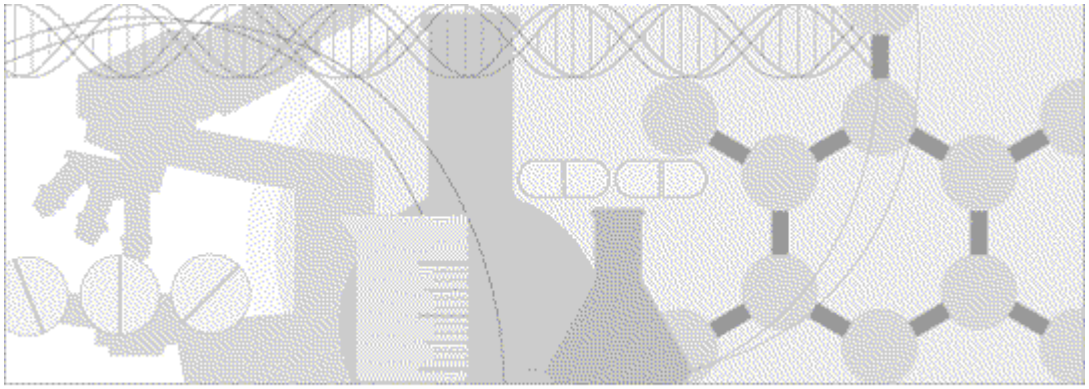
Secure Configuration Guide

Oracle® Health Sciences InForm Adapter Release 1.3.8



ORACLE

Part Number: E68197-01

Copyright © 2016, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

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.

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 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

About this guide v

Overview of this guide vi
Audience vi
Documentation vii
Documentation accessibility vii
If you need assistance viii
Finding InForm Adapter information and patches on My Oracle Support viii
Finding Oracle documentation ix
Finding prerequisite software for Oracle Health Sciences applications ix

Chapter 1 Security overview 1

Application security overview 2
General security principles 3

Chapter 2 Secure installation and configuration 5

Installation overview 6
Restrict network access to critical services 6
Secure Socket Layer (SSL) 6
Installation username and password 7
Close all unused ports and open necessary ports 7
Disable all unused Windows services 7
Restrict access to the Register Trial tool 7
Post-installation configuration 8
Restrict access to the server machines 8
Ensure restrictive access control 8
Restrict access to the Certificate Configuration tool 8

Chapter 3 Security features 9

web.config settings that secure the Web services 10
Restrict access to service metadata 10
WCF—Turn off includeExceptionsDetailsInFaults attribute 11
Turn off customErrors 11
Configure user authentication for applicable web services 12
Adapter Administration and Central Administration configuration 13

About this guide

In this preface

Overview of this guide vi
Documentation vii
If you need assistance viii

Overview of this guide

The *Secure Configuration Guide* provides an overview of the security features provided with the Oracle® Health Sciences InForm Adapter application, including details about the general principles of application security, and how to install, configure, and use the InForm Adapter application securely.

Audience

This guide is for users who install and configure the InForm Adapter application, and developers who develop and test custom study-specific code using the interfaces provided by the software.

Documentation

The product documentation is available from the following locations:

- **My Oracle Support** (https://support.oracle.com)—*Release Notes* and *Known Issues*.
- **Oracle Technology Network** (http://www.oracle.com/technetwork/documentation/hsgbu-154445.html)—The most current documentation set, excluding the *Release Notes* and *Known Issues*.

If the software is available for download, the complete documentation set is available from the Oracle Software Delivery Cloud (https://edelivery.oracle.com).

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

Document	Description
Release Notes	The *Release Notes* document describes hardware and software requirements and describes the new features, enhancements, and fixed issues in this release.
Known Issues	The *Known Issues* document provides detailed information about the known issues in this release, along with workarounds, if available.
Installation Guide	The *Installation Guide* provides a brief overview of the InForm Adapter software, step-by-step instructions for installing and uninstalling the software, setting security options, and troubleshooting information.
Interfaces Guide	The *Interfaces Guide* provides information on using the interfaces that are included with the InForm Adapter software.
Secure Configuration Guide	The *Secure Configuration Guide* provides an overview of the security features provided with the InForm Adapter application including details about the general principles of application security and how to install, configure, and use the InForm Adapter application securely.
Third Party Licenses and Notices	The *Third Party Licenses and Notices* document includes licenses and notices for third party technology that may be included with the InForm Adapter software.
Secure Development Guide	The *Secure Development Guide* provides an overview of common security risks for developers using Application Programming Interfaces (APIs) with the InForm Adapter application, and information on how to address those risks.

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

Access to Oracle Support

Oracle customers that have purchased support 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.

Finding InForm Adapter information and patches on My Oracle Support

The latest information about the InForm Adapter application is on the Oracle Support self-service website, My Oracle Support. Before you install and use the InForm Adapter 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 before you can enter the site.

1 Open a 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.
- Keywords 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.

