



# **Micro Focus Security ArcSight Connectors**

## **SmartConnector for Microsoft Windows Event Log – Native: Oracle Audit**

### **Supplemental Configuration Guide**

Document Release Date: April 16, 2018

Software Release Date: April 16, 2018

## Legal Notices

### Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Micro Focus") are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

### Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is 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

© Copyright 2010-2018 Micro Focus or one of its affiliates.

### Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

## Support

### Contact Information

<b>Phone</b>	A list of phone numbers is available on the Technical Support Page: <a href="https://softwaresupport.softwaregrp.com/support-contact-information">https://softwaresupport.softwaregrp.com/support-contact-information</a>
<b>Support Web Site</b>	<a href="https://softwaresupport.softwaregrp.com/">https://softwaresupport.softwaregrp.com/</a>
<b>ArcSight Product Documentation</b>	<a href="https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ctp/productdocs">https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ctp/productdocs</a>

## Document Revision History

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

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.

To check for recent updates or to verify that you are using the most recent edition of a document, go to the : [ArcSight Product Documentation Community on Protect 724](#).

### Document Changes

Date	Product Version	Description

# Contents

SmartConnector for Microsoft Windows EventLog – Native: Oracle Audit .....	5
Product Overview .....	5
Configuration .....	5
Enable Auditing .....	5
Audit Administrative Users .....	5
Connector Installation and Configuration .....	6
Collect Events from the Event Log .....	6
Device Event Mapping to ArcSight Fields .....	7
Oracle Windows Event Log Mappings to ArcSight ESM Fields .....	7
Event ID 4 .....	8
Event ID 5 .....	8
Event ID 8 .....	8
Event ID 12 .....	8
Oracle Audit SYSDBA Event Mappings to ArcSight ESM Fields .....	9
Event ID 34 .....	9
Oracle Audit Trail Event Mappings to ArcSight ESM Fields .....	9
Event ID 34 .....	9
Send Documentation Feedback .....	11

# SmartConnector for Microsoft Windows Event Log – Native: Oracle Audit

This guide provides information about the SmartConnector for Microsoft Windows Event Log – Native: Oracle Audit and its event mappings to ArcSight data fields. Oracle database versions 10g, 11g, and 12cR1 with Microsoft Windows Server 2012 are supported.

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: Oracle Audit.

## Product Overview

Auditing is a default feature of the Oracle server. The standard audit commands allow all system privileges to be audited along with access at the object level to any table or view on the database for select, delete, insert or update. Audit can be run for either successful or unsuccessful attempts or both. It can be for each individual user or for all users, and it can also be done at the session level or access level. At action level a single record is created per action and at session level one record is created for all audit actions per session.

## Configuration

For complete information about Oracle database auditing, see "Configuring Auditing" in the *Oracle Database Security Guide* for your database version.

## Enable Auditing

Database auditing is enabled and disabled by the AUDIT\_TRAIL initialization parameter in the database initialization parameter file, `init.ora`. Setting it to OS enables database auditing and directs all audit records to an operating system file:

```
AUDIT_TRAIL=OS
```

## Audit Administrative Users

Sessions for users who connect as SYS can be fully audited, including all users connecting as SYSDBA or SYSOPER. Use the AUDIT\_SYS\_OPERATIONS initialization parameter to specify whether such users are to be audited. For example, the following setting specifies that SYS is to be audited:

```
AUDIT_SYS_OPERATIONS = TRUE
```

The default value, FALSE, disables SYS auditing.

