CAST AIC Portal - Configuring user authentication

CAST AIC Portal is unsupported. We encourage you to **switch** to **AIP Console.**

On this page:

Target audience:

CAST AI Administrators

Summary: This section describes how to configure **access security** for your CAST AIC Portal.

Introduction

The CAST AIC Portal has various **authentication modes** available for use:

Mode	Description	Notes
Default authentication	This mode is **active by default** and relies on simple username /password authentication defined in the **application-security-default.xml** configuration file within the web application.	• **CAST recommends using Active Directory with LDAP** or **Standard LDAP** because this avoids having to manually manage individual usernames and passwords via the **Default authentication** mode. • Only **one mode** can be active at a time.
Active Directory with LDAP	This mode is **inactive by default** and allows users to authenticate with their corporate Active Directory login.	
Standard LDAP	This mode is **inactive by default** and allows users to authenticate with a standard LDAP server that is not Active Directory compatible.	
SAML	This mode is **inactive by default** and allows users to authenticate via **SAML**.	

The activation and configuration of the above modes is governed by the **security.properties** configuration file within the web application:

```
%CATALINA_HOME%\webapps\CAST-AICP\WEB-INF\security.properties
```

Authentication mode activation

Activation of any of the authentication modes is handled by the following section in the **security.properties** file:

```
# ============================
# CAST AICP security parameters
# ============================

# Applicable security mode
# ------------------------
#  - default    ->    The initial mode when you deploy AICP
#  - ldap       ->    Set this mode for authentication over LDAP(S)
#  - ad         ->    Set this mode for authentication over LDAP(S) with basic Active Directory instances
(simplified mode)
#  - saml               ->    Set this mode for authentication over SAML2
security.mode=default
```

In the "out of the box" state, the **default** security mode is active as shown above. Only **one mode** can be active at a a time.

Activation and deactivation action

To activate a mode, change the following line to the required security mode. For example, to change from the **Default authentication** security mode to **Act ive Directory with LDAP**, do as follows:

Change

```
security.mode=default
```

to:

```
security.mode=ad
```

Following any changes you make, **save the security.properties** file and then **restart** your application server so that the changes are taken into account.

Configuring each mode

Default authentication mode

This mode is enabled **by default** "out of the box" with the following case sensitive username and password:

Username	Password	User Group
cast	cast	ADMINISTRATORS

Note that the "cast" user is a member of the ADMINISTRATORS user group, which has access to all configuration options and can interact with any Domain and deliver any Application. CAST recommends that you retain at least one user that is a member of the ADMINISTRATORS user group.

If you would like to alter the password for this existing user or you would like to add additional "in memory authentication" users, you need to modify the **ap plication-security-default.xml** configuration file within the web application. This file contains the following section which defines the users that can access the CAST AIC Portal in **Default security mode**:

```
<user-service>
        <user name="cast" password="cast" authorities="ADMINISTRATORS"/>
</user-service>
```

As shown in the above code, the user is defined in a **<user>** element using the "**name**" attribute. This element also defines:

- the user's **password**
- the **User Group** the user has been assigned to

Adding a new user

To add a new username, add in an additional **<user>** tag, for example this will add in a username "jhu" with the password "mypassword", assigned to the user group "DELIVERY_GROUP1" (please see the section **User groups and roles** below for more information about groups and roles):

```
<user-service>
        <user name="cast" password="cast" authorities="ADMINISTRATORS"/>
        <user name="jhu" password="mypassword" authorities="DELIVERY_GROUP1"/>
</user-service>
```

Note that you can assign a user to **multiple groups** if required, for example to assign the user to "DELIVERY_GROUP1", "DELIVERY_GROUP2" and "DELIVERY_GROUP3", use the following syntax:

```
<user name="jhu" password="mypassword" authorities="DELIVERY_GROUP1,DELIVERY_GROUP2,DELIVERY_GROUP3"/>
```

Following any changes you make, **save the application-security-default.xml file** and then **restart** your application server so that the changes are taken into account.

Removing an existing user

To remove an existing user, simply remove the corresponding **<user>** tag from the **application-security-default.xml file**. Following any changes you make, **save the application-security-default.xml file** and then **restart** your application server so that the changes are taken into account.

Editing an existing user

To edit an existing user, simply edit the corresponding **<user>** tag in the **application-security-default.xml file**. Following any changes you make, **save the application-security-default.xml** file and then **restart** your application server so that the changes are taken into account.

Disabling a user without removing it from the application-security-default.xml file

To disable a user, add **disabled="true"** as an attribute to the **<user>** tag:

```
<user name="cast" password="cast" authorities="ADMINISTRATORS" disabled="true"/>
```

Following any changes you make, **save the application-security-default.xml file** and then **restart** your application server so that the changes are taken into account.

