Oracle® Enterprise Data Quality for Product Data

Security Guide

Release 11g R1 (11.1.1.6)

E35849-02

February 2013

This document describes the general principles of security of the Oracle Enterprise Data Quality for Product Data (EDQP) application and contains the following:

General Security Principles

The following sections describe the fundamental principles of using the EDQP application securely.

Keep Software Up To Date

One of the principles of good security practice is to keep all software versions and patches up to date.

1. Ensure that the latest version of EDQP is installed.
2. Ensure that the compatible version of the EDQP Java client (the client applications) is downloaded and used for development of Data Service Applications and data lenses.
3. Ensure that the latest version of EDQP Services for Excel is installed.

Restrict Network Access to Critical Services

Oracle Platform Security Services (OPSS) is the underlying platform on which the Oracle Fusion Middleware security framework is built. OPSS is standards-based and complies with role-based-access-control (RBAC), Java Enterprise Edition (Java EE), and Java Authorization and Authentication Service (JAAS). Oracle Platform Security Services enable the shared security framework to furnish uniform security and identity management across the enterprise. For more information about Oracle Platform Security Services, see *Oracle Fusion Middleware Application Security Guide* at

`http://docs.oracle.com/cd/E23943_01/core.1111/e10043/toc.htm`

EDQP uses the OPSS standard Oracle authentication sub-system. Both user authentication and password encryption meet industry standards. Passwords are never transmitted in the clear. This allows users outside the firewall to safely access

and use the system. For reasons of performance and ease of integration, network data traffic is not encrypted. It is recommended that access of EDQP using our standard product APIs and web services is placed behind your corporate firewall.

Follow the Principle of Least Privilege

Controlling access to system resources is achieved by requiring users to authenticate at log in (authentication) and by restricting users to only the resources for which they are authorized (authorization). EDQP application implements Roles and Permissions using the recommended Oracle framework. Roles can be assigned to users; the privileges associated with each role grants users access to particular components in EDQP. For more information about restricting user privileges, see *Oracle Enterprise Data Quality for Product Data Oracle DataLens Server Administration Guide.*

Keep Up To Date on Latest Security Information

Oracle continually improves its software and documentation. Check the Security What's New Web site on the Oracle Technology Network yearly for news and updates at

`http://www.oracle.com/technetwork/topics/security/whatsnew/index.html`

EDQP Security Overview

The EDQP security model is built on the Oracle Fusion Middleware security framework, which incorporates the Java security model. The Java model is a role-based, declarative model that employs container-managed security where resources are protected by roles that are assigned to users. For more information about restricting user privileges, see *Oracle Enterprise Data Quality for Product Data Oracle DataLens Server Administration Guide.*

For more information about EDQP, see the documents listed in Related Documents.

Security Features

The following sections describe the specific security mechanisms offered by EDQP.

The Security Model

EDQP is tightly integrated with the Oracle Fusion Middleware Security architecture and delegates core security functionality to components of that architecture. Specifically, any Oracle Enterprise Data Quality for Products installation makes use of the following types of security providers:

- An authentication provider that knows how to access information about the users and groups accessible to EDQP and is responsible for authenticating users.
- A policy store provider that provides access to Application Roles and Application Policies, which forms a core part of the security policy and determines what users are able to view and access in EDQP.

By default, an EDQP installation is configured with an authentication provider that uses the Oracle WebLogic Server embedded LDAP server for user and group information. The EDQP default policy store provider and credential store provider stores Credentials, Application Roles and Application Policies in files in the domain.

After installing EDQP, you can reconfigure the domain to use alternative security providers. For example, you might want to reconfigure your installation to use an Oracle Internet Directory service, or another LDAP server for authentication.

Key Security Features

The key EDQP security features are:

Authentication

Each EDQP installation has an associated Oracle WebLogic Server domain. EDQP delegates user authentication to the authentication provider configured for the associated WebLogic domain. The authentication provider accesses user and group information stored in the associated LDAP server. The default LDAP server at time of installation is the WebLogic embedded LDAP server. The WebLogic Administrative Console is used to create and manage users and groups for the EDQP domain, updating the embedded LDAP server.

