



ArcSight SmartConnectors

Software Version: 8.4.3

Configuration Guide for Oracle Audit XML File SmartConnector

Document Release Date: October 2023

Software Release Date: October 2023

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2023 Open Text.

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

Trademark Notices

“OpenText” and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

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:

<https://www.microfocus.com/support-and-services/documentation>

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://www.microfocus.com/documentation/arcsight/

Contents

- Configuration Guide for Oracle Audit XML File SmartConnector 4
- Product Overview 5
- Configuration 6
 - Activities Always Audited 6
 - Standard Auditing 6
 - Configuring Oracle XML Auditing 7
 - Increase Memory Size for XML Reports 9
- Installing the SmartConnector 10
 - Preparing to Install the SmartConnector 10
 - Installing the SmartConnector 10
- Device Event Mapping to ArcSight Fields 12
 - Oracle XML Audit Event Mappings to ArcSight ESM Fields 12
- Send Documentation Feedback 14

Configuration Guide for Oracle Audit XML File SmartConnector

This guide provides information for installing the SmartConnector for Oracle Audit XML Connector and configuring your Oracle database for Database Audit Trail using XML.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

- [Technical Requirements Guide for SmartConnector](#), which provides information about operating system, appliance, browser, and other support details for SmartConnector.
- [Installation and User Guide for SmartConnectors](#), which provides detailed information about installing SmartConnectors.
- [Configuration Guides for ArcSight SmartConnectors](#), which provides information about configuring SmartConnectors to collect events from different sources.
- [Configuration Guide for SmartConnector Load Balancer](#), which provides detailed information about installing Load Balancer.

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the [documentation site for ArcSight SmartConnectors 8.4](#).

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to MFI-Documentation-Feedback@opentext.com.

For specific product issues, [contact Open Text Support for Micro Focus products](#).

Product Overview

This connector collects events from Database Audit Trail log tables written in XML. This guide provides information about the types of auditing and configuring the Database Audit Trail to write to the log tables in XML. For more information about Oracle database auditing, see "Verifying Security Access with Auditing" in the *Oracle Database Security Guide* for your database version.



Note: None of the connector versions supports Oracle Multitenant at this time.

Configuration

Oracle XML Auditing

Activities Always Audited

Oracle Database always audits certain database-related operations and writes them to the operating system audit files. The operating system audit file captures the complete archived messages for these types of activities. Mandatory auditing includes the following operations:

- **Administrative privilege connections to the database instance.**
An audit record is generated that lists the operating system user connecting to Oracle Database as SYSOPER or SYSDBA. This provides for accountability of users with administrative privileges.
- **Database startup.**
An audit record is generated that lists the operating system user starting the instance, the user terminal identifier, and the date-and-time stamp. This data is stored in the Operating System Audit Trail because the Database Audit Trail is not available until after the startup has successfully completed.
- **Database shutdown.**
An audit record is generated that lists the operating system user shutting down the instance, the user terminal identifier, and the date-and-time stamp. You can set the location of this file by using the AUDIT_FILE_DEST initialization parameter.

Standard Auditing

Standard auditing includes auditing the following:

- SQL statements
- privileges
- schema objects
- network activity

Standard audit records can be written to either the database audit trail or to operating system audit files. You enable the standard audit trail by setting the AUDIT_TRAIL initialization parameter. This parameter determines whether to create the audit trail in

the database audit trail, write the audit activities to an operating system file, or to disable auditing.

