Oracle Financial Services Transactions Filtering
Administration Guide

Release 8.0.4.0.0
February 2017

Oracle Financial Services Transactions Filtering
Administration Guide

Release 8.0.4.0.0
February 2017

Part Number: E82599-01

Oracle Financial Services Software, Inc.
1900 Oracle Way
Reston, VA 20190

Part Number: E82599-01
Second Edition (February 2017)

Oracle Financial Services Software, Inc.
1900 Oracle Way
Reston, VA 20190
Phone: (703) 478-9000
Fax: (703) 318-6340
Internet: www.oracle.com/financialservices

Table of Contents

List of Figures

List of Tables

About this Guide

This guide provides comprehensive instructions for proper system administration and the daily operations and maintenance of Oracle Financial Services Transaction Filtering. The logical architecture provides details of the Transaction Filtering process for a better understanding of the pre-configured application, which allows you to make site-specific enhancements using OFSAAI. This section focuses on the following topics:

- Who Should Use this Guide
- How this Guide is Organized
- Where to Find More Information
- Conventions Used in this Guide

Who Should Use this Guide

This *Administration Guide* is designed for use by the Installers and System Administrators. Their roles and responsibilities, as they operate within Oracle Financial Services Transaction Filtering, include the following:

- **Installer:** Installs and configures Oracle Financial Services Transaction Filtering at a specific deployment site. The Installer also installs and upgrades any additional Oracle Financial Services solution sets, and requires access to deployment-specific configuration information (For example, machine names and port numbers).
- **System Administrator:** Configures, maintains, and adjusts the system, and is usually an employee of a specific Oracle customer. The System Administrator maintains user accounts and roles, configures the EDQ, archives data, loads data feeds, and performs post-processing tasks. In addition, the System Administrator can reload cache. However, the scenario description is not visible to the System Administrator.

How this Guide is Organized

The *Oracle Financial Services Transaction Filtering Administration Guide*, includes the following chapters:

- *About Oracle Financial Services Transaction Filtering*, provides a brief overview of the Oracle Financial Services Transaction Filtering application.
- *Getting Started*, provides information on how to log on to the Transaction Filtering application and the tab available on the home page.
- *Managing User Administration*, provides information on the user administration of the Oracle Financial Services Transaction Filtering application.
- *Configuring EDQ*, describes how to configure the EDQ in the Oracle Financial Services Transaction Filtering application.

Where to Find More Information

For more information about Oracle Financial Services Transaction Filtering, refer to the following Transaction Filtering application documents, which can be found on the OTN page:

- *User Guide*
- *Installation and Configuration Guide*

To find additional information about how Oracle Financial Services solves real business problems, see our website at www.oracle.com/financialservices.

Conventions Used in this Guide

This table lists the conventions used in this guide and their associated meanings.

Table 1. Conventions Used in this Guide

Convention	Meaning
Italics	• Names of books, chapters, and sections as references • Emphasis
Bold	• Object of an action (menu names, field names, options, button names) in a step-by-step procedure • Commands typed at a prompt • User input
`Monospace`	• Directories and subdirectories • File names and extensions • Process names • Code sample, including keywords and variables within text and as separate paragraphs, and user-defined program elements within text
<Variable>	• Substitute input value

CHAPTER 1 About Oracle Financial Services Transaction Filtering

This chapter provides a brief overview of Oracle Financial Services Transaction Filtering in terms of its architecture and process flow.

This section covers the following topics:

- About Oracle Financial Services Transaction Filtering
- Oracle Transaction Filtering Process Flow

About Oracle Financial Services Transaction Filtering

The Oracle Financial Services (OFS) Transaction Filtering application is a real-time filtering system that identifies financial transactions done by blacklisted, sanctioned, and restricted individuals, entities, cities and countries. The application can interface with any clearing systems, payment systems, or source systems. The application accepts messages from the source systems in real time and scans them against different watch lists maintained within the system to identify any blacklisted data present within the transaction message, which is in a SWIFT format. The OFS Transaction Filtering application is built using three components: a scoring engine (EDQ), a user interface and a rule engine (IPE).

Financial institutions use OFS Transaction Filtering for the following tasks:

- Identify transactions done by customers, organizations, and countries which are sanctioned.
- Perform daily checks of customers' names and filter customers' transactions against the OFAC and HMT sanctions lists.
- Generate risk scores for entities with whom business or transactions are prohibited.

Oracle Transaction Filtering Process Flow

Figure 1 describes the Oracle Transaction Filtering Process Flow:

