



# **Micro Focus Security ArcSight Connectors**

## **SmartConnector for Oracle Audit DB**

### **Configuration Guide**

**January 25, 2019**

## Configuration Guide

### SmartConnector for Oracle Audit DB

January 25, 2019

Copyright © 2004 – 2017; 2018 Micro Focus and its affiliates and licensors.

### 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.

### 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.

### Revision History

---

| Date       | Description   |
|------------|---|
| 01/25/2019 | Added step to the section "Create a Unique Tablespace for the Audit Table".   |
| 10/17/2017 | Added encryption parameters to Global Parameters.   |
| 05/15/2017 | Updated Troubleshooting information regarding TCPS and SSL v3 support.  |
| 02/15/2017 | Corrected path to sample scripts.   |
| 11/30/2016 | Updated installation procedure for setting preferred IP address mode.   |
| 11/17/2015 | Added information to Troubleshooting section. Updated information about configuring TCPS and using SSL v3 connections in Troubleshooting section. |
| 03/31/2015 | Added support for TCPS and updated parameters. Added information about configuring TCPS and using SSL v3 connections in Troubleshooting section.  |
| 03/31/2014 | Added support for SQL bind mappings.  |
| 02/14/2014 | Added support for v12cR1. Updated parameter screen image.   |
| 02/15/2013 | Added mappings for IPv6.  |

---

---

## SmartConnector for Oracle Audit DB

---

This guide provides information for installing the SmartConnector for Oracle Audit DB and configuring the device for event collection. Oracle Database Versions 8i, 9i, 10g, 11g, 11gR2, and 12cR1 are supported.

### 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.

### Log In and View Audit Parameters

The Oracle Database must be configured before SmartConnector installation as detailed in the following sections.

1 Login to the machine where the Oracle database is running.

2 Run **sqlplus** and connect as **sysdba**:

```
sqlplus /nolog
```

At the sqlplus prompt (SQL>), enter:

```
connect logon as sysdba
```

You will then be asked to enter a password.

Alternatively, log in as usual to sqlplus (not as sysdba) and at the prompt, enter:

```
connect sys/<password> as sysdba
```

3 View the audit parameters by entering the following command at the sqlplus prompt: **show parameter audit**. You will see output such as the following:

| Name            | Type   | Value                            |
|-----------------|--------|----------------------------------|
| audit_file_dest | string | /opt/app/oracle/admin/orcl/adump |

| Name                 | Type    | Value |
|----------------------|---------|-------|
| audit_sys_operations | boolean | FALSE |
| audit_syslog_level   | string  |       |
| audit_trail          | string  | NONE  |

- 4 If the value of the **audit\_trail** parameter is NONE as shown in the previous example, modify the value to **db** for versions prior to 10.x and **db,extended** for versions 10.x, 11.x and 12.x. You can do this by running one of the SQL scripts included with this connector. You can find it in:

ARCSIGHT\_HOME/current/agent/config/oracle\_db



These scripts work only when spfile already exists. Create this file prior to running the following scripts. Also, be aware that running these scripts results in the database shutting down.

For Oracle versions prior to 10.x, the script is [enableOracleAuditTrail.sql](#)

```
PROMPT -----;
PROMPT -- Enable audit_trail in DB mode, and
PROMPT -- Restart the database.
PROMPT -----;

ALTER SYSTEM SET audit_sys_operations=TRUE scope=spfile;
ALTER SYSTEM SET audit_trail=db scope=spfile;
CREATE pfile FROM spfile;
SHUTDOWN IMMEDIATE;
STARTUP;
QUIT;
```

For Oracle versions 10.x, 11.x, and 12.x, the script is [enableOracleAuditTrail10g.sql](#).

```
PROMPT -----;
PROMPT -- Enable audit_trail in DB mode, and
PROMPT -- Restart the database.
PROMPT -----;

ALTER SYSTEM SET audit_sys_operations=TRUE scope=spfile;
ALTER SYSTEM SET audit_trail=db,extended scope=spfile;
CREATE pfile FROM spfile;
SHUTDOWN IMMEDIATE;
STARTUP;
QUIT;
```

A script for disabling auditing is also provided. The script is [DisableOracleAuditTrail.sql](#).

```
PROMPT -----;
PROMPT -- Disable audit_trail in DB mode, and
PROMPT -- Restart the database.
PROMPT -----;

alter system set audit_trail=NONE scope=SPFILE;

create pfile from spfile;

Shutdown immediate;

Startup;

quit;
```

## Grant Oracle Audit DB User Privileges

Following is an example of granting select privileges to a new Oracle user, *thinuser*. You must be connected as *sysdba* to run these commands.

```
SQL> create user thinuser identified by <password>;
SQL> grant connect to thinuser;
SQL> alter user thinuser account unlock;

SQL> grant select on sys.dba_audit_trail to thinuser;
SQL> grant select on sys.v_$instance to thinuser;
SQL> grant select on sys.audit$ to thinuser;
SQL> grant select any dictionary to thinuser;
```

If the connector just needs *sys.dba\_audit\_trail*, *sys.v\_\$instance*, and *sys.audit\$*, there is no need to give the oracle user full privileges to view the entire Oracle Data Dictionary.



