CAST AIC Portal - Configuring the Audit Trail feature

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

On this page:

Target audience:

CAST AI Administrators

Summary: this page explains how to enable and configure the Audit Trail feature in the CAST AIC Portal to log successful user logins, failed logins, logouts, web application startup/stop etc.

Introduction

By default, the CAST AIC Portal **does not** log **significant user events**. If you would like to see this information in a log file for security reasons, then you can enable the **Audit Trail** feature. The Audit Trail feature will log all of the following events:

- User login failed
- User login successful
- User logout
- Application startup
- Application shutdown (only if server process is not killed)
- User created a domain
- User updated a domain name
- Granting delivery rights to a user group
- Denying delivery rights to a user group
- User deleted a domain
- User created a new Application
- User updated an Application name
- User moved an Application from one domain to another
- User unregistered an Application
- CAST Delivery Manager Tool (DMT) was downloaded using JNLP
- User delivered an Application version
- User delivered a package for an Application version
- User delivered and closed an Application version
- User refreshed an Application
- User refreshed an Application version
- User refreshed a package for an Application version

Enabling the Audit Trail feature

To enable the Audit Trail feature, you need to modify the following file with a text editor:

```
%CATALINA_HOME%\webapps\CAST-AICP\WEB-INF\log4j2.xml
```

- Search for the following line in the file:

```
<Property name="auditLevel">OFF</Property>
```

- Change the **OFF** value to **ALL**:

```
<Property name="auditLevel">ALL</Property>
```

- Following any changes you make, **save the log4j2.xml file** and then **restart** your application server so that the changes are taken into account.

Consulting the Audit Trail log file

- By default, when enabled, the Audit Trail feature will provide a log file in the following location:

```
%CATALINA_HOME%\webapps\CAST-AICP\audit\audit.log
```

- Messages relating to **user events** will be displayed in the log file in the following format:

```
[ DATE YYYY-MM-DD HH:MM:SS,MS | USER_HOST | USER_NAME | LEVEL | EVENT/MESSAGE ]
```

- For example:

```
2015-04-10 14:58:47,426 | 10.0.1.50 | James | INFO | Application startup
2015-04-10 14:58:59,945 | 10.0.1.52 | cast | INFO | Login successful
2015-04-10 16:52:13,335 | 10.0.1.52 | cast | INFO | Login successful
2015-04-10 16:52:29,406 | 10.0.1.52 | cast | INFO | Application created [guid: c18ca3b9-ea4d-4ade-842b-
b051cb5e8e56, name: MEUDON]
2015-04-10 16:53:00,188 | 10.0.1.52 | cast | INFO | User Logout
2015-04-10 16:53:42,660 | 10.0.1.50 | James | INFO | Application shutdown
2015-04-10 16:53:46,459 | 10.0.1.50 | James | INFO | Application startup
2015-04-10 16:54:07,000 | 10.0.1.52 | cast | WARN | Login failed
2015-04-10 16:54:09,882 | 10.0.1.52 | cast | INFO | Login successful
2015-04-10 16:54:12,629 | 10.0.1.52 | cast | INFO | User Logout
```

Changing the log file storage location

Audit Trail log files are created and archived by default in the CAST AIC Portal application deployment folder, under the **audit** folder. To change this location, you need to modify the following file with a text editor:

```
%CATALINA_HOME%\webapps\CAST-AICP\WEB-INF\log4j2.xml
```

To change the location of the log folder within the limits of the web application:

- Search for the following line in the file:

```
<Property name="auditPath">$${web:rootDir}/audit</Property>
```

- Change **/audit** to the required location (for example **/test**) within the web application file hierarchy:

```
<Property name="logPath">$${web:rootDir}/test</Property>
```

- Following any changes you make, **save the log4j2.xml file** and then **restart** your application server so that the changes are taken into account
- Your log files will now be stored in the new location. For example:

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

Changing the log file rotation strategy

The Audit Trail log file has a default rotation strategy as follows:

- Logs will be sent to **audit.log** for **one month**
- After this time period, logging will cease to this file and the file will be zipped into an **audit-yyyy-MM.log.zip** file stored in the default log storage location
- At the same time a **new audit.log** will be created and used.

