Oracle® Documaker

Enterprise Security Guide

12.7.1
Part number: F76382-01
January 2023

U.S. GOVERNMENT RIGHTS

Contents

Preface

This document provides guidelines for securing an Oracle Documaker Enterprise Edition (ODEE) system, highlighting the configuration and installation steps needed to meet security goals.

Audience

This document is intended for Oracle Documaker Enterprise Edition users.

Documentation Accessibility

Accessibility of Links to External Websites in Documentation

This documentation may contain links to Websites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Websites.

TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, seven days a week. For TTY support, call 800.446.2398.

Oracle Customer Support

If you have any questions about the installation or use of our products, please visit the My Oracle Support website: https://support.oracle.com, or call (800) 223-1711.

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.

Contact

USA:+1.800.223.1711

Canada: 1.800.668.8921 or +1.905.890.6690

Latin America: 877.767.2253

For other regions including Latin America, Europe, Middle East, Africa, and Asia Pacific regions: Visit- http://www.oracle.com/us/support/contact/index.html.

Follow us

https://blogs.oracle.com/insurance

https://www.facebook.com/oraclefs

https://twitter.com/oraclefs

https://www.linkedin.com/groups?gid=2271161

Conventions

The following text conventions are used in this document:

Convention	Description
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands, URLs, code in examples, and information you enter.

Tips, Notes, and Warnings

- A *Tip* provides a better way to use the software.
- A *Note* contains special information and reminders.
- A *Warning* contains critical information that if ignored, may cause errors or result in the loss of information.

OVERVIEW

Protecting your company's sensitive data is a mission critical operation. Proper goals and security policies established within the organization drive the security plan that protects the livelihood of the company. Understanding these policies can help you to ensure that the security offered by each application within the enterprise aligns with the needs of the company.

The Oracle Documaker Enterprise Edition (ODEE) system may contain sensitive, confidential, or protected information and therefore requires that security measures are taken to protect this data in accordance with your organization's policies.

This document provides guidelines for securing an ODEE system. It highlights the configuration and installation steps needed to meet security goals. Details on the types of security features and services that are available to detect and prevent a potential security breach are provided. These details encompass secure system deployment, protection of sensitive data, reliability and availability of the application, authentication and authorization mechanisms.

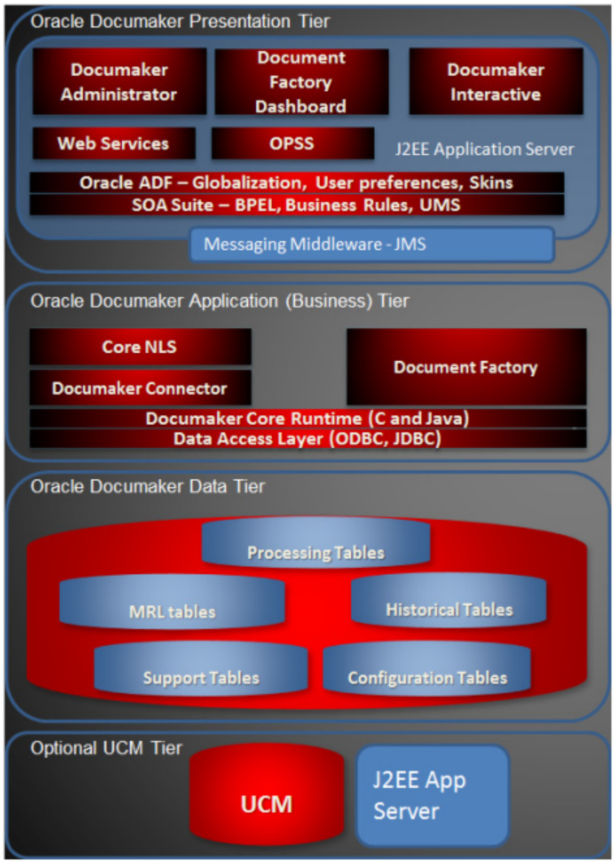
It is critical that an organization set security standards and properly implement them. The development and review of security documentation, an evaluation of business requirements, and the configuration and validation of available security measures and services should all be performed.

DISCLAIMER

This guide discusses the security options and features available in Oracle Documaker Enterprise Edition and its supporting component software. Note that the set of recommendations in this guide are not exhaustive and that no guarantee is given that implementing all the topics in this guide provides sufficient protection for all security threats from all potential attackers. The reason for this disclaimer is that you cannot delegate responsibility for secure application development to a third party or a single document but yet, as mentioned, the whole infrastructure and environment are critical components.