For Oracle 10g, 11g, and 12c also grant select privileges on *sys.dba\_common\_audit\_trail* table to the SmartConnector Oracle user.

## Enable Auditing Processes

To enable Oracle auditing processes, the following scripts are provided in the [ARCSIGHT\\_HOME/current/agent/config/oracle\\_db](#) directory.



Micro Focus Security ArcSight strongly recommends that you execute the Oracle auditing scripts with the assistance of an Oracle DBA. These scripts require SYSDBA permissions using *sqlplus*.

### [oracleAuditing.sql](#)

This script is used to enable specific items to be audited. Only use this if you really understand what these different auditing recommendations mean in your environment.

### [oracleMoveAudit.sql](#)

This script is used to move the audit table that holds Oracle auditing events to a newly

created tablespace. This is necessary because the current location of the audit table is in the sys tablespace and it will fill and crash the database. Please MODIFY the path for the new datafiles as well as the size.

#### [createTruncatePackage.sql](#)

This script is used to create a procedure that will truncate the audit table. Only use this if you really want to remove all the events from this table on a scheduled basis. This should be run before [scheduleTruncate.sql](#).

#### [scheduleTruncate.sql](#)

This script is used to schedule the previously created procedure. Only use this if you really want to remove all the events from this table on a scheduled basis. This should be run after [createTruncatePackage.sql](#).



The SmartConnector for Oracle Audit does not log sysdba login/logout behavior. There is a SmartConnector for Oracle SYSDBA Audit to support this logging. To provide a full audit solution for Oracle, install both the SmartConnector for Oracle Audit and the SmartConnector for Oracle SYSDBA Audit.

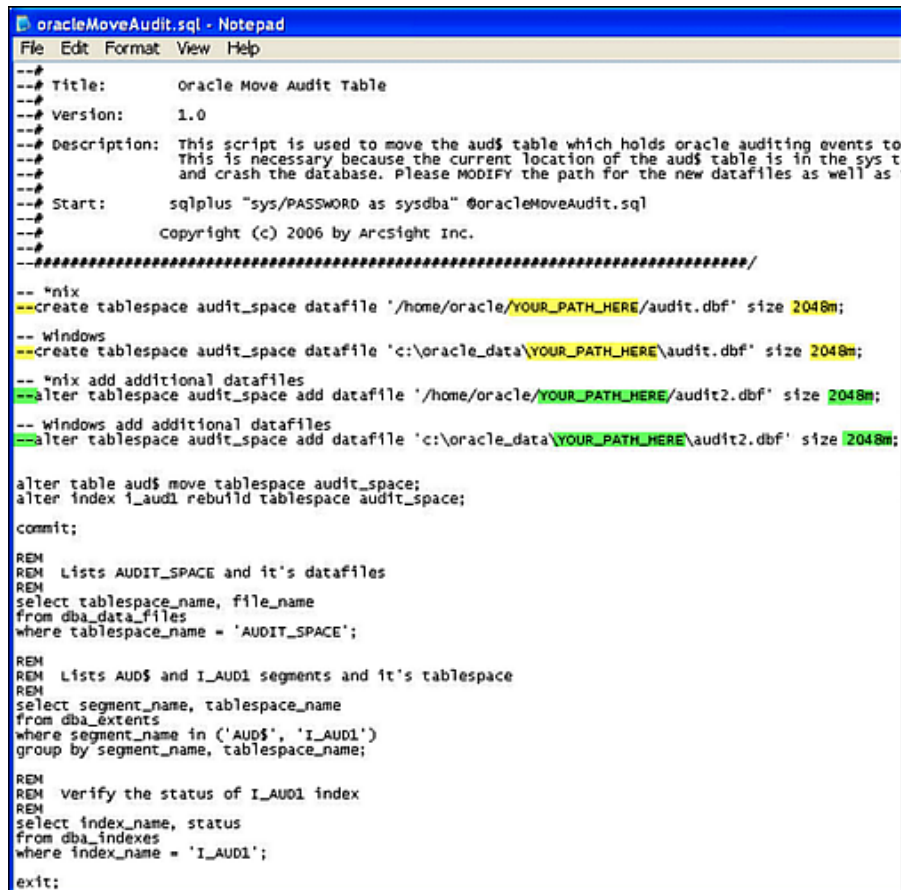
---

## Create a Unique Tablespace for the Audit Table

The first process creates a separate tablespace just for auditing. The Oracle audit table is stored in sys table space. Because Oracle generates a lot of audit messages, this fills up the audit table, which can cause the database to crash.

