Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for Oracle Audit XML File

Configuration Guide

October 17, 2017

Configuration Guide

SmartConnector for Oracle Audit XML File

October 17, 2017

Warranty

Restricted Rights Legend

Revision History

Date	Description
10/17/2017	Added encryption parameters to Global Parameters.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
02/14/2014	Added support for Oracle 12cR1.
06/28/2013	Updated mappings for parser changes.
03/29/2013	Updated mapping for Device Action; added mapping for Reason.
02/15/2013	Added mappings for IPv6.
11/15/2012	First edition of this guide.

SmartConnector for Oracle Audit XML File

This guide provides information for installing the SmartConnector for Oracle Audit XML Connector and configuring your Oracle database for Database Audit Trail using XML. Event collection from Oracle database versions 11g, 11gR2, and 12cR1 are supported.

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.

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.

Configuration

Configure Oracle XML Auditing

To enable standard auditing and 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.

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.

Install 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.

Prepare to Install Connector

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

For complete product information, read the *Administrator's Guide* as well as the *Installation and Configuration* guide for your ArcSight product before installing a new SmartConnector. If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center*

Administrator's Guide for instructions, and start the installation procedure at "Set Global Parameters (optional)" or "Select Connector and Add Parameter Information."

Before installing the SmartConnector, be sure the following are available:

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

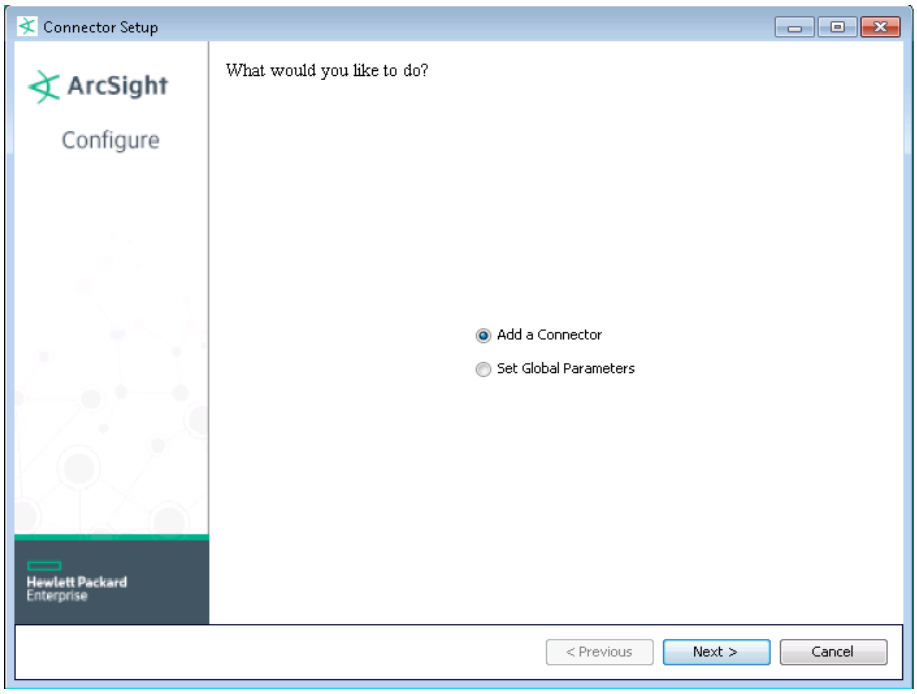
Install Core Software

Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the HPE SSO and Protect 724 sites.

1. Download the SmartConnector executable for your operating system from the HPE SSO site.
2. Start the SmartConnector installation and configuration wizard by running the executable.

   Follow the wizard through the following folder selection tasks and installation of the core connector software:

   Introduction
   Choose Install Folder
   Choose Shortcut Folder
   Pre-Installation Summary
   Installing...
3. When the installation of SmartConnector core component software is finished, the following window is displayed:



Set Global Parameters (optional)

If you choose to perform any of the operations shown in the following table, do so before adding your connector. You can set the following parameters:

Parameter	Setting
FIPS mode	Select 'Enabled' to enable FIPS compliant mode. To enable FIPS Suite B Mode, see the SmartConnector User Guide under "Modifying Connector Parameters" for instructions. Initially, this value is set to 'Disabled'.
Remote Management	Select 'Enabled' to enable remote management from ArcSight Management Center. When queried by the remote management device, the values you specify here for enabling remote management and the port number will be used. Initially, this value is set to 'Disabled'.
Remote Management Listener Port	The remote management device will listen to the port specified in this field. The default port number is 9001.
Preferred IP Version	When both IPv4 and IPv6 IP addresses are available for the local host (the machine on which the connector is installed), you can choose which version is preferred. Otherwise, you will see only one selection. The initial setting is IPv4.

The following parameters should be configured only if you are using HPE SecureData solutions to provide encryption. See the *HPE SecureData Architecture Guide* for more information.

Parameter	Setting
Format Preserving Encryption	Data leaving the connector machine to a specified destination can be encrypted by selecting ‘Enabled’ to encrypt the fields identified in ‘Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of the encryption parameters again will require a fresh installation of the connector.
Format Preserving Policy URL	Enter the URL where the HPE SecureData Server is installed.
Proxy Server (https)	Enter the proxy host for https connection if any proxy is enabled for this machine.
Proxy Port	Enter the proxy port for https connection if any proxy is enabled for this machine.
Format Preserving Identity	The HPE SecureData client software allows client applications to protect and access data based on key names. This key name is referred to as the identity. Enter the user identity configured for HPE SecureData.
Format Preserving Secret	Enter the secret configured for HPE SecureData to use for encryption.
Event Fields to Encrypt	Recommended fields for encryption are listed; delete any fields you do not want encrypted and add any string or numeric fields you want encrypted. Encrypting more fields can affect performance, with 20 fields being the maximum recommended. Also, because encryption changes the value, rules or categorization could also be affected. Once encryption is enabled, the list of event fields cannot be edited.

