Micro Focus Security ArcSight SmartConnectors

Software Version: 8.3.0

SmartConnector for Oracle Audit DB

Document Release Date: February 2022
Software Release Date: February 2022

Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

https://www.microfocus.com

Copyright Notice

Trademark Notices

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

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

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Document Revision History

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.

To check for recent updates or to verify that you are using the most recent edition of a document, go to ArcSight Product Documentation Community on the Micro Focus Security Community.

Document Changes

Date	Product Version	Description
MM/DD/YYYY	X.X.X.X	Description of change

Contents

Configuration Guide for Oracle Audit DB SmartConnector

This guide provides information for installing the SmartConnector for Oracle Audit DB and configuring the device for event collection.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight SmartConnectors.

Additional Documentation

The ArcSight SmartConnectors documentation library includes the following resources:

- *Installation Guide for ArcSight SmartConnectors*, which provides detailed information about installing SmartConnectors.
- *Configuration Guides for ArcSight SmartConnectors*, which provides information about configuring SmartConnectors to collect events from different sources.
- *Release Notes for ArcSight SmartConnectors*, which provides information about the latest release

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the documentation site for ArcSight SmartConnectors.

Contact Information

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

For specific product issues, contact Micro Focus Customer Care.

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, refer to the *Oracle Database Security Guide* for your database version.

Viewing 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
```

3 At the sqlplus prompt (SQL>), enter:

```
connect logon as sysdba
```

4 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
```

5 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
audit_sys_operations	boolean	FALSE
audit_syslog_level	string	
audit_trail	string	NONE

6 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;
```

To disable auditing 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;
```

Granting 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_trial, 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.

Enabling 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.

Creating 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`.

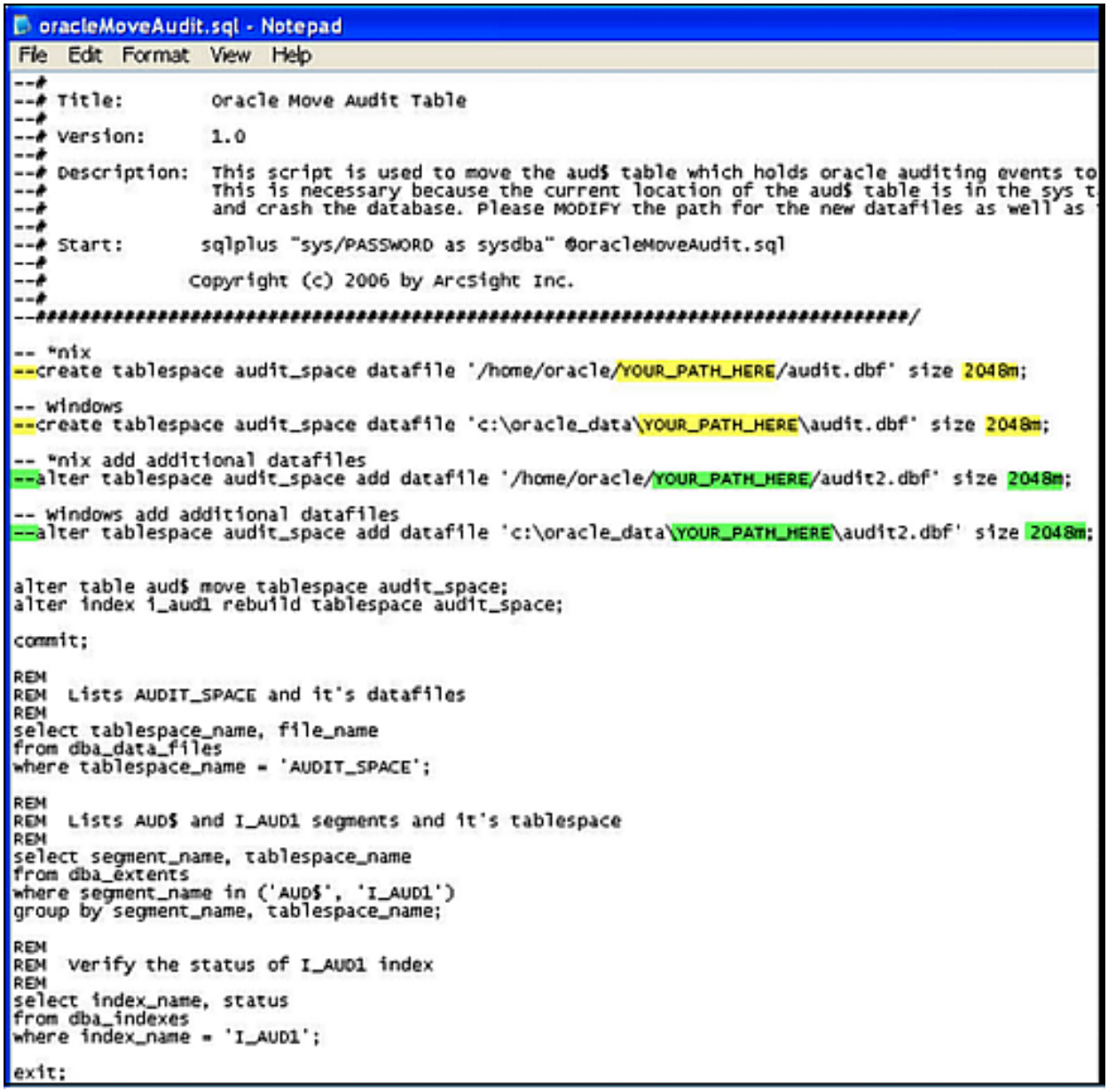
2 Make a backup copy of the file `oracleMoveAudit.sql`.