To avoid this problem, move the Oracle audit table into its own table space with its own data files separate from the core Oracle tables.

- 1 From a command prompt, change directory to [ARCSIGHT\\_HOME/current/agent/config/oracle\\_db](#).
- 2 Make a backup copy of the file [oracleMoveAudit.sql](#).
- 3 In a text editor, open the original file [oracleMoveAudit.sql](#) and do the following:
  - a Un-comment the [create tablespace](#) line appropriate for your operating system (by removing the two hyphens (--) as shown highlighted in yellow in the figure) and replacing [YOUR\\_PATH\\_HERE](#) with the new path to where you want your Oracle datafile to be located. As an option, you can also change the default size of 2048m.
  - b As an option, you can add additional data files if you want to extend the tablespace by uncommenting the [alter tablespace](#) line appropriate for your operating system (by removing the two hyphens (--) as shown highlighted in green in the figure) and replacing [YOUR\\_PATH\\_HERE](#) with the new path to where you want your additional Oracle datafile to be located. You also can change the default size of 2048m.
  - c Save and close the file.



```

--# Title:      Oracle Move Audit Table
--# Version:    1.0
--# Description: This script is used to move the aud$ table which holds oracle auditing events to
--#              This is necessary because the current location of the aud$ table is in the sys t
--#              and crash the database. Please MODIFY the path for the new datafiles as well as
--# Start:      sqlplus "sys/PASSWORD as sysdba" @oracleMoveAudit.sql
--# Copyright (c) 2006 by ArcSight Inc.
--#####/

-- *nix
--create tablespace audit_space datafile '/home/oracle/YOUR_PATH_HERE/audit.dbf' size 2048m;
-- windows
--create tablespace audit_space datafile 'c:\oracle_data\YOUR_PATH_HERE\audit.dbf' size 2048m;
-- *nix add additional datafiles
--alter tablespace audit_space add datafile '/home/oracle/YOUR_PATH_HERE/audit2.dbf' size 2048m;
-- windows add additional datafiles
--alter tablespace audit_space add datafile 'c:\oracle_data\YOUR_PATH_HERE\audit2.dbf' size 2048m;

alter table aud$ move tablespace audit_space;
alter index i_aud1 rebuild tablespace audit_space;

commit;

REM
REM Lists AUDIT_SPACE and it's datafiles
REM
select tablespace_name, file_name
from dba_data_files
where tablespace_name = 'AUDIT_SPACE';

REM
REM Lists AUD$ and I_AUD1 segments and it's tablespace
REM
select segment_name, tablespace_name
from dba_extents
where segment_name in ('AUD$', 'I_AUD1')
group by segment_name, tablespace_name;

REM
REM Verify the status of I_AUD1 index
REM
select index_name, status
from dba_indexes
where index_name = 'I_AUD1';

exit;

```

- 4 To run the script, at the command prompt, enter the following command:

```
sqlplus "sys/<your sys password> as sysdba"
@oracleMoveAudit.sql
```

The operation is successful when you see the tablespace name and audit space name displayed successfully.

Some databases do not have I\_AUD1 index for table audits. If the error "does not existing index i\_aud1" pops, follow these steps to create the index manually:

- 1 Comment the "create tablespace" line.
- 2 Comment the "alter table space" line.
- 3 Add the following query after the "alter tablespace" line: "create index I\_AUD1 on aud\$ (sessionid, ses\$tid) tablespace audit\_space;"
- 4 Save the file and re-run the script.

## Configure Audit Options

The next process tells Oracle the exact statements and actions to audit.

- 1 From a command prompt, change directory to:  
  
ARCSIGHT\_HOME/current/agent/config/oracle\_db
- 2 Make a backup of the file `oracleAuditing.sql`.
- 3 In a text editor, open the original `oracleAuditing.sql` and evaluate the default options and configure them so they are appropriate for your environment.
- 4 Configure the recommended auditing statements. By default, all the recommended auditing statements are enabled. To disable any that you do not want to audit, comment them out by adding two hyphens to the beginning of the line, as indicated by the red arrow in the figure.

```

oracleAuditing.sql - Notepad
File Edit Format View Help
--#
--# Title:      Enable oracle Auditing
--#
--# Version:    1.0
--#
--# Description: This script is used to enable specific things to be audited
--#              Only use this if you really understand what these different auditing
--#              mean in your environment
--#
--# Start:      sqlplus "sys/PASSWORD as sysdba" @oracleAuditing.sql
--#
--# Copyright (c) 2006 by ArcSight Inc.
--#
--#####/
-- Insider Threat Solution Package Recommended Auditing Statements for Oracle.

audit all;
audit session;
-- audit session whenever not successful;
audit ALTER TABLE;
audit DELETE TABLE;
audit GRANT DIRECTORY;
audit GRANT PROCEDURE;
audit GRANT SEQUENCE;
audit GRANT TABLE;
audit ALTER ANY ROLE;
audit SELECT ANY TABLE;
audit ALTER USER;
audit GRANT ANY ROLE;
audit GRANT ANY PRIVILEGE;
audit INSERT ANY TABLE;
audit UPDATE ANY TABLE;
audit CREATE TABLE;
audit CREATE USER;
audit INSERT TABLE by system by access;
audit SELECT TABLE by system by access;
audit UPDATE TABLE by system by access;
audit UPDATE, INSERT, DELETE, SELECT on sys.DBA_USERS by ACCESS;
audit UPDATE, DELETE on sys.AUD$ by ACCESS;

-- Be cautious auditing all selects, deletes, and inserts on database tables with high
-- Be sure you have a DBA assist with this.

-- audit SELECT, INSERT, DELETE, UPDATE on user.table_name by ACCESS;
-- audit SELECT on user.table_name by ACCESS;
-- audit INSERT on user.table_name by ACCESS;
-- audit DELETE on user.table_name by ACCESS;
-- audit UPDATE on user.table_name by ACCESS;
-- audit SELECT TABLE by user_name;
-- audit INSERT TABLE by user_name;
-- audit UPDATE TABLE by user_name;
-- audit DELETE TABLE by user_name;
-- audit UPDATE TABLE, SELECT TABLE, DELETE TABLE, INSERT TABLE by user_name, user_name;

commit;
exit;