Active Directory with LDAP

This mode is not **enabled by default** "out of the box". It allows users to login with their corporate Active Directory login. CAST has provided place holder parameters, so you must change these before authentication will work correctly. To do so, modify the **security.properties** configuration file within the web application. This file contains the following commented section which defines the Active Directory **domain** and the **URL** to your internal LDAP server that handles Active Directory authentication:

```
# Parameters for ad mode
# ----------------------
security.ad.url=ldap://directory.example.com/
security.ad.domain=example.com
```

- You need to change the two parameters to match your own environment:
- Following any changes you make, save the **security.properties** file and then **restart** your application server so that the changes are taken into account.

User groups

Users will be automatically assigned roles (please see the section **User groups and roles** below for more information about groups and roles) corresponding to the CN of the Active Directory groups that they are members of.

> **Nested groups are supported** for role assignments. For instance, if user **jdoe** is member of **groupA**, which is member of **groupB** which is used to define a role, then **jdoe** will be attributed the **groupB** role.

Standard LDAP

This mode is **not enabled by default** "out of the box". It may be used with any LDAP compatible corporate directory, including Active Directory (though most of time the **Active Directory with LDAP** mode should be preferred in this case). It allows users to login to the CAST AIC Portal with their corporate LDAP login. CAST has provided place holder parameters, so you must change these before authentication will work correctly. To do so, modify the **security.properties** configuration file within the web application. This file contains the following commented section which defines the required parameters:

```
# Parameters for ldap mode
# ------------------------
security.ldap.url=ldap://directory.example.com/
security.ldap.account.dn=cn=serviceaccount,dc=example,dc=com
security.ldap.account.password=password
security.ldap.account.key=
security.ldap.usersearch.base=dc=example,dc=com
security.ldap.usersearch.filter=(&(objectClass=inetOrgPerson)(uid={0}))
security.ldap.groupsearch.base=dc=example,dc=com
security.ldap.groupsearch.filter=(&(objectClass=groupOfNames)(member={0}))
```

- You first need to change the following parameters to match the URL and the service account required to connect to your directory:

```
security.ldap.url=ldap://directory.example.com/
security.ldap.account.dn=cn=serviceaccount,dc=example,dc=com
security.ldap.account.password=password
```

- You then need to change the following parameters related to searching the users in your directory (search base and search filter):

```
security.ldap.usersearch.base=dc=example,dc=com
security.ldap.usersearch.filter=(&(objectClass=inetOrgPerson)(uid={0}))
```

- For Active Directory, the **security.ldap.usersearch.filter** parameter usually takes the following form:

```
security.ldap.usersearch.filter=(&(objectClass=user)(sAMAccountName={0}))
```

- Following any changes you make, save the **security.properties** file and then **restart** your application server so that the changes are taken into account.

> Note that if you need to **encrypt** the login and password parameters to avoid entering values in clear text, please see: CAST AIC Portal - Encrypt login and password for LDAP.

User groups

Users will be automatically assigned roles (please see the section **User groups and roles** below for more information about groups and roles) corresponding to the CN of the LDAP groups that they are members of.

> **Nested groups are supported** for role assignments. For instance, if user **jdoe** is member of **groupA**, which is member of **groupB** which is used to define a role, then **jdoe** will be attributed the **groupB** role.

- To enable LDAP group retrieval, modify the **security.properties** configuration file (this file is described above) within the web application - with the focus on the following section:

```
# Parameters for ldap mode
# ------------------------
security.ldap.url=ldap://directory.example.com/
security.ldap.account.dn=cn=serviceaccount,dc=example,dc=com
security.ldap.account.password=password
security.ldap.account.key=
security.ldap.usersearch.base=dc=example,dc=com
security.ldap.usersearch.filter=(&(objectClass=inetOrgPerson)(uid={0}))
security.ldap.groupsearch.base=dc=example,dc=com
security.ldap.groupsearch.filter=(&(objectClass=groupOfNames)(member={0}))
```

- You need to change the following parameters to match your directory's structure (group search base, group search filter, group role attribute):

```
security.ldap.groupsearch.base=dc=example,dc=com
security.ldap.groupsearch.filter=(&(objectClass=groupOfNames)(member={0}))
```

- For Active Directory, the **security.ldap.groupsearch.filter** parameter usually takes the following form:

```
security.ldap.groupsearch.filter=(&(objectClass=group)(member={0}))
```

- Following any changes you make, save the **security.properties** file and then **restart** your application server so that the changes are taken into account.

SAML mode

This mode is **not enabled by default** "out of the box".

