Oracle® Study, Subject, and Visit Synchronization Integration Pack for Siebel Clinical and Oracle Clinical

Security Guide

Release 11.1

E47756-01

August 2013

This guide describes important security guidelines for Oracle Study, Subject, and Visit Synchronization Integration Pack for Siebel Clinical and Oracle Clinical (Study, Subject and Visit Synch: Siebel Clinical - Oracle Clinical Process Integration Pack) 11.1.

1 Introduction

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, "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, see *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.

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.

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

Oracle recommends you to secure the communication between the SOA server and the Siebel server. This includes invoking the Siebel web service over SSL and having Siebel write to the JMS queue using SSL.

Note: The Application Integration Architecture (AIA) message resubmission tool does not support SSL. Hence, you must resubmit the failed messages over non-SSL port.

This section contains the following topics:

- Section 5.1, "Configuring SSL on Siebel Server"
- Section 5.2, "Creating Custom Keystore on SOA Server"
- Section 5.3, "Enabling Secure Sockets Layer on SOA Server"
- Section 5.4, "Configuring SOA Server to Invoke Siebel Webservice Over HTTPS"
- Section 5.5, "Configuring Siebel Server to Invoke JMS Consumer Over T3S"

5.1 Configuring SSL on Siebel Server

If Siebel is running on Oracle HTTP server, perform the following steps:

1. Launch the Oracle Wallet manager.
2. Navigate to **Wallet menu > New**.
3. Click **Yes** to create the default wallet directory.
4. Click **Yes** to continue.
5. Enter a password for the wallet.
6. Click **Yes** to create a new certificate request.
7. In the Create Certificate Request screen, enter the following values to create an identity.

- Common Name

  Enter the web server machine name.

- Organization Unit
- Organization
- Locality / City
- State / Province
- Country
- Key Size
- DN

8. Click **OK** to create the certificate request.
9. Select the certificate requested from the left-hand tree and navigate to the **Operations** menu.
10. Select **Export Certificate Request**.
11. Specify a file name to save the CSR.
12. Save the wallet at <Siebel_home> / web / Oracle_ WT1 / instances / instance1 / config / OPMN / opmn / wallet.

    The CSR file is submitted to a trusted CA. The CA returns a certificate or a certificate chain.

13. Import the trusted CA and the signed certificate by navigating to **Wallet > Import user Certificate**.

    The import must be successful.

14. Save the wallet and check the auto login (**Wallet > Auto Login**).
15. Edit the ssl.conf file located at . / <Siebel_home> / web / Oracle_ WT1 / instances / instance1 / config / OHS / ohs1 / ssl.conf.

    Note: Ensure to back up the original ssl.conf file before editing.

    - Edit the port number to 8888 in the following lines:

      Listen <machine_name>:

      <VirtualHost _default_:

    - Provide the wallet path for SSLWallet file: / <Siebel_home> / web / Oracle_ WT1 / instances / instance1 / config / OPMN / opmn / wallet.
    - Precede the line **downgrade-1.0 force-response-1.0** with the comment character.
    - Delete \ from the line **nokeepalive ssl-unclean-shutdown**.

16. Take a copy of the eapps.cfg file located at <Siebel_home> / eappweb / bin.
17. Change the https port to 8888.
18. Connect to the siebsrvr and execute the following command:

    ```
    change param secureBrowse=True for comp SCCObjmgr_enu
    ```

```
change param secureLogin=True for comp eClinicalObjMgr_enu
```

19. Restart all the services:

    stop_http

    stop_server all

    stop_ns

    start_ns

    start_server all

    start_http

20. Launch the application by changing the port to 8888 and edit it to https.

> **Note:** If Siebel is running on other Web servers, see the respective Security Guide.

5.2 Creating Custom Keystore on SOA Server

To create custom keystore on the SOA server, perform the following steps:

The keytool utility performs some of the following steps. The keytool is present in the jre_home/bin directory. If JAVA_HOME is not set, invoke the keytool using the `<JRE_HOME>/bin/keytool` command.

1. Create a directory on the SOA server to store keystores and certificates. For example, create a directory **<servername_security>** under /slot/prod/oracle. Navigate to this directory.

2. Create keystore with a private key on the SOA server.

   ```
   keytool -genkeypair -alias <privkey> -keyalg RSA -keysize 1024
   -keystore <keystore.jks> -dname <"CN=test, C=US">
   ```

   Enter the passwords when prompted.

3. Generate Certificate Signing Request (CSR) on the SOA server using the following command:

   ```
   keytool -certreq -alias <privatekey> -file <XXXXX.req> -keystore
   <keystorename>
   ```

   Enter the passwords when prompted.

   The CSR file is submitted to a trusted CA. The CA returns a certificate or a certificate chain.

4. Add the trusted certificate of the Certificate Authority (CA) to the keystore. This is the trust certificate of the signing authority.

   ```
   keytool - importcert -alias <aliasfortrustedcacert> -trustcacerts -file
   <trustedcafilename>

   -keystore <keystore.jks>
   ```

5. Import the CA signed crt file back to the SOA server. This is the signed certificate that the CA sends in response to the CSR generated in step 3.

   ```
   keytool -importcert -alias <alias for privkey> -file <signed crt
   filename> -trustcacerts -keystore <keystore name>
   ```

Enter the passwords when prompted.

6. Restart the SOA server.

5.3 Enabling Secure Sockets Layer on SOA Server

To enable Secure Sockets Layer (SSL) on the SOA server, perform the following steps:

1. Login to the Weblogic console (http://<host_name>:port/console).
2. On the left-hand side navigation hierarchy, navigate to **soa_domain > Environment > Servers > Select Managed Server (soa_server1)**.
3. Navigate to the **General** tab.

