Table of Contents

1 Preparation and Requirements ................................................................. 4
  1.1 Introduction ......................................................................................... 4
  1.2 Server Requirements ......................................................................... 5
    1.2.1 Supported Operating Systems .................................................. 5
    1.2.2 Supported Browsers .................................................................. 5
    1.2.3 Supported Server ...................................................................... 5
    1.2.4 Supported Databases .................................................................. 5
    1.2.5 Execution Environment ............................................................. 5
    1.2.6 Hardware Requirements ............................................................. 5
  1.3 Third Party Software Requirements .................................................... 6
    1.3.1 Java Development Kit .................................................................. 6
    1.3.2 Application Server ..................................................................... 6
    1.3.3 Database .................................................................................... 6

2 Upgrade Instruction ...................................................................................... 8
  2.1 Introduction ......................................................................................... 8
  2.2 Application Upgrade .......................................................................... 8
  2.3 Database Upgrade .............................................................................. 9
    2.3.1 Derby Database ......................................................................... 9
    2.3.2 Oracle Database ......................................................................... 9
    2.3.3 MySQL Database ....................................................................... 9

3 Installation .................................................................................................. 10
  3.1 Introduction ......................................................................................... 10
  3.2 Configuring Database ......................................................................... 10
    3.2.1 Derby Database ......................................................................... 10
    3.2.2 Oracle Database ......................................................................... 11
    3.2.3 MySQL Database ....................................................................... 11
  3.3 Configuring Secure HTTP .................................................................... 12
  3.4 Deploying Cigital SecureAssist Portal ................................................ 13
    3.4.1 Deploying using Tomcat Manager ............................................ 13
    3.4.2 Deploying on a running Tomcat server ..................................... 15
  3.5 Installing MySQL database connector ................................................. 15
  3.6 Deploying Cigital SecureAssist Eclipse update site ......................... 15

4 Initial Configuration .................................................................................... 15
  4.1 Configuring Logging ........................................................................... 15
  4.2 First Start Configuration .................................................................... 16
    4.2.1 License Terms ........................................................................... 16
    4.2.2 Product License ......................................................................... 16
    4.2.3 Database Setup .......................................................................... 17
    4.2.4 Administrator Account Setup .................................................. 18
  4.3 Configuring links on index page ........................................................... 20
  4.4 Serving Rulepacks ............................................................................... 21
1 Preparation and Requirements

1.1 Introduction

Welcome to the Cigital SecureAssist™ Portal installation guide. This document provides instructions on how to install and configure Cigital SecureAssist Portal. This document contains only installation and initial configuration steps. For more detailed information on configuration and use please refer to the Cigital SecureAssist Portal User's Guide.
1.2 Server Requirements

1.2.1 Supported Operating Systems
- Linux (Ubuntu, RedHat 5)

1.2.2 Supported Browsers
- Internet Explorer 7,8,9
- Firefox 26 and higher
- Chrome 37 and higher

1.2.3 Supported Server
- Apache Tomcat 6
- Apache Tomcat 7

1.2.4 Supported Databases
- MySQL Community Server 5
- Oracle Database 11g
- Apache Derby 10

1.2.5 Execution Environment
- Java 1.6, 1.7

1.2.6 Hardware Requirements
- 500MB of free disk space, 2 GB recommended
- 2 GB memory, 4 GB recommended
1.3 Third Party Software Requirements

1.3.1 Java Development Kit
Cigital SecureAssist Portal requires the use of Java Development Kit 6 or higher. Installation and configuration of the Java Development Kit is beyond the scope of this installation guide. Latest version of Java SE can be downloaded from here: http://www.oracle.com/technetwork/java/javase/downloads/index.html

1.3.2 Application Server
Apache Tomcat web server must be installed. Installation and configuration of the Apache Tomcat web server is beyond the scope of this installation guide. For more information about the Apache Tomcat web server, please refer to the Apache Tomcat website at: http://tomcat.apache.org
Make sure that the Apache Tomcat is using Java Development Kit 6 or higher.