Prerequisites

Before you can configure your CAST AIP web applications to use SAML authentication, the following prerequisites must already be in place:

CAST AIP web applications deployed and functioning	The CAST AIP web applications must be deployed and functioning before you can proceed. In particular you must ensure that any **roles** and **data authorizations** are already configured.
Apache Tomcat configured for HTTPS	The Apache Tomcat host server and any CAST AIP web applications must be configured to use the HTTPS protocol. See Configuring the use of secure https protocol with Tomcat for the CAST web applications for more information.
FederationMetadata.xml	This file must be provided by your IT administrators before you can proceed.
Key pair generation	A public/private key pair must be generated on the Apache Tomcat host server in a dedicated keystore to allow encrypted communication with the Active Directory Federation Server (ADFS). See below for more information. **Note:** Dashboard supports the SAML Keystore file, which is generated using the SHA256 algorithm.

Supported versions of SAML

Version	Supported
2.0	✓
1.1	✗
1.0	✗

Configuration process

Request FederationMetadata.xml

You must request the **FederationMetadata.xml** file from your IT administrators. When you have received the file, you should store it in a location that can be accessed from the CAST AIP web application, within the Apache Tomcat installation location. For example:

```
Windows: D:/apache-tomcat/conf/FederationMetadata.xml
Linux: file:/opt/apache-tomcat/conf/FederationMetadata.xml
```

Key pair generation

A public/private key pair must be generated on the Apache Tomcat host server in a dedicated keystore to allow encrypted communication with the Active Directory Federation Server (ADFS). This keystore should be specific to the SAML configuration. To do so, you need to use the **keytool** command line utility (provided with the JRE - see https://docs.oracle.com/javase/8/docs/technotes/tools/unix/keytool.html for more information) on the workstation on which the web application server is running. For example:

```
%JAVA_HOME%\keytool -genkeypair -alias <some-alias> -keyalg RSA -keypass <keypass> -keystore <samlKeystore.jks> -storepass <storepass>
```

Where:

-alias	Choose an alias that is specific to the key pair.
-keypass	This configured a password that is used to protect the private key of the generated key pair. The value must be at least 6 characters.

-keystore	Choose a keystore location in which to store the key pair, for example:
	`Windows: D:/apache-tomcat/conf/samlKeystore.jks`
	`Linux: /opt/apache-tomcat/conf/samlKeystore.jks`

-storepass	Choose a password to protect the keystore.

Activate and configure the authentication mode in the CAST AIP web application

Activation and configuration of the SAML authentication mode is governed by the **security.properties** configuration file within the CAST AIP web application:

```
CATALINA_HOME\webapps\<deployed_war_file>\WEB-INF\security.properties
```

To activate the SAML authentication mode, change the following line. For example, to change from the **Default authentication** security mode to **SAML**, do as follows. Change:

```
security.mode=default
```

to:

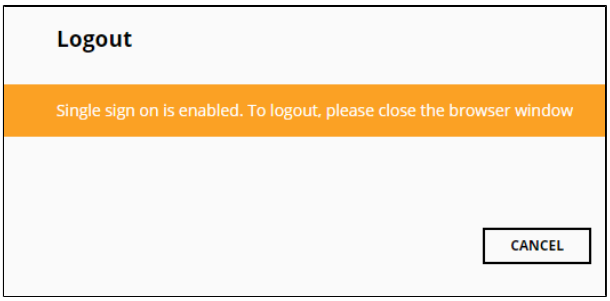
```
security.mode=saml
```

Save the **security.properties** file.

Configure SAML authentication

Find the SAML paremeters section in the **security.properties** configuration file and modify each uncommented line to match the items you have already configured. Save the **security.properties** file when complete.

```
# Parameters for saml mode
# ------------------------
# idp metadata file
security.saml.idp.metadata.location=file:/opt/apache-tomcat/conf/FederationMetadata.xml
# attribute name for group in saml response
security.saml.idp.metadata.group.attribute.name=http://schemas.xmlsoap.org/claims/Group
# Key store path
security.saml.keystore.path=file:/opt/apache-tomcat/conf/myKeystore.jks
# key store password
security.saml.keystore.password=changeit
# Key alias
security.saml.key.alias=somealias
# Key password
security.saml.key.password=changeit
# is Single Logout implemented in the customer IDP ?
security.saml.single.logout=true
```

security.saml.idp.metadata.location	Location of the **FederationMetadata.xml** file.
security.saml.idp.metadata.group.attribute.name	Name of the **group attribute** (please discuss with your IT administrators if the example provided in **security.properties** is not satisfactory).
security.saml.keystore.path	Location of the **keystore** you created previously.
security.saml.keystore.password	The keystore **password** you created previously (corresponds to the **-storepass** option for keytool)
security.saml.key.alias	The keystore **alias** you created previously.
security.saml.key.password	The key **password** you created previously (corresponds to the **-keypass** option for keytool).
security.saml.single.logout	If SAML authentication is in operation, but no Single Logout service is provided in the IdP, you can force the dashboard to handle this situation gracefully and display a message explaining what to do by setting the option to **true** (default): 

Restart Apache Tomcat

Now restart your Apache Tomcat server so that the changes you made are taken into account.