Authorization

Once a user has been authenticated, authorization security is used to limit their access to only the system resources that you want them to see and use. Authorization for EDQP is controlled by a security policy defined in terms of applications roles.

For information about configuring and using authentication with the EDQP WebLogic Server domain, see *WebLogic Administration Console Online Help* at

`http://docs.oracle.com/cd/E23943_01/wls.htm`

Secure Installation and Configuration

The following sections describe how to securely install and configure EDQP.

Installation Overview

EDQP is installed into an Oracle WebLogic Server domain during installation, which is a logically related group of resources that are managed as a unit. During a typical installation, an Oracle WebLogic Server domain named dls_domain (a shortened version of DataLens System domain) is created, and the EDQP Web application is installed into this domain. The domain name can vary depending on your preferences. One instance of Oracle WebLogic Server is installed as an Oracle DataLens Administration Server. This Administration Server provides a central point for managing an Oracle WebLogic Server domain. The Administration Server hosts the Administration Console, which is a Web application accessible from any supported Web browser with network access to the Administration Server. EDQP uses the active security realm configured for the Oracle WebLogic Server domain into which it is installed.

EDQP authentication is handled by the Oracle WebLogic Server authentication providers. An authentication provider performs the following functions:

1. Establishes the identity of users and system processes
2. Transmits identity information

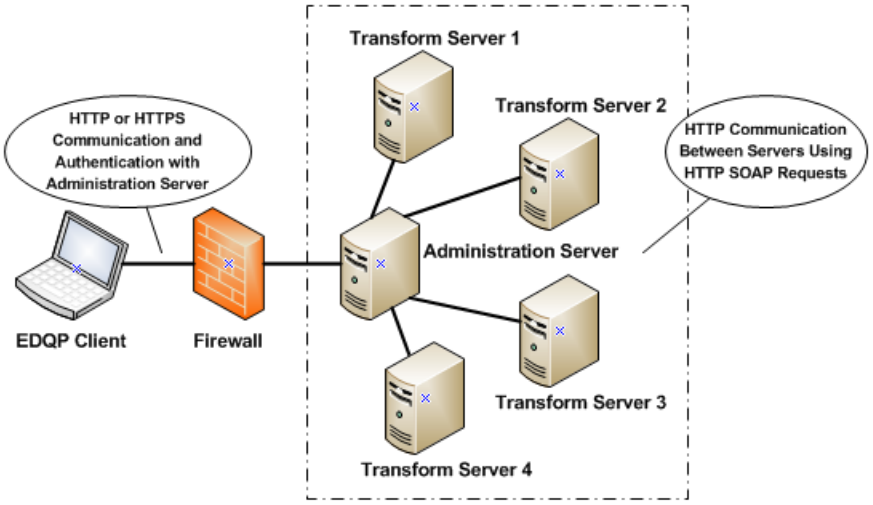
Upon installation, EDQP is configured to use the directory server embedded in Oracle WebLogic Server as both the default authentication provider and the repository for users and groups. You can use and manage alternate authentication providers in the Oracle WebLogic Administration Console.

Caution: The use of Oracle Virtual Directory in combination with Microsoft Directory Server is not supported. Do not use this combination.

Secure EDQP Installation Architecture

The following diagram represents typical deployment structure of the EDQP.

Figure 1 EDQP Secure Topology



The EDQP client applications can be any of the following:

1. Browser-based user interface including the Welcome and Administration Web pages.
2. Java WebStart based clients: AutoBuild, Governance Studio, Application Studio, Knowledge Studio, and Task Manager.
3. Services for Excel, which is an Add-In to Excel.

Installing EDQP

Use the following the guides to securely install EDQP into your enterprise.

Note: All administration users created must be unique to ensure a secure environment.