```

Micro Focus Security ArcSight recommends auditing SELECTS, UPDATES, INSERTS to critical tables, such as salary info, credit card info, patient info, financial data, national secrets, intellectual property, and so on.





DO NOT audit things that are accessed regularly by automated accounts. These automated actions can flood the audit logs. Also, be cautious when auditing SELECTS, INSERTS, and DELETES on databases with high transaction rates. They will fill up the ADM\$ table in the sys tablespace, which causes database failure.

As an option, you can configure the `user.table_name` with the name of the table for which you want to enable auditing for that action (as shown highlighted in yellow in the figure). To activate the user table line, uncomment it by removing the two hyphens (--) at the head of the line.

You also can configure `user_name` with the names of users whose specific actions you want to audit (as shown highlighted in yellow in the figure). To activate the user\_name line, uncomment it by removing the two hyphens (--) at the head of the line.

- 5 Save and close the file.
- 6 To verify that the settings you made are correct, test them on a non-production system. For example, log in as one of the users you want to audit, do the action you want to audit, and see whether the action is displayed in the audit log.
- 7 Run the script at command prompt from the `ARCSIGHT_HOME/current/agent/config/oracle_db` directory:

```
Sqlplus "sys/<your password here> as sysdba"
@oracleAuditing.sql
```

The operation is successful when you see the message **Audit succeeded**.

## Truncate Oracle Audit Logs

After auditing is enabled for some time, the security administrator may want to delete records from the database audit trail, both to free audit trail space and to facilitate audit trail management.

To accomplish this optional housekeeping feature, the SmartConnector for Oracle Audit DB includes a truncate script that truncates (clears) the auditing table, and another script to run the truncate procedure on a regular schedule.



This step deletes items from the audit table. Although Micro Focus Security ArcSight maintains a record of all events for the configured retention period, if you must maintain records of every transaction for auditors, you should probably not perform this step. Only the user SYS, a user with the DELETE ANY TABLE privilege, or a user to whom SYS has granted DELETE privilege on SYSAUD\$ can delete records from the database audit trail.

## Create a Truncate Package

This script creates a truncate procedure, which tells the database to truncate the audit table.

- 1 From a command prompt, change directory to:

```
ARCSIGHT_HOME/current/agent/config/oracle_db
```

- 2 At the command prompt, enter:

```
Sqlplus "sys/<your password here> as sysdba"  
@createTruncatePackage.sql
```

For example, if your sysdba password is mypassword, enter:

```
Sqlplus "sys/mypassword as sysdba"  
@createTruncatePackage.sql
```

The operation is successful when you see the output Procedure created.

## Schedule a Truncate Procedure

This script schedules the truncate procedure that we created in the previous step. By default, the procedure is scheduled to run at 2:00 a.m. local system time.

- 1 At the command prompt, enter:

```
Sqlplus "sys/<your password here> as sysdba"  
@scheduleTruncate.sql
```

- 2 Once the schedule script has been run, check the database to ensure that the `job_queue_prcoesses` parameter is set correctly to run scheduled jobs.

At a command prompt, enter `sqlplus "sys as sysdba"`

Next, run `show parameter job`. The output will look like this. The number at the end indicates the job queue process setting.

| NAME                | TYPE    | VALUE |
|---------------------|---------|-------|
| -----               | -----   | ----- |
| ---                 |         |       |
| job_queue_processes | integer | 0     |

- 3 If the job queue process setting is 0, it means there are no queue processes and no jobs will run. If this is the case, then run the following (this should be done by an Oracle DBA):

```
alter system set job_queue_processes=2;  
create pfile from spfile;
```

This sets the job queue processes to 2.