1.3.3 Database
Cigital SecureAssist Enterprise Portal supports multiple different databases. While installation and configuration is beyond the scope of this guide, a link is provided for more information along with the version tested. Please choose a database and follow its installation steps for the version specified.

1.3.3.1 MySQL Database
Cigital SecureAssist Portal has been tested using MySQL Community Edition version 5.5 while other commercial and community versions should work. For more information about the MySQL database and installation steps, please refer to the MySQL website at: http://www.mysql.com

1.3.3.2 Oracle Database
Cigital SecureAssist Portal has been tested using Oracle Database version 11g. For more information about the Oracle database and installation steps, please refer to the Oracle website at: http://www.oracle.com/us/products/database/overview/index.html

1.3.3.3 Apache Derby Database
Cigital SecureAssist Portal has been tested using Apache Derby database version 10.10. For more information about the Apache Derby database and
installation steps, please refer to the Apache Derby website at:
http://db.apache.org/derby/
2 Upgrade Instruction

2.1 Introduction

This section describes the upgrade instructions of the Cigital SecureAssist Portal from version 2.2.5 to version 2.3. In order to upgrade server to version 2.3 it is necessary to run database update script and deploy new version of web application.

2.2 Application Upgrade

1. Stop Apache Tomcat
2. Create backup directory
3. Backup following directories/files:
   a. Copy following directories to backup folder:
      - <tomcat>/webapps/CSA_Server/key
      - <tomcat>/webapps/CSA_Server/stats
      - <tomcat>/webapps/CSA_Server/rulepacks
   b. Copy following files from <tomcat>/webapps/CSA_Server/WEB-INF/ folder to backup folder:
      - cron.properties
      - db.properties
      - <company_name>-SecureAssist-PriKey.der
      - SecureAssist.license
      - classes/log4j.xml (optional please see step 9 c)
4. Delete CSA_Server.war file from <tomcat>/webapps folder
5. Delete <tomcat>/webapps/CSA_Server folder
6. Copy new CSA_Server.war file to <tomcat>/webapps folder
7. Upgrade database by following instruction in section 2.3 Database Upgrade
8. Start Apache Tomcat
9. Copy backed up directories/files:
   a. Copy following directories to <tomcat>/webapps/CSA_Server
      - <backup>/key-file
      - <backup>/stats
      - <backup>/rulepacks
   b. Copy following files to <tomcat>/webapps/CSA_Server/WEB-INF
      - <backup>/cron.properties
      - <backup>/db.properties
      - <backup>/<company>-SecureAssist-PriKey.der
      - <backup>/SecureAssist.license
   c. Copy file <backup>/log4j.xml to <tomcat>/webapps/CSA_Server/WEB-INF/classes

   NOTE: Log4j configuration file in release 2.3 contains additional loggers to improve logging configuration. It is recommended to configure new log4j.xml instead of replacing it with previous version of the file.
10. Make sure that all directories and files copied from backup folder are readable and writable by user running tomcat (e.g. chown tomcat:tomcat path/to/file)
11. Copy MySQL Connector (mysql-connector-java-5.X.X.jar) to <tomcat>/webapps/CSA_Server/WEB-INF/lib/
12. Remove Apache Tomcat work cache (e.g. /var/cache/tomcat6/work/Catalina/localhost/CSA_Server/*, <tomcat>/work/Catalina/localhost/CSA_Server/*)
13. Restart Apache Tomcat

2.3 Database Upgrade

2.3.1 Derby Database
Start Apache Derby scripting tool by executing <derby>/bin/ij.bat (Windows) or <derby>/bin/ij.ksh (Unix) script in terminal.
In ij run following command

```bash
run 'path_to/upgrade/2.2_to_2.3/portal_csa_derby.sql';
```

2.3.2 Oracle Database
Login to SQL*Plus as sysdba using following command

```bash
sqlplus /as sysdba
```
Execute SQL script

```bash
@/path_to/upgrade/2.2_to_2.3/portal_csa_oracle.sql
```
Exit from SQL*Plus

```bash
exit;
```

