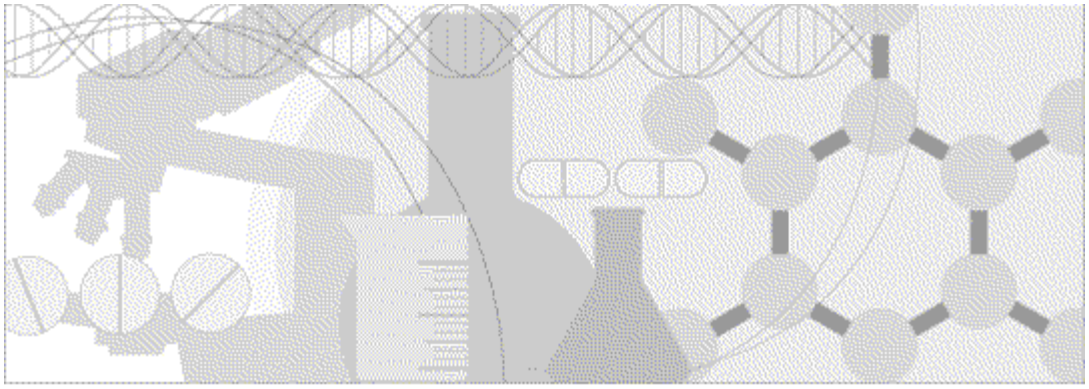
Secure Configuration Guide

Oracle® Health Sciences InForm Adapter Release 1.3.9



ORACLE

Part Number: E92700-01

Contents

CHAPTER 1

Security overview

In this chapter

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

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.
- If you are using ODM WCF, secure the ODM web service by running WebConfigFileSelector F5Cert. For this, you must upload an X509 digital certificate from your ODM client application

to the personal certificate store on the InForm Adapter application server.

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

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.

  For more information, see *Configure user authentication for applicable web services* (on page 11).

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 ODM Export WSE 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.

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)—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=trs* or visit *http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info* if you are hearing impaired.