Hewlett Packard
Enterprise

# HPE Security ArcSight Connectors

## SmartConnector for Windows Event Log – Native: Microsoft WINS Server

## Supplemental Configuration Guide

August 15, 2017

# 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



Follow this link to see a complete statement of copyrights and acknowledgements:
https://community.saas.hpe.com/t5/Discussions/Third-Party-Copyright-Notices-and-License-Terms/td-p/1589228

# Revision History

| Date | Description |
|---|---|
| 08/15/2017 | Updated the "Collect Events from the Application or System Event Log" procedure to remove the 'arcsight connectorsetup' command. |
| 11/30/2016 | Added Windows Server 2016 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://community.saas.hpe.com/t5/ArcSight/ct-p/arcsight |

# Contents

# SmartConnector for Windows Event Log – Native: Microsoft WINS Server

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

Supported versions:

- Microsoft Windows 8
- Microsoft Windows Server 2012
- Microsoft Windows Server 2016

The *SmartConnector for Microsoft Windows Event Log – Native 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 the SmartConnector for Windows Event Log – Native: Microsoft WINS Server.

# Product Overview

Microsoft WINS servers are designed to prevent the administrative difficulties that are inherent in the use of both IP broadcasts and static mapping files such as LMHOSTS files. Microsoft WINS is designed to eliminate the need for IP broadcasts (which use valuable network bandwidth and cannot be used in routed networks), while providing a dynamic, distributed database that maintains computer name-to-IP-address mappings.

WINS servers use a replicated database that contains NetBIOS computer names and IP address mappings (database records). When Windows-based computers log on to the network, their computer name and IP address mapping are added (registered) to the WINS server database, providing support for dynamic updates. The WINS server database is replicated among multiple WINS servers in a LAN or WAN. One of the benefits of this database design is that it prevents different users from registering duplicate NetBIOS computer names on the network.

WINS clients, referred to as WINS- enabled clients, are configured to use the services of a WINS server. Windows NT- based clients are configured with the IP address of one or more WINS servers by using the WINS Address tab on the Microsoft TCP/IP Properties page in Control Panel -> Network.

# WINS Configuration

You can run the Registry Editor program at the command prompt to configure a WINS server by changing the values of the Registry parameters.  Parameters for logging include:

| Configuration Option | Description |
|---|---|
| Logging Enabled | Specifies whether logging of database changes to J50.log files should be turned on. |
| Log Detailed Events | Specifies whether logging events is verbose mode. (This requires considerable computer resources and should be turned off if you are tuning for performance.) |

# 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.

# Collect Events from the Application or System Event Log

When collecting events from System Event logs (such as NTServicePack, Service Control Manager, WINS), select System for Windows Log type.

When collecting events from application event logs (such as Microsoft Forefront Protection 2010 for Exchange, Microsoft SQL Server Audit), select Application for Windows Log type.

To collect events from the event logs, set the host parameter eventlogtypes as follows:

```
eventlogtypes=application,system
```

Access the connectors advanced parameters to specify the event log types:

1. From the $ARCSIGHT_HOME\current\user\agent directory, open `agent.properties` to edit.
2. Locate the `eventlogtypes` parameter; the initial value is null. Enter the appropriate event log names.

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

# Windows 2016, 2012, and 8

## General

| ArcSight Field | Vendor Field |
|---|---|
| Device Vendor | 'Microsoft' |
| Device Product | 'Microsoft Windows' |
| Device Custom String 4 | Reason or Error Code |

## 4097

| ArcSight Field | Vendor Field |
|---|---|
| Name | 'WINS initialized properly and is now fully operational' |

## 4098

| ArcSight Field | Vendor Field |
|---|---|
| Name | 'WINS was terminated by the service controller' |
| Message | 'WINS will gracefully terminate' |

## 4119

| ArcSight Field | Vendor Field |
|---|---|
| Name | 'WINS received a packet that has the wrong format' |

## 4143

| ArcSight Field | Vendor Field |
|---|---|
| Name | 'WINS scavenged its records in the WINS database' |
| Message | 'The number of records scavenged is given in the data section' |

## 4178

| ArcSight Field | Vendor Field |
|---|---|
| Name | 'The WINS Pull configuration key could not be created or opened' |
| Message | 'Check to see if the permissions on the key are set properly, system resources are low, or the registry is having a problem' |

## 4179

| ArcSight Field | Vendor Field |
|---|---|
| Name | 'The WINS Push configuration key could not be created or opened' |
| Message | 'Check to see if the permissions on the key are set properly, system resources are low, or the registry is having a problem' |

## 4180

| ArcSight Field | Vendor Field |
|---|---|
| Name | 'The WINS\\Parameters key could not be created or opened' |
| Message | 'Check to see if the permissions on the key are set properly, system resources are low, or the registry is having a problem' |

## 4181

| ArcSight Field | Vendor Field |
|---|---|
| Name | '# The subkey could not be created or opened' |
| Message | 'This key should be there if you want WINS to do consistency checks on its database periodically. NOTE: Consistency checks have the potential of consuming large amounts of network bandwidth. Check to see if the permissions on the key are set properly, system resources are low, or the registry is having a problem' |

## 4224

| ArcSight Field | Vendor Field |
|---|---|
| Name | 'WINS encouintered a database error' |
| Message | 'This may or may not be a serious error. WINS will try to recover from it' |

## 4252

| ArcSight Field | Vendor Field |
|---|---|
| Name | 'WINS did not find any subkeys under the Pull key' |

## 4253

| ArcSight Field | Vendor Field |
|---|---|
| Name | 'WINS did not find any subkeys under the Push key' |

## 4309

| ArcSight Field | Vendor Field |
|---|---|
| Name | 'System Resource Information' |
| Device Custom Number 1 | Processor Count |
| Device Custom Number 2 | Physical Memory |
| Device Custom Number 3 | Memory available for allocation |

## 4318

| ArcSight Field | Vendor Field |
|---|---|
| Name | 'WINS could not start due to a missing or corrupt database' |
| Message | 'Restore the database using WINS Manager (or winscl.exe found in the Windows 2000 Resource Kit) and restart WINS' |

## 4325

| ArcSight Field | Vendor Field |
|---|---|
| Name | 'WINS could not read the Initial Challenge Retry Interval from the registry' |

## 4326

| ArcSight Field | Vendor Field |
|---|---|
| Name | 'WINS could not read the Challenge Maximum Number of Retries from the registry' |

## 4329

| ArcSight Field | Vendor Field |
|---|---|
| Name | 'The WINS server has started a scavenging operation' |

## 4330

| ArcSight Field | Vendor Field |
|---|---|
| Name | 'The WINS server has completed the scavenging operation' |

## 4337

| ArcSight Field | Vendor Field |
|---|---|
| Name | 'WINS Server could not initialize security to allow the read-only operations' |

## 5001

| ArcSight Field | Vendor Field |
|---|---|
| Name | 'WINS is scavenging the locally owned records from the database' |
| Message | 'The version number range that is scavenged is given in the data section, in the second to fifth words, in the order: from_version_number (low word, high word) to_ version_number (low word, high word)' |

## 5002

| ArcSight Field | Vendor Field |
|---|---|
| Name | 'WINS is scavenging a chuck on N records in the version number range from X to Y' |
| Message | 'N, X and Y (low word, high word for version numbers) are given in the second to sixth words in the data section' |

# 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!