Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for Windows Event Log – Native: Microsoft Remote Access

Supplemental Configuration Guide

November 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
11/30/2016	Added Windows Server 2016 support.
02/15/2016	Added Windows 10 support.
02/16/2015	First edition of this guide.

Support

Contact Information

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

Contents

SmartConnector for Microsoft Windows Event Log – Native: Remote Access 4
Product Overview 4
Remote Access Configuration 4
Connector Installation and Configuration 5
Mappings for Windows 2016, 2012, 2012 R2, 8, and 10 5
General 5
20088 5
20106 5
20169 6
20184 6
20249 6
20252 6
20255 7
20258 7
20266 8
20271 8
20272 9
20274 9
20275 10
Mappings for Windows 2008 R2 10
General 10
Event 20088 10
Event 20106 11
Event 20184 11
Event 20249 11
Event 20252 11
Event 20255 12
Event 20258 12
Event 20266 12
Event 20271 13
Event 20272 13
Event 20274 14
Event 20275 14

Send Documentation Feedback 15

SmartConnector for Microsoft Windows Event Log – Native: Remote Access

This guide provides information about the SmartConnector for Microsoft Windows Event Log – Native: Remote Access Service and its event mappings to ArcSight data fields.

Supported Versions:

- Microsoft Windows 8
- Microsoft Windows 10
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016

The *SmartConnector for Microsoft Windows Event Log – Windows Security Event Mappings* document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this document are specifically for Microsoft Remote Access.

Product Overview

Routing and Remote Access is a network service in Windows Server 2012, Windows Server 2012 R2, Windows Server 2008, and Windows Server 2016 that provides the following services:

- Dial-up remote access server
- Virtual private network (VPN) remote access server
- Internet Protocol (IP) router for connecting subnets of a private network
- Network address translator (NAT) for connecting a private network to the Internet
- Dial-up and VPN site-to-site demand-dial router

Remote Access Configuration

For complete information about Microsoft's Reporting and Remote Access Service, see Microsoft's TechNet Library for Windows Server, "Remote Access (DirectAccess, Routing and Remote Access)":

http://technet.microsoft.com/en-us/library/hh831416

When configuring the Remote Access Log, specify **system** as the event log type for Microsoft Remote Access.

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. During installation, select **true** for the **System Logs** field for system events to be collected.

Mappings for Windows 2016, 2012, 2012 R2, 8, and 10

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Microsoft Windows'

20088

ArcSight Field	Vendor Field
Name	'Remote Access Server acquired IP Address'
Message	Both ('The Remote Access Server acquired IP Address ',%1,' to be used on the Server Adapter.')
Destination Address	%1 (Assigned Address)

20106

ArcSight Field	Vendor Field
Name	'Unable to add interface'
Message	One of ('Unable to add the interface ',%1,' with the Router Manager for the ',%2,' protocol. The following error occurred: ',%3), ('Unable to add the interface ',%2,' with the Router Mnager for the ',%3,' protocol. The following error occurred: ',%4))
Device Outbound Interface	One of (%1, %2)
Application Protocol	One of (%2, %3)
Device Custom String 5	Routing Domain ID

20169

ArcSight Field	Vendor Field
Name	'Unable to contact a DHCP server'
Message	Both ('The Automatic Private IP Address ',%1,' will be assigned to dial-in clients. Clients may be unable to access resources on the network.')
Source Address	%2 (Address)

20184

ArcSight Field	Vendor Field
Name	'Interface is unreachable'
Message	Both ("Interface ",One of(%1,%2)," is unreachable because it is not currently connected to the network.")
Device Inbound Interface	One of (%1, %2)
Device Custom String 5	Routing Domain ID

20249

ArcSight Field	Vendor Field
Name	'Failed to authenticate'
Message	Both ('The user ',%2,' has connected and failed to authenticate on port ',%3,'. The line has been disconnected.')
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Application Protocol	%3 (Protocol)
Source Port	%3 (Port)

20252

ArcSight Field	Vendor Field
Name	'Authentication process did not complete'
Message	Both ('The user connected to port ',%2,' has been disconnected because the authentication process did not complete within the required amount of time.')