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.



oracleMoveAudit.sql - Notepad

File Edit Format View Help

```
--#
--# 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.

Configuring Audit Options

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

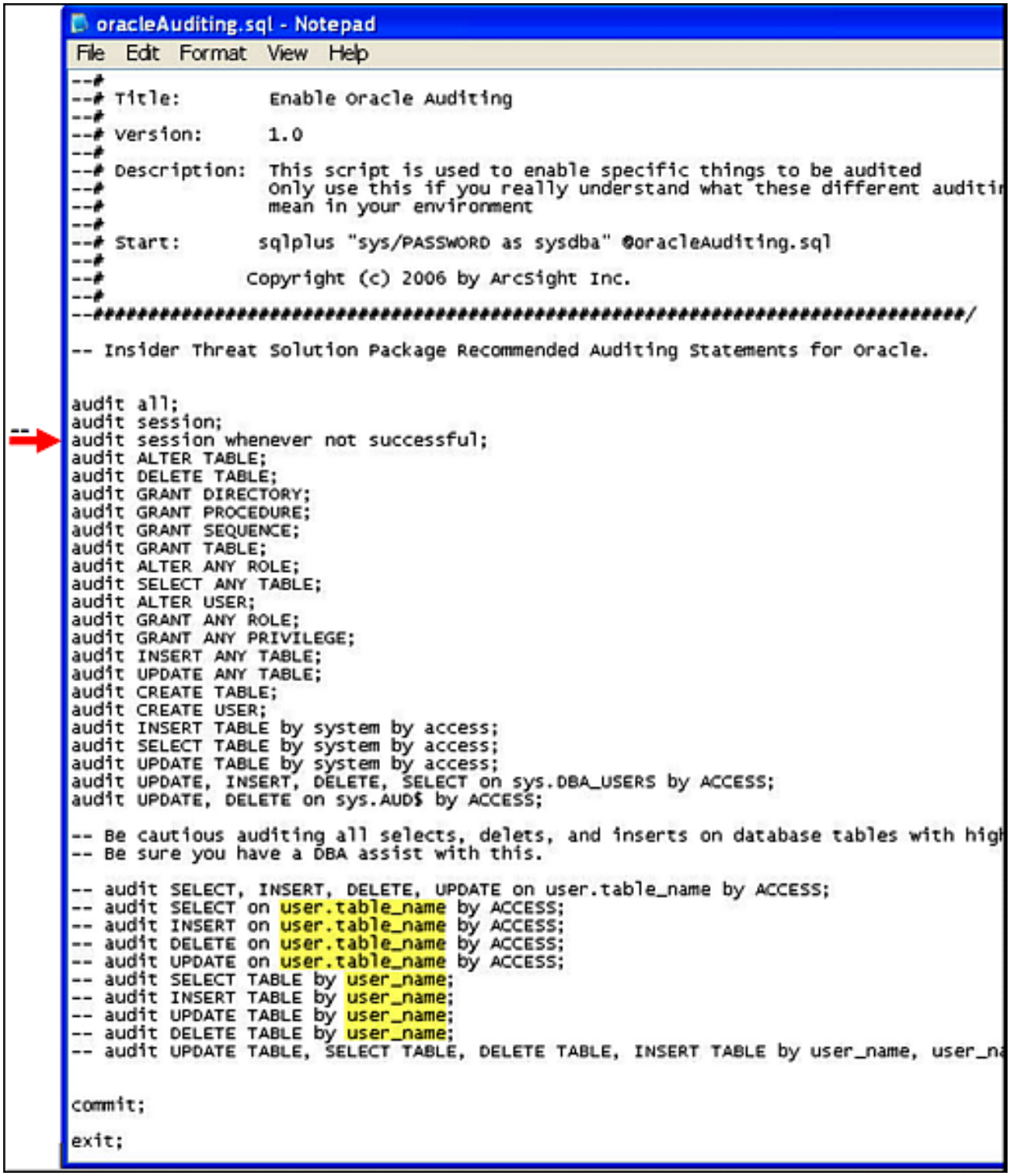
1 From a command prompt, change directory to:

```
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.



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**.

Truncating 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.

Creating 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.

Scheduling 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.

Installing the SmartConnector

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

Preparing to Install Connector

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

For complete product information, refer to the *Administrator's Guide to ArcSight Platform*, available on ArcSight Documentation.

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

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

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

Installing and Configuring the SmartConnector

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. Specify the relevant Global Parameters, when prompted.
4. Select **Oracle Audit DB** as the **Type** drop-down, then click **Next**.
5. Enter following parameters, then click **Next**.

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.
Periodically Change Passwords	Select false or true from the drop-down list or accept the default value of false. This determines whether the password must be changed periodically after logging in to the database.

Parameter	Description
Password Changing Interval (in seconds)	If periodically change passwords is set to true, specify the interval at which the password must be changed. Tthe default value id 86400 seconds(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.

6. Click **Add**, then specify the following information:

Parameter	Description
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 who has access to the database instance.
Password	Enter the password for the Oracle database user.
Frequency	Enter the frequency in seconds, the SmartConnector is to poll the Oracle database.
Model	Enter the database model

In a multitenant architecture, each PDB stores its logs in separate databases, add those URLs here.

7. Click **Add** and specify the parameter details to add additional databases. Click **Next** to continue.
8. Select a destination and configure parameters.
9. Specify a name for the connector.

10. 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.
11. Select whether you want to run the connector as a service or in the standalone mode.
12. Complete the installation.
13. Run the SmartConnector.

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

Configuring Start at Date

When you want the connector to start at specific timestamps, the connector requires one timestamp as bind variable. Therefore, you must define one value for `startatdate`. 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:

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

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 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'

ArcSight ESM Field	Device-Specific Field
Device Version	VERSION
Event Outcome	One of(Success, Failure)
File ID	SQL_BIND
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 18c 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

ArcSight ESM Field	Device-Specific Field
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
File Name	OBJ_NAME
File Permission	RLS_INFO
File Type	DATABASE_TYPE
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
Source User Privileges	CURRENT_USER
Transport Protocol	Extract PROTOCOL from COMMENT_TEXT