Finding prerequisite software for Oracle Health Sciences applications

Prerequisite software for Oracle Health Sciences applications is available from the following locations:

- Download the latest major or minor release from the Oracle Software Delivery Cloud (https://edelivery.oracle.com/).

  For information on the credentials that are required for authorized downloads, click **FAQ** on the main page of the Oracle Software Delivery Cloud portal.

- Download subsequent patch sets and patches from My Oracle Support (https://support.oracle.com).

  To find patch sets or patches, select the **Patches & Updates** tab.

If a previous version of prerequisite software is no longer available on the Oracle Software Delivery Cloud, log a software media request Service Request (SR). Previous versions of prerequisite software are archived and can usually be downloaded. After you open an SR, you can check its status:

- US customers: Call 1-800-223-1711.
- Outside the US: Check www.oracle.com/us/support/contact/index.html for your local Oracle Support phone number.

For more information on logging a media request SR, go to My Oracle Support for Document 1071023.1: Requesting Physical Shipment or Download URL for Software Media (https://support.oracle.com/epmos/faces/DocumentDisplay?id=1071023.1).

CHAPTER 1

Security overview

In this chapter

Application security overview 2
General security principles 3

Application security overview

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

- Internet Information Services (IIS) for Windows Server.
- Firewalls.
- Load balancers.
- Virtual Private Networks (VPNs).

General security principles

Use the latest versions of software and documentation

Before beginning the installation, check My Oracle Support (http://support.oracle.com) for the latest patches and *Release Notes* for the product.

Use the latest recommended versions of the InForm Adapter software, Windows server, .Net Framework, and Oracle database server.

Keep passwords private and secure

The InForm Adapter software requires a database password during installation. Use standard security procedures to ensure that this password is known only to those who require the information.

Lock computers to protect data

Encourage users to lock computers that are left unattended.

Monitor system activity

Ensure system security with good security protocols, proper system configuration, and system monitoring. You can monitor the Windows event log for failed logins to InForm Adapter interfaces.

Protect sensitive data

Collect only the minimum amount of sensitive information needed for the study.

Tell users not to send sensitive information over email.

Provide access to sensitive data only to users who need it for their jobs.

CHAPTER 2

Secure installation and configuration

In this chapter

Installation overview 6
Post-installation configuration 8

Installation overview

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

Restrict network access to critical services

Set up a firewall between the internet and an isolated server, and between the isolated server and the intranet. This configuration creates a demilitarized zone (DMZ), which blocks any illegal traffic and contains intrusions.

Keep the InForm Adapter server behind a firewall to provide assurance that access is restricted to a known network route that can be monitored and restricted, if necessary. As an alternative, a firewall router can substitute for multiple, independent firewalls.

Secure Socket Layer (SSL)

Configure your environment so that the InForm Adapter application server is hosted behind a firewall with an appliance such as an F5 load balancer for handling HTTPS and converting to HTTP.

The InForm Adapter web services allow for SSL setup so data that is transported between the client and web services is encrypted (if the InForm Adapter application server is not behind an F5 and is accessed directly).

Clients calling the InForm Adapter web service should be configured to send data over SSL using TLS. Do not use SSL 3.0 and earlier.

Depending on the client applications you are running, secure the corresponding web services as follows:

- If you are using CIS 4.6.2 or above, secure the Transaction Adapter and Central Admin web services by running WebConfigFileSelector F5Cert. For this, you must upload an X.509 digital certificate from the CIS system to the personal certificate store on the InForm Adapter machine.
- If you are using Central Coding 3.0.4 or above, secure the Adapter Admin WCF web service by running WebConfigFileSelector F5Cert. For this, you must upload an X.509 digital certificate from the Central Coding system to the personal certificate store on the InForm Adapter machine.

  You can also secure the Coding and Enhanced Discrepancy web services using digital certificates as described above or you can configure them to use username/password authentication over HTTPS by running WebConfigFileSelector F5. For this, the authentication user account must be active in the InForm study and the username and password must be stored in the Central Coding system. Change passwords on a regular basis to ensure security.
- If you are using the InForm-Argus integration, configure the Safety web service to use username/password authentication over HTTPS by running WebConfigFileSelector F5. For this, the authentication user account must be active in the InForm study and the username and password must be stored in the integration software. Change passwords on a regular basis to ensure security.

Follow the best practices for configuring IIS. For more information, see the documentation available on the Microsoft TechNet website.

Installation username and password

During installation of the InForm Adapter software, you are prompted for a database username and password. Make sure the username and password that you provide follow these guidelines:

- Contain a minimum of eight characters.
- Include at least one number.
- Contain a combination of upper and lowercase characters.
- Do not contain repeating words or characters.

Close all unused ports and open necessary ports

Keep open only the minimum number of ports needed. Close all ports not in use. Follow best practices for unused and necessary ports.

Disable all unused Windows services

Disable all unused Windows services.

Restrict access to the Register Trial tool

The Register Trial Tool is a command line tool that you use to register a study, register a server adapter, decommission a study in the InForm Adapter software, and view lists of existing studies, server adapters, and decommissioned studies.

