Process Name	'Information Store'

Event ID 1013

ArcSight ESM Field	Device-Specific Field
Name	'Forefront Protection Monitor is active.'

Event ID 1014

ArcSight ESM Field	Device-Specific Field
Name	'Forefront Protection Monitor is inactive.'

FSE On Demand Nav

Event ID 1049

ArcSight ESM Field	Device-Specific Field
Name	'The FseOnDemandNav service is running.'
Destination Process Name	'FseOnDemandNav'

Event ID 1050

ArcSight ESM Field	Device-Specific Field
Name	'The FseOnDemandNav service has stopped.'
Destination Process Name	'FseOnDemandNav'

FSE Mail Pickup

Event ID 1029

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection Mail Pickup service is running.'
Destination Service Name	'Forefront Protection Mail Pickup'

Event ID 1030

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection Mail Pickup service has stopped.'
Destination Service Name	'Forefront Protection Mail Pickup'

FSE IMC

Event ID 1002

ArcSight ESM Field	Device-Specific Field
Name	'FSEIMC service started.'
Destination Service Name	'FSEIMC'

Event ID 1003

ArcSight ESM Field	Device-Specific Field
Name	'FSEIMC sertice stopped.'
Destination Service Name	'FSEIMC'

FSE VS API

Event ID 5066

ArcSight ESM Field	Device-Specific Field
Name	'Realtime scan exceeded the allowed scan time limit'

FSC VSS Writer

Event ID 1094

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection VSS Writer Service has started.'
Destination Service Name	'Forefront Protection VSS Writer Service'

Event ID 1095

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection VSS Writer Service has stopped.'
Destination Service Name	'Forefront Protection VSS Writer Service'

Get Engine Files

Event ID 2011

ArcSight ESM Field	Device-Specific Field
Name	‘Microsoft Forefront Protection did not detect any new scan engine updates’
Additional data	%1 (scan engine)
Request URL	%2 (request URL)

Event ID 2012

ArcSight ESM Field	Device-Specific Field
Name	'Microsoft Forefront Protection performed a successful scan engine update’
Additional data	%1 (scan engine)
Request URL	%2 (request URL)

Event ID 2017

ArcSight ESM Field	Device-Specific Field
Name	‘Forefront Protection has rolled back a scan engine’
Additional data	%1 (scan engine)

Event ID 2034

ArcSight ESM Field	Device-Specific Field
Name	'Microsoft Forefront Protection is attempting a scan engine update.'
Request URL	%2 (request url)
Additional data	%1 (scan engine)

Event ID 2109

ArcSight ESM Field	Device-Specific Field
Name	'The VBuster scan engine is no longer supported'
Message	'Updates are no longer available for this engine, and therefore the update check for this engine has been disabled. Please review the scan engine chosen for your scan jobs and make another selection to ensure up-to-date protection'
Additional data	%1 (scan engine)
Request URL	%2 (request URL)

Event ID 6012

ArcSight ESM Field	Device-Specific Field
Name	'Microsoft Forefront Protection encountered an error while performing a scan engine update'
Additional data	%1 (scan engine)
Reason	%2 (Error Code)
Message	%3 (Error Detail)

Event ID 6014

ArcSight ESM Field	Device-Specific Field
Name	'Microsoft Forefront Protection encountered an error while performing a scan engine update.'
Additional data	%1 (scan engine)
Request URL	%2 (request url)
Additional data	%3 (proxy settings)
Reason	%4 (Error Code)
Message	%5 (Error Detail)

Event ID 6019

ArcSight ESM Field	Device-Specific Field
Name	'Microsoft Forefront Protection encountered an error while performing a scan engine update'
Additional data	%1 (scan engine)

ArcSight ESM Field	Device-Specific Field
Message	%2 (Error Detail)

Event ID 6020

ArcSight ESM Field	Device-Specific Field
Name	'Microsoft Forefront Protection encountered an error while performing a scan engine update'
Additional data	%1 (scan engine)
Request URL	%2 (request URL)
Message	%3 (Message)

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Supplemental Configuration Guide (Connectors)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to arc-doc@hpe.com.

We appreciate your feedback!