Oracle 12.cR1 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

ArcSight ESM Field	Device-Specific Field
Destination Service Name	ACTION_NAME
Destination User Name	USERNAME
Destination User Privileges	PRIV_USED
Device Action	ACTION
Device Custom IPv6 Address 2	Extract HOST from COMMENT_TEXT
Device Custom String 1	COMMENT_TEXT
Device Custom String 2	TERMINAL
Device Custom String 3	OWNER
Device Custom String 4	_DB_URL
Device Custom String 5	SES_ACTIONS
Device Custom String 6	GRANTEE
Device Event Class Id	ACTION plus RETURNCODE
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
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 12.cR2 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 Name	USERNAME
Destination User Privileges	PRIV_USED
Device Action	ACTION
Device Custom IPv6 Address 2	Extract HOST from COMMENT_TEXT
Device Custom Number 1	STATEMENTID
Device Custom Number 2	SID
Device Custom String 1	COMMENT_TEXT
Device Custom String 2	TERMINAL
Device Custom String 3	OWNER
Device Custom String 4	_DB_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 Vendor	'ORACLE'
Device Version	VERSION
Event Outcome	One of(Success, Failure)
File ID	SQL_BIND
File Name	OBJ_NAME
File Permission	RLS_INFO
FileType	DATABASE_TYPE

ArcSight ESM Field	Device-Specific Field
Message	One of((SQL_TEXT,ACTION_NAME)
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
Source User Privileges	CURRENT_USER
Transport Protocol	Extract PROTOCOL from COMMENT_TEXT

Multi-tenant 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 Date 1	PDB_OPEN_TIME
Device Custom Date 2	CREATION_TIME
Device Custom IPv6 Address 2	Extract HOST from COMMENT_TEXT
Device Custom Number 1	STATEMENTID
Device Custom Number 1	STATEMENTID
Device Custom Number 2	SID (SESSION_ID)
Device Custom Number 2	SID
Device Custom Number 3	CON_ID
Device Custom String 1	COMMENT_TEXT
Device Custom String 2	TERMINAL

ArcSight ESM Field	Device-Specific Field
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
DeviceCustomNumber3	CON_ID
Event Outcome	One of(Success, Failure)
File ID	SQL_BIND
File Name	OBJ_NAME
File Permission	RLS_INFO
File Type	DATABASE_TYPE
Message	One of((SQL_TEXT,ACTION_NAME)
Name	ACTION_NAME
OldFileID	PDB_NAME
Reason	RETURNCODE
requestContext	All of (PDB_OPEN_MODE,PDB_TOTAL_SIZE,PDB_BLOCK_SIZE)
requestCookies	All of (APPLICATION_ROOT,APPLICATION_PDB,APPLICATION_SEED,IS_PROXY_PDB,APPLICATION_CLONE)
requestMethod	PDB_RECOVERY_STATUS
Source Address	Extract HOST from COMMENT_TEXT
Source Host Name	USERHOST
Source Port	Extract PORT from COMMENT_TEXT
Source User Name	OS_USERNAME
Source User Privileges	CURRENT_USER
Transport Protocol	Extract PROTOCOL from COMMENT_TEXT

Single 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 Date 1	PDB_OPEN_TIME
Device Custom IPv6 Address 2	Extract HOST from COMMENT_TEXT
Device Custom Number 1	STATEMENTID
Device Custom Number 2	SID (SESSION_ID)
Device Custom Number 3	CON_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
File Name	OBJ_NAME

ArcSight ESM Field	Device-Specific Field
Message	SQL_TEXT
Name	ACTION_NAME
OldFileID	PDB_NAME
Reason	RETURNCODE
requestContext	All of (PDB_OPEN_MODE,PDB_TOTAL_SIZE,PDB_BLOCK_SIZE)
requestMethod	PDB_RECOVERY_STATUS
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

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 auditions 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

please confirm that when customer used MySQL JDBC driver 5.1.38, they had issue to receivee events. And the workaround is to apply older driver 5.0.8, after that connector is able to received events.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on SmartConnector for Oracle Audit DB (SmartConnectors 8.3.0)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to Documentation-Feedback@microfocus.com.

We appreciate your feedback!