ArcSight Field	Vendor Field
Device Custom String 4	Correlation-ID
Application Protocol	%2 (Protocol)
Source Port	%2 (Port)

20255

ArcSight Field	Vendor Field
Name	'Connection was prevented'
Device Custom String 4	Correlation-ID
Application Protocol	%2 (Protocol)
Source Port	%2 (Port)
Source User Name	%3 (Connected User)
Source NT Domain	%3 (Domain of Connected User)
Message	%4 (Message Text)

20258

ArcSight Field	Vendor Field
Name	'Account does not have Remote Access privilege'
Message	Both ('The account for user ',%3,' connected on port ',%4,' does not have Remote Access privilege. The line has been disconnected.')
Device Custom String 4	Correlation-ID
Source User Name	%3 (Connected User)
Source NT Domain	%3 (Domain of Connected User)
Application Protocol	%4 (Protocol)
Source Port	%4 (Port)

20266

ArcSight Field	Vendor Field
Name	'Successfully authenticated'
Message	Both ('The user ',One of (%2, %3),' has connected and has been successfully authenticated on port ',One of (%3, %4),'. Data sent and received over this link is strongly encrypted.')
Device Custom String 4	Correlation-ID
Device Custom String 5	Routing Domain ID
Source User Name	One of (%2, %3)
Source NT Domain	One of (%2, %3)
Application Protocol	One of (%3, %4)
Source Port	One of (%3, %4)

20271

ArcSight Field	Vendor Field
Name	'Failed an authentication attempt'
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Source Address	%3 (Address)
Message	Both ('The user ',%2,' connected from ',%3,' but failed an authentication attempt due to the following reason: ',%4')
Reason	%5 (Reason)

20272

ArcSight Field	Vendor Field
Name	'User connected and disconnected'
Message	Both (The user ',One of (%2, %3),' connected on port ',One of (%3, %4),' on ',One of (%4, %5),' at ',One of (%5, %6),' and disconnected on ',One of (%6, %7),' at ',One of (%7, %8),'. The user was active for ',One of (%8, %9),' minutes ', One of (%9, %10),' seconds. ', One of (%10, %11),' bytes were received. The reason for disconnecting was ', One of (%12, %13),'. The tunnel used was ', One of (%13, %14),'. The quarantine state was ', One of (%14, %15),'.')
Device Custom String 4	Correlation-ID
Device Custom String 5	Routing Domain ID
Source User Name	One of (%2, %3)
Source NT Domain	One of (%2, %3)
Application Protocol	One of (%3, %4)
Source Port	One of (%3, %4)
Start Time	Both (One of (%4, %5),' ',One of (%5, %6)))
End Time	Both (One of(%6,%7)," ",One of(7,%8))
Device Custom Number 1	User active minutes
Device Custom Number 2	User active seconds
Bytes Out	One of (%10, %11)
Bytes In	One of (%11, %12)
Additional data	One of (%12, %13)
Additional data	One of (%13, %14)
Additional data	One of (%14, %15)

20274

ArcSight Field	Vendor Field
Name	'User connected and has been assigned address'
Message	Both ('The user ',One of (%2, %3),' connected on port ',One of (%3, %4),' has been assigned address ',One of (%4, %5))
Device Custom String 4	correlation-ID
Device Custom String 5	Routing Domain ID

ArcSight Field	Vendor Field
Source User Name	One of (%2, %3)
Source NT Domain	One of (%2, %3)
Application Protocol	One of (%3, %4)
Source Port	One of %3, %4)
Destination Address	One of (%4, %5)

20275

ArcSight Field	Vendor Field
Name	'User disconnected'
Message	Both ('The user with ip address ',One of (%2, %3),' has disconnected')
Device Custom String 4	Correlation-ID
Device Custom String 5	Routing Domain ID
Source Address	One of (%2, %3)

Mappings for Windows 2008 R2

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Microsoft Windows'

Event 20088

ArcSight Field	Vendor Field
Name	Remote Access Server acquired IP Address
Destination Address	%1 (Assigned Address)
Message	Both ('The Remote Access Server acquired IP Address ',%1,' to be used on the Server Adapter.')