Generate spring_metadata

When you have successfully restarted the Apache Tomcat host server, please browse to the following URL to generate the **spring_metadata**:

```
https://tomcat/<deployed_war_file>/saml/metadata
```

This will download a file called **spring_saml_metadata.xml**. Send this file to your IT administrators who will then register it in the ADFS allowing users to login to the web application.

User groups and roles

The CAST AIC Portal provides a means to restrict access to certain functions through the use of **groups** and **roles**. Currently, two **roles** are available:

Role	Description
Platform Administrator	Is granted full access to all the AIC Portal's functions: • Create, Read, Update, Delete **any Domain** and **any Application** • Can **deliver** any Application using the CAST Delivery Manager Tool • Can **assign groups to domains** giving members of the group the **Delivery Manager role** Out of the box, the CAST AIC Portal has one Platform Administrator - the "cast" user, a member of the ADMINISTRATORS group and enabled by default.
Delivery Manager	Is granted access as follows: • Read access to specific Domains and Applications • Can **deliver** specific Applications using the CAST Delivery Manager Tool Out of the box, the CAST AIC Portal has no Delivery Managers defined.

Configuring the Platform Administrator role

The Platform Administrator role is configured using the following XML file - all groups (and their members) defined in this XML configuration file will be granted the Platform Administrator role:

```
%CATALINA_HOME%\webapps\CAST-AICP\WEB-INF\administrators.xml
```

By default, the "in memory authentication" **cast** user is a member of the "ADMINISTRATORS" group, which in turn has been granted the **Platform Administrators role** (CAST recommends that you leave this configuration at its default):

```
<?xml version="1.0" encoding="UTF-8"?>
<administrators xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                xsi:noNamespaceSchemaLocation="administrators.xsd">
    <!-- The default ADMINISTRATORS group is attributed to the default user cast.
    Please do not remove this value. -->
    <group>ADMINISTRATORS</group>
</administrators>
```

Behaviour in each authentication mode

Depending on the authentication mode you are using, the Platform Administrator role behaves as follows:

Authentication Mode	Behaviour
Default Authentication	In order to gain the Platform Administrator role, the **user** must be a member of the default ADMINISTRATORS group, or a custom group that has been added to the **administrators.xml** file. Users are assigned to groups via the **application-security-default.xml** configuration file as described above.
Active Directory with LDAP and **Standard LDAP**	In order to gain the Platform Administrator role, the **user** must be a member of an Active Directory or LDAP group whose CN (Common Name) **matches** the default ADMINISTRATORS group defined in the **administrators.xml** file, or a custom group that has been added to the **administrators.xml** file.

Granting the Platform Administrator role to a group

To assign another group the Platform Administrator role, insert a new **<group>** element as shown below:

Active Directory with LDAP and Standard LDAP

In this mode simply add the **Common Name (CN)** of the Active Directory group that you want to assign the Platform Administrator role to. In this example, the Active Directory group "**company.development.castadmins**" has been added:

```
<?xml version="1.0" encoding="UTF-8"?>
<administrators xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                xsi:noNamespaceSchemaLocation="administrators.xsd">
    <!-- The default ADMINISTRATORS group is attributed to the default user cast.
    Please do not remove this value. -->
    <group>ADMINISTRATORS</group>
    <group>company.development.castadmins</group>
</administrators>
```

Following any changes you make, **save the administrators.xml file** and then **restart** your application server so that the changes are taken into account.

Default Authentication

In this mode simply add the name of the group that you want to assign the Platform Administrator role to. In this example, the group "ITADMINS" has been added:

```
<?xml version="1.0" encoding="UTF-8"?>
<administrators xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                xsi:noNamespaceSchemaLocation="administrators.xsd">
    <!-- The default ADMINISTRATORS group is attributed to the default user cast.
    Please do not remove this value. -->
    <group>ADMINISTRATORS</group>
    <group>ITADMIN</group>
</administrators>
```

Following any changes you make, **save the administrators.xml file** and then **restart** your application server so that the changes are taken into account.

Configuring the Delivery Manager role

In contrast to the Platform Administrator role, the configuration the Delivery Manager role is achieved using the CAST AIC Portal's GUI. This is discussed in further detail in:

- Register the Application in the CAST AIC Portal
- Configure the Delivery Manager role

Note that the information related to the Delivery Manager role (i.e. users/groups who have been granted this role) is stored in a **HSQLDB** (HyperSQL DataBase). Data is stored in the following location:

```
%CATALINA_HOME%\webapps\CAST-AICP\database
```