


Front Office deployment


 CAST AIC Portal is unsupported. We encourage you to [switch](#) to [AIP Console](#).

On this page:

- [Introduction](#)
- [Delivery folder](#)
- [CAST Storage Service](#)
- [Web application server and web applications](#)
 - [Web application server](#)
 - [Web applications](#)
 - [CAST AIC Portal](#)
 - [Health Dashboard - Engineering Dashboard - RestAPI](#)
- [End-users / Delivery Managers and the CAST Delivery Manager Tool](#)
 - [Security tab](#)
 - [Advanced tab](#)
 - [Recommended settings](#)

Target audience:

CAST Platform Administrators

 **Summary:** this section provides details about deploying and configuring the "Front Office" components as part of a **secured deployment**.

Introduction

As described in [Deployment - security](#), to deploy CAST AIP securely, the various CAST AIP components are divided into two distinct groups known as **Front** and **Back Office**. A standard CAST AIP installation is described in [Installing CAST AIP](#) which you should read and understand. However, this section describes all the **additional configuration** that should be completed for the **Front Office components** (over and above the standard CAST AIP installation) to ensure that the deployment of CAST AIP conforms to security standards.

Delivery folder

The Delivery folder is first and foremost a location used by the **CAST AIC Portal** for storing successive and compressed versions of an application's source code as packaged by the Delivery Manager(s) using the CAST Delivery Manager Tool. In addition, the **CAST Management Studio** also requires access to this **same Delivery folder** so that source code packaged by the Delivery Manager(s) can be acquired and then analyzed.

As such, the **choice of location** for the Delivery folder is extremely important and may impact where the **CAST AIC Portal** is installed.

Please see:

- [Source code delivery - an introduction](#)
- [Where should the Delivery folder be located](#)

CAST Storage Service

If you decide to use the **CAST Storage Service** (a dedicated database system provided by CAST) to host the **Storage** components (the CAST schemas: Management Service, Analysis Service, Dashboard Service and Measurement Service) instead of using a commercially available (and [supported](#)) RDBMS (such as Microsoft SQL Server or Oracle Server), you will need to use a **dedicated physical machine**.

You can deploy the CAST Storage Service either on **Linux** or **Windows**, however, for **security and performance reasons**, it is highly recommended to deploy the CAST storage Service on **Linux**:

- CAST provides a dedicated **Windows installer** (see [Install CAST AIP from setup](#)) for the **CAST Storage Service**
- For **Linux environments**, please refer to [PostgreSQL for Linux or Docker](#)

Web application server and web applications

The objective is to configure the CAST web applications in accordance with [OWASP](#) (Open Web Application Security Project) guidelines. This configuration has been tested by CAST via a security audit. To secure the web applications, you will need to configure:

- The **web application server** on a **dedicated machine** (CAST provides documentation for [deployment on Apache Tomcat](#) only. Other web application servers may be compatible (see [Supported Platforms](#)), but no documentation is provided).
- Each **web application** (i.e. the CAST AIC Portal, Health Dashboard (HD), Engineering Dashboard (ED) etc.):
 1. Use of **Active Directory/LDAP** authentication methods
 2. Use of the **Audit Trail** to trace end user activities
 3. Secure configuration of back-end **database access** (only relevant for the HD/ED/RestAIP web applications)

Additionally, you can also configure a [reverse proxy](#) (using an **Apache web server**) to hide the Apache Tomcat web application server or take advantage of [secure access via HTTPS](#).

Web application server

Before deploying the CAST web applications on the web application server, ensure you configure the web application server as discussed in [Common security configuration options for web application deployment](#). This page details the following security configuration options:

- [Configuring the use of secure https protocol with Tomcat for the CAST web applications](#)
- [Setting up a Reverse Proxy on Apache web server](#)
- [Disabling insecure HTTP methods in Apache Tomcat - webdav](#)
- [Disabling weak SSL cipher suites to improve security](#)

Web applications

CAST AIC Portal

Securely configure the CAST AIC Portal as described in [CAST AIC Portal - security configuration options](#). This page details the following security configuration options:

- [CAST AIC Portal - Configuring user authentication](#)
- [CAST AIC Portal - Configuring the Audit Trail feature](#)
- [CAST AIC Portal - Encrypt login and password for LDAP](#)

Health Dashboard - Engineering Dashboard - RestAPI

Securely configure the Health Dashboard / Engineering Dashboard / CAST Rest-API as described in [HD - ED - RestAPI - security configuration options](#). This page details the following security configuration options:

- [HD - Configuring user authentication](#)
- [HD - Configuring user roles](#)
- [HD - Configuring data authorization](#)
- [ED - Configuring user authentication](#)
- [ED - Configuring user roles](#)
- [ED - Configuring data authorization](#)
- [HD-ED - Configuring the Log and Audit Trail](#)
- [HD-ED - Encrypt login and password for database and LDAP](#)