2.3.3 MySQL Database
Update CSA Portal database schema by running command as a MySQL super user or user created during initial database setup

```bash
mysql -u root -p csa_portal < path_to/upgrade/2.2_to_2.3/portal_csa_mysql.sql
```
Replace ‘csa_portal’ with database schema created during initial installation.
Replace ‘path_to’ with path to portal_csa_mysql.sql file with upgrade script.
3 Installation

3.1 Introduction

This section describes the installation of the Cigital SecureAssist Portal and Cigital SecureAssist Eclipse update site. The portal and update site can be deployed on the same (application) server, but they can also be deployed on separate servers. This document assumes that they are installed on the same server.

3.2 Configuring Database

3.2.1 Derby Database

3.2.1.1 Configure database and user

To modify database name, user and password you need to modify Apache Derby specific SQL script located in <CSA_Portal_Package>/Database/portal_csa_derby.sql. Password change is required.

In order to modify credentials of user that will be used to connect to CSA Portal database please modify following line in the SQL Script

```
CALL SYSCS_UTIL.SYSCS_SET_DATABASE_PROPERTY('derby.user.portal_csa', 'Passw0rd');
```

To change password replace Passw0rd with password of your choice.

To change user name replace derby.user.portal_csa with derby.user.selected_username.

In order to change database name please modify following line in the SQL Script

```
CONNECT 'jdbc:derby:portal_csa;create=true';
```

To change database name replace portal_csa with database name of your choice.

3.2.1.2 Running SQL Script

Note: Make sure that Apache Derby is running. To Start Apache Derby database as the network server by executing the <derby>/bin/startNetworkServer.bat (Windows) or <derby>/bin/startNetworkServer.ksh (Unix) script. This will start the Network Server up on port 1527.

Start Apache Derby scripting tool by executing <derby>/bin/ij.bat (Windows) or <derby>/bin/ij.ksh (Unix) script in terminal.

In ij run following command
3.2.2 Oracle Database

3.2.2.1 Configure database user

To modify database name, user and password you need to modify Oracle specific SQL script located in `<CSA_PortalPackage>/Database/portal_csa_oracle.sql`. Password change is required.

In order to modify credentials of user that will be used to connect to CSA Portal database please modify following line in the SQL Script

```
CREATE USER portal_csa IDENTIFIED BY Passw0rd DEFAULT TABLESPACE USERS TEMPORARY TABLESPACE TEMP;
```

Replace ‘portal_csa’ and ‘Passw0rd’ with username and password of your choice. Make sure to update all following lines with updated information

```
connect portal_csa/Passw0rd;
```

3.2.2.2 Running SQL Script

Login to SQL*Plus as sysdba using following command

```
sqlplus /as sysdba
```

To log output of SQL script execution turn on spool

```
spool /<path>/<to>/log.txt ;
```

Execute SQL script

```
@/path/to/portal_csa_oracle.sql
```

Turn off spool

```
spool off;
```

Exit from SQL*Plus

```
exit;
```

Review log file with SQL script execution output to validate that there are no errors.

3.2.3 MySQL Database

3.2.3.1 Configure MySQL database and user

Run the “mysql” command as a MySQL super user.

```
mysql -u root -p
```
Create an empty CSA Portal database schema. Replace ‘portal_csa’ with a database name of your choice.

```sql
CREATE DATABASE portal_csa;
```

Create CSA Portal database user.

```sql
GRANT ALL PRIVILEGES ON portal_csa.* TO 'csauser'@'localhost' IDENTIFIED BY 'csauserpassword';
```

Replace ‘portal_csa’ with the name of the database that you have created in the step above. Additionally replace ‘csauser’ and ‘csauserpassword’ with username and password of your choice. If Cigital SecureAssist Portal is not running on the same server as you MySQL database server, replace ‘localhost’ with the hostname or IP address of the Cigital SecureAssist server.