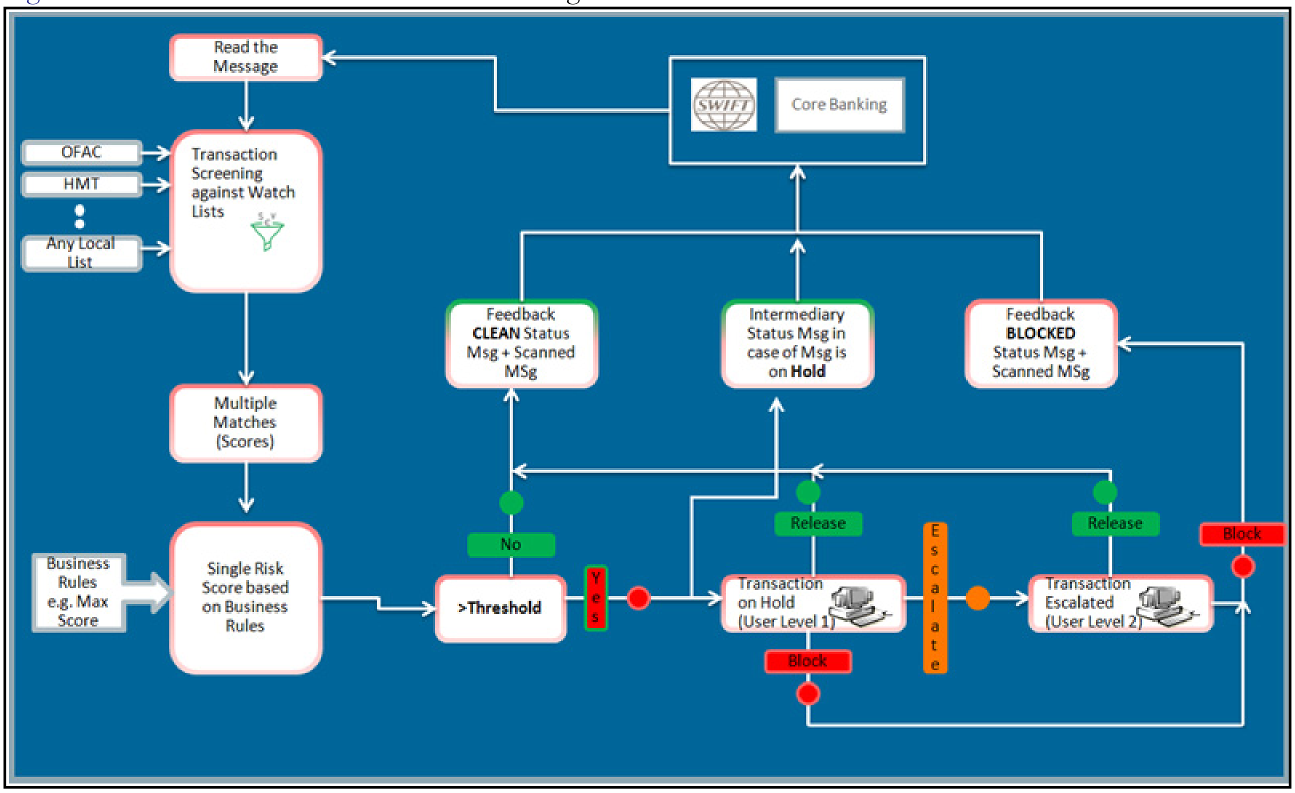

Figure 1. Oracle Transaction Filtering Process Flow

The following steps describe the Transaction Filtering process flow:

1. The Transaction Filtering application receives the transaction message from a JMS queue. The message is in a SWIFT format.

Note: All field details of the message are stored within the application.

---

2. The transaction message is screened against a watch list through the Enterprise Data Quality (EDQ) platform. The message is sent to the EDQ platform, and the EDQ sends back a response. The watch list checks for any blacklisted or suspicious data using a matching logic.

Note: There may be more than one transaction present within a message. In this case, each transaction is screened against external and internal watch lists.

---

3. For every match, a match score is generated through the IPE platform. If a match is not found, then the system generates a zero score.

Note: Different scores can also be assigned to different watch list using rules. All scores are based on multiple rules set up in the application and are configurable. In case of multiple scores, the logic is used to take the maximum score out of all the scores, and the score is treated as a final score for any given transaction.

Note: For information on IPE, see *OFS Online Processing Engine User Guide*.

4. The final score is checked against a threshold limit set within the application. If the score is greater than the threshold limit, then the transaction is treated as a suspicious transaction. If the score is lesser than the threshold limit, then the transaction is treated as a clean transaction.

Note: If all the transactions within a message are clean, then a feedback message is sent back to the central banking system with a *CLEAN* status. The message contains the status, message reference ID, and transaction reference ID. If any transaction within a message is found to be suspicious, then the complete message is moved into a *HOLD* status and is available for user action. For more information, see *Oracle Transaction Filtering User Guide*.

CHAPTER 2 # Getting Started

This chapter provides step-by-step instruction to login to the Transaction Filtering System and different features of the Oracle Financial Services Analytical Applications (OFSAA) Application page.

This chapter discusses the following topics:

- Accessing OFSAA Applications
- Managing OFSAA Application Page
- Troubleshooting Your Display

Accessing OFSAA Applications

Access to the Oracle Financial Services Transaction Filtering application depends on the Internet or Intranet environment. Oracle Financial Services Transaction Filtering is accessed through Microsoft Internet Explorer (IE). Your system administrator provides the intranet address uniform resource locator (URL).

Your system administrator provides you with a User ID and Password. Login to the application through the Login page. You will be prompted to change your password on your first login. You can change your password whenever required by logging in. For more information, see the *Troubleshooting Your Display* section.

To access the Oracle Financial Services Analytical Applications, follow these steps:

1. Enter the URL into your browser using the following format:

   `<scheme/ protocol>://<ip address/ hostname>:<port>/<context-name>/login.jsp`

   For example: `https://myserver:9080/ofsaaapp/login.jsp`

   The OFSAA Login page is displayed.