System Overview

ODEE systems have three different tiers that must be individually considered with respect to security configuration. Overall, the system should be within the company's internal network.


Oracle Documaker Presentation Tier
Documaker Administrator
Document Factory Dashboard
Documaker Interactive
Web Services
OPSS
J2EE Application Server
Oracle ADF – Globalization, User preferences, Skins
SOA Suite – BPEL, Business Rules, UMS
Messaging Middleware - JMS
Oracle Documaker Application (Business) Tier
Core NLS
Documaker Connector
Document Factory
Documaker Core Runtime (C and Java)
Data Access Layer (ODBC, JDBC)
Oracle Documaker Data Tier
Processing Tables
MRL tables
Historical Tables
Support Tables
Configuration Tables
Optional UCM Tier
UCM
J2EE App Server

Network Security

When deploying ODEE on a network there are many security issues to take into consideration, especially the use of firewall and Virtual Private Network (VPN) technologies. A firewall will permit or deny network permissions based on configured rules, to protect the internal network from unauthorized access while permitting legitimate communications. Firewalls perform the following functions in a typical ODEE environment:

- Guard the company Intranet from unauthorized outside access.
- Separate Intranet users accessing the ODEE system from internal subnetworks where critical corporate information and services reside.
- Protect from IP spoofing and routing threats.
- Prohibit unauthorized users from accessing protected networks and control access to restricted services.

The ODEE user interface is browser-based and can be used to allow home-office users to access the functions deployed within ODEE. It is recommended that the users access the application from within the company network, secured behind the outside firewall. Virtual Private Network (VPN) technology should be used to allow employees working remotely to access the ODEE application. A VPN tunnels outside traffic through the firewall, placing outside clients virtually inside the firewall.

Make sure that the firewalls used to secure an ODEE's environment support the HTTP 1.1 protocol. This enables browser cookies and inline data compression for improved performance.

A typical ODEE environment usually has the following security zones:

- **Internet:** External web service clients may come from outside of the company network.
- **Intranet:** A company network separated by the external firewall that gives home users access to the ODEE user interface. This is also where ODEE web servers and load balancers may be placed. Alternatively, for additional protection, web and load balancing servers may be placed in a separate demilitarized zone (DMZ) where external and internal clients first interact with the ODEE environment.
- **ODEE application server and database zone:** ODEE application servers, including Web servers, database servers and possibly authentication servers (for example, if a customer chooses to implement a single sign-on using Lightweight Directory Access Protocol (LDAP) servers) reside in this zone. Access to the database that holds critical client information must be secured, with access restricted to system and database administrators only.

DATABASE

Setup for appropriate database users of the ODEE application can be found in the ODEE Installation Guide.

Typically, the database contains two schemas, which may be named using any convention desired. The default schema names are DMKR_ADMIN, which houses system tables for ODEE, and DMKR_ASLINE, which houses the ODEE processing tables. A database user may be an Administrator (ADMIN) or an Assembly Line (ASLINE) user. The ADMIN user connects to the database for all administrative purposes and managing the administration layer completely, including managing other users/groups and their corresponding rights and privileges. ASLINE is shorthand for “Assembly Line” which roughly corresponds to the single Media Resource Library (MRL).

It should be noted that certain ODEE components have a 1:1 relationship with an Assembly Line, such as Documaker Web Services (DWS), Documaker Interactive (DI), Document Factory (Factory), and Docupresentment (IDS). These components are tied to a single Assembly Line. If multiple Assembly Lines are used, each must have a dedicated instance of these components. Other components, such as Documaker Administrator (DA) and Dashboard are used across Assembly Lines. In general, any database users should not have more permissions than required for proper application workflow.

Data-at-rest

To protect sensitive data while at rest (data-at-rest) in Oracle database data files and in backup files the Oracle database's Transparent Database Encryption (TDE) feature should be used. (See https://docs.oracle.com/database/121/ASOAG/introduction-to-transparent-data-encryption.htm#ASOAG10117 or related Oracle documentation for your Oracle Database version).

Note TDE is enabled and used by default in Oracle Cloud's PaaS Database Cloud Service for securing data files and backup files within the cloud. (See https://docs.oracle.com/en/cloud/paas/database-dbaas-cloud/csdbi/data-security.html).

Data-in-transit

To protect sensitive data while in transit (data-in-transit) going between Oracle database server and client Oracle Net Services encryption and integrity capabilities to secure connections should be implemented. (See https://docs.oracle.com/en/database/oracle/oracle-database/12.2/dbseg/configuring-network-data-encryption-and-integrity.html#GUID-7F12066A-2BA1-476C-809B-BB95A3F727CF or related Oracle document for your Oracle Database version).