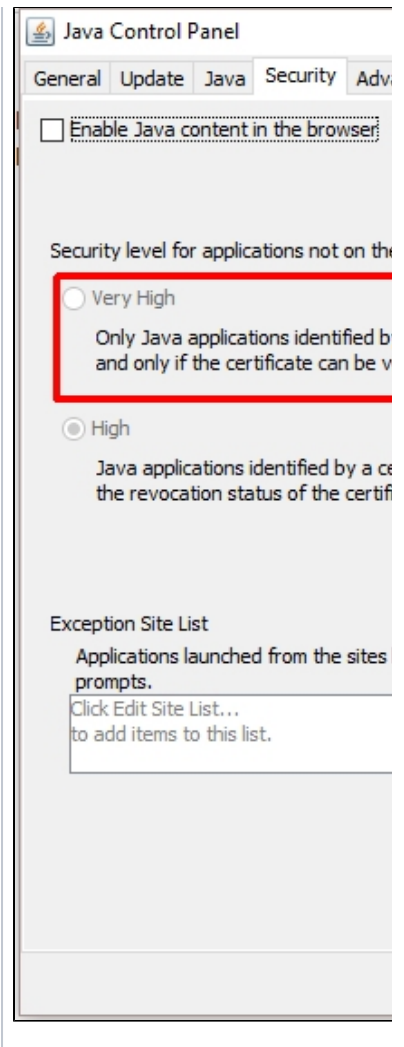
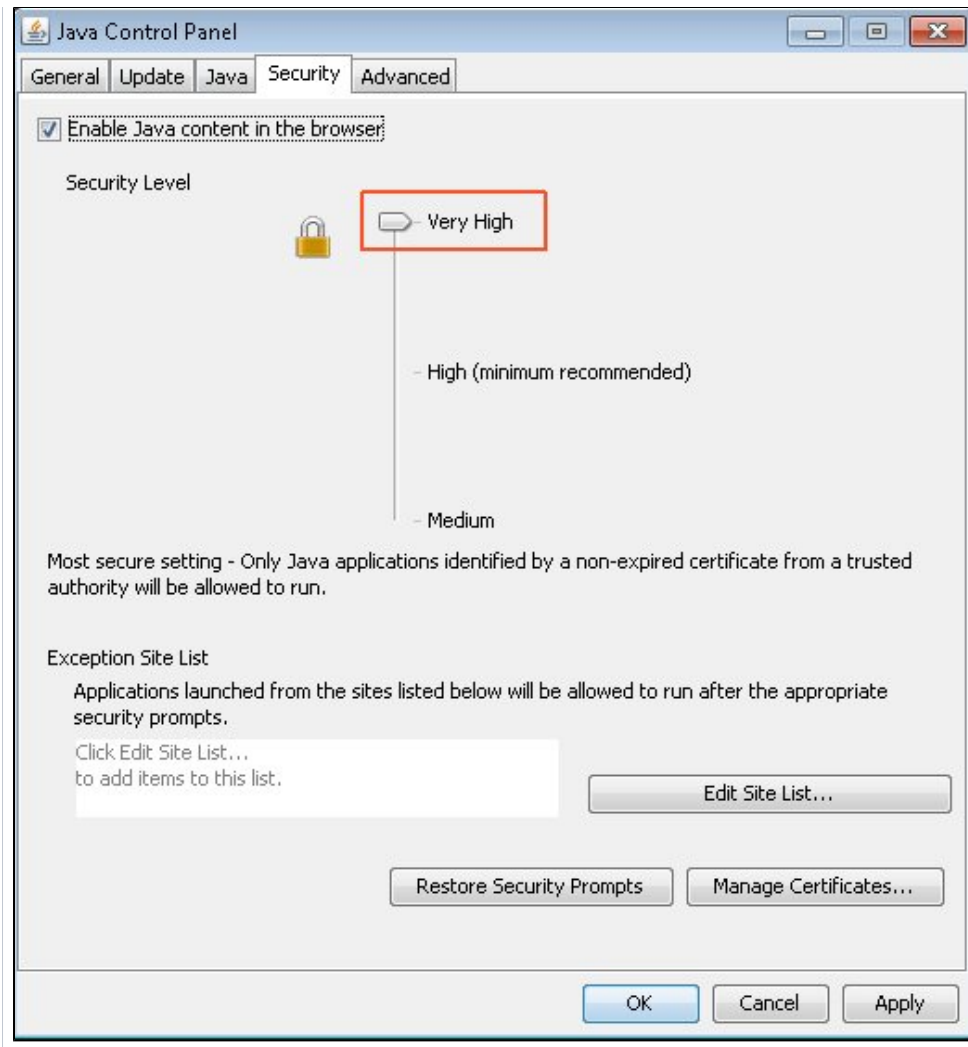
End-users / Delivery Managers and the CAST Delivery Manager Tool