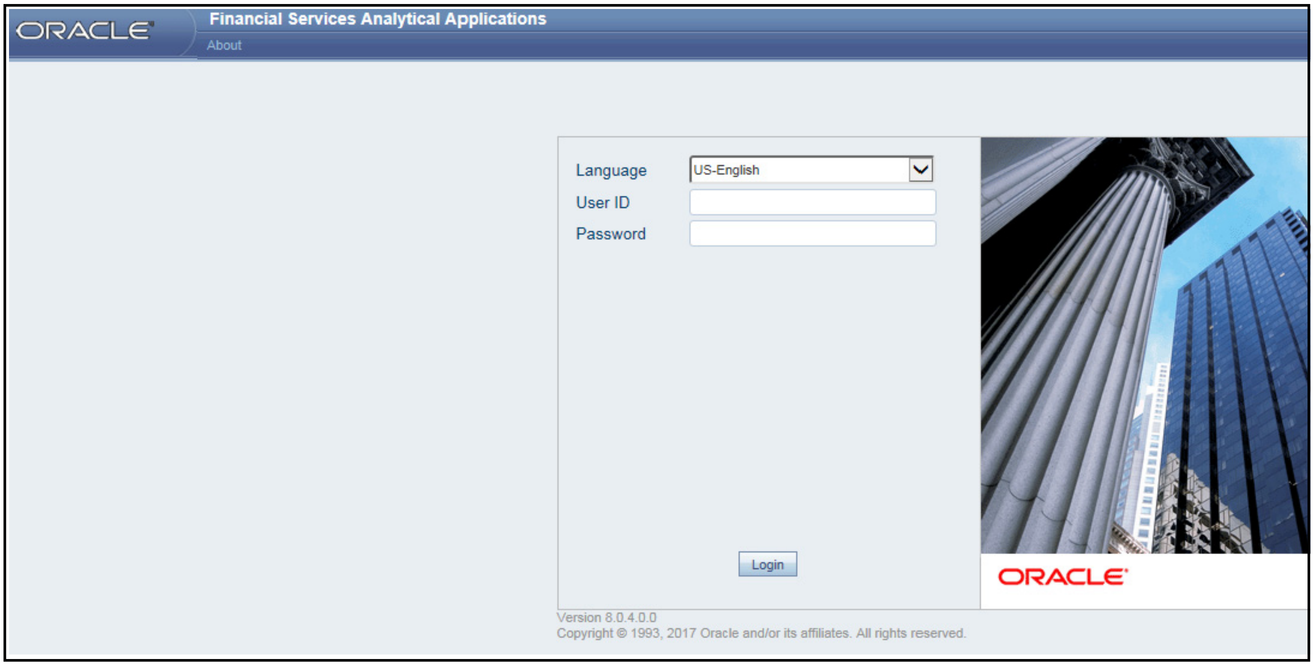

Figure 2. OFSAA Login Page

2. Select the Language from the Language drop-down list. This allows you to use the application in the language of your selection.
3. Enter your User ID and Password in the respective fields.
4. Click **Login**. The Oracle Financial Services Analytical Applications page is displayed.

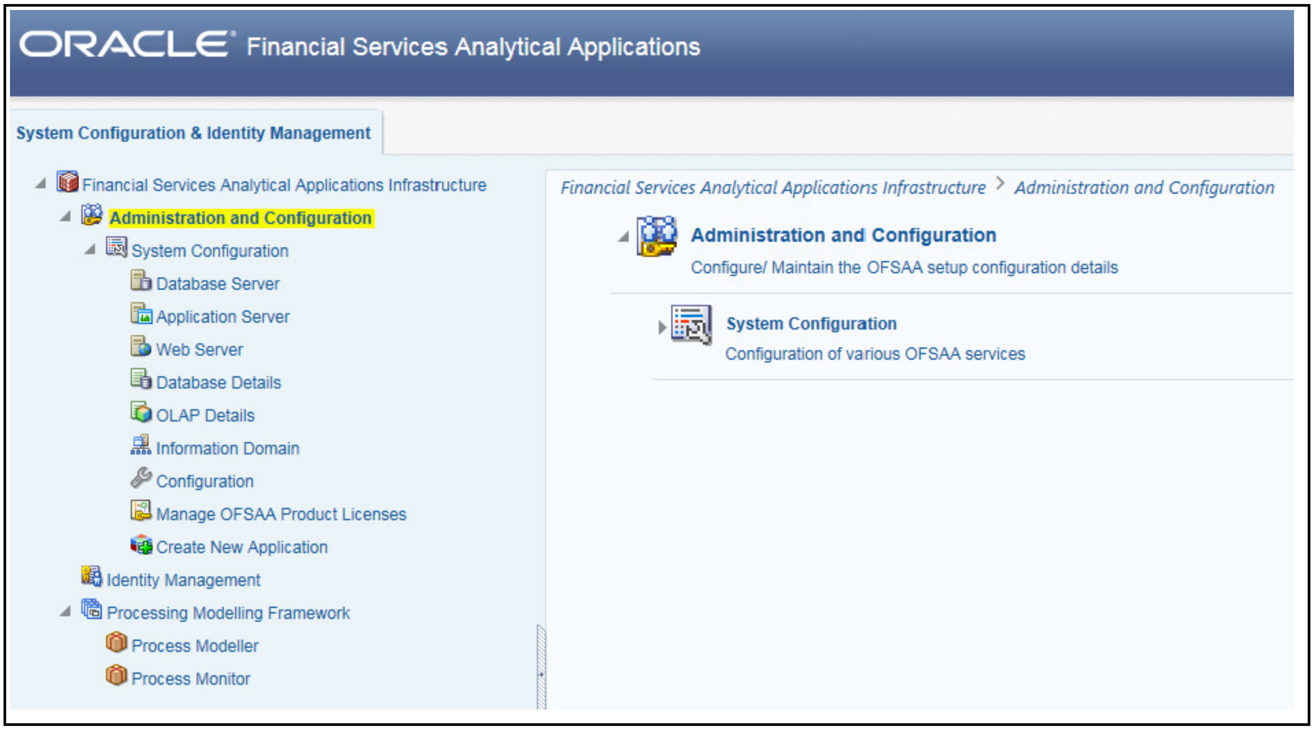

Figure 3. OFSAA Application Page

The Oracle Financial Services Analytical Applications page is a common landing page for all users until a preferred application page is set. For more information about how to set your preferred application page, see OFSAAI User Guide. You can use the OFSAA Application page to access the Oracle Financial Services applications in your environment.

