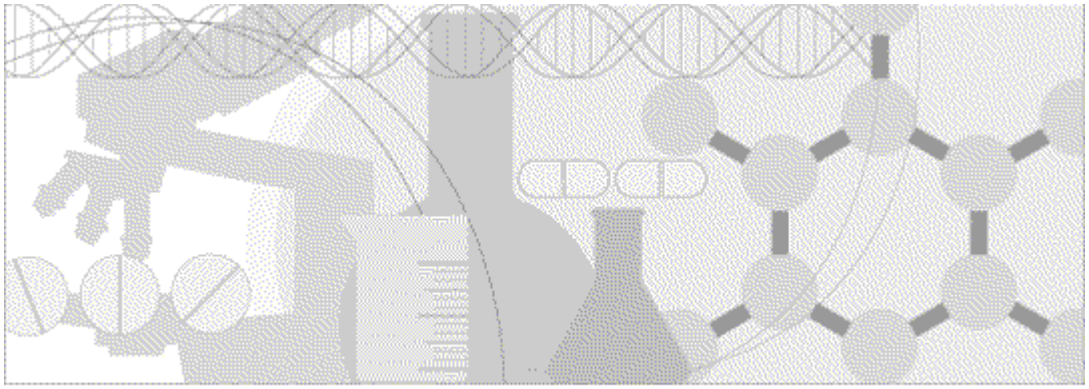
Secure Configuration Guide

Oracle® Health Sciences InForm Publisher On Demand Release 2.0



ORACLE

Part Number: E53275-01

Contents

About this guide

In this preface

Overview of this guide

The *Secure Configuration Guide* provides essential secure configuration considerations for the InForm Publisher application.

Audience

This guide is for everyone who installs and configures the InForm Publisher application.

Documentation

The product documentation is available from the following locations:

- **Oracle Software Delivery Cloud** (https://edelivery.oracle.com)—The complete documentation set.
- **My Oracle Support** (http://support.oracle.com)—*Release Notes* and *Known Issues*.
- **Oracle Technology Network** (http://www.oracle.com/technetwork/documentation)—The most current documentation set, excluding the *Release Notes* and *Known Issues*.

All documents may not be updated for every InForm Publisher release. Therefore, the version numbers for the documents in a release may differ.

Document	Description
Installation Guide	The *Installation Guide* provides instructions for installing the InForm Publisher software.
Release Notes	The *Release Notes* document includes: • System requirements. • Descriptions of the new features, enhancements, and bug fixes.
Known Issues	The *Known Issues* document provides detailed information about the known issues in this release, along with workarounds, if available.
Integration Guide	The *Integration Guide* provides detailed information about defining custom events and triggers and publishing events using web services, FTP, and Local Directory.
Secure Configuration Guide	The *Secure Configuration Guide* provides essential secure configuration considerations for the InForm Publisher application.
Third Party Licenses and Notices	This document includes licenses and notices for third party technology that may be included in or distributed with the InForm Publisher software.

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.

If you need assistance

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

Finding product information and patches on My Oracle Support

The latest information about the InForm Publisher application is on the Oracle Support self-service website, My Oracle Support. Before you install and use the InForm Publisher application, check My Oracle Support for the latest information, including *Release Notes* and *Known Issues*, alerts, white papers, bulletins, and patches.

Creating a My Oracle Support account

You must register at My Oracle Support to obtain a user name and password account before you can enter the site.

1 Open a Web browser to https://support.oracle.com.

2 Click the **Register** link.

3 Follow the instructions on the registration page.

Finding information and articles

1 Sign in to My Oracle Support at https://support.oracle.com.

2 If you know the ID number of the article you need, enter the number in the text box at the top right of any page, and then click the magnifying glass icon or press Enter.

3 To search the knowledge base, click the **Knowledge** tab, and then use the options on the page to search by:

- Product name or family.
- Key words or exact terms.

Finding patches

You can search for patches by patch ID or number, product, or family.

1 Sign in to My Oracle Support at https://support.oracle.com.

2 Click the **Patches & Updates** tab.

3 Enter your search criteria and click **Search**.

4 Click the patch ID number.

The system displays details about the patch. You can view the Read Me file before downloading the patch.

5 Click **Download**, and then follow the instructions on the screen to download, save, and install the patch files.

Finding Oracle documentation

The Oracle website contains links to Oracle user and reference documentation. You can view or download a single document or an entire product library.

Finding Oracle Health Sciences documentation

For Oracle Health Sciences applications, go to the Oracle Health Sciences documentation page at http://www.oracle.com/technetwork/documentation/hsgbu-clinical-407519.html.

Note: Always check the Oracle Health Sciences Documentation page to ensure you have the most up-to-date documentation.

Finding other Oracle documentation

1 Do one of the following:

- Go to http://www.oracle.com/technology/documentation/index.html.
- Go to http://www.oracle.com, point to the **Support** tab, and then click **Product Documentation**.