### 3.2.3.2 Configuring portal database schema

Create CSA Portal database schema by running command as a MySQL super user.

```bash
mysql -u root -p portal_csa < path_to/portal_csa_mysql.sql
```

Replace ‘csa_portal’ with database schema created in step 2.2.1.
Replace ‘path_to’ with path to portal_csa_mysql.sql file.

### 3.3 Configuring Secure HTTP

Cigital SecureAssist Portal supports both HTTP and Secure HTTP (https). Cigital strongly recommends using secure HTTP. Installation of server-side SSL certificate and configuration of web server is beyond the scope of this installation guide. For more information about configuring the Apache Tomcat web server to use secure http, please refer to web server documentation.
3.4 Deploying Cigital SecureAssist Portal

3.4.1 Deploying using Tomcat Manager

If your instance of Tomcat is running the Tomcat Web Application Manager, you can use its browser interface to deploy CSA Portal.

In ‘tomcat_home/conf/tomcat_users.xml’ create a role named “manager-gui” and assign a user to this role. Afterwards restart your Tomcat instance.

```
<tomcat-users>
    <role rolename="manager-gui"/>
    <user username="USERNAME" password="PASSWORD"
          roles="manager-gui"/>
</tomcat-users>
```

Start up your favorite browser and navigate to default Tomcat home page.

Click on the “Manager App” link from Tomcat startup page. Before the Tomcat manager page load you will be asked for a username and password.
Navigate to the section named “WAR file to deploy” and click on the **Browse…** button.

Select CSA Portal web application WAR file and click **Open**. Click **Deploy** button.

After Tomcat Web Application Manager has finished deploying CSA Portal it should be listed in “Applications” section and be ready to use.
3.4.2 Deploying on a running Tomcat server
To deploy application on a running Tomcat server, autoDeploy attribute, needs to be set to true. Host will deploy web application when war file is copied to deployment directory which by default is CATALINA_HOME/webapps.
To deploy CSA Portal simply copy CSA_Server.war file to CATALINA_HOME/webapps. After Tomcat has finished deploying CSA Portal, CSA_Server directory should be created in CATALINA_HOME/webapps.

3.5 Installing MySQL database connector
The MySQL Connector/J (official JDBC driver for MySQL database) is required when installing Cigital SecureAssist Enterprise Portal. To install MySQL connector, please follow steps described below:
2. Extract mysql-connector-java-5.x.x-bin.jar file from archive downloaded in previous step and copy into the CATALINA_HOME/webapps/CSA_Server/WEB-INF/lib directory.

3.6 Deploying Cigital SecureAssist Eclipse update site
To deploy Cigital SecureAssist Eclipse update site simply copy /update folder to CATALINA_HOME/webapps folder.

4 Initial Configuration

4.1 Configuring Logging
Log4j configuration file is stored in CATALINA_HOME/webapps/CSA_Server/WEB-INF/classes/log4j.xml file. You can edit this file to make it suitable for the deployment environment. For more information about configuring log4j please refer to log4j documentation (http://logging.apache.org/log4j/1.2/index.html).

Note: Any changes made to logging configuration file will take affect after restarting Tomcat application server.
4.2 First Start Configuration

After successful deployment of Cigital SecureAssist Portal, open your browser and navigate to the following URL: \texttt{http://<Host>:<Port>/CSA\_Server} in order to finish configuration of the portal.

4.2.1 License Terms

Read terms and conditions and press \textbf{I Agree} to continue.