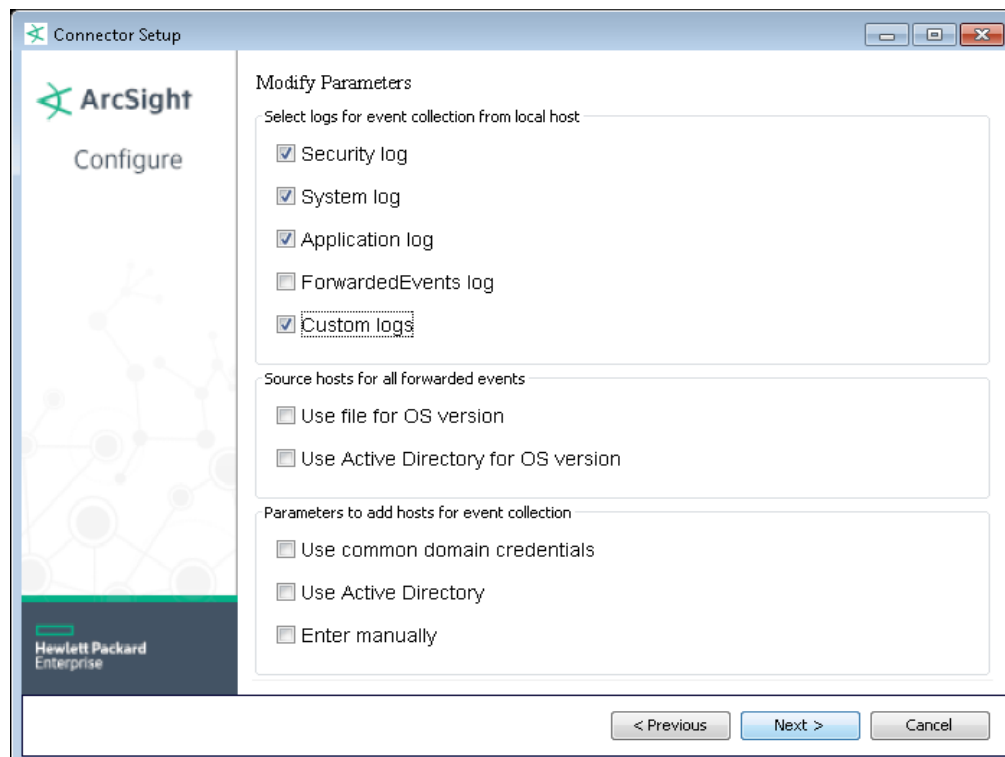
## Connector Installation and Configuration

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

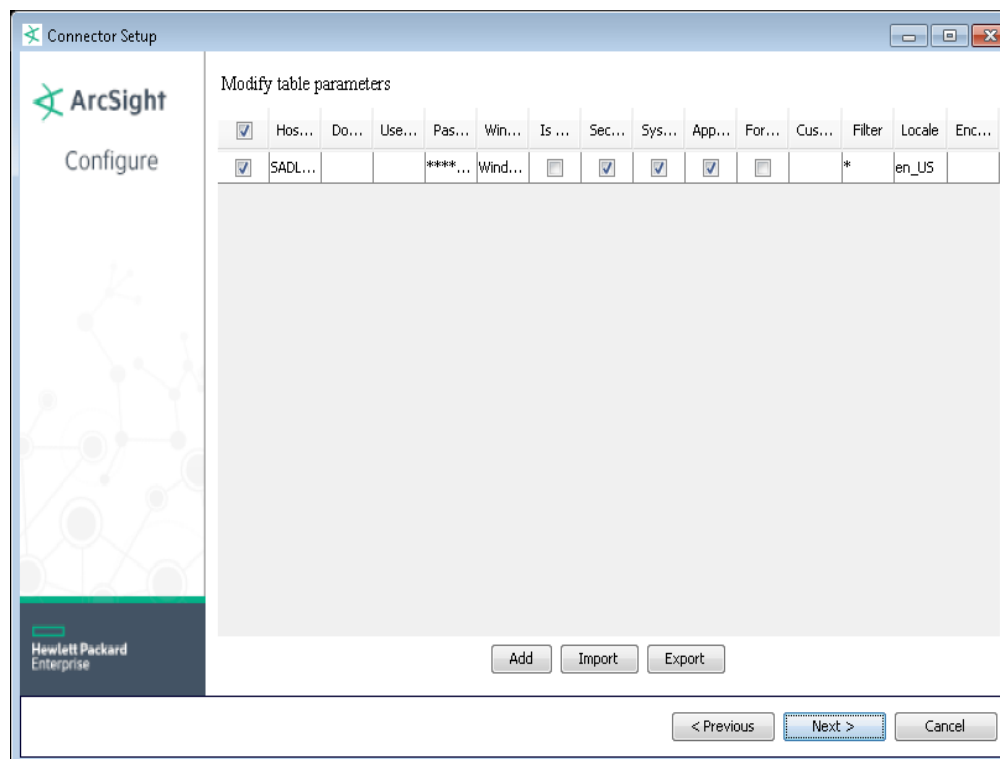
To set up the connector to collect application events:

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. Parameter modification windows are displayed based on your initial connector configuration. To ensure the table parameter modification window is displayed for you to add Oracle Audit logs, select **Custom logs** on the initial modify parameter window.