Managing OFSAA Application Page

This section describes the options available for system configuration in the OFSAA Application page.

The OFSAA Application page has the following tab:

- System Configuration and Identity Management Tab

System Configuration and Identity Management Tab

System Configuration and Identity Management is an integral part of the Infrastructure administration process. This tab helps System Administrators to provide security and operational framework required for the Infrastructure.

System Administrators can configure Server details, Database details, OLAP details, and Information Domains, along with other configuration processes such as segment and meta data mapping, mapping segments to securities, and rules setup. The System Configuration is a one-time activity, which helps the System Administrator make the Infrastructure system operational.

The System Configuration and Identity Management tab lists the OFSAA Infrastructure System Configuration and Identity Management modules. These modules work across Applications and Information Domains, so there is no Application and Information Domain drop-down list in this tab.

Figure 4. System Configuration and Identity Management Tab

Selecting Identity Management allows System Administrators to manage Users, User Groups, and the functions each User or User Group may access. For more information about managing Users and User Groups, see *OFSAAI Administration Guide*.

Troubleshooting Your Display

If you experience problems logging into Oracle Financial Services Transaction Filtering or with your display, the browser settings may be incompatible with running OFSAA applications. The following sections provide instructions for setting your Web display options for OFSAA applications within IE.

Note: The following procedures apply to all versions of IE listed in section . A separate procedures are listed for each version where differences exist in the locations of settings and options.

This section covers the following topics:

- Enabling JavaScript
- Enabling Cookies
- Enabling Temporary Internet Files
- Enabling File Downloads
- Setting Printing Options
- Enabling Pop-Up Blocker
- Setting Preferences

Enabling JavaScript

This section describes how to enable JavaScript.

To enable JavaScript, follow these steps:

1. Navigate to the Tools menu, click **Internet Options**. The Internet Options dialog box is displayed.
2. Click the **Security** tab and click the **Local Intranet** icon as your Web content zone.
3. Click **Custom Level**. The Security Settings dialog box displays.
4. In the Settings list and under the Scripting setting, enable all options.
5. Click **OK,** then click **OK** again to exit the Internet Options dialog box.

Enabling Cookies

Cookies must be enabled. If you have problems troubleshooting your display, contact your System Administrator.

Enabling Temporary Internet Files

Temporary Internet files are pages that you view on the Internet and store in a folder for quick viewing later. You must adjust this setting to always check for new versions of a stored page.

To adjust your Temporary Internet File settings, follow these steps:

1. Navigate to the Tools menu, click **Internet Options**. The Internet Options dialog box is displayed.
2. On the General tab, click **Settings**. The Settings dialog box displays.
3. Click the **Every visit to the page** option.

4. Click **OK**, then click **OK** again to exit the Internet Options dialog box.

Enabling File Downloads

This section describes how to enable file downloads.

To enable file downloads, follow these steps:

1. Navigate to the Tools menu, click **Internet Options**. The Internet Options dialog box is displayed.
2. Click the **Security** tab and then click the **Local Intranet** icon as your Web content zone.
3. Click **Custom Level**. The Security Settings dialog box displays.
4. Under the Downloads section, ensure that **Enable** is selected for all options.
5. Click **OK**, then click **OK** again to exit the Internet Options dialog box.

Setting Printing Options

This section explains the how to enable printing background colors and images must be enabled.

To enable this option, follow these steps:

1. Navigate to the Tools menu, click **Internet Options**. The Internet Options dialog box is displayed.
2. Click the **Advanced** tab. In the Settings list, under the Printing setting, click **Print background colors and images**.
3. Click **OK** to exit the Internet Options dialog box.

Tip: For best display results, use the default font settings in your browser.

Enabling Pop-Up Blocker

You may experience difficulty running the Oracle Financial Services Transaction Filtering application when the IE Pop-up Blocker is enabled. It is recommended to add the URL of the application to the *Allowed Sites* in the Pop-up Blocker Settings in the IE Internet Options.

To enable Pop-up Blocker, follow these steps:

1. Navigate to Tools menu, click **Internet Options**. The Internet Options dialog box is displayed.
2. Click the **Privacy** tab. In the Pop-up Blocker setting, select the **Turn on Pop-up Blocker** option**.** The **Settings** enable.
3. Click **Settings** to open the Pop-up Blocker Settings dialog box.
4. In the Pop-up Blocker Settings dialog box, enter the URL of the application in the text area.
5. Click **Add**. The URL appears in the Allowed site list.
6. Click **Close**, then click **Apply** to save the settings.
7. Click **OK** to exit the Internet Options dialog box.

Setting Preferences

The Preferences section enables you to set your OFSAA Home Page.

To access this section, follow these steps:

1. Click **Preferences** from the drop-down list in the top right corner, where the user name is displayed. The Preferences page is displayed.

