Micro Focus Security ArcSight Connectors

SmartConnector for Oracle Audit Vault DB

Configuration Guide

November 22, 2019

Configuration Guide

SmartConnector for Oracle Audit Vault DB

November 22, 2019

Legal Notices

Micro Focus

The Lawn

22-30 Old Bath Road

Newbury, Berkshire RG14 1QN

UK

https://www.microfocus.com.

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://community.microfocus.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Revision History

Date	Description
11/22/2019	Added new mappings for Oracle Audit Vault DB v 12.2.x.
10/17/2019	Added encryption parameters to Global Parameters.
10/17/2017	Added encryption parameters to Global Parameters.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
03/31/2015	Changed ArcSight field mapping from "Event Name" to "Name".
06/28/2013	Added support for v10.3.0.
11/15/2012	Removed section "Enable FIPS Mode" as Oracle driver does not support FIPS-enabled mode.
05/15/2012	Added new installation procedure.

SmartConnector for Oracle Audit Vault DB

This guide provides information for installing the SmartConnector for Oracle Audit Vault DB and configuring the device for event collection. Oracle Audit Vault versions 10.2 and 10.3 are supported.

Product Overview

Oracle Audit Vault is an enterprise-wide audit solution that consolidates, detects, monitors, alerts, and reports on audit data for security auditing and compliance. Oracle Audit Vault consolidates audit data and critical events into a centralized and secure audit warehouse.

Configuration

For complete information about Oracle Audit Vault, see the *Oracle Audit Vault Administrator's Guide* and the *Oracle Audit Vault Auditor's Guide*. The *Oracle Audit Vault Auditor's Guide* explains how Oracle Audit Vault auditors can use the Audit Vault Console to audit data in Oracle and Microsoft SQL Server databases. The *Oracle Audit Vault Administrator's Guide* provides usage information for Audit Vault administrators who perform administrative tasks on an Audit Vault system.

Oracle 8i: Connector Upgrade

With the addition of Oracle 11g support, ArcSight replaced the 10.2.0.1 oracle-jdbc driver in `$ARCSIGHT_HOME\current\lib\agent` with the oracle-jdbc-11.1.0.6.jar. This driver no longer connects to Oracle 8i databases; therefore, before upgrading the connector:

1. Go to $ARCSIGHT_HOME\Current\lib\agent and locate the oracle-jdbc-10.2.0.1.jar file. Copy it to a temporary location.

2. After completing connector upgrade and before running the connector, replace the 11.1.0.6.jar file with the 10.2.0.1.jar file.