Click **Next** to 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 **Oracle Audit** in the **Custom Log Names** field.



You can specify multiple **Custom Log Names** in a comma-separated format, for example:

Oracle Audit, Exchange Auditing

6. Click **Next** to view the **Summary** window. 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.

### Oracle Windows Event Log Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Source Service Name	EventSource
Device Vendor	'Oracle'

## Event ID 4

ArcSight ESM Field	Device-Specific Field
Device Custom String 3	Instance Name
Device Product	'Oracle'
Message	Both ('Initializing SGA for instance '%1')
Name	'Initializing SGA for instance'

## Event ID 5

ArcSight ESM Field	Device-Specific Field
Device Custom String 3	Instance Name
Device Product	'Oracle'
Message	'Both ('Initializing SGA for process '%1,' in instance '%2')
Name	'Initializing SGA for process in instance'
Destination Process Name	%1 (Destination Process Name)

## Event ID 8

ArcSight ESM Field	Device-Specific Field
Device Custom String 3	Instance Name
Device Product	'Oracle'
Message	Both ('Shutdown normal performed on instance '%1')
Name	'Shutdown normal performed on instance'

## Event ID 12

ArcSight ESM Field	Device-Specific Field
Device Custom String 3	Instance Name
Device Product	'Oracle'
Message	Both ('All process in instance '%1,' stopped')
Name	'All process in instance stopped'



## Oracle Audit SYSDBA Event Mappings to ArcSight ESM Fields

### Event ID 34

ArcSight ESM Field	Device-Specific Field
Destination Process Name	ProcessId
Destination User Name	DATABASE USER
Destination User Privileges	PRIVILEGE
Device Action	first word from ACTION
Device Custom Number 1	STATUS
Device Custom String 6	CLIENT TERMINAL
Device Event Class Id	first word of ACTION
Device External ID	DBID
Device Product	'ORACLESYSDBA'
Device Vendor	'ORACLE'
Message	first word from ACTION
Name	first word from ACTION
Source Host Name	CLIENT TERMINAL
Source User Name	CLIENT USER

## Oracle Audit Trail Event Mappings to ArcSight ESM Fields

### Event ID 34

ArcSight ESM Field	Device-Specific Field
Additional data	LOGOFF_DEAD
Additional data	LOGOFF_LREAD
Additional data	LOGOFF_LWRITE
Additional data	LOGOFF_PREAD
Additional data	OBJ_CREATOR
Additional data	SESSIONCPU
Additional data	SES_TID
Additional data	STATEMENT

ArcSight ESM Field	Device-Specific Field
Destination Host Name	USERHOST
Destination NT Domain	USERHOST
Destination Process Name	ProcessId
Destination User Name	USERID
Destination User Privileges	PRIV_USED
Device Action	ACTION
Device Custom Number 1	RETURNCODE
Device Custom Number 2	SESSIONID
Device Custom Number 3	ENTRYID
Device Custom String 1	COMMENT_TEXT
Device Custom String 2	TERMINAL
Device Custom String 4	SES_LABEL
Device Custom String 5	SES_ACTIONS
Device Event Class Id	ACTION
Device External ID	DBID
Device Product	'Oracle'
Device Severity	RETURNCODE
Device Vendor	'ORACLE'
File Name	Object name
Name	ACTION
Source Address	extracted IP address from SES_LABEL (will auto map to Source Host Name)
Source NT Domain	OSSUSERID
Source User Name	OS_USERID
Reason	RETURNCODE
Transport Protocol	PROTOCOL
Device Custom IPv6 Address 2	Source IPv6 Address
File Name	Name
Source Port	Port

# 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 )**

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](mailto:arc-doc@hpe.com).

We appreciate your feedback!