4.2.2 Product License

Cigital SecureAssist Portal license is tied to specific server and can be used only on that single server. In order to acquire license, please copy server information and send it to SecureAssist support (\texttt{SecureAssistHelp@cigital.com}).
4.2.3 Database Setup

Note: Before setting up database connection make sure to setup database schema and create user as described in section 2.2.1. Please complete all fields and click **Save**.
Examples:

<table>
<thead>
<tr>
<th>Database Type</th>
<th>MySQL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>jdbc:mysql://&lt;db_server&gt;:3306</td>
</tr>
<tr>
<td>Database Name/Scheme Name</td>
<td>portal_csa</td>
</tr>
<tr>
<td>Database User</td>
<td>csauser</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Database Type</th>
<th>Derby</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>jdbc:derby://&lt;db_server&gt;:1527/portal_csa</td>
</tr>
<tr>
<td>Database Name/Scheme Name</td>
<td>APP</td>
</tr>
<tr>
<td>Database User</td>
<td>portal_csa</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Database Type</th>
<th>Oracle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>jdbc:oracle:thin:@&lt;db_server&gt;:1521:orcl</td>
</tr>
<tr>
<td>Database Name/Scheme Name</td>
<td>portal_csa</td>
</tr>
<tr>
<td>Database User</td>
<td>portal_csa</td>
</tr>
</tbody>
</table>

4.2.4 Administrator Account Setup

In the last step of initial configuration, administrator account needs to be created. Please provide username and password for administrator account and click Create.
Upon successful Cigital SecureAssist Portal initial configuration you will be redirected to index page and you will be able to login using administrator credentials created during initial configuration.
4.3 Configuring links on index page

Index page contains section with links to location where Cigital SecureAssist IDE plug-in/add-in can be downloaded and/or installed from.

In order to configure those links navigate to the following directory

CATALINA_HOME/webapps/CSA_Server/WEB-INF/jsp/tiles/index. Open file installation.jsp and edit following lines.

```
<set var="eclipseUpdateUrl" value="http://SecureAssist.cigital.com/update"/>
<set var="eclipseUpdateZip" value="http://SecureAssist.citical.com/eclipse/csa_update.zip"/>
<set var="vsZip" value="http://SecureAssist.citical.com/vs/csa_addin.zip"/>
```

eclipseUpdateUrl – URL to Eclipse update site from where Cigital SecureAssist plugin can be installed
eclipseUpdateZip – URL to location where archive containing update site can be downloaded
vsZip – URL to location where Visual Studio add-in installation package can be downloaded

If you do not want any or all of those links to be displayed please leave value as empty for example:

```
<set var="vsZip" value=""/>
```
4.4 Uploading Rulepacks

Cigital SecureAssist Rulepacks contain elements that are used by the SecureAssist plug-in to identify parts of the code that can lead to security weaknesses and provide developers with immediate guidance.

When the enterprise server is initially deployed, it will contain no rulepacks. To serve a rulepack to clients, one or more must be uploaded to the enterprise server and enabled.

The Cigital Default Rulepack contains Cigital SecureAssist’s core rules and guidance. This rulepack has been provided with the enterprise server installation files and will likely be the first rulepack you will enable.

First, log into the enterprise portal as an administrator and click the RULEPACK link in the top menu. You will be brought to a rulepack management page with a rulepack upload interface and rulepacks list.

To upload a rulepack click Browse … and from the file selector, choose the rulepack you wish to upload. Click the Upload File button. Once uploaded it will appear in the rulepacks list.

A disabled rulepack on the server will not be downloaded by IDE plug-ins. Click the Enable button next to the rulepack that you uploaded to enable the rulepack. You will receive verification that the rulepack has been enabled by a brief confirmation message on screen. Once the rulepack is enabled, the Enable button will be replaced with a Disable button that can be used to disable the rulepack.
About Cigital, Inc.

Cigital, Inc., a leading software security and quality consulting firm, was established in 1992 with a single focus of helping organizations improve software. Our consultants are thought leaders who specialize in programs that help organizations ensure their applications are secure and reliable while also improving how they build and deploy software. We provide advice across the enterprise using a combination of proven methodologies, tools, and best practices that are tuned to meet each client's unique requirements. Cigital has enabled some of the most well-known organizations in financial services, communications, insurance, hospitality, e-commerce and government to reduce their mission-critical software business risks. Cigital is headquartered near Washington, D.C. with regional offices in the U.S., Europe and India.