Note Oracle Net Services encrytion and integrity capabilities are deployed by default in Oracle Cloud's PaaS Database Cloud Service for securing database server and client communications within the cloud. (See https://docs.oracle.com/en/cloud/paas/database-dbaas-cloud/csdbi/data-security.html).

SSL in WebLogic

WebLogic Server supports Secured Sockets Layer (SSL) on a dedicated listen port which defaults to 7002. To establish an SSL connection over HTTP, a Web browser connects to WebLogic Server by supplying the SSL listen port and the HTTPs protocol in the connection URL, for example, `https://myserver:7002.`

SSL can be configured one-way or two-way. With one-way SSL, the server must present a certificate to the client, but the client is not required to present a certificate to the server. The client must authenticate the server, but the server accepts a connection from any client. With two-way SSL (SSL with client authentication), the server presents a certificate to the client and the client presents a certificate to the server. WebLogic Server can be configured to require clients to submit valid and trusted certificates before completing the SSL connection.

A host name verifier ensures the host name in the URL to which the client connects matches the host name in the digital certificate that the server sends back as part of the SSL connection. A host name verifier is useful when an SSL client (for example, WebLogic Server acting as an SSL client) connects to an application server on a remote host. It helps to prevent man-in-the-middle attacks. WebLogic Server includes two host name verifiers - Default WebLogic Server Host Name Verifier and Wildcarded Host Name Verifier.

As an alternative to the host name verifiers available from WebLogic Server, you can also use a custom host name verifier. The default WebLogic Server Host Name Verifier is enabled by default. If you are using the default WebLogic Server host name verifier, host name verification passes if both of the following conditions exist:

- The host name in the certificate matches the local machine's host name.
- The URL specifies localhost, 127.0.0.1, or the default IP address of the local machine.

WebLogic Server ensures that each certificate in a certificate chain was issued by a certificate authority. All X509 V3 CA certificates used with WebLogic Server must have the Basic Constraint extension defined as CA, thus ensuring that all certificates in a certificate chain were issued by a certificate authority. By default, any certificates for certificate authorities not meeting this criterion are rejected. WebLogic Server SSL has built-in certificate validation. Given a set of trusted CAs, this validation:

- Verifies that the last certificate in the chain is either a trusted CA or is issued by a trusted CA.
- Completes the certificate chain with trusted CAs.
- Verifies the signatures in the chain.
- Ensures that the chain has not expired.

It is important to protect passwords that are used to access resources in a WebLogic domain. In the past, usernames and passwords were stored in clear text in a WebLogic security realm. Now all the passwords in a WebLogic domain are hashed. If the file containing the hashes for passwords is destroyed or is corrupted, you must reconfigure the WebLogic domain. Therefore it is essential that the file is backed up in a safe location and appropriate permissions are set on the file such that the system administrator of a WebLogic Server deployment has write and read privileges and no other users have any privileges.

WebLogic Server defines a set of configuration options to protect user accounts from intruders. In the default security configuration, these options are set for maximum protection. Documaker Enterprise Edition uses web application server security frameworks for authentication and authorization of users. The web application servers typically utilize frameworks that include support for external user and group repositories that can be accessed via industry-standard protocols, such as LDAP. The ODEE installation process includes the deployment of a user and group data store that works with the demonstration library.

To configure WebLogic for external user/group data stores, you will need access to the Documaker domain within the WebLogic web console. Note that it is possible to complete this configuration using WebLogic Scripting Tool (WLST) – see online documentation to do this.

WebLogic Server includes the following *Authentication providers*:

- Oracle Internet Directory Authentication provider
- Oracle Virtual Directory Authentication provider
- iPlanet Authentication provider
- Active Directory Authentication provider
- Open LDAP Authentication provider
- Novell Authentication provider
- generic LDAP Authentication provider

Each LDAP Authentication provider stores user and group information in an *external* LDAP server. WebLogic Server does not support or certify any particular LDAP server. Any LDAP v2 or v3 compliant LDAP server should work with WebLogic Server. The following LDAP directory servers have been tested:

- Oracle Internet Directory
- Oracle Virtual Directory
- Sun iPlanet version 4.1.3
- Open LDAP version 2.0.7
- Novell NDS version 8.5.1

Note If your configuration has only one configured Authentication provider for the security realm used by Documaker, then the user that is configured for starting WebLogic Server (the “boot user”) must meet the following requirements:

- Exist in the LDAP directory
- Be a member of a group that has the Admin role

By default, the Admin role is granted to the Administrators group so you may create this group in the LDAP directory if it does not exist. If you wish to use a different group, include the WebLogic Server boot user in the group and grant the Admin role to the group.