Configuring Oracle XML Auditing

To enable standard auditing and to write the audit record in XML, perform the following procedure:

1. Start **Database Control**.
2. Log in as **SYS** and connect with the **SYSDBA** privilege.
 - **User Name:** SYS
 - **Password:** Enter your password.
 - **Connect As:** SYSDBA
3. Click **Server** to display the Server subpage.
4. In the **Database Configuration** section, click **Initialization Parameters**.
The Initialization Parameters screen displays.
5. Click **SPFile**.
The SPFile screen displays.
If the SPFile tab does not display, then you did not install Oracle Database using a server parameters file. Proceed to the next step.
6. In the **Name** field, enter **audit_trail** to find the AUDIT_TRAIL initialization parameter, and then click **Go**.
7. In the **Value** field, select from the following values:
 - **DB:** Directs audit records to the database audit trail (the SYS.AUD\$ table), except for mandatory and SYS audit records, which are always written to the operating system audit trail. DB is the default setting for the AUDIT_TRAIL parameter.
 - **DB, Extended:** Behaves the same as AUDIT_TRAIL=DB, but also populates the SQL bind and SQL text CLOB-type columns of the SYS.AUD\$ table, when available. This setting captures the SQL statement used in the action that was audited.
 - **OS:** Directs all audit records to an operating system file. If you set AUDIT_TRAIL to OS, then set the following additional initialization parameters:

AUDIT_FILE_DEST	Specifies the location of the operating system audit record file.
AUDIT_SYS_OPERATIONS	If you want to audit the top-level SQL statements directly issued by users who have connected with the SYSDBA or SYSOPER privileges set this setting to True. If you set AUDIT_SYS_OPERATIONS to True and AUDIT_TRAIL to XML or XML, EXTENDED, then Oracle Database writes SYS audit records operating system files in XML format.
AUDIT_SYSLOG_LEVEL	Writes SYS and standard OS audit records to the system audit log using the SYSLOG utility. This option only applies to UNIX environments.

- **XML:** Writes to the operating system audit record file in XML format. Prints all elements of the AuditRecord node (as specified by the by the XML schema in http://xmlns.oracle.com/oracleas/schema/dbserver_audittrail-11_2.xsd) except Sql_Text and Sql_Bind to the operating system XML audit file. This .xsd file represents the schema definition of the XML audit file. An XML schema is a document written in the XML Schema language. If you set the XML value, then also set the AUDIT_FILE_DEST parameter. For all platforms, including Windows, the default location for XML audit trail records is \$ORACLE_BASE/admin/\$ORACLE_SID/adump. The XML AUDIT_TRAIL value does not affect syslog audit file. If you have set the AUDIT_TRAIL parameter to XML, then the syslog audit records will still be in text format, not XML file format. You can control the output for SYS and mandatory audit records as follows:

To write SYS and mandatory audit files to operating system files in XML format:

Set AUDIT_TRAIL to XML or XML,EXTENDED, set AUDIT_SYS_OPERATIONS to **TRUE**, but do not set the AUDIT_SYSLOG_LEVEL parameter.

To write SYS and mandatory audit records to syslog audit files and standard audit records to XML audit files: Set AUDIT_TRAIL to XML or XML, EXTENDED set AUDIT_SYS_OPERATIONS to **TRUE**, and set the AUDIT_SYSLOG_LEVEL parameter.

- **XML EXTENDED:** Specifies XML, EXTENDED which performs all actions of XML and also populates the SQL bind and SQL text CLOB-type columns of the SYS.AUD\$ table, wherever possible. (These columns are populated only when this parameter is selected.)
- **None:** Disables standard auditing.



Note: For more information about AUDIT_TRAIL initialization parameter settings, see "Verifying Security Access with Auditing" in the *Oracle Database Security Guide*.

8. Click **Apply**.

9. Restart the Oracle Database instance:
 - a. Click the **Database Instance** link.
 - b. Click **Home** to display the Database Control home page.
 - c. Under **General**, click **Shutdown**.
 - d. In the **Startup/Shutdown Credentials** page, enter your credentials.
 - e. After the shutdown completes, click **Startup**.

Increase Memory Size for XML Reports

The connector cannot process reports that are too lengthy. With the default 256M memory setting, the connector can safely process reports up to 250K in length. If memory is increased to the maximum limit of 1024M, the connector can process reports up to a million lines in length. Longer reports cannot be processed. ArcSight's recommendation for long reports is to split the scan into multiple smaller reports and import them individually.

