Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for Oracle Unified Audit Trail DB

Configuration Guide

October 17, 2017

Configuration Guide

SmartConnector for Oracle Unified Audit Trail DB

October 17, 2017

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 Development LP shall not be liable for technical or editorial 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. Hewlett Packard Enterprise Development LP 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 Development LP 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.

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

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.
06/30/2016	Adding troubleshooting information about resolving Oracle error messages ORA-00942 and ORA-22835.
09/30/2015	First edition supporting Oracle 12c Unified Audit Trail.

SmartConnector for Oracle Unified Audit Trail DB

This guide provides information for installing the SmartConnector for Oracle Unified Audit Trail DB and configuring the device for event collection. Oracle Database version 12c is supported.

Product Overview

In previous releases of Oracle Database, there were separate audit trails for individual components. With Oracle 12c, these are unified into one audit trail, which are viewable from the UNIFIED_AUDIT_TRAIL data dictionary view for single-instance installations or Oracle Database Real Application Clusters environments.

With Unified Auditing and Conditional Auditing, you can configure context-dependent logging to reduce performance overhead and enable more effective analysis of audit logs.

- Conditional Auditing's logging policies can minimize log entries to specific events, such as particular SQL statements that include CREATE or ALTER actions that originate from outside specific application servers.
- Unified Auditing lets you run analysis reports on an entire set of audit data in one operation. With a unified audit trail, the audit information is consistently formatted and contains consistent fields.

Configuration

For complete information about Oracle database auditing, see "Introduction to Auditing" (https://docs.oracle.com/database/121/DBSEG/auditing.htm#DBSEG1023) and "Configuring Audit Policies" (https://docs.oracle.com/database/121/DBSEG/audit_config.htm#DBSEG1025 in the Oracle Database Online Documentation 12c Release 1 *Database Security Guide*.

Install the SmartConnector

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

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

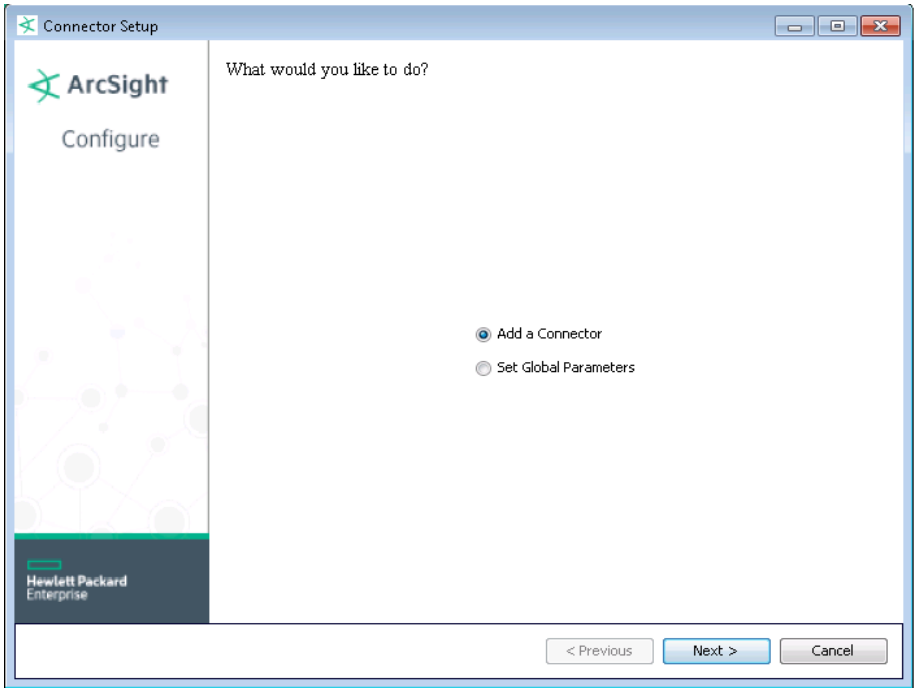
Install Core Software

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.

