Micro Focus Security ArcSight Connectors

SmartConnector for Windows Event Log – Native: Microsoft Netlogon Logs

Supplemental Configuration Guide

Document Release Date: December 3, 2020
Software Release Date: December 3, 2020

Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

https://www.microfocus.com

Copyright Notice

Trademark Notices

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

ArcSight Product Documentation on the Micro Focus Security Community

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Revision History

Date	Description
12/03/2020	First edition of this Configuration Guide, for initial support of these events.

Contents

SmartConnector for Microsoft Windows Event Log – Native: Microsoft Netlogon Logs

This guide provides information about the SmartConnector for Microsoft Windows Event Log – Native: Microsoft Netlogon Logs 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
- Microsoft Windows Server 2019

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

Product Overview

Netlogon is a Windows Server process in Windows Server 2019, Windows Server 2016, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2008. The process is responsible for communication between systems in response to a logon request. This handles authentication of users and other services within a domain.

Microsoft Netlogon Logs Configuration

For information about Microsoft's netlogon events logs configuration, see https://support.microsoft.com/en-in/help/4557222/how-to-manage-the-changes-in-netlogon-secure-channel-connections-assoc in the Microsoft TechNet Library.

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 Microsoft Netlogon Logs

General

ArcSight Field	Vendor Field
Device Product	"NETLOGON"
Device Vendor	'Microsoft'

Event 5827

ArcSight Field	Vendor Field
Device Custom String 1	%3 (Account Type)
Device Custom String 1 Label	"Account Type"
Device Custom String 4	%4 (Machine Operating System)
Device Custom String 4 Label	"Machine Operating System"
Device Custom String 5	%5 (Machine Operating System Build)
Device Custom String 5 Label	"Machine Operating System Build"
Device Custom String 6	%6 (Machine Operating System Service Pack)
Device Custom String 6 Label	"Machine Operating System Service Pack"
Event Outcome	"Denied"
Source Host Name	%1 (Machine SamAccountName)
Source Nt Domain	%2 (Domain)
Name	"Netlogon service denied vulnerable Netlogon secure channel connection from a machine account"

Event 5828

ArcSight Field	Vendor Field
Destination Nt Domain	%3 (Trust Target)
Device Custom String 1	%1 (Account Type)
Device Custom String 1 Label	"Account Type"
Event Outcome	"Denied"
Source Address	%4 (Client IP Address)
Source Nt Domain	%2 (Trust Name)
Name	"Netlogon service denied a vulnerable Netlogon secure channel connection using a trust account"

Event 5829

ArcSight Field	Vendor Field
Device Custom String 1	%3
Device Custom String 1 Label	"Account Type"
Device Custom String 4	%4
Device Custom String 4 Label	"Machine Operating System"
Device Custom String 5	%5
Device Custom String 5 Label	"Machine Operating System Build"
Device Custom String 6	%6
Device Custom String 6 Label	"Machine Operating System Service Pack"
Event Outcome	"Allowed"
Source Host Name	%1
Source Nt Domain	%2
Name	"Netlogon service allowed a vulnerable Netlogon secure channel connection"

Event 5830

Device Custom String 1	%3
Device Custom String 1 Label	"Account Type"
Device Custom String 4	%4

Device Custom String 4 Label	"Machine Operating System"
Device Custom String 5	%5
Device Custom String 5 Label	"Machine Operating System Build"
Device Custom String 6	%6
Device Custom String 6 Label	"Machine Operating System Service Pack"
Event Outcome	"Allowed"
Source Host Name	%1
Source Nt Domain	%2
Name	"Netlogon service allowed a vulnerable Netlogon secure channel connection because account is allowed in group policy"

Event 5831

ArcSight Field	Vendor Field
Destination Nt Domain	%3
Device Custom String 1	%1
Device Custom String 1 Label	"Account Type"
Event Outcome	"Allowed"
Source Address	%4
Source Nt Domain	%2
Name	"Netlogon service allowed a vulnerable Netlogon secure channel connection because trust account is allowed in group policy"

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 computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Supplemental Configuration Guide (Connectors 8.1.0)

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 Documentation-Feedback@microfocus.com.

We appreciate your feedback!