To increase the memory size for stand-alone connectors from the command line, change the following line in `$ARCSIGHT_HOME\current\bin\scripts\connectors.bat` (Windows) or `$ARCSIGHT_HOME/current/bin/scripts/connectors.sh` (Unix)

```
ARCSIGHT_MEMORY_OPTIONS=" -Xms256m -Xmx256m "
```

to

```
ARCSIGHT_MEMORY_OPTIONS=" -Xms1024m -Xmx1024m "
```

To increase the memory size for connectors being run as a service, change the following lines in `user/agent/agent.wrapper.conf` from:

```
wrapper.java.initmemory=256  
wrapper.java.maxmemory=256
```

to:

```
wrapper.java.initmemory=1024  
wrapper.java.maxmemory=1024
```

To increase the memory size for connectors managed by the Connector Appliance/ArcSight Management Center, the heap size can be set using a container level command.

Installing the SmartConnector

The following sections provide instructions for installing and configuring your selected SmartConnector.



Connector Appliance/ArcSight Management Center supports mounting for Network File System (NFS) and CIFS (Windows) shares. When you install this connector on one of these devices, establish a CIFS mount on the device before adding the connector. Provide this share name during connector configuration. For more information, see **Remote File Systems** in the Connector Appliance or ArcSight Management Center Administrator's Guide.

Preparing to Install the SmartConnector

Before you install any SmartConnectors, make sure that the OpenText ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger).

For complete product information, refer to the *Administrator's Guide to ArcSight Platform*, available on [ArcSight Documentation](#).

If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* available on [ArcSight Documentation](#) for instructions.

Before installing the SmartConnector, make sure that the following are available:

- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords

Installing the SmartConnector

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. Specify the relevant [Global Parameters](#), when prompted.
4. Select **Oracle Audit XML Connector** from the **Type** drop-down, then click **Next**.
5. In the **Log File Folder** field, specify the name of the folder into which the logs are to be deposited.

6. Select a [destination and configure parameters](#).
7. Specify a name for the connector.
8. (Conditional) If you have selected **ArcSight Manager** as the destination, the certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination**, and then click **Next**. The certificate is imported and the **Add connector Summary** window is displayed.



Note: If you select Do not import the certificate to connector from destination, the connector installation will end.

9. Select whether you want to install the connector as a service or in the standalone mode.
10. Complete the installation.
11. [Run the SmartConnector](#).

For instructions about upgrading the connector or modifying parameters, see [Installation and User Guide for SmartConnector](#).

Device Event Mapping to ArcSight Fields

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

Oracle XML Audit Event Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Destination User Name	dbuser
Destination User Privileges	privilege
Device Action	action
Device Custom Floating Point 1	Session ID
Device Custom IPv6 Address 2	Source IPv6 Address
Device Custom Number 1	Instance Number
Device Custom Number 3	Entry ID
Device Custom String 3	Policy Name
Device Custom String 4	Sql Text
Device Custom String 5	sqlbind
Device Custom String 5 Label	Sql Bind
Device Custom String 6	Terminal
Device Event Category	audittype("1=Standard XML Audit","2=Fine Grained XML Audit","4=SYS XML Audit","8=Mandatory XML Audit")
Device Event Class ID	One of (action, returncode)
Device External ID	dbid
Device Host Name	oshost
Device Process Name	osprocess
Device Product	'ORACLESYSDBA'
Device Receipt Time	timestamp

ArcSight ESM Field	Device-Specific Field
Device Vendor	'ORACLE'
Message	commenttext
Name	One of (action, returncode)
Raw Event	XMLEvent
Reason	returncode
Source Address	Extract HOST from commenttext
Source Host Name	userhost
Source Port	Extract PORT from commenttext
Source User Name	clientuser
Source User Privileges	CURRENT_USER
Transport Protocol	Extract PROTOCOL from commenttext

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 Configuration Guide for Oracle Audit XML File SmartConnector
(SmartConnectors 8.4.3)**

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 MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!