Changes or new features - 8.3.17

On this page:

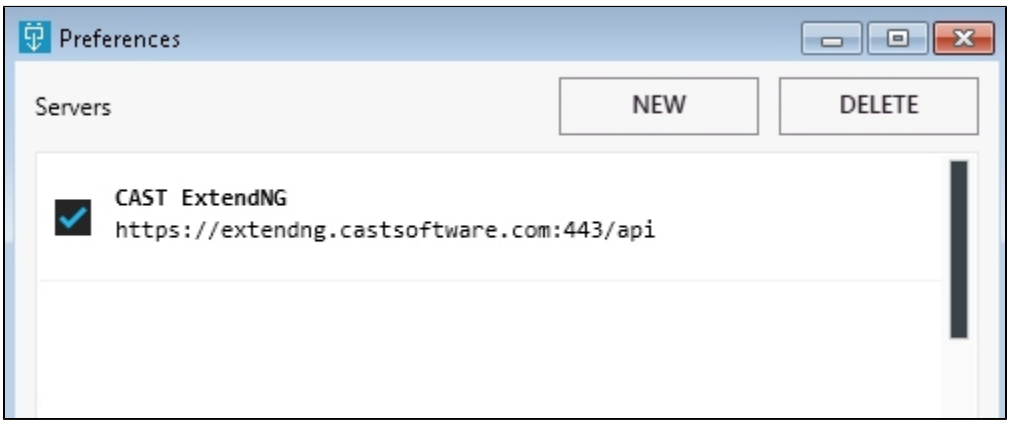
Summary: CAST AIP 8.3.17 introduces a number of features and changes as listed below.

CAST Extension Downloader

Some changes have been made to switch extension downloads to the "next generation" CAST Extend (https://extend.castsoftware.com). This new CAST Extend is a replacement for the existing CAST Extend which will be phased out in due course. Note that to use https://extend.castsoftware.com, you will need to **register a new account** (https://extend.castsoftware.com/register) - however, accounts from the existing CAST Extend service **will be transferred in over the coming weeks.**

Installing CAST AIP 8.3.17 from scratch

When installing CAST AIP 8.3.17 from scratch when no previous release of CAST AIP exists, the following server will be pre-configured for extension downloads (the server will be **ticked and enabled**):



Note that you can manually add the URL of the existing CAST Extend service if you prefer to use it, however, you should bear in mind that this service will be **phased out** in due course.

Installing CAST AIP 8.3.17 when a previous release of CAST AIP already exists

When installing CAST AIP 8.3.17 and a previous release of CAST AIP already exists (more specifically if the %PROGRAMDATA%\CAST\CAST\Extensions\ServerList.xml file exists) then the following will occur:

- https://extendng.castsoftware.com/api will be added as CAST ExtendNG and will be **ticked and enabled**
- https://extend.castsoftware.com:443/V2/api/v2 will be deleted
- All other servers will be remain as they were previously.

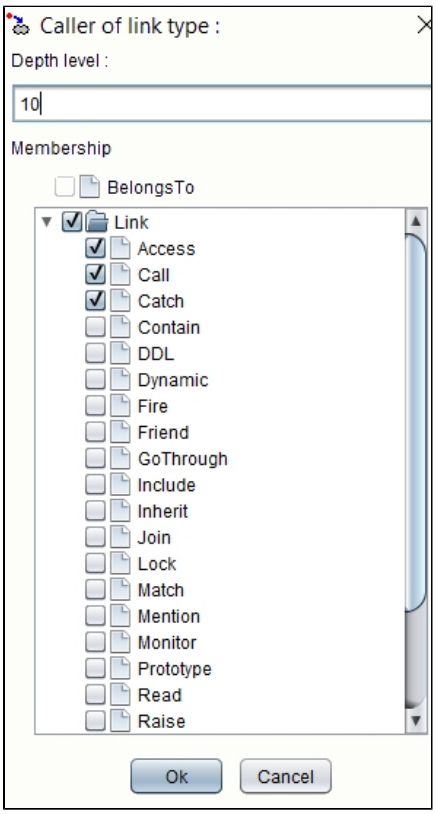
Note that you can manually add the URL of the existing CAST Extend service if you prefer to use it, however, you should bear in mind that this service will be **phased out** in due course.

CAST Transaction Configuration Center

Set/layer creation with Caller-Of and Callee-Of blocks

It is now possible to create **Caller-Of** and **Callee-Of** blocks using **multiple link types**. Previously, only one single link type could be selected. See TCC - Working with block elements for more information.

Click to enlarge



Configurations built with this new feature **cannot be used with CAST Transaction Configuration 8.3.16** (i.e. importing a .TCCSetup file that contains this new configuration). Erroneous results will be produced