2 Scroll to the product you need, and click the link.

CHAPTER 1

Security overview

In this chapter

Application security overview

To ensure security in the InForm Publisher application, carefully configure all system components, including the following third-party components:

- Firewalls
- Load balancers
- Virtual Private Networks (VPNs)

General security principles

Keep software up to date

Keep all software versions and patches up to date.

Keep up to date on the latest Critical Patch Updates

Oracle continually improves its software and documentation. Critical Patch Updates are the primary means of releasing security fixes for Oracle products to customers with valid support contracts. They are released on the Tuesday closest to the 17th day of the following months:

- January
- April
- July
- October

Oracle highly recommends that customers apply these patches as soon as they are released.

Configure strong passwords on the database

Make sure all your passwords are strong passwords. Oracle recommends that you use a mix of uppercase and lowercase letters, numbers, and symbols.

You can strengthen passwords by creating and using password policies for your organization. For guidelines on securing passwords and for additional ways to protect passwords, see the *Oracle Database Security Guide* specific to the database release you are using.

You should modify the following passwords so that they comply with your password policies, such as a minimum length or character requirements:

- Passwords for the database default accounts, such as SYS and SYSTEM.
- Passwords for the database application-specific schema accounts.

Additionally, you should not configure a password for the database listener because a configured password enables remote administration. For more information, see ***Removing the Listener Password*** in the documentation for Oracle® Database Net Services Reference 11g Release 2 (11.2).

For more information about configuring strong passwords, see the *Security Guide* for Oracle Database 11g Release 2 (11.2).

Follow the principle of least privilege

The principle of least privilege states that users should be given the least amount of privilege to perform their jobs. Oracle recommends reviewing user privileges periodically to determine relevance to current job responsibilities.

Before executing data definition language (DDL) scripts, create a database user with the specified limited set of privileges. Do not provide users with DBA access.

Design multiple layers of protection

When designing a secure deployment, design multiple layers of protection. For example, if someone were to gain unexpected access to a layer, such as the application server, the person should not automatically have access to other layers, such as the database server.

Providing multiple layers of protection might include the following activities:

- Enabling only those ports required for communication between different tiers. For example, you can allow communication to the database tier only on the port used for SQL*NET communications (1521 by default).
- Placing firewalls between servers so that only expected traffic can move between servers.

CHAPTER 2

Secure installation and configuration

In this chapter

Installation overview

Use the information in this chapter to ensure the InForm Publisher application is installed and configured securely. For information about installing and configuring the InForm Publisher application, see the *Installation Guide*.

Secure Sockets Layer (SSL)

Configure your environment so that the InForm Publisher application servers are hosted behind a firewall and all communication through the firewall is over HTTPS.

About entering passwords

The InForm Publisher software and installation scripts do not contain default or hard-coded passwords. You must supply passwords for predefined users, such as Oracle database users.

Installation scripts prompt for passwords on the command line or allow a file containing the passwords to be passed in as parameters. For more information, see the *Installation Guide*.

Note: If you use password parameter files, delete the files after installation.

Configure strong administrator passwords

When you install the InForm Publisher service, the InForm Publisher user is created. Make sure that the password for this user is strong.

Close all unused ports

Keep only the minimum number of ports open. Close all ports not in use.

The InForm Publisher application defaults to the following ports, but can be configured to use non-standard ports.

- **Port 1521**—Default connection to the Oracle database.
- **Port 80**—For the client connection (HTTP).
- **Port 443**—For the client connection (HTTPS).
- **Port 22**—For the client connection (SSH for secure file transfer)

Note: The InForm Publisher application does not require both Port 80 and Port 443. However, you must configure the InForm Publisher application to use either HTTP or HTTPS.

Disable all unused services

Disable all unused services.

The InForm Publisher application uses the InForm Publisher Service.

Disable unnecessary services provided by the operating system

The InForm Publisher application does not use the following services:

- Identification Protocol (identd).

  This protocol is generally used to identify the owner of a TCP connection on UNIX.

- Simple Network Management Protocol (SNMP).

  This protocol is a method for managing and reporting information about different systems.

If you are not using these services for other applications, Oracle recommends that you disable these services to minimize your security exposure. If you need SMTP, identd, or SNMP for other applications, upgrade to the latest version of the protocol to provide the most up-to-date security for your system.

Revoke unnecessary grants

For security purposes, you must revoke all unnecessary grants on the schema. You must have DBA privileges to perform this action.

Post-installation configuration

Restrict access to the InForm Publisher server

Allow only administrator and system accounts access to the InForm Publisher server.

Limit the number of users with access to the server machine. Disable or delete any unnecessary users.

Restrict access to the file server

The InForm Publisher application can be configured to write files to a remote file server using secure file transfer protocol. Allow only administrator and system accounts access to the file server.

Limit the number of users with access to the server machine. Disable or delete any unnecessary users.

CHAPTER 3

Security features

In this chapter

Data security features

Restricted viewing of Protected Health Information

You can configure the InForm Publisher software to write clinical data that might contain protected health information (PHI) to local directory or remote file server. For example, ODM extract files might contain PHI. You must restrict access to these locations to administrator or system users.