1. To install Oracle WebLogic Server securely, see *Oracle Fusion Middleware Getting Started With Installation for Oracle WebLogic Server 11g Release 1 (10.3.6)* at

   http://docs.oracle.com/cd/E23943_01/core.1111/e10043.pdf

   Also, see the following documents related to Oracle WebLogic Server security:

   Oracle Fusion Middleware Securing a Production Environment for Oracle WebLogic Server 11g at

   http://docs.oracle.com/cd/E14571_01/web.1111/e13705/toc.htm

Oracle Fusion Middleware Managing Server Startup and Shutdown for Oracle WebLogic Server11g Release 1 (10.3.6) at

http://docs.oracle.com/cd/E23943_01/web.1111/e13708/toc.htm

Oracle recommends that you change the default WebLogic domain password for EDQP to ensure a secure installation. The default credentials are user, `dlsadmin`, and password, `dlsadmin1`.

2. To install EDQP, see *Oracle Enterprise Data Quality for Product Data Oracle DataLens Server Installation Guide* at

   http://docs.oracle.com/cd/E35636_01/index.htm

3. To install EDQP with enterprise wide Single Sign-On capabilities, see *Oracle Access Manager Integration Guide 10g* at

   http://docs.oracle.com/cd/E12530_01/oam.1014/e10356.pdf

Secure Installation of EDQP Configuration Database

EDQP installs a configuration schema into the Oracle database of your choice. EDQP is certified with Oracle, PostgreSQL, and JavaDB databases. The EDQP configuration schema is used to persist system configuration information, such as server configurations and database connections, job history, and the history of important system assets, such as data lenses, and Data Services Applications (DSAs).

For a secure installation, Oracle recommends that you use an Oracle database because it provides full password security; JavaDB does *not* provide encrypted password security.

The *Oracle Enterprise Data Quality for Product Data Oracle DataLens Server Installation Guide* contains the details on how to select your secure configuration schema data source at the time of installation.

Post-Installation Configuration

This section explains how to configure security for a new installation of EDQP.

Changing the Default WebLogic Domain Password

If you did not change the default EDQP WebLogic Domain administrative password prior to installation, change this password once the installation is complete using the WebLogic Administration Console. For more information about changing domain passwords, see *WebLogic Administration Console Online Help* at

http://docs.oracle.com/cd/E23943_01/wls.htm

Changing the Default WebLogic Domain Configuration Database Password

You must change the default EDQP WebLogic Domain data source password to secure the database using the WebLogic Administration Console. The data source is named `PDQRepository`, which must *not* be changed. These instructions apply to the Oracle configuration database type; you cannot change the JavaDB install data source password. For more information about changing domain passwords, see *WebLogic Administration Console Online Help* at

http://docs.oracle.com/cd/E23943_01/wls.htm

Using HTTPS for all Client Applications

The use of HTTPS with your EDQP client applications is detailed in *Oracle Enterprise Data Quality for Product Data Getting Started Guide* at

http://docs.oracle.com/cd/E35636_01/index.htm

To configure a *Oracle Fusion Middleware Securing a Production Environment for Oracle WebLogic Server 11g* at

http://docs.oracle.com/cd/E14571_01/web.1111/e13705/toc.htm

Using Enterprise Integrations Behind a Firewall

Ensure that all EDQP server APIs, including web services, database access, and SOAP APIs are accessed by enterprise applications residing within your corporate firewall.

Related Documents

For more information, see the following documents in the EDQP documentation set:

- The *Oracle Enterprise Data Quality for Product Data Getting Started Guide* provides information about how to get started with EDQP.
- The *Oracle Enterprise Data Quality for Product Data Oracle DataLens Server Installation Guide* provides detailed Oracle DataLens Server installation instructions.
- The *Oracle Enterprise Data Quality for Product Data Oracle DataLens Server Administration Guide* provides information about managing an Oracle DataLens Server including users and user roles.

See the latest version of this and all documents in the Oracle Enterprise Data Quality for Product Data Documentation Web site at

http://docs.oracle.com/cd/E35636_01/index.htm

The WebLogic Server Documentation Library that includes all the WebLogic documents referenced herein is found at

http://docs.oracle.com/cd/E23943_01/wls.htm

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Oracle Enterprise Data Quality for Product Data Security Guide, Release 11g R1 (11.1.1.6)
E35849-02

to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.