Event 20106

ArcSight Field	Vendor Field
Name	Unable to add interface
Device Outbound Interface	%1 (Interface)
Application Protocol	%2 (Protocol)
Message	%3 (Message Text)

Event 20184

ArcSight Field	Vendor Field
Name	Interface is unreachable
Device Inbound Interface	%1 (Interface)
Message	Both ('Interface ',%1,' is unreachable because it is not currently connected to the network.')

Event 20249

ArcSight Field	Vendor Field
Name	Failed to authenticate
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Application Protocol	%3 (Protocol)
Source Port	%3 (Port)
Message	Both ('The user ',%2,' has connected and failed to authenticate on port ',%3,'. The line has been disconnected.')

Event 20252

ArcSight Field	Vendor Field
Name	Authentication process did not complete
Device Custom String 4	Correlation-ID

ArcSight Field	Vendor Field
Application Protocol	%2 (Protocol)
Source Port	%2 (Port)
Message	Both ('The user connected to port ',%2,' has been disconnected because the authentication process did not complete within the required amount of time.')

Event 20255

ArcSight Field	Vendor Field
Name	Connection was prevented
Device Custom String 4	Correlation-ID
Source User Name	%3 (Connected User)
Source NT Domain	%3 (Domain of Connected User)
Application Protocol	%2 (Protocol)
Source Port	%2 (Port)
Message	%4 (Message Text)

Event 20258

ArcSight Field	Vendor Field
Name	Account does not have Remote Access privilege
Device Custom String 4	Correlation-ID
Source User Name	%3 (Connected User)
Source NT Domain	%3 (Domain of Connected User)
Application Protocol	%4 (Protocol)
Source Port	%4 (Port)
Message	Both ('The account for user ',%3,' connected on port ',%4,' does not have Remote Access privilege. The line has been disconnected.')

Event 20266

ArcSight Field	Vendor Field
Name	Successfully authenticated
Device Custom String 4	Correlation-ID

ArcSight Field	Vendor Field
Source User Name	%3 (Connected User)
Source NT Domain	%3 (Domain of Connected User)
Application Protocol	%4 (Protocol)
Source Port	%4 (Port)
Message	Both ('The user ',One of (%2,%3),' has connected and has been successfully authenticated on port ',One of (%3,%4),'. Data sent and received over this link is strongly encrypted.')

Event 20271

ArcSight Field	Vendor Field
Name	Failed an authentication attempt
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Source Address	%3 (Address)
Reason	%5 (Reason)
Message	%4 (Message Text)

Event 20272

ArcSight Field	Vendor Field
Name	User connected and disconnected
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Application Protocol	%3 (Protocol)
Source Port	%3 (Port)
Start Time	Both (%4, %5)
End Time	Both (%5, %6)
Device Custom Number 1	User active minutes
Device Custom Number 2	User active seconds

ArcSight Field	Vendor Field
Bytes Out	%10 (Bytes Out)
Bytes In	%10 (Bytes In)
Additional data	%12
Additional data	%13
Additional data	%14
Message	Both ('The user ',%2,' connected on port ',%3,' on ',%4,' at ',%5,' and disconnected on ',%6,' at ',%7,'. The user was active for ',%8,' minutes, ',%9,' seconds, ',%10,' bytes were sent and ',%11,' bytes were received. The reason for disconnecting was ',%12,. The tunnel used was ',%13,'. The quarantine state was ',%14,'.')

Event 20274

ArcSight Field	Vendor Field
Name	User connected and has been assigned address
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Application Protocol	%3 (Protocol)
Source Port	%3 (Port)
Destination Address	%4 (Assigned Address)
Message	Both ('The user ',%2,' connected on port ',%3,' has been assigned address ',%4')

Event 20275

ArcSight Field	Vendor Field
Name	User disconnected
Device Custom String 4	Correlation-ID
Source Address	%2 (Address)
Message	Both ('The user with ip address ',%2,' has disconnected')

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!