## Oracle 8i: Connector Upgrade

With the addition of Oracle 11g support, Micro Focus Security 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

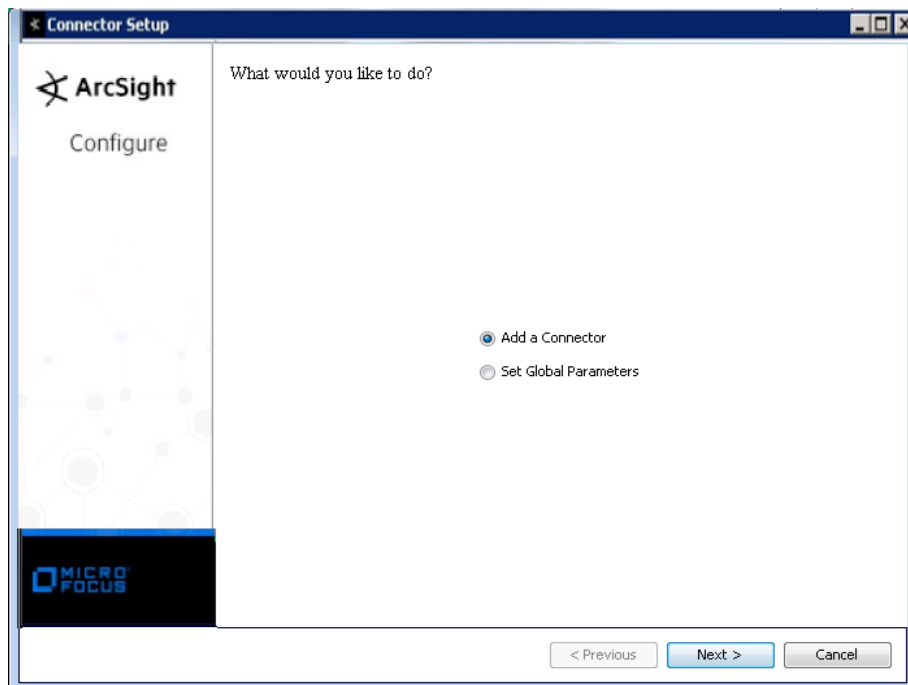
Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the Micro Focus SSO and Protect 724 sites.

- 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:



### 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.

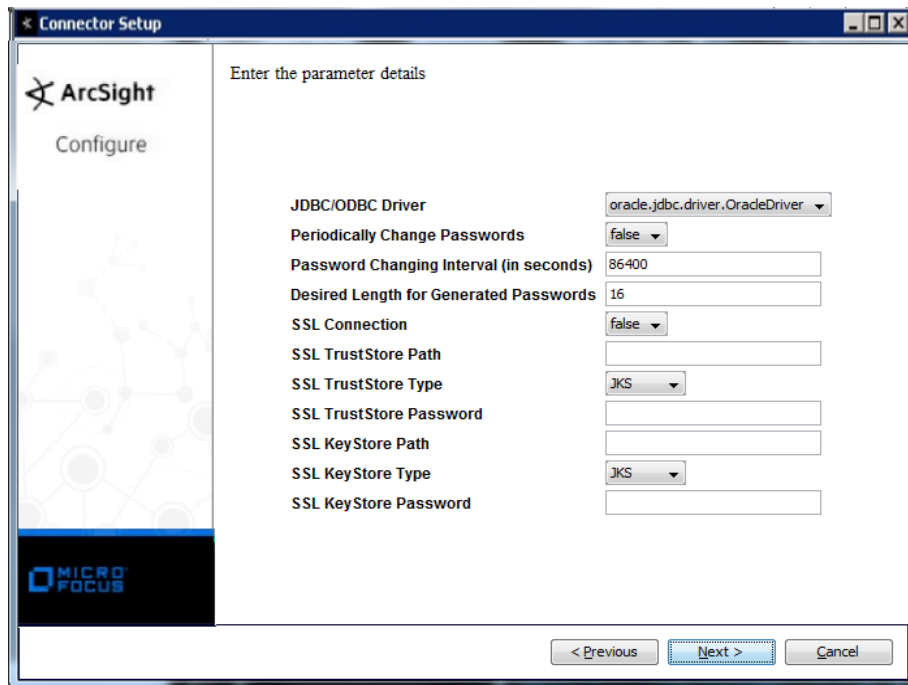
| Parameter                    | Setting  |
|------------------------------|--|
| Format Preserving Encryption | Data leaving the connector machine to a specified destination can be encrypted by selecting 'Enabled' to encrypt the fields identified in 'Event Fields to Encrypt' before forwarding events. 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.  |
| 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 DB** and click **Next**.
- 3 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.

