Oracle® Health Sciences Adverse Event Integration Pack for Oracle Health Sciences InForm and Oracle Argus Safety

Security Guide

Release 1.0.1

E39184-01

June 2013

1 Introduction

Adverse Event: InForm and Argus Safety integration automates the process of clinical study sites reporting serious or clinically significant adverse events for a drug or a medical device from InForm to the Oracle Argus Safety system. This automation increases productivity by reducing the amount of reconciliation needed between the two systems. For instance, if an event is recorded in the Electronic data capture (EDC) system the clock starts ticking for these reporting deadlines. This integration will automate the sending of the Information to Argus Safety so that the Safety users can start work on the case.

You can define which data should be sent to safety using Central Designer Logical Schemas. You can also define which data should trigger a follow-up to safety if the data is changed. Potentially related adverse events, labs, and concomitant medications are sent to safety based on time frames you configure.

If desired, the Argus Case #, whether the safety user accepted or rejected the case and the rejection reason can be sent back to InForm

This document contains the following sections:

- Section 2, "General Security Principles"
- Section 3, "Disabling Unnecessary Operating System Level Services"
- Section 4, "Designing Multiple Layers of Protection"
- Section 5, "Security Guidelines for the Integration Pack"
- Section 6, "Related Documents"
- Section 7, "Documentation Accessibility"

2 General Security Principles

The following principles are fundamental to using any application securely.

2.1 Keeping Software Up to Date

One of the principles of good security practice is to keep all software versions and patches up to date.

2.2 Keeping Up to Date on the Latest Security Information 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 January, April, July and October. We highly recommend customers to apply these patches as soon as they are released.

2.3 Configuring Strong Passwords on the Database

Although the importance of passwords is well known, the following basic rule of security management is worth repeating:

Ensure all your passwords are strong passwords. Oracle recommends that you use a mix of uppercase and lowercase alphabets, 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, refer to the Oracle Database Security Guide specific to the database release you are using.

You should modify the following passwords to use your policy-compliant strings:

- Passwords for the database default accounts, such as SYS and SYSTEM.
- Passwords for the database application-specific schema accounts.
- You should not configure a password for the database listener as that will enable remote administration. For more information, see the section “Removing the Listener Password” of *Oracle® Database Net Services Reference 11g Release 2 (11.2).*

For more information, see *Oracle® Database Security Guide 11g Release 2 (11.2).*

2.4 Following 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. Overly ambitious granting of responsibilities, roles, grants - especially early on in an organization's life cycle when people are few and work needs to be done quickly - often leaves a system wide open for abuse. User privileges should be reviewed periodically to determine relevance to current job responsibilities.

Before executing DDL scripts, a database user should be created with the specified limited set of privileges. DBA access should not be given to the user.

When new users are created in WebLogic security realm, you must ensure to associate new users to the least privilege group required to perform their job. For example, if you create a new user in WebLogic security realm for InForm Publisher message authentication, this user must not be associated with groups that have administrative privileges. For more information, see *Oracle® Health Sciences Adverse Event Integration Pack for Oracle Health Sciences InForm and Oracle Argus Safety Installation Guide.*

3 Disabling Unnecessary Operating System Level Services

This section suggests various unused operating system level services that you can disable to improve security.

3.1 Disabling the Telnet Service

The integration does not use the Telnet service.

Telnet listens on port 23 by default. If the Telnet service is available on any computer, Oracle recommends that you disable Telnet in favor of Secure Shell (SSH). Telnet, which sends clear-text passwords and user names through a log-in, is a security risk to your servers. Disabling Telnet tightens and protects your system security.

3.2 Disabling Other Unused Services

The integration does not use the following services or information for any functionality:

- 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.
- File transfer Protocol (FTP). This protocol is used for downloading or uploading files from the file server.

Therefore, restricting these services or information does not affect the use of the integration. 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, be sure to upgrade to the latest version of the protocol to provide the most up-to-date security for your system.

4 Designing Multiple Layers of Protection

When designing a secure deployment, design multiple layers of protection. If a hacker should gain access to one layer, such as the application server, that should not automatically give them easy access to other layers, such as the database server.

Providing multiple layers of protection may include:

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

5 Security Guidelines for the Integration Pack

5.1 Security Guidelines for Database Objects and Database Options

This integration pack uses tablespace encryption mechanism for persisting safety event data that has not been dequeued. Tablespace encryption is a component of the Oracle Advanced Security option for Oracle Database 11g Release 2 Enterprise Edition. It facilitates encryption of the entire tablespace contents rather than having to configure encryption on a column-by-column basis. It encrypts data at the datafile level to keep users from viewing the Oracle datafiles directly. Oracle recommends tablespace encryption for maximum protection of the data.

For performing tablespace encryption, see *Oracle® Health Sciences Adverse Event Integration Pack for Oracle Health Sciences InForm and Oracle Argus Safety Installation Guide*.

5.2 Securing Web Services

Integration pack installs all web services in a secured manner using Oracle Web Services Manager WS-Security policies. For more information about the security policies associated with this integration pack web services, see *Oracle® Health Sciences Adverse Event Integration Pack for Oracle Health Sciences InForm and Oracle Argus Safety Installation Guide*.

5.3 Enabling SSL

Due to the complexity in setting up SSL, it is not enabled by default during installation. Communications between the browser and the application servers should be restricted to SSL.

The integration pack uses user name token authentication global security policy for inbound communication. This policy requires user name token to be present in the inbound message header. The integration processes the message only after successful authentication. The SOA server must be enabled for SSL to receive user name token in the message header. Unless SOA Server web service endpoint is HTTPS enabled, the InForm Publisher will not send the user name token in the incoming message header.

For more information on how to set up SSL communication between InForm Adapter, InForm Publisher, and this integration, see the following guides:

- *Oracle Health Sciences Adverse Event Integration Pack for Oracle Health Sciences InForm and Oracle Argus Safety Installation Guide*
- *InForm Adapter Installation Guide*
- *InForm Publisher Installation Guide*

6 Related Documents

- *Oracle Argus Safety Minimum Security Configuration Guide*

7 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.

Access to Oracle Support

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.

Oracle® Health Sciences Adverse Event Integration Pack for Oracle Health Sciences InForm and Oracle Argus Safety Security Guide, Release 1.0.1
E39184-01