The **CAST Delivery Manager Tool** is a standalone end-user tool that entirely manages the discovery, selection, extraction and delivery of source code ready for analysis in the CAST Management Studio. The CAST Delivery Manager Tool will be **prevented** from being downloaded from the CAST AIC Portal to a workstation if the following **Java JRE settings** available in the **Java Control Panel** are **all enabled**:

Security tab

Security Level set to Very High

Java 7	Java 8

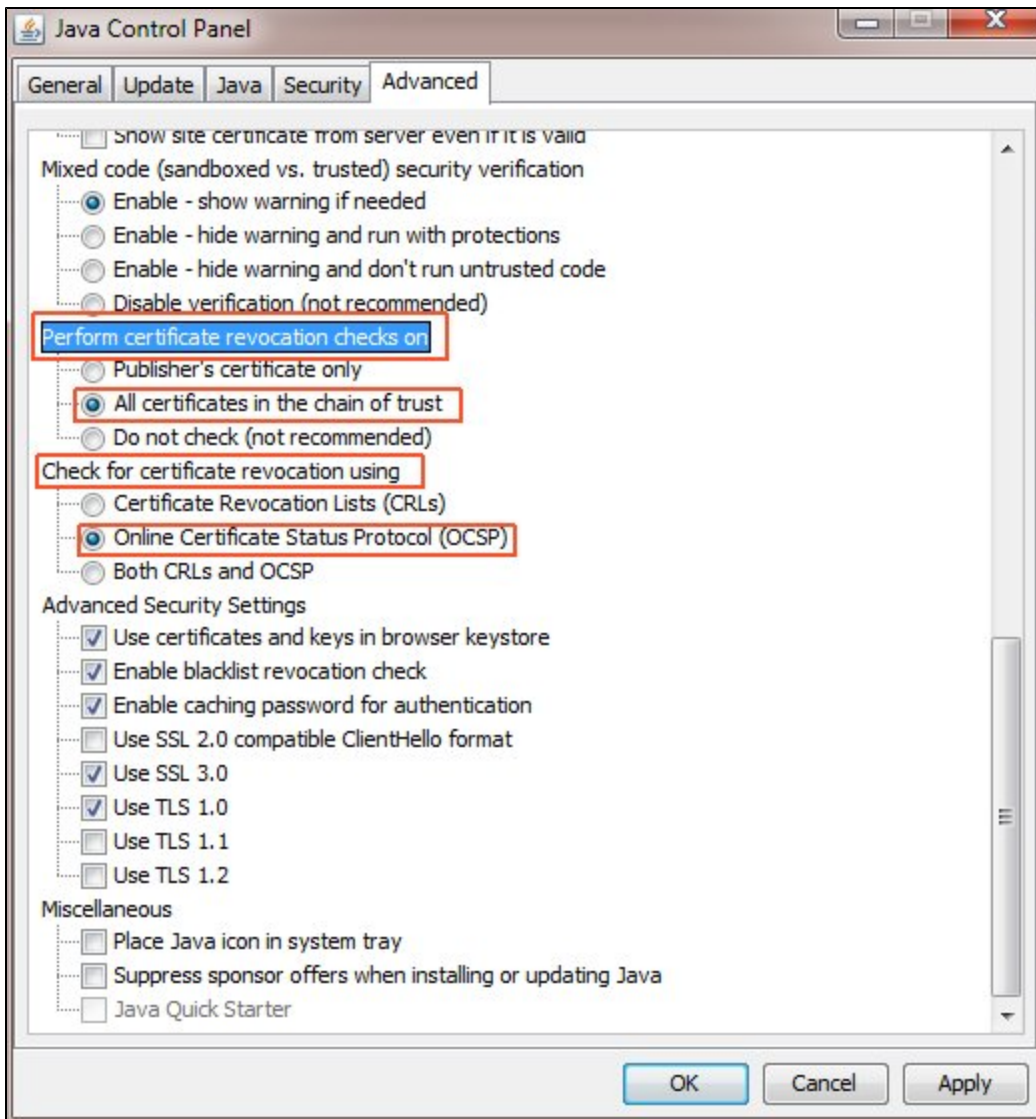


Advanced tab

- **Perform certificate revocation checks on** is set to **All certificates in the chain of trust**

AND

- **Check for certificate revocation using** is set to **Online Certificate Status Protocol (OCSP)**



Recommended settings

CAST recommends that ONE of the following settings is used instead:

- Set the **Security Level** to **High**

OR

- Set **Perform certificate revocation checks on** to **Publisher's certificate only**

OR

- Set **Check for certificate revocation using** to **Certificate Revocation Lists (CRLs)**

OR

- Set **Check for certificate revocation using** to **Both CRLs and OCSP**

OR

- Put the CAST AIC Portal's **URL** into the **Exception Site List** in the (**Security tab** of the **Java Control Panel**):