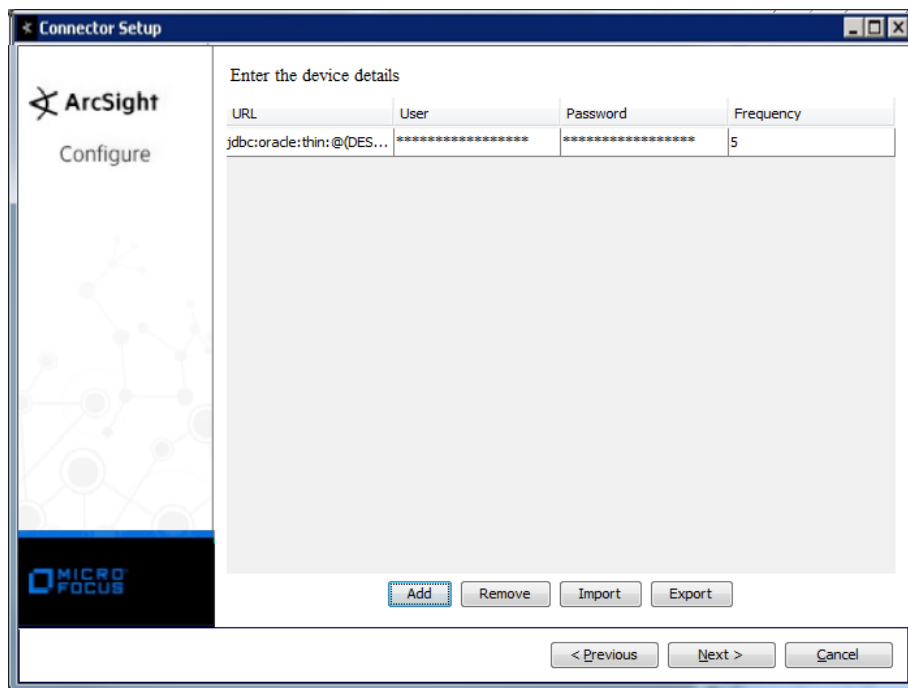
Enter the parameters on the first window, then click Next for the second parameter entry window. Click Add for default values to be entered.



The screenshot shows the 'Connector Setup' window with the 'Enter the parameter details' tab selected. The window includes the ArcSight logo and a 'Configure' button. The settings are as follows:

| Parameter                               | Value                           |
|---|---------------------------------|
| JDBC/ODBC Driver                        | oracle.jdbc.driver.OracleDriver |
| Periodically Change Passwords           | false                           |
| Password Changing Interval (in seconds) | 86400                           |
| Desired Length for Generated Passwords  | 16                              |
| SSL Connection                          | false                           |
| SSL TrustStore Path                     |                                 |
| SSL TrustStore Type                     | JKS                             |
| SSL TrustStore Password                 |                                 |
| SSL KeyStore Path                       |                                 |
| SSL KeyStore Type                       | JKS                             |
| SSL KeyStore Password                   |                                 |

Navigation buttons at the bottom: < Previous, Next >, Cancel.



The screenshot shows the 'Connector Setup' window with the 'Enter the device details' tab selected. The window includes the ArcSight logo and a 'Configure' button. A table lists the device details:

| URL                      | User  | Password | Frequency |
|--------------------------|-------|----------|-----------|
| jdbc:oracle:thin:@DES... | ***** | *****    | 5         |

Buttons at the bottom: Add, Remove, Import, Export. Navigation buttons at the bottom: < Previous, Next >, Cancel.

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. When you have finished adding databases, click Next to continue.

| Parameter                               | Description  |
|---|--|
| 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 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.   |
|   | Enter the following information for each database instance; click Add to see the default values:   |
| 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.   |
| URL                                     | Enter the URL for the Oracle Database instance being audited in this field starting with the following URL template:<br><br>jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP) (HOST=<HostName>)(PORT=1521)) (CONNECT_DATA=(SERVICE_NAME=<sid>)))<br><br>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.  |

## 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 10.g/11.g/12.c Database Field Mappings

| ArcSight ESM Field           | Device-Specific Field   |
|------------------------------|---|
| Agent (Connector) Severity   | Very High = 1034, 12154, 12203, 12224, 12545; High = 1, 942, 1000, 1013, 4043; Medium = 2..941, 943..999, 1001, 1012, 1014..1033, 1035..4042, 4044..12153, 12155..12202, 28009; Low = 0 |
| Destination Host Name        | HOST_NAME   |
| Destination Service Name     | ACTION_NAME   |
| Destination User Name        | USERNAME  |
| Destination User Privileges  | PRIV_USED   |
| Device Action                | ACTION  |
| Device Custom IPv6 Address 2 | Source IPv6 Address   |
| Device Custom Number 1       | STATEMENTID   |
| Device Custom Number 2       | SID (SESSION_ID)  |
| Device Custom String 1       | COMMENT_TEXT  |
| Device Custom String 2       | TERMINAL  |
| Device Custom String 3       | OWNER   |
| Device Custom String 4       | Database URL  |
| Device Custom String 5       | SES_ACTIONS   |
| Device Custom String 6       | GRANTEE   |
| Device Event Class Id        | ACTION plus RETURNCODE  |
| Device External Id           | _DB_NAME  |
| Device Host Name             | _DB_HOST  |
| Device Product               | 'Oracle'  |
| Device Receipt Time          | One of (LOGOFF_TIME, TIMESTAMP)   |
| Device Vendor                | 'ORACLE'  |
| Device Version               | VERSION   |
| Event Outcome                | One of (Success, Failure)   |
| File ID                      | SQL_BIND  |