This tool is provided with the InForm Adapter installation. Restrict access to only those individuals who need to use this tool.

Post-installation configuration

Restrict access to the server machines

Limit the number of users with access to the InForm Adapter servers. Disable or delete any unnecessary users.

Ensure restrictive access control

Limit the number of users who have access to the following items, which contain critical information:

- Configuration files.
- Application paths and directories.
- Assembly files (DLLs).
- The registry.

These items should have the most restrictive access control possible.

The InForm Adapter installation does not write any temporary files. Therefore, after installation is complete the directories can be made read-only.

Restrict access to the Certificate Configuration tool

The Certificate Configuration tool is provided with the InForm Adapter installation. Restrict access to this tool. Allow access to only those users who need to use it.

CHAPTER 3

Security features

In this chapter

web.config settings that secure the Web services 10
Adapter Administration and Central Administration configuration 13

web.config settings that secure the Web services

Settings in the web.config file control various aspects of the use of InForm Adapter interfaces. These settings are determined by the behavior you want to control and whether the particular interface uses WCF or WSE as its web service.

By default, these settings are off (disabled). When developing your client, you might want to enable certain settings for testing purposes. However, before deploying your client to production, be sure to disable the settings to ensure web services are secure.

Settings in the web.config file affect the following:

- Access to metadata.

  Metadata that is output by InForm Adapter interfaces can be used as input to client programs that you build. Settings in the web.config file control whether metadata is output by an interface, and whether client programs have access to this metadata.

  For more information, see *Restrict access to service metadata* (on page 10).

- The amount of detail provided in exceptions.

  For more information, see *WCF—Turn off includeExceptionsDetailsInFaults attribute and Turn off customErrors* (on page 11).

- User authentication against the InForm release.

  For more information, see Require user authentication against the InForm software.

Restrict access to service metadata

WCF—Enabling and disabling metadata

By default WCF services do not publish the metadata. If you want the configuration to allow access to the metadata through the use of import tools such as **svcUtil.exe** to generate the client code, you must explicitly set the following in the web.config file:

```
<serviceBehaviors>
    <behavior name="DiscrepancyServiceBehavior">
                <serviceMetadata httpGetEnabled="true" />
                <serviceDebug includeExceptionDetailInFaults="true" />
    </behavior>
```

After successfully developing and deploying the client, set the values to false, which prevents unwanted clients from generating proxy files or looking at potentially sensitive information.

```
<serviceBehaviors>
    <behavior name="DiscrepancyServiceBehavior">
                <serviceMetadata httpGetEnabled="false" />
                <serviceDebug includeExceptionDetailInFaults="false" />
    </behavior>
```

If you do not need to publish metadata, leave the setting turned off.

WSE—Enabling and disabling metadata

Hiding the service metadata prevents unwanted clients from generating proxy files or looking at potentially sensitive information.

By default, WSE services do not publish metadata. If you need access to the service metadata to develop the client code, you must explicitly set the following values in the web.config file:

```
<system.web>
   <webServices>
      <protocols>
         <add name="Documentation/">
         <add name="HttpGet"/>
         <add name="HttpPost"/>
      </protocols>
   </webServices>
```

After developing and deploying the client, turn off access to metadata by replacing the values, as follows:

```
<system.web>
   <webServices>
      <protocols>
         <remove name="Documentation/">
         <remove name="HttpGet"/>
         <remove name="HttpPost"/>
      </protocols>
   </webServices>
```

WCF—Turn off includeExceptionsDetailsInFaults attribute

Make sure that the includeExceptionsDetailsInFaults attribute is turned off (set to False) for all the behaviors. This attribute should be turned on (set to True) for debugging purposes only.

```
<serviceDebug includeExceptionDetailInFaults="False" />
```

Turn off customErrors

To prevent sensitive information from being released, customErrors in the web.config file must be turned off. This ensures that the stack trace of an error is not shown publicly.

```
<customErrors mode="Off" />
```

The setting is off by default. If you customize the file, verify that the value is set to "Off" before deploying to production.

Configure user authentication for applicable web services

If you are using the Discrepancy Original or the ODM Export interface, configure it for username/password authentication:

- In the web.config file:
  - Set the value of InFormusernameTokenManager.AuthenticateRequests to True.
  - Make sure that the uncommented securityTokenManager value corresponds to username/password authentication:

```
<securityTokenManager qname="wsse:UsernameToken"
type="PhaseForward.InFormAdapter.Framework.Security.InFormUsernameTokenManage
r, PhaseForward.InFormAdapter.Framework.Security"
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd" />
```

- For all external interfaces, client requests with the InFormusername token must go through the firewall over HTTPS to be authenticated against the InForm trial database.

For WCF interfaces, the WebConfigFileSelector.cmd tool allows authentication with either the F5 or Secure selection. For more information, see the *Installation Guide*.

Adapter Administration and Central Administration configuration

Do not expose the WSE version of Adapter Administration or Central Administration interface externally. These services do not provide username authentication. They should only be hosted behind a firewall.