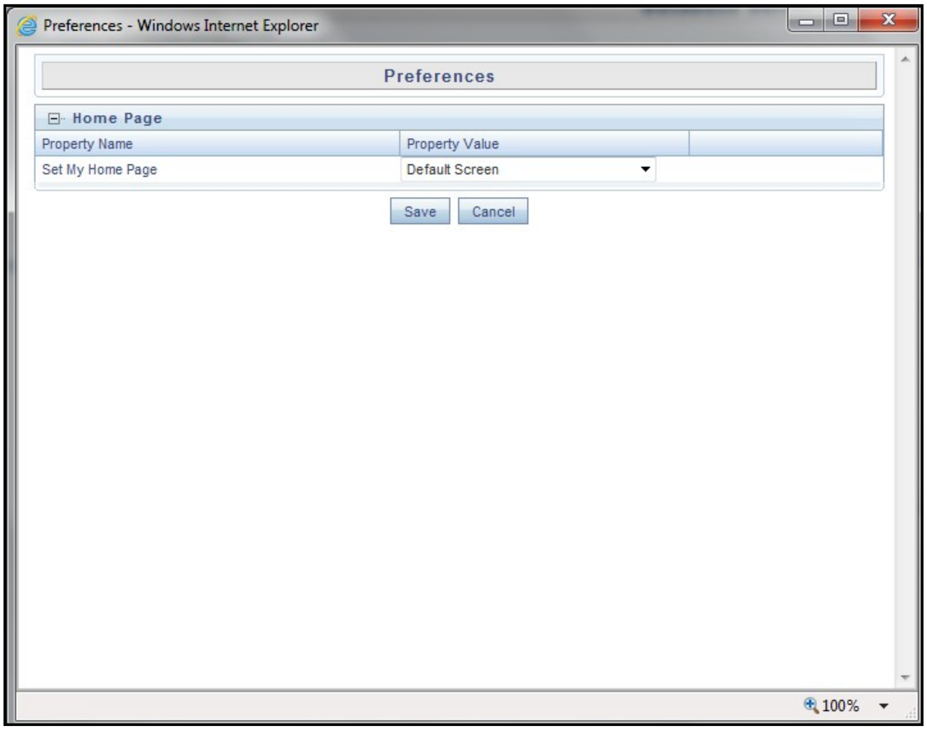

Figure 5. Preference screen.

2. In the Property Value drop-down list, select the application which you want to set as the Home Page.

   Note: Whenever new application is installed, the related value for that application is found in the drop-down list.

3. Click **Save** to save your preference.

CHAPTER 3 Managing User Administration

This chapter provides instructions for performing the user administration of Oracle Financial Services (OFS) Transaction Filtering.

This chapter focuses on the following topics:

- About User Administration
- Managing User Administration

About User Administration

User administration involves creating and managing users and providing access rights based on their roles. This section discusses the following:

- Administrator permissions
- Creating roles and granting and authorizing a user

Managing User Administration

This section allows you to create and authorize a user and map the users to user groups in the Transaction Filtering application.

This section covers the following topics:

- Creating and Authorizing a User
- Mapping a User with a User Group

The following table lists the various actions and associated descriptions of the user administration process flow:

Table 2. Administration Process Flow

Action	Description
Creating and Authorizing a User	Create a user. This involves providing a user name, user designation, and the dates between which the user is active in the system.
Mapping a User with a User Group	Map a user to a user group. This enables the user to have certain privileges that the mapped user group has.

Creating and Authorizing a User

The sysadmn user creates a user and the sysauth user authorizes a user in the Transaction Filtering application. For more information on creating and authorizing a user, see *Oracle Financial Services Analytical Applications Infrastructure User Guide*.

Mapping a User with a User Group

This section explains how to map Users and User Groups. With this, the user has access to the privileges as per the role. The sysadm user maps a user to a user group in the Transaction Filtering application. The following table describes the predefined User Roles and corresponding User Groups.

Table 3. Roles and User Groups

Role	Group Name	User Group Code
Administrator	Transaction Filtering Analyst Group	TFLTANALYSTGRP
Analyst	Transaction Filtering Supervisor Group	TFLTSUPERVISORGRP
Supervisor	Transaction Filtering Administrator Group	TFLTADMINISTATORGRP

CHAPTER 4 Configuring EDQ

This chapter explains how to import the `.dxi` files into the Enterprise Data Quality (EDQ) application, run the EDQ jobs, and change the EDQ URL for the Transaction Filtering application.

This chapter focuses on the following topics:

- About EDQ
- EDQ Configuration Process Flow

About EDQ

The Oracle Financial Services Transactions Filtering application is built using EDQ as a platform. EDQ provides a comprehensive data quality management environment that is used to understand, improve, protect and govern data quality. EDQ facilitates best practices such as master data management, data integration, business intelligence, and data migration initiatives. EDQ provides integrated data quality in customer relationship management and other applications.

EDQ has the following key features:

- Integrated data profiling, auditing, and cleansing and matching
- Browser-based client access
- Ability to handle all types of data (for example, customer, product, asset, financial, and operational)
- Connection to any Java Database Connectivity (JDBC) compliant data sources and targets
- Multi-user project support (Role-based access, issue tracking, process annotation, and version control)
- Services Oriented Architecture (SOA) support for designing processes that may be exposed to external applications as a service
- Designed to process large data volumes
- A single repository to hold data along with gathered statistics and project tracking information, with shared access
- Intuitive graphical user interface designed to help you solve real world information quality issues quickly
- Easy, data-led creation and extension of validation and transformation rules
- Fully extensible architecture allowing the insertion of any required custom processing

---

Note: For information on configuring a host in the Transaction Filtering application, see *Host Configuration.*

Note: For more information on EDQ, see *Oracle Enterprise Data Quality Documentation*.