| ArcSight ESM Field | Device-Specific Field              |
|--------------------|------------------------------------|
| File Name          | OBJ_NAME                           |
| Message            | SQL_TEXT                           |
| Name               | ACTION_NAME                        |
| Reason             | RETURNCODE                         |
| Source Address     | Extract HOST from COMMENT_TEXT     |
| Source Host Name   | USERHOST                           |
| Source Port        | Extract PORT from COMMENT_TEXT     |
| Source User Name   | OS_USERNAME                        |
| Transport Protocol | Extract PROTOCOL from COMMENT_TEXT |

## Oracle 9.x Database Field Mappings

| ArcSight ESM Field          | Device-Specific Field   |
|-----------------------------|---|
| Agent (Connector) Severity  | Very High = 1034, 12154, 12203, 12224, 12545; High = 1, 942, 1000, 1013, 4043; Medium = 2..941, 943..999, 1001, 1012, 1014..1033, 1035..4042, 4044..12153, 12155..12202, 28009; Low = 0 |
| Destination Host Name       | HOST_NAME   |
| Destination User Name       | USERNAME  |
| Destination User Privileges | PRIV_USED   |
| Detect Time                 | One of (LOGOFF_TIME, TIMESTAMP)   |
| Device Address              | EngineIP  |
| Device Custom String 1      | COMMENT_TEXT  |
| Device Custom String 3      | OWNER   |
| Device Custom String 5      | SES_ACTIONS   |
| Device Custom String 6      | GRANTEE   |
| Device Event Class Id       | ACTION plus RETURNCODE  |
| Device External Id          | _DB_NAME  |
| Device Host Name            | _DB_HOST  |
| Device Product              | 'Oracle'  |
| Device Vendor               | 'ORACLE'  |
| Device Version              | VERSION   |
| Event Name                  | ACTION_NAME   |
| Event Outcome               | One of (Success, Failure)   |
| File Name                   | OBJ_NAME  |
| Reason                      | RETURNCODE  |
| Service                     | ACTION_NAME   |
| Source Host Name            | TERMINAL  |
| Source User Id              | OS_USERNAME   |
| Source User Name            | OS_USERNAME   |

## Troubleshooting

### Why does connection fail when using JDBC driver?

There is a known Oracle BUG:6051243 that causes our connectors to fail to establish a connection using the JDBC driver when the sqlnet.ora file contains the entry "SQLNET.ALLOWED\_LOGON\_VERSION=10." The workaround is to use =8 in the sqlnet.ora file, or download patch:67790.

### **Why are portions of the raw event truncated?**

Different UNIX operating systems implement the syslog() call in different ways. This results in Oracle audit records to be written in different formats. For raw audit events from Oracle with ACTION fields, the connector can parse only the first message into a Micro Focus Security ArcSight event. The truncated portions of the raw event will be missing.

### **Why don't I see any events when I start the Audit DB Connector?**

Make sure that the Audit\_DB is on (as described above), then login as the user you specified in the Configuration Wizard. Start sqlplus using this name and password:

```
Sqlplus username/password
```

Execute the following query:

```
select * from dba_audit_trail
```

If the query result displays events, your structure is okay. Now trigger something that you are auditing (for instance, the Audit Session example described above).

### **I understand less information is captured using audit\_trail db rather than audit\_trail db,extended, but will the connector recognize the Oracle 10g logs using audit\_trail db without the 'extended'?**

Yes, audit\_trail db mode can be used, but the event.message field will be empty because the DB column SQL\_TEXT will not be populated. This column stores the actual SQL query that triggered the audits and will be populated only in the 'db,extended' mode. Using audit\_trail db mode can save some processor cycles that would otherwise be used for storing two character large objects (2000 characters each) for SQL-TEXT and SQL\_BIND.

### **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. Use TLS 1.2

## Action Codes

The field event.deviceEventClassId is the concatenation of the action and the return code. For example, a successful login will be 100|0. A failed login will be 100|1017. The detailed action code/name mapping is shown below (after **Severity Event Mapping**). The logon and logoff codes (100 logon and 101 logoff) are of special interest whether the return code indicates success or failure.