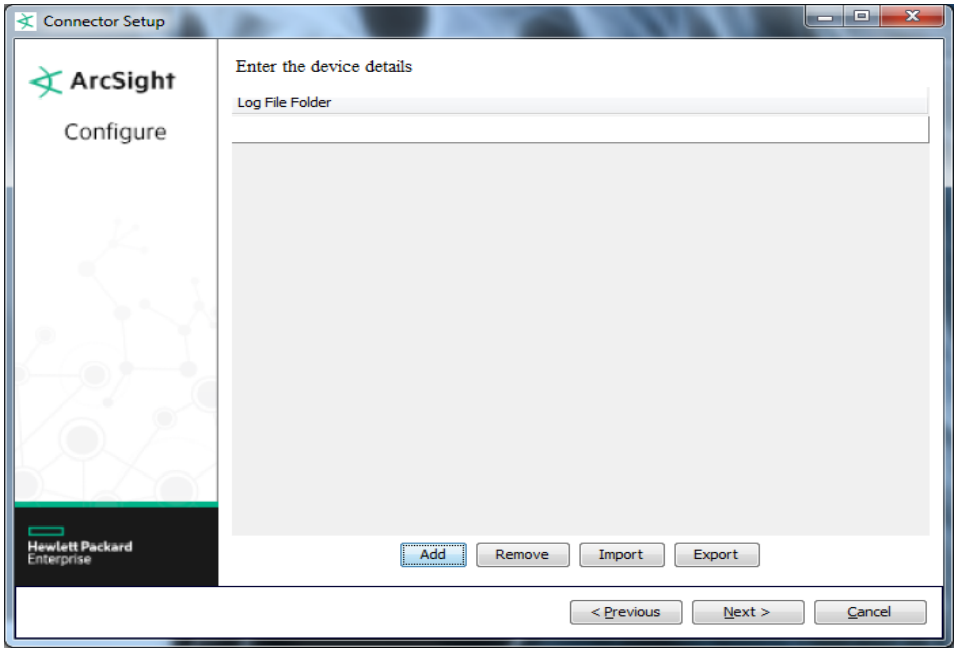
After making your selections, click **Next**. A summary screen is displayed. Review the summary of your selections and click **Next**. Click **Continue** to return to proceed with "Add a Connector" window. Continue the installation procedure with "Select Connector and Add Parameter Information."

Select Connector and Add Parameter Information

1. Select **Add a Connector** and click **Next**. If applicable, you can enable FIPS mode and enable remote management later in the wizard after SmartConnector configuration.

2. Select **Oracle Audit XML Connector** and click **Next**.

3 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Parameter	Description
Log File Folder	Enter the name of the folder into which the logs are to be deposited

You can click the 'Export' button to export the host name data you have entered into the able into a CSV file; you can click the 'Import' button to select a CSV file to import into the table rather than add the data manually. See the "SmartConnector User's Guide" for more information.

Select a Destination

1 The next window asks for the destination type; select a destination and click **Next**. For information about the destinations listed, see the *ArcSight SmartConnector User Guide*.

2 Enter values for the destination. For the ArcSight Manager destination, the values you enter for **User** and **Password** should be the same ArcSight user name and password you created during the ArcSight Manager installation. Click **Next**.

3 Enter a name for the SmartConnector and provide other information identifying the connector's use in your environment. Click **Next**. The connector starts the registration process.

4 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 click **Next**. (If you select **Do not import the certificate to connector from destination**, the connector installation will end.) The certificate is imported and the **Add connector Summary** window is displayed.

Complete Installation and Configuration

1. Review the **Add Connector Summary** and click **Next**. If the summary is incorrect, click **Previous** to make changes.

2. The wizard now prompts you to choose whether you want to run the SmartConnector as a stand-alone process or as a service. If you choose to run the connector as a stand-alone process, select **Leave as a standalone application**, click **Next**, and continue with step 5.

3. If you chose to run the connector as a service, with **Install as a service** selected, click **Next**. The wizard prompts you to define service parameters. Enter values for **Service Internal Name** and **Service Display Name** and select **Yes** or **No** for **Start the service automatically**. The **Install Service Summary** window is displayed when you click **Next**.

4. Click **Next** on the summary window.

5. To complete the installation, choose **Exit** and Click **Next**.

For instructions about upgrading the connector or modifying parameters, see the *SmartConnector User Guide*.

Run the SmartConnector

SmartConnectors can be installed and run in stand-alone mode, on Windows platforms as a Windows service, or on UNIX platforms as a UNIX daemon, depending upon the platform supported. On Windows platforms, SmartConnectors also can be run using shortcuts and optional Start menu entries.

If the connector is installed in stand-alone mode, it must be started manually and is not automatically active when a host is restarted. If installed as a service or daemon, the connector runs automatically when the host is restarted. For information about connectors running as services or daemons, see the *ArcSight SmartConnector User Guide*.

To run all SmartConnectors installed in stand-alone mode on a particular host, open a command window, go to `$ARCSIGHT_HOME\current\bin` and run: `arcsight connectors`

To view the SmartConnector log, read the file `$ARCSIGHT_HOME\current\logs\agent.log`; to stop all SmartConnectors, enter `Ctrl+C` in the command window.

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

ArcSight ESM Field	Device-Specific Field
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 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
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
Transport Protocol	Extract PROTOCOL from commenttext