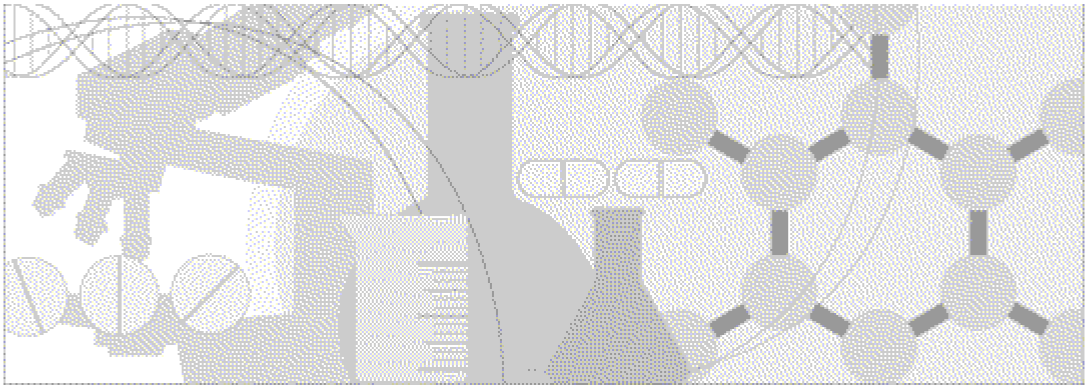
Secure Configuration Guide

Oracle® Health Sciences InForm Publisher
Release 2.1.1



Part Number: E96218-01

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them 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 END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

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.

This software or hardware and documentation may provide access to or information about 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 unless otherwise set forth in an applicable agreement between you and Oracle. 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, except as set forth in an applicable agreement between you and Oracle.

This documentation may include references to materials, offerings, or products that were previously offered by Phase Forward Inc. Certain materials, offerings, services, or products may no longer be offered or provided. Oracle and its affiliates cannot be held responsible for any such references should they appear in the text provided.

Contents

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.

The InForm Publisher application sends messages over HTTPS using Transport Layer Security (TLS). Configure the web service that receives messages from the InForm Publisher application to expect TLS.

For more information on system requirements, see the *Release Notes*.

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.

About the documentation

Where to find the product documentation

The product documentation is available from the following locations:

- My Oracle Support (https://support.oracle.com)—Release Notes and Known Issues.
- Oracle Help Center (***https://docs.oracle.com/en/industries/health-sciences/inform-publisher/index.html***)—The most current documentation set.

Documentation accessibility

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

Access to Oracle Support

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