This strategy can be modified as follows:

- Modify the following file with a text editor:

```
%CATALINA_HOME%\webapps\CAST-AICP\WEB-INF\log4j2.xml
```

- Find the following line which controls the strategy by using the name of the ZIP log output:

```
filePattern="${auditPath}/audit-%d{yyyy-MM}.log.zip"
```

- Modify the options as necessary using the following date pattern letters:

Letter	Date or Time Component	Examples
G	Era designator	`AD`
y	Year	`1996`; `96`
M	Month in year	`July`; `Jul`; `07`
w	Week in year	`27`
W	Week in month	`2`
D	Day in year	`189`
d	Day in month	`10`
F	Day of week in month	`2`
E	Day in week	`Tuesday`; `Tue`
a	Am/pm marker	`PM`
H	Hour in day (0-23)	`0`
k	Hour in day (1-24)	`24`
K	Hour in am/pm (0-11)	`0`
h	Hour in am/pm (1-12)	`12`
m	Minute in hour	`30`
s	Second in minute	`55`
S	Millisecond	`978`
z	General Time zone	`Pacific Standard Time`; `PST`; `GMT-08:00`
Z	RFC 822 Time zone	`-0800`

Note that:

- Plain text can be quoted using single quotes (') to avoid interpretation, like for example: **%d{yyyy-'w'w}** that generates the output **2015-w11**
- The output generated by the date format pattern is dependent on the locale of the machine hosting the web application server

- Following any changes you make, **save the log4j2.xml file** and then **restart** your application server so that the changes are taken into account.

Size based rotation policy

A supplementary Audit Trail log rotation **by size** can be achieved by uncommenting the **SizeBasedTriggeringPolicy** available in the Policies list, as follows:

```
<!-- Audit log rotation policies -->
<Policies>
...
    <!-- <SizeBasedTriggeringPolicy size="10 MB"/> -->
</Policies>
...
```

The size based policy causes a rotation once the file has reached the specified size. The size can be specified in bytes, with the suffix KB, MB or GB, for example “10 MB”.

Log file rotation examples

The **time based policy** and the **size based** policies can be used together. The following section provides some examples of how to modify the rotation policy:

- ***"${auditPath}/audit-%d{yyyy-MM}.log.zip"*** for a rotation by month, e.g.: **audit-2015-03.log.zip**
- ***"${auditPath}/audit-%d{yyyy-'w'w}.log.zip"*** for a rotation by week in year, e.g.: **audit-2015-w11.log.zip**
- ***"${auditPath}/audit-%d{yyyy-MM-'w'W}.log.zip"*** for a rotation by week in month, e.g.: **audit-2015-03-w2.log.zip**
- ***"${auditPath}/audit-%d{yyyy-MM-dd}.log.zip"*** for a rotation by day, e.g.: **audit-2015-03-10.log.zip**
- ***"${auditPath}/audit-%d{yyyy-MM}_%i.log.zip"*** when rotating by size in addition to a rotation by month, e.g.: **audit-2015-03_1.log.zip**, **audit-2015-03_2.log.zip**, **audit-2015-03_3.log.zip**

Changing the user event message output format

As described previously, messages relating to **user events** will be displayed in the log file in the following format:

```
[ DATE YYYY-MM-DD HH:MM:SS,MS | USER_HOST | USER_NAME | LEVEL | EVENT/MESSAGE ]
```

This output format is governed by the following line in the **log4j2.xml** file:

```
<PatternLayout pattern="%date{DEFAULT} | %mdc{audittrail.remotehost} | %mdc{audittrail.username} | %level | %
message%n" charset="UTF-8"/>
```

Where the following is true:

- ***%date{DEFAULT}*** represents the date and time when the user event occurred.
- ***%mdc{audittrail.remotehost}*** represents the host from where the user makes the audited action. This is a custom pattern and is set by the CAST AIC Portal when the action is logged and the **format must not be changed**.
- ***%mdc{audittrail.username}*** represents the user name that is doing the action. As user host pattern, it’s a value that is set by the web application when the user action is logged and the **format must not be changed**.
- ***%level*** is the Log4j logging level corresponding to the priority of the user action. For example a successful authentication will be logged with a simple “INFO” level, meanwhile a failure in authentication will be logged with a “WARN” level.
- ***%message*** is the pattern corresponding to the user action that is audited.

It is possible to modify this output by changing the pattern layout. Please refer to the following Log4j2 documentation page: http://logging.apache.org/log4j/2.0/manual/layouts.html#PatternLayout for more information.

Changing the message output

All Audit Trail messages that are output to the log file can be customized if required. Messages are stored in an XML properties file in the following location:

```
%CATALINA_HOME%\webapps\CAST-AICP\WEB-INF\classes\audittrail
```

Two files are provided by default: one to provide messages in English, the other in French - see the section **Internationalization** below for more information about how these two files work.