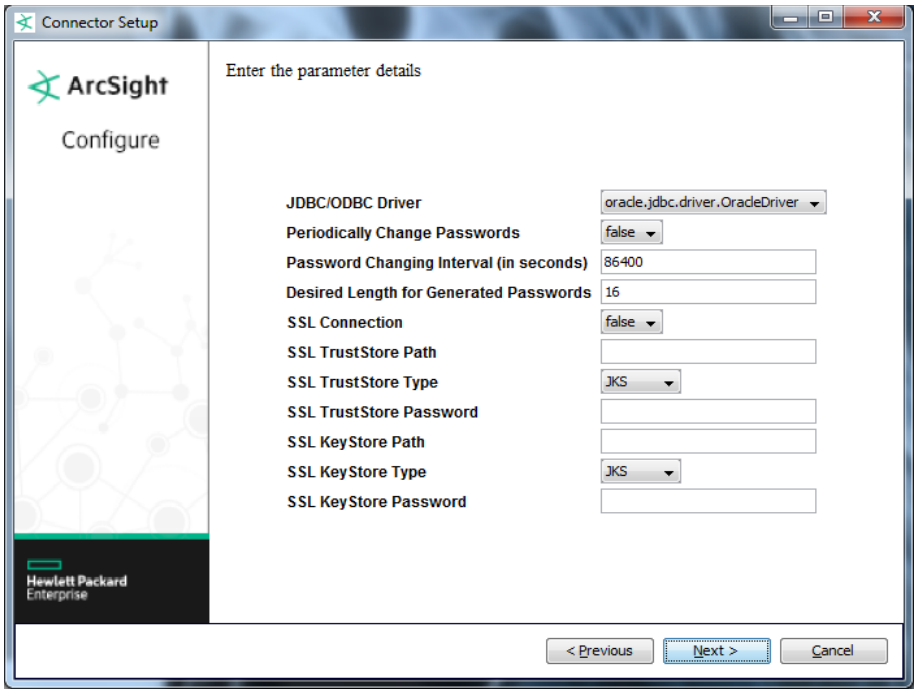
Parameter	Setting
Format Preserving Encryption	Data leaving the connector machine to a specified destination can be encrypted by selecting ‘Enabled’ to encrypt the fields identified in ‘Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of 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.

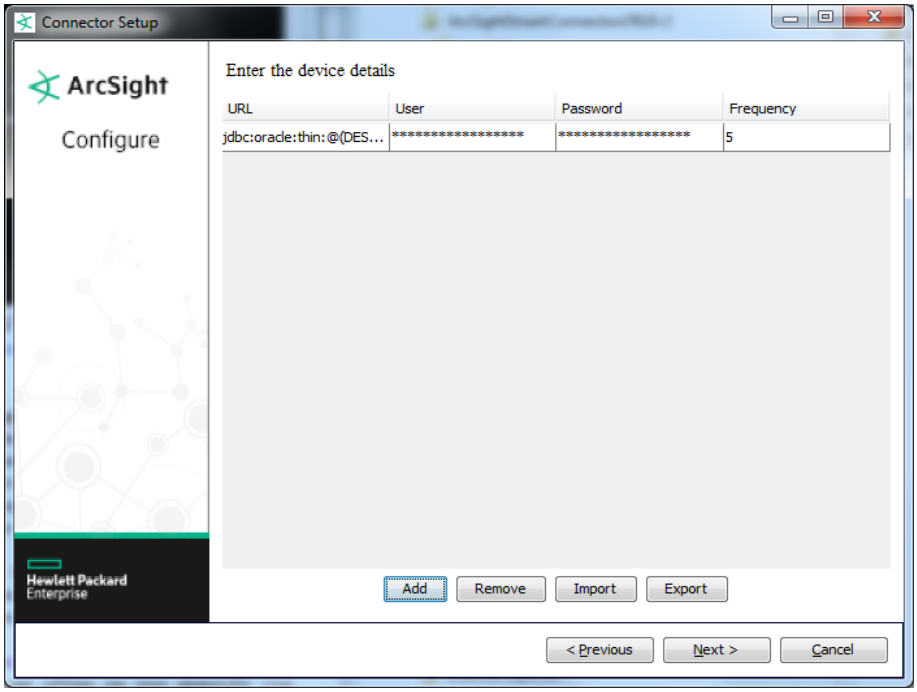
After making your selections, click **Next**. A summary screen is displayed. Review the summary of your selections and click **Next**. Click **Continue** to return to proceed with "Add a Connector" window. Continue the installation procedure with "Select Connector and Add Parameter Information."