Web Service Security

The web application servers that implement the Web Service-Security (WS-S) standards secure Documaker Web Services (DWS). Both WebLogic and WebSphere provide standard WS-S implementations that allow for the definition of security policies including access and authorization for web service consumption. Ensure DWS is configured with appropriate policies and roles to prevent unauthorized consumption of web services. The best practice for securing web services for Documaker in environments requiring higher levels of security is to implement the following measures with WebLogic Server:

- Message-level security
- Transport-level security
- Access control security (only required if corporate security policy dictates that access to web services should be restricted)

You can attach two types of policies to WebLogic Web Services: Oracle Web Services Manager policy and WebLogic Web Service policy.

WebLogic Server includes pre-packaged WS-Policy files which are static and you cannot change them. Predefined policies are available in the following categories:

- Reliable Messaging
- SOAP Message Transmission Optimization Mechanism (MTOM)
- Two sets of pre-packaged security policy files available for configuring message-level security. One set of security policy files conforms to the OASIS WS-SecurityPolicy 1.2 specification and the other set of security policy files conforms to a proprietary Oracle Web services security policy schema.

Oracle WSM includes a set of predefined policies in the following categories:

- Security
- WS-Addressing
- MTOM
- Reliable Messaging
- Management

Note The Administration Console allows you to associate as many WS-Policy files as you want to a Web service and its operations, even if the policy assertions in the files contradict each other. It is up to you to ensure that multiple associated WS-Policy files work together. If any contradictions do exist, WebLogic Server will return a runtime error when a client application invokes the Web service.

HARDENING

Hardening is the act of applying security to each component of the infrastructure, including:

- Web Servers
- Application Servers
- Identity and Access Management solutions
- Database systems
- Operating systems

Oracle WebLogic Server uses a more specific type of hardening known as lockdown, which refers to securing the subsystems and applications that run on a server instance. In contrast, hardening is more general and involves doing a security survey to determine the threat model that may impact your site, and identifying all aspects of your environment (such as components in the Web tier) that could be insecure. The following aspects of WebLogic Server should be considered for lockdown:

- SSL-enabling components and component routes
    - Documaker web applications install with SSL enabled
    - LDAP Authentication providers should be configured for SSL
    - Configure two-way SSL - one-way SSL is a configuration where clients request a server certificate and the server accepts all connections. Two-way SSL configurations require the client and the server to exchange certificates, thereby providing an additional layer of trust by ensuring that non-trusted clients cannot invoke services.
- SSL-enabling web services
    - Documaker Web Services install with SSL disabled and should be enabled
- Managing ports and other features of the site such as:
    - default deployed application – remove any non-essential default apps such as the welcome page
    - demonstration/samples – remove demoApp, demo keystores, demo trust, and demo SSL certificate
    - change default ports for common services e.g. admin port – Documaker services ship with standard ports; however, these are not common and could remain as-is. The base WebLogic components (e.g. console) are configured standard ports and should be changed from the default (7001).
- Password management
- Roles and Policies for access – role- and policy-based security should be configured for authorized access to:
    - web services

- data sources
- applications: configured for DD-only security (deployment descriptor) which means that if you wish to add role- and/or policy-based security on top of this, you must modify the deployment descriptors for the affected application(s). Keep in mind this will affect upgrade capability as you have to re-apply deployment descriptor changes

USE CASES

The following access scenarios indicate typical use cases for the Documaker system and can be used to guide your security policy definition. These descriptions outline the *default out-of-the-box* configuration of the system.

- Web Services for Document Generation: Applicable for all Documaker Web Services (DWS) endpoints and operations.
- Interactive User Document Editing: Applicable for all Documaker applications deployed within the web application server (e.g. Documaker Dashboard, Documaker Administrator, and Documaker Interactive).

Note The Administration Console allows you to associate as many WS-Policy files as you want to a Web service and its operations, even if the policy assertions in the files contradict each other. It is up to you to ensure that multiple associated WS-Policy files work together. If any contradictions do exist, WebLogic Server will return a runtime error when a client application invokes the Web service.

SUMMARY

This guide reviews some of the primary security features that can be configured within the Oracle Documaker Enterprise Edition environment. Remember that security is a mix of awareness, education, and technology in use. Please check Oracle Support for additional information and knowledge based articles to stay current on this topic.