- 1 CREATE TABLE
- 2 INSERT
- 3 SELECT
- 4 CREATE CLUSTER
- 5 ALTER CLUSTER
- 6 UPDATE
- 7 DELETE
- 8 DROP CLUSTER
- 9 CREATE INDEX
- 10 DROP INDEX
- 11 ALTER INDEX
- 12 DROP TABLE
- 13 CREATE SEQUENCE
- 14 ALTER SEQUENCE
- 15 ALTER TABLE
- 16 DROP SEQUENCE
- 17 GRANT OBJECT
- 18 REVOKE OBJECT
- 19 CREATE SYNONYM
- 20 DROP SYNONYM
- 21 CREATE VIEW
- 22 DROP VIEW
- 23 VALIDATE INDEX
- 24 CREATE PROCEDURE
- 25 ALTER PROCEDURE
- 26 LOCK
- 27 NO-OP
- 28 RENAME
- 29 COMMENT
- 30 AUDIT OBJECT
- 31 NOAUDIT OBJECT
- 32 CREATE DATABASE LINK
- 33 DROP DATABASE LINK

34 CREATE DATABASE  
35 ALTER DATABASE  
36 CREATE ROLLBACK SEG  
37 ALTER ROLLBACK SEG  
38 DROP ROLLBACK SEG  
39 CREATE TABLESPACE  
40 ALTER TABLESPACE  
41 DROP TABLESPACE  
42 ALTER SESSION  
43 ALTER USER  
44 COMMIT  
45 ROLLBACK  
46 SAVEPOINT  
47 PL/SQL EXECUTE  
48 SET TRANSACTION  
49 ALTER SYSTEM  
50 EXPLAIN  
51 CREATE USER  
52 CREATE ROLE  
53 DROP USER  
54 DROP ROLE  
55 SET ROLE  
56 CREATE SCHEMA  
57 CREATE CONTROL FILE  
59 CREATE TRIGGER  
60 ALTER TRIGGER  
61 DROP TRIGGER  
62 ANALYZE TABLE  
63 ANALYZE INDEX  
64 ANALYZE CLUSTER  
65 CREATE PROFILE  
66 DROP PROFILE  
67 ALTER PROFILE  
68 DROP PROCEDURE  
70 ALTER RESOURCE COST  
71 CREATE SNAPSHOT LOG  
72 ALTER SNAPSHOT LOG  
73 DROP SNAPSHOT LOG  
74 CREATE SNAPSHOT  
75 ALTER SNAPSHOT  
76 DROP SNAPSHOT  
77 CREATE TYPE  
78 DROP TYPE  
79 ALTER ROLE  
80 ALTER TYPE  
81 CREATE TYPE BODY  
82 ALTER TYPE BODY  
83 DROP TYPE BODY  
84 DROP LIBRARY

85 TRUNCATE TABLE  
86 TRUNCATE CLUSTER  
91 CREATE FUNCTION  
92 ALTER FUNCTION  
93 DROP FUNCTION  
94 CREATE PACKAGE  
95 ALTER PACKAGE  
96 DROP PACKAGE  
97 CREATE PACKAGE BODY  
98 ALTER PACKAGE BODY  
99 DROP PACKAGE BODY  
100 LOGON  
101 LOGOFF  
102 LOGOFF BY CLEANUP  
103 SESSION REC  
104 SYSTEM AUDIT  
105 SYSTEM NOAUDIT  
106 AUDIT DEFAULT  
107 NOAUDIT DEFAULT  
108 SYSTEM GRANT  
109 SYSTEM REVOKE  
110 CREATE PUBLIC SYNONYM  
111 DROP PUBLIC SYNONYM  
112 CREATE PUBLIC DATABASE LINK  
113 DROP PUBLIC DATABASE LINK  
114 GRANT ROLE  
115 REVOKE ROLE  
116 EXECUTE PROCEDURE  
117 USER COMMENT  
118 ENABLE TRIGGER  
119 DISABLE TRIGGER  
120 ENABLE ALL TRIGGERS  
121 DISABLE ALL TRIGGERS  
122 NETWORK ERROR  
123 EXECUTE TYPE  
157 CREATE DIRECTORY  
158 DROP DIRECTORY  
159 CREATE LIBRARY  
160 CREATE JAVA  
161 ALTER JAVA  
162 DROP JAVA  
163 CREATE OPERATOR  
164 CREATE INDEXTYPE  
165 DROP INDEXTYPE  
167 DROP OPERATOR  
168 ASSOCIATE STATISTICS  
169 DISASSOCIATE STATISTICS  
170 CALL METHOD  
171 CREATE SUMMARY

172 ALTER SUMMARY  
173 DROP SUMMARY  
174 CREATE DIMENSION  
175 ALTER DIMENSION  
176 DROP DIMENSION  
177 CREATE CONTEXT  
178 DROP CONTEXT  
179 ALTER OUTLINE  
180 CREATE OUTLINE  
181 DROP OUTLINE  
182 UPDATE INDEXES  
183 ALTER OPERATOR