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 Unified Audit Trail DB** and click **Next**.
3. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.

   Enter the parameters on the first window, then click 'Next' for the second parameter entry window.





If you have additional databases to add, click 'Add' again and click on the new row's boxes to change the values as needed to add the next database. To remove a row, select the row and click 'Remove.' When you have finished, click 'Next' to continue.

Parameter	Description
JDBC/ODBC Driver	Select a JDBC Database driver from the drop-down list or accept the default value. The default Oracle JDBC driver provided works with Oracle 9i, 10g, 11g and 12c database versions. If you are using Oracle 8i, see "Oracle 8i: Connector Upgrade" in the Configuration section of this guide.
Periodically Change Passwords	Select false or true from the drop-down list or accept the default value of false. This determines whether the password should be changed periodically once it logs on to the database
Password Changing Interval (in seconds)	If periodically change passwords is set to true, the password will be changed as often as you specify (in seconds), or you can accept the default value of 86400 (24 hours).
Desired Length for Generated Passwords	Specify the desired password length for generated passwords or accept the default value of 16.
SSL Connection	Default is 'false'. Change to 'true' for TCPS.
SSL TrustStore Path	Enter the absolute path for the truststore file.
SSL TrustStore Type	Select either JKS (default) or PKCS12 as needed.
SSL TrustStore Password	Enter password for the truststore.
SSL KeyStore Path	Enter the absolute path for the keystore file.
SSL KeyStore Type	Select either JKS (default) or PKCS12 as needed.
SSL KeyStore Password	Enter password for the keystore.
	Enter the following information for each database instance; click Add to see the default values:
URL	Enter the URL for the Oracle Database instance being audited in this field starting with the following URL template: jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=<HostName>)(PORT=1521))(CONNECT_DATA=(SERVICE_NAME=<sid>))). For example: 'jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS= (PROTOCOL=TCP) (HOST=x.x.x.x or hostname) (PORT=1521)) (CONNECT_DATA= (SERVICE_NAME=xxxx)))'
User	Enter the name of an Oracle database user having access the database instance.
Password	Enter the password for the Oracle database user.
Frequency	Enter how often, in seconds, the SmartConnector is to poll the Oracle database. The default value is 5.

You can click the 'Export' button to export the host name data you have entered into the table 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*.

Configure Start at Date (Optional)

When you want the connector to start at specific timestamps, the connector requires two timestamps as bind variables; therefore, two values for `startatdate` should be defined. To do this, before running the SmartConnector, open the `agent.properties` file (located at `$ARCSIGHT_HOME\current\user\agent`), and add a second value to the `startatdate` variable as shown in the following example.

For example, change:

```
agents[0].oracledatabases[0].startatdate=04/22/2011 14:40:40
```

to:

```
agents[0].oracledatabases[0].startatdate=04/22/2011 14:40:40,04/22/2011
14:40:40
```

Save your changes and continue with "Run the SmartConnector."

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 Unified Audit Trail 12c Database Field Mappings