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**

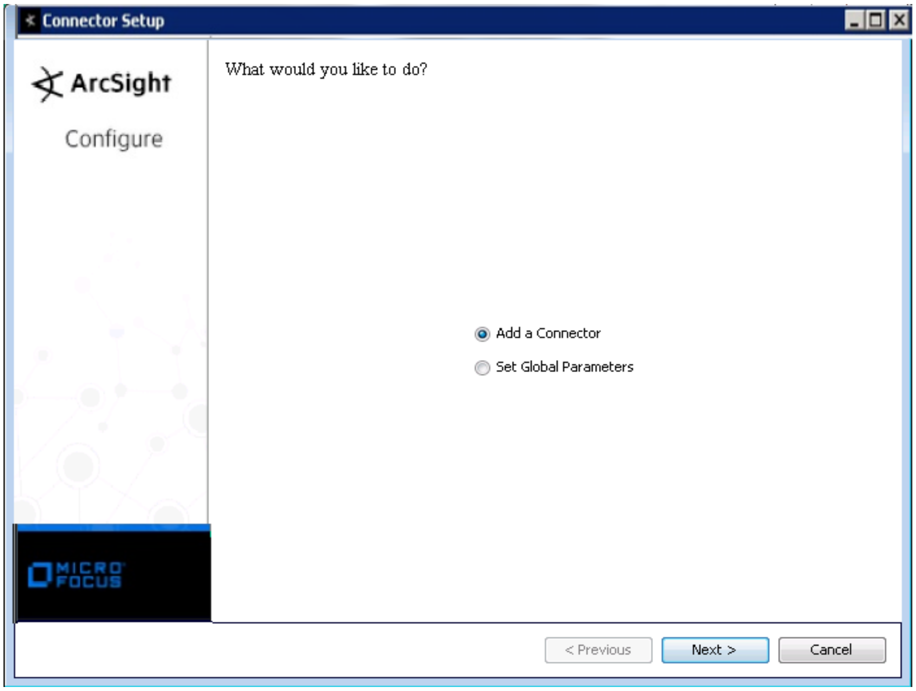
Install Core Software

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 Micro Focus SSO and Protect 724 sites.

1. **Download the SmartConnector executable for your operating system from the Micro Focus 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:**



What would you like to do?

● Add a Connector

○ Set Global Parameters

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 Micro Focus SecureData solutions to provide encryption. See the *Micro Focus 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 Micro Focus SecureData Server is installed.
Proxy Server (https)	Enter the proxy host for https connection if any proxy is enabled for this machine.

Parameter	Setting
Proxy Port	Enter the proxy port for https connection if any proxy is enabled for this machine.
Format Preserving Identity	The Micro Focus 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 Micro Focus SecureData.
Format Preserving Secret	Enter the secret configured for Micro Focus 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.

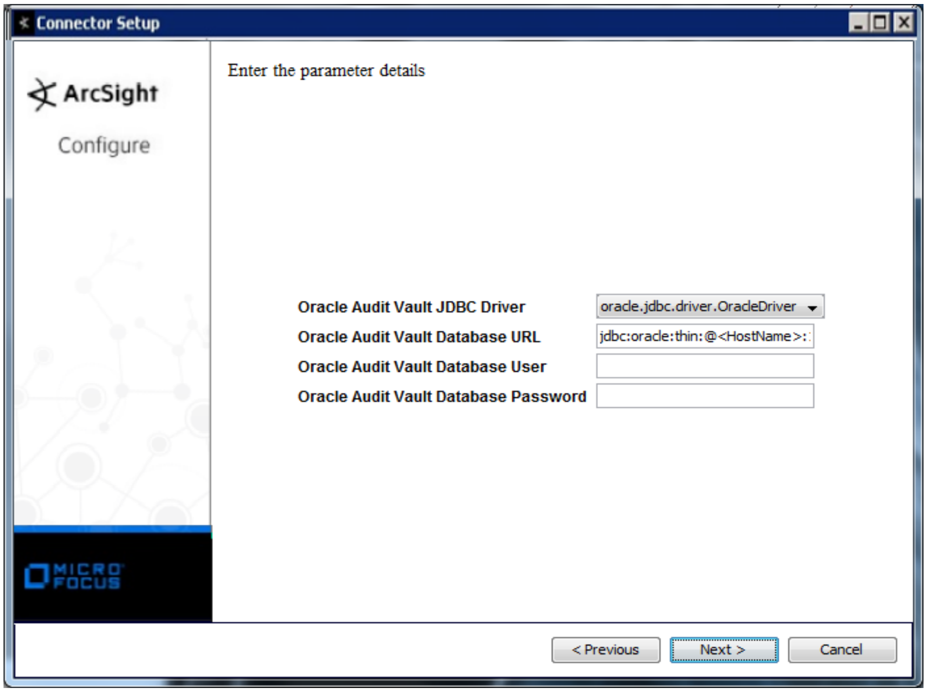
After making your selections, click Next. A summary screen is displayed. Review the summary of your selections and click Next. Click Continue to return to proceed with "Add a Connector" window. Continue the installation procedure with "Select Connector and Add Parameter Information."

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 Vault DB and click Next.