- AuditTrailMessages.xml
- AuditTrailMessages_fr.xml

If you wish to customise the output message, you can do so by editing the XML file with a text editor. All output messages are configured using the **<entry>** tag, for example the message that is output when a user login fails is configured in the following line - the message is "Login failed":

```
<entry key="USER_LOGIN_FAILED">Login failed</entry>
```

To change this, simply update the text between the <entry> tags:

```
<entry key="USER_LOGIN_FAILED">A user login failed</entry>
```

Use of variables

Some output messages contain variables, for example:

```
<entry key="CREATE_DOMAIN">Created application domain %2$s [guid: %1$s]</entry>
```

These variables are used to display specific values. In the example above, the message would look something like the following, where the domain name is **TEST** and its GUID is **50037cba-12ef-43f1-8514-b16660a3b492**:

```
Created application domain TEST [guid: 50037cba-12ef-43f1-8514-b16660a3b492]
```

A full run down of all the variables used in messages is provided below:

Entry Key	Message	Variable
CREATE_DOMAIN	Created application domain %2$s [guid: %1$s]	%1$s - application domain guid %2$s - application domain name
UPDATE_DOMAIN_NAME	Updated name of application domain %2$s [guid: %1$s] to %3$s	%1$s - application domain guid %2$s - old application domain name %3$s - new application domain name
GRANT_DELIVERY_MANAGER	Granted delivery manager rights to %3$s on application domain %2$s [guid: %1$s]	%1$s - application domain guid %2$s - application domain name %3$s - delivery manager name
DENY_DELIVERY_MANAGER	Denied delivery manager rights to %3$s on application domain %2$s [guid: %1$s]	%1$s - application domain guid %2$s - application domain name %3$s - delivery manager name
DELETE_DOMAIN	Deleted application domain %2$s [guid: %1$s]	%1$s - application domain guid %2$s - application domain name
CREATE_APPLICATION	Created application %2$s [guid: %1$s] in application domain %4$s [guid: %3$s]	%1$s - application guid %2$s - application name %3$s - application domain guid %4$s - application domain name
UPDATE_APPLICATION_NAME	Updated name of application %2$s [guid: %1$s] to %3$s	%1$s - application guid %2$s - old application name %3$s - new application name

MOVE_APPLICATION	Moved application %2$s [guid: %1$s] from domain %4$s [guid: %3$s] to domain %6$s [guid: %5$s]	%1$s - application guid %2$s - application name %3$s - old application domain guid %4$s - old application domain name %5$s - new application domain guid %6$s - new application domain name
DELETE_APPLICATION	Deleted application %2$s [guid: %1$s]	%1$s - application guid %2$s - application name
APPLICATION_VERSION_DELIVERY	Delivered version %4$s [guid: %3$s], application %2$s [guid: %1$s]	%1$s - application guid %2$s - application name %3$s - version guid %4$s - version name
APPLICATION_PACKAGE_DELIVERY	Delivered package %6$s [guid: %5$s], version %4$s [guid: %3$s] in application %2$s [guid: %1$s]	%1$s - application guid %2$s - application name %3$s - version guid %4$s - version name %5$s - package guid %6$s - package name
APPLICATION_VERSION_DELIVERY_CLOSE	Closed version %4$s [guid: %3$s], application %2$s [guid: %1$s]	%1$s - application guid %2$s - application name %3$s - version guid %4$s - version name
REFRESH_APPLICATION	Refreshed application %2$s [guid: %1$s]	%1$s - application guid %2$s - application name
REFRESH_VERSION	Refreshed version %4$s [guid: %3$s], application %2$s [guid: %1$s]	%1$s - application guid %2$s - application name %3$s - version guid %4$s - version name
REFRESH_PACKAGE	Refreshed package %6$s [guid: %5$s], version %4$s [guid: %3$s], application %2$s [guid: %1$s]	%1$s - application guid %2$s - application name %3$s - version guid %4$s - version name %5$s - package guid %6$s - package name

Removing variables

If you do not want the real names of Applications, Domains, Delivery Managers, Versions and Packages to appear in the Audit Trail ouput log, then you can simply remove them. For example to remove the name of the Domain from the following message simply change it from:

```
<entry key="GRANT_DELIVERY_MANAGER">Granted delivery manager rights to %3$s on application domain %2$s [guid: %1$s]</entry>
```

to:

```
<entry key="GRANT_DELIVERY_MANAGER">Granted delivery manager rights to %3$s on application domain [guid: %1$s]</entry>
```

Internationalization

Audit trail messages are by default internationalized and come in two translations: English (default language if the machine language is not supported) and French. The translations into French are stored in XML properties file types under:

```
%CATALINA_HOME%\webapps\CAST-AICP\WEB-INF\classes\audittrail
```

If desired, additional language translation files can be added under this path.