


Modify the user access port for 2.x JAR or ZIP deployments

- [Introduction](#)
- [Prerequisites](#)
- [Configure an alternative insecure port](#)
- [Configure an alternative secure port](#)


 **Summary:** this page describes how to change the CAST Dashboard access port, for example to enable HTTPS.

 This information is only valid for CAST Dashboard 2.x when using a ZIP/JAR file deployment (i.e. without Apache Tomcat). If you are deploying WAR files using Apache Tomcat, see [Configuring Apache Tomcat to use secure https protocol](#) for more information.

Introduction

By default, an insecure **HTTP** connection on port **8080** will be used for end-user access to the **CAST Dashboards**. This page explains how to change the running port number, for example to enable a secured connection using **HTTPS** on port **443** or to change to an alternative HTTP port such as port **80**.

Prerequisites

 If you intend to change the port numbers in **order to enable HTTPS** then you must already have a **Java keystore file** containing the X.509 certificate (from a trusted authority). Obtaining the certificate and generating the keystore files are out of the scope of this document. See https://tomcat.apache.org/tomcat-9.0-doc/ssl-howto.html#Prepare_the_Certificate_Keystore for more information about importing existing signed X.509 certificates into a keystore and generating new self-signed certificates and storing them in a keystore.

- CAST Dashboards support only the following format keystores:
 - JKS
 - PKCS11
 - PKCS12
- You should ensure that the release of Java used to generate the certificate is identical to the release of Java used to import the certificate otherwise the Dashboard service may fail to start. This is especially true of the certificate is being generated on another machine.

Configure an alternative insecure port

By default, CAST Dashboards are configured to run on **port 8080**. If you want to change this to an alternative port, edit the following file:

```
<install_folder>\configurations\application.properties  
or  
%PROGRAMDATA%\CAST\Dashboards\<dashboard>\application.properties
```

Locate the following line in the file:

```
# Configure server port. This is necessary only for the .jar mode/version  
# server.port=8080
```

Uncomment the `server.port` line and modify the port number and save the file:

```
# Default Port  
server.port=80
```

Restart the application to ensure the changes are taken into account.

Configure an alternative secure port

To force the dashboards to use a secure HTTPS port, edit the following file:

```
<install_folder>\configurations\application.properties  
or  
%PROGRAMDATA%\CAST\Dashboards\<dashboard>\application.properties
```

Locate the following lines in the file:

```
# Configure server port. This is necessary only for the .jar mode/version  
# server.port=8080  
...  
...  
...  
# -----  
#  ssl configuration, ssl is required when enable the saml mode  
# -----  
server.ssl.enabled=false  
# The format used for the keystore. It could be set to JKS in case it is a JKS file  
server.ssl.key-store-type=  
# The path to the keystore containing the certificate  
server.ssl.key-store=  
# The password used to generate the certificate  
server.ssl.key-store-password=  
# The alias mapped to the certificate  
server.ssl.key-alias=
```

Modify these options as follows:

server.port	Uncomment this line and change this to the required port. CAST highly recommends that you use port 443 .
server.ssl.enabled	Change this to true .
server.ssl.key-store-type	The type of the key store , enter JKS , PKCS11 or PKCS12 .
server.ssl.key-store	This configures the path (with forward slashes) to the Java keystore containing the certificate to be used.
server.ssl.key-store-password	This configures the password to the Java keystore . By default this is set to changeit .
server.ssl.key-alias	The alias that identifies the key in the key store. This alias is defined when generating the keystore files.

For example:

```
# Default Port  
server.port=443  
...  
...  
...  
# -----  
#  ssl configuration, ssl is required when enable the saml mode  
# -----  
server.ssl.enabled=true  
# The format used for the keystore. It could be set to JKS in case it is a JKS file  
server.ssl.key-store-type=PKCS12  
# The path to the keystore containing the certificate  
server.ssl.key-store=D:/CAST/deploy/keystore/keystore.p12  
# The password used to generate the certificate  
server.ssl.key-store-password=changeit  
# The alias mapped to the certificate  
server.ssl.key-alias=my_alias
```

Restart the application to ensure the changes are taken into account.