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



Enter the parameter details

Oracle Audit Vault JDBC Driver: oracle.jdbc.driver.OracleDriver
Oracle Audit Vault Database URL: jdbc:oracle:thin:@<HostName>:
Oracle Audit Vault Database User:
Oracle Audit Vault Database Password:

Parameter	Description
Oracle Audit Vault JDBC 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 8i, 10g, and 11g database versions. If you are using Oracle 8i, see "Oracle 8i: Connector Upgrade" in the Configuration section of this guide.
Oracle Audit Vault Database URL	Enter the URL for the Oracle Database instance being audited in this field (for example, 'jdbc:oracle:thin:@<hostname>:<port>:<sid>'). You can connect to a database in an RAC setup, using 'jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP) (SERVICE_NAME=DATABASE_SERVICENAME)))'. For example: 'jdbc:oracle:thin:@(DESCRIPTION= (ADDRESS LIST= (ADDRESS= (PROTOCOL=TCP) (HOST=x.x.x.x) (PORT=1521))) (CONNECT_DATA= (SERVICE_NAME=xxxx) (SERVER=DEDICATED)))'
Oracle Audit Vault Database User	Enter the name of an Oracle database user having access to the database instance.
Oracle Audit Vault Database Password	Enter the password for the Oracle Audit Vault database user.

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 Audit Vault DB Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Connector Severity	High = 2; Medium = 1
Destination Address	SOURCE_HOSTIP
Destination Host Name	SOURCE_HOST
Destination User Name	USERNAME
Device Custom Date 1	ALERTTIME
Device Custom Number 1	PROCESS#
Device Custom Number 2	EVENT_STATUS
Device Custom String 1	ALERTNAME
Device Custom String 2	SOURCE_NAME
Device Custom String 3	TARGET_OWNER
Device Custom String 4	_DB_URL

ArcSight ESM Field	Device-Specific Field
Device Custom String 5	OSUSER_NAME
Device Custom String 6	ALERTRULE
Device Event Class ID	All of (EVENT_ID,'|', EVENT_STATUS)
Device Host Name	_DB_HOST
Device Product	'Audit Vault'
Device Receipt Time	AVTIME
Device Severity	ALERT_SEVERITY
Device Vendor	'Oracle'
External ID	ALERT_SEQUENCE
File Name	TARGET_OBJECT
Message	One of (ALERTDESC, EVENTDESC)
Name	EVENT_NAME
Source Address	CLIENT_HOSTIP
Source Host Name	CLIENT_HOST

Oracle Audit Vault DB 12.2.x Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Destination Address	HOST_IP
Destination Host Name	HOST_NAME
Destination User Name	TARGET_OWNER
Device Action	ACTION_TAKEN
Device Custom Date 1	ALERTTIME
Device Custom Number 1	ALERT_RAISED;
Device Custom Number 2	MONITORING_POINT_ID
Device Custom String 1	ALERT_NAME
Device Custom String 2	SECURED_TARGET_NAME
Device Custom String 3	SECURED_TARGET_TYPE
Device Custom String 4	THREAT_SEVERITY
Device Custom String 5	POLICY_NAME
Device Custom String 6	ALERT_RULE
Device Event Category	LOG_CAUSE
Device Event Class ID	(EVENT_NAME,"|",EVENT_STATUS)
Device Host Name	_DB_HOST
Device Product	Audit Vault and Database Firewall
Device Receipt Time	AV_ALERT_TIMESTAMP
Device Severity	ALERT_SEVERITY
Device Vendor	Oracle
Event Outcome	EVENT_STATUS
File Name	TARGET_OBJECT
File Type	TARGET_TYPE
Message	(DESCRIPTION,"|",ERROR_MESSAGE)
Name	EVENT_NAME

ArcSight ESM Field	Device-Specific Field
Reason	ERROR_CODE
Request Client Application	CLIENT_PROGRAM
Request Context	COMMAND_PARAM
Request Cookies	_DB_URL
Request Method	COMMAND_CLASS
Request Url	COMMAND_TEXT
Source User Privileges	USER_NAME
Start Time	EVENT_TIME