ArcSight ESM Field	Device-Specific Field
Destination Address	One of (COMMENT_TEXT, HOST)
Destination Port	One of (COMMENT_TEXT, PORT)
Destination User Name	One of (USERNAME, TARGET_USER)
Destination User Privileges	One of (USED_PRIVILEGE, PRIVILEGE)
Device Action	ACTION_NAME
Device Custom Floating Point 1	SID (Session ID)
Device Custom Number 1	INSTANCEID
Device Custom Number 2	ERROR_CODE
Device Custom Number 3	ENTRYID
Device Custom String 1	COMMENT_TEXT
Device Custom String 2	GRANTEE (Privilege)
Device Custom String 3	POLICIES
Device Custom String 4	_DB_URL
Device Custom String 5	ACTION_OBJECT_NAME
Device Custom String 6	RULE_SET_NAME
Device Event Category	AUDIT_TYPE
Device Event Class ID	One of (ACTION, '|', RETURN_CODE)
Device External ID	DBID
Device Process Name	OS_PROCESS
Device Product	'Unified Audit Trail'
Device Vendor	'Oracle'
File ID	SQL_BINDS
File Name	One of (SCHEMA, OBJECT_NAME)
Message	One of (SQL_TEXT, DV_COMMENT)
Name	ACTION_NAME
Reason	RETURN_CODE
Source Address	One of (COMMENT_TEXT, HOST)
Source Port	One of (COMMENT_TEXT, PORT)

ArcSight ESM Field	Device-Specific Field
Source Service Name	TERMINAL
Transport Protocol	One of (COMMENT_TEXT, PROTOCOL)

Troubleshooting

Can I use JDBC with SSL to make a connection using TCPS protocol?

First, in the connector installation parameters screen, set the SSL connection to 'true'. Then, set other SSL-related parameters accordingly, including the truststore and keystore paths, types, and passwords. That information is available from your DB administrator.

Next, on the connector side, you need to add the connection URL with parameters:

jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=**TCPS**)(HOST=<server>)(PORT=<port>))(CONNECT_DATA=(SERVICE_NAME=<sid>)))

Note that in the DB connection URL, the value for PROTOCOL changes from 'TCP' to 'TCPS'.

You will also need to configure the connection on database server. Refer to Oracle documentation for information about that side of the connection.

I receive an SSL v3 error message when setting up the connector.

After entering the database connection information for TCPS in the Device Details screen, an error message might occur if your database connection uses the SSL v3 protocol. It will say: "Server chose SSL v3, but that protocol version is not enabled or supported by the client." This error message occurs because Oracle, for security reason, does not recommend using SSL v3.

HPE ArcSight does not recommend configuring your server to use SSLv3. If SSLv3 is required, enable SSLv3 in the connector JRE. Go to current\jre\lib\security, edit java.security, and comment out the line: `jdk.tls.disabledAlgorithms=SSLv3`

I receive Oracle error messages associated with a parser.

The connector parser oracle_unified_audit_trail.sdktbdatabase.properties results in Oracle errors:

- ORA-00942
- ORA-22835

To fix the ORA-00942 error:

- Grant read access on `sys.unified_audit_trails` to arcsight
- Grant select on `sys.all_audited_system_actions` to arcsight

To fix ORA-22835 (to limit the text fields size to 4000), the Oracle admin must add the two lines shown below to the following query:

```
SUBSTR(SQL_BINDS,1,4000) AS SQL_BINDS,
```

```
SUBSTR(SQL_TEXT,1,4000) AS SQL_TEXT,
```

The changes are shown in bold below.

```
CREATE OR REPLACE VIEW ARCSIGHT.UNIFIED_AUDIT_TRAIL
AS SELECT
ACTION_NAME, ADDITIONAL_INFO, APPLICATION_CONTEXTS,
       AUDIT_OPTION, AUDIT_TYPE, AUTHENTICATION_TYPE,
       CLIENT_IDENTIFIER, CLIENT_PROGRAM_NAME, DBID,
       .
       (Lines deleted for brevity)
       .
       RMAN_SESSION_STAMP, ROLE, SCN,
       SESSIONID,
       SUBSTR(SQL_BINDS,1,4000) AS SQL_BINDS,
       SUBSTR(SQL_TEXT,1,4000) AS SQL_TEXT,
       STATEMENT_ID, SYSTEM_PRIVILEGE, SYSTEM_PRIVILEGE_USED,
       TARGET_USER, TERMINAL, TRANSACTION_ID,
       .
       (Lines deleted for brevity)
       .
       XS_USER_NAME
FROM SYS.UNIFIED_AUDIT_TRAIL;
```