   Ensure that SSL port is enabled and it does not conflict with any other ports.
4. Navigate to the **Keystores** tab and enter the following values:
   a. In the **Keystores** field, select **Custom Identity and Custom Trust**.
   b. Enter the custom identity keystore as the keystore location in the SOA server (for example: /slot/prod/oracle/<security_name)/keystore.jks).
   c. Enter custom identity keystore type as jks.
   d. Enter the custom identity keystore passphrase value that was specified during keystore creation.
   e. Confirm the passphrase.
   f. Repeat steps a to e for trust keystore.
   g. Click **Save**.
5. Go to the **SSL** tab. Enter the following values:
   a. Enter the private key alias value that was specified during keystore creation.
   b. Enter the private key passphrase value that was specified during keystore creation.
   c. Confirm the private key passphrase.
   d. Click **Save**.
6. Configure the admin server to use custom identity and custom trust.
   a. On the left-hand side navigation hierarchy, navigate to s**oa_domain > Environment > Servers > AdminServer**.
   b. Repeat steps 4 and 5 for the admin server.
7. Configure the node manager to use custom identity and custom trust.
   a. Open **<Middleware_Home>/wlserver_10.3/common/nodemanager/nodemanager.properties**.
   b. Add the following properties to properties file.

      SecureListener = true

      KeyStores = CustomIdentityAndCustomTrust

      CustomIdentityKeyStoreFileName = /slot/prod/oracle/<security_name>/keystore.jks (see Section 5.2)

CustomIdentityAlias = key alias value that was specified during keystore creation

CustomIdentityPrivateKeyPassPhrase = <passphrase for private key>

CustomTrustKeyStoreFileName = /slot/prod/oracle/<security_name>/keystore.jks (see Section 5.2)

c. Save and close the file.

8. Restart SOA server, admin server and node manager.

For more information on how to enable SSL, see *Oracle® Fusion Middleware Securing Oracle WebLogic Server 11g Release 1 (10.3.3), Configuring SSL*.

5.4 Configuring SOA Server to Invoke Siebel Webservice Over HTTPS

To invoke Siebel Webservice over HTTPS in secure mode, perform the following steps:

The https certificate to access Siebel Webservice must be loaded into the trusted keystore on the SOA server. You need the certificate that is installed on the Siebel server.

1. Add the certificate to the WebLogic trust keystore. The following example shows how to add the certificate to DemoTrust.jks.

   The following link provides algorithm for locating trust store by WebLogic:

   http://docs.oracle.com/cd/E11035_01/wls100/secmanage/identity_trust.html#wp1183754

   Based on this, you can add the downloaded certificate to any trust keystores.

   a. Ensure that the SOA server can access the certificate. If the SOA server is on a different machine, copy the certificate to a folder in the SOA server machine.

      For example, copy Siebel certificate to the SOA server folder <Oracle Home>/<certs>/folder.

   b. Navigate to the location of the trust keystore. For example, if you are adding certificate to DemoTrust.jks, then navigate to `<Middleware_Home>/wlserver_10.3/server/lib`.

   c. Execute the following command:

      ```
      keytool -import -trustcacerts -v -keystore DemoTrust.jks -file
      <Oracle Home>/<certs>/<cert_name> -alias SiebelWSCert
      ```

   d. Enter the password when prompted.

   e. Enter **Yes** when prompted “Trust this certificate? [no]:”.

   f. Execute the following command to ensure that the certificate is added:

      ```
      keytool -v -list -keystore DemoTrust.jks
      ```

   g. Enter the password when prompted.

   h. Modify the startWebLogic.sh script in `<MIDDLEWARE_HOME>/user_projects/domains/soa_domain/bin/startWebLogic.sh` as follows:

      a. Open the startWebLogic.sh script.

      b. Modify the line `JAVA_OPTIONS="${SAVE_JAVA_OPTIONS}"` to `JAVA_OPTIONS="${SAVE_JAVA_OPTIONS} -Djavax.net.ssl.trustStore=<full path to keystore>"`.

Note: startWebLogic.sh requires the location of the custom trust keystore and hence modifying this script is necessary.

i. Restart SOA server, admin server, and node manager.

5.5 Configuring Siebel Server to Invoke JMS Consumer Over T3S

To configure Siebel Server to invoke JMS consumer over T3 over SSL (T3S), perform the following steps:

1. Navigate to <directory>/WLSJMS.
2. Open **jndi.properties** and modify the java.naming.provider.url to `t3s://<host_name>:<soa_port>`.
3. The keytool utility performs some of the following steps. The keytool is present in the jre_home/bin directory.

   If JAVA_HOME is not set, invoke the keytool using the `<JRE_ HOME>/bin/keytool` command.

   Follow steps 2 to 5 of Section 5.2.

   Note: You must use the same **-dname** used in step 1 to create the keystore. See Section 5.2.

   a. In the Siebel application, navigate to **Administrator Server Configuration > Enterprises > Profile Configuration**.

   b. Query for alias `java` and add the following arguments at the end of the **JVM Options** variable:

   ```
   -Dweblogic.security.SSL.ignoreHostnameVerification=true
   -Dweblogic.security.TrustKeyStore=CustomTrust
   -Dweblogic.security.CustomTrustKeyStoreFileName=<Path of the keystore>
   -Dweblogic.security.CustomTrustKeyStoreType=jks
   ```

   c. Restart the Siebel server.

6 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® Study, Subject, and Visit Synchronization Integration Pack for Siebel Clinical and Oracle Clinical Security Guide, Release 11.1
E47756-01