This section covers the following topics:

- EDQ Configuration Process Flow

- Changing the EDQ URL

EDQ Configuration Process Flow

The following image shows the EDQ configuration process flow:

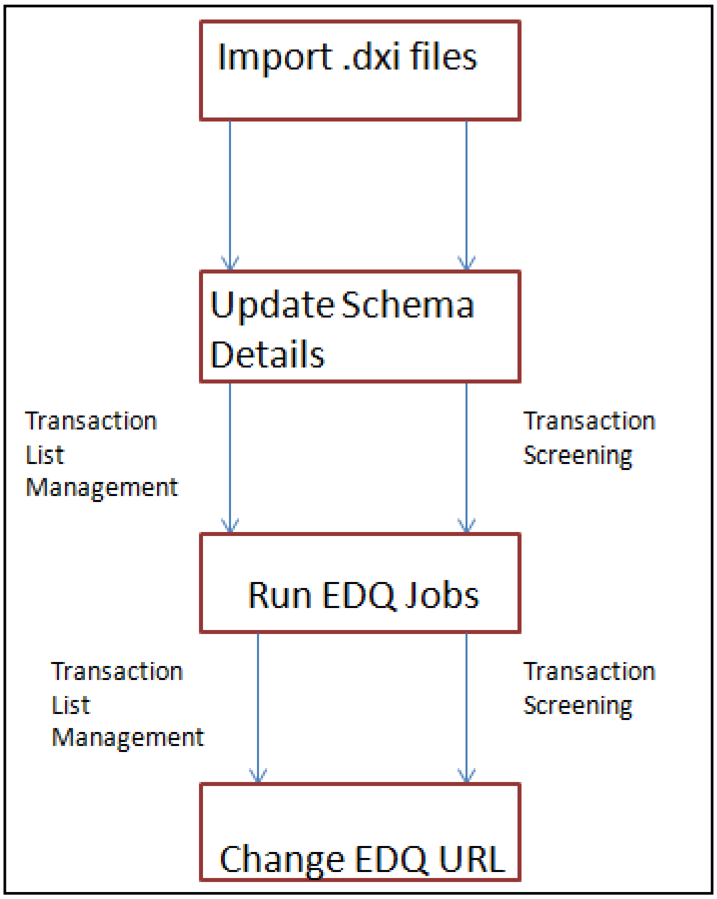

Figure 6. EDQ Configuration Process Flow

To configure the EDQ, follow these steps:

1. Import the Transaction List management and Transaction screening `.dxi` files from the `FIC_HOME/Transaction_Processing` path.

2. Enter the organization-specific Atomic schema details as shown below:

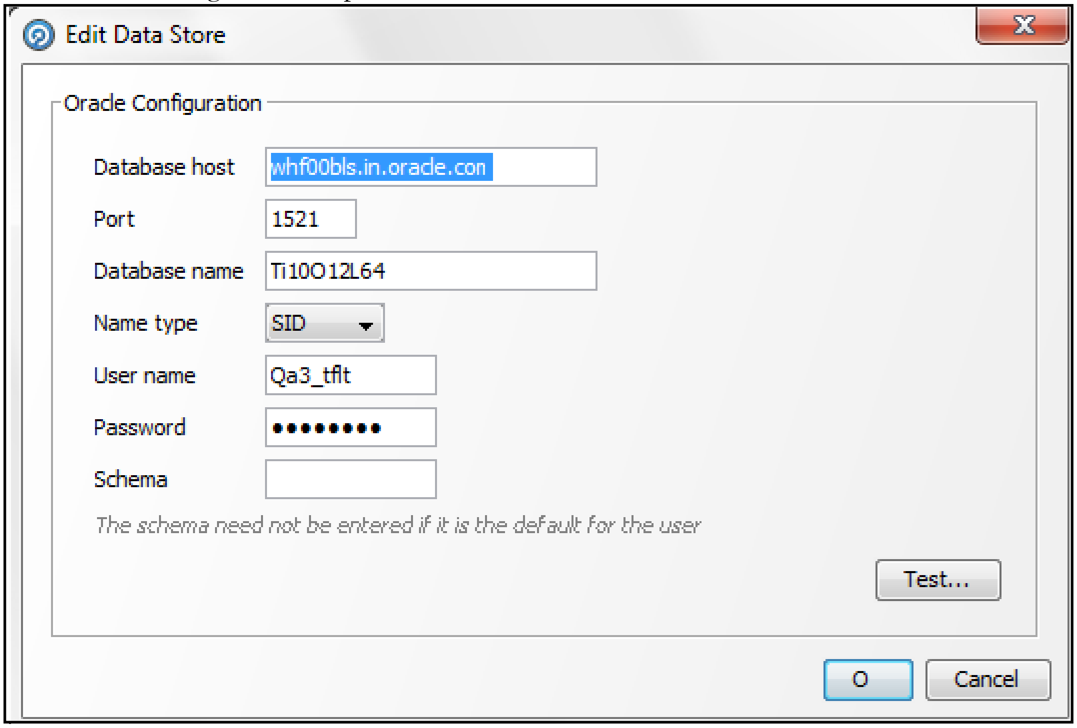

Figure 7. Updating the Schema Details

3. Run the following jobs under the Transaction List management project:

- Analyze Reference data quality
- Download Prepare & filter export list data
- Generate StopPhrases

4. Run the Transaction Filtering job under the Transaction Screening project.
5. Change the EDQ URL in the Transaction Filtering application. This is done the first time you set up the Transaction Filtering application as the application needs to know the location of the EDQ.

Changing the EDQ URL

To change the EDQ URL, follow these steps:

1. Navigate to the Oracle Financial Services Sanctions application home page.
2. On the right pane, click **Transaction Filtering Admin**.

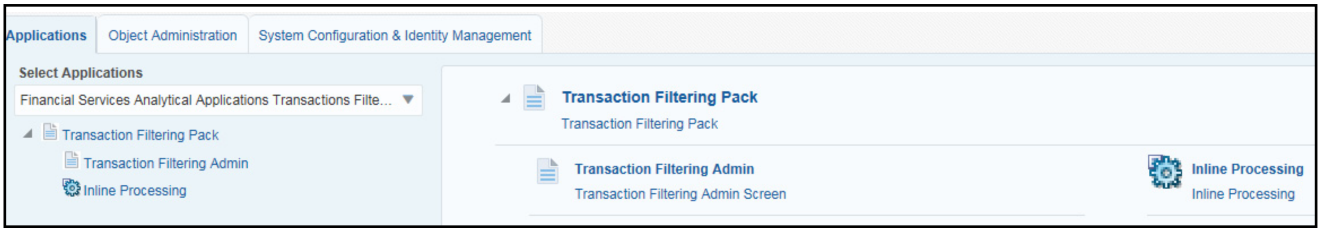

Figure 8. Changing the EDQ URL

3. To view the Debug details, select **Yes**. To view the Info details, select **No**.

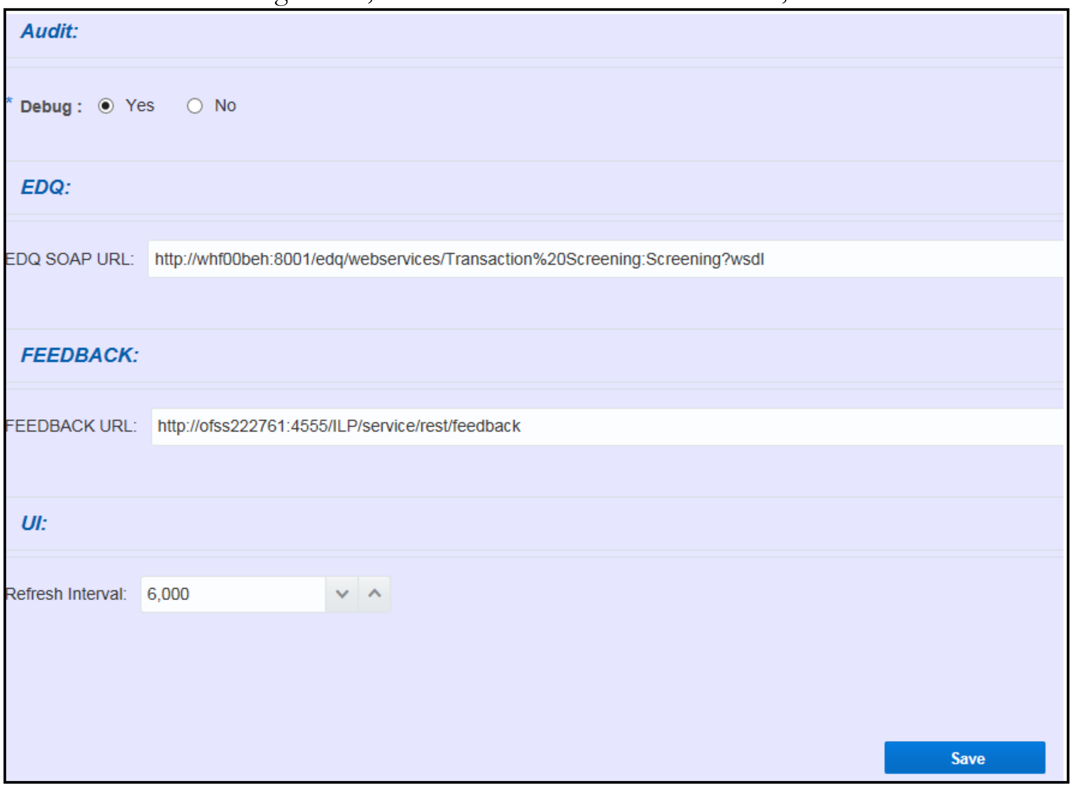

Figure 9. Admin Screening Page

If you select Yes in the Debug field, then all the steps are logged in the system irrespective of the value in the Status column. If you select No in the Debug field, then only those steps for which the value is Y in the Status column are logged in the system.

Note: For more information on the values in the Status column, see *System Audit Logging Information*.

---

4. In the EDQ SOAP URL field, enter the URL.
5. In the FEEDBACK field, enter the URL where we need to post messages for HOLD, RELEASE, CLEAN, BLOCK in the feedback Queue.
6. In the Refresh Interval field, select the refresh interval for viewing the notification count in the Transaction Filtering screen.

Note: This time is in milliseconds.

7. Click **Save**. The following confirmation message is displayed: *Records Updated Successfully*.

APPENDIX A Watch Lists

This appendix contains details of each of the pre-configured watch lists that can be used by Oracle Watchlist Screening and contains the following topics:

- HM Treasury Reference Data
- OFAC Reference Data

HM Treasury Reference Data

The HM Treasury publishes a sanctions list that can be used for screening in Oracle Watchlist Screening. The sanctions list provides a consolidated list of targets listed by the United Nations, European Union and United Kingdom under legislation relating to current financial sanctions regimes.

The HM Treasury website provides more details about the list at the following location:

https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets

Oracle Watchlist Screening uses the list in a semi-colon delimited form. It can be downloaded from the following location:

http://hmt-sanctions.s3.amazonaws.com/sanctionsconlist.csv

OFAC Reference Data

The US Treasury website states that *The US Treasury's Office of Foreign Assets Control (OFAC) administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries, terrorists, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction.* More details on the OFAC list can be found on the US Treasury website available at the following location:

http://www.treasury.gov/ofac/

Oracle Watchlist Screening supports two lists that are produced by OFAC. The OFAC Specially Designated Nationals (SDN) list, which is available for download in three separate parts from the following links:

https://www.treasury.gov/ofac/downloads/sdn.csv

https://www.treasury.gov/ofac/downloads/add.csv

https://www.treasury.gov/ofac/downloads/alt.csv

The OFAC Consolidated Sanctions List, which can be downloaded in three separate parts from the following links:

https://www.treasury.gov/ofac/downloads/consolidated/cons_prim.csv

https://www.treasury.gov/ofac/downloads/consolidated/cons_add.csv

https://www.treasury.gov/ofac/downloads/consolidated/cons_alt.csv

APPENDIX B Match Score Rules

This appendix provides information on the match rules involved in the Transaction Filtering application.

The following match rules are used for matching

- Elimination rules: These are used in various positions in the rule templates to eliminate any records that have conflicting supporting data. The elimination rules may be moved up and down in order to change when they are applied during the matching process.
- Name matching rules: These are organized by the level of name match, with the strongest name matching rules placed at the top of the decision table.

Note: This means that the match rules are not ordered by strength across all identifiers. For example, a weaker name match that is strengthened by matches on date of birth, city and country is likely to be a stronger overall match than a strong name with strongly contradictory data in the other fields.

Oracle Watchlist Screening includes many match rules for each level of name match, reflecting the match strength of any additional information, particularly date of birth and location data. These rules allow records which fulfill the specified level of name match but have conflicting supporting data fields indicating that a true match is unlikely.

- Loose name matching rules: These are also based around name matching, but identify looser matches and are not enabled by default. These rules are likely to result in a large number of false positive matches and are most likely to be of use when screening against sanctions lists, where it is important that no true matches are missed.

APPENDIX C Host Configuration

This appendix contains information on how to configure a host in the Transaction Filtering application.

To configure the Transaction Filtering application for a particular host location, add the following details:

- Host name of the location
- Port number of the location
- User name and password of the location

APPENDIX D

System Audit Logging Information

This appendix contains information on the logs related to the Debug and Info log files. It covers the following topics:

- Activities for System Audit
- Steps for System Audit Activities

Activities for System Audit

The following table contains information related to the system audit activities:

Table 4. Activities for System Audit

Activity Identifier	Activity Name	Activity Sequence
1.	Raw Message Processing	1
2.	Message Parser Processing	2
3.	WatchList Processing	3
4.	Alert Manager Processing	4
5.	Hold	5
6.	Assigned	6
7.	Escalated	7
8.	Blocked	8
9.	Released	9

Steps for System Audit Activities

The following table contains information related to the steps for the system audit activities:

Table 5. Steps for System Audit Activities

Step Identifier	Activity Name	Step Name	Step Sequence	Status
1.	Raw Message Processing	Record the receipt of raw message	1	Y
2.	Raw Message Processing	Raw Message persisted into structure table	2	N

Table 5. Steps for System Audit Activities (Continued)

Step Identifier	Activity Name	Step Name	Step Sequence	Status
3.	Message Parser Processing	Raw Message parsed	1	N
4.	Message Parser Processing	Parsed Raw Message persisted into structure table	2	N
5.	WatchList Processing	Matching data prepared	1	N
6.	WatchList Processing	Matching Engine Invoked	2	Y
7.	WatchList Processing	Scoring Engine Invoked	3	Y
8.	WatchList Processing	Scoring performed	4	Y
9.	WatchList Processing	Response Received	5	Y
10.	WatchList Processing	Response persisted	6	N
11.	Alert Manager Processing	Transaction Hold	1	N
12.	Alert Manager Processing	Alert Persisted	2	N
13.	Hold	Hold Transaction Workflow Invoked	1	Y
14.	Hold	Hold Transaction Workflow completed	2	Y
15.	Assigned	Assigned Transaction Workflow Invoked	1	Y
16.	Assigned	Assigned Transaction Workflow completed	2	Y

Table 5. Steps for System Audit Activities (Continued)

Step Identifier	Activity Name	Step Name	Step Sequence	Status
17.	Escalated	Escalated Transaction Workflow Invoked	1	Y
18.	Escalated	Escalated Transaction Workflow completed	2	Y
19.	Blocked	Blocked Transaction Workflow Invoked	1	Y
20.	Blocked	Blocked Transaction Workflow completed	2	Y
21.	Released	Released Transaction Workflow Invoked	1	Y
22.	Released	Released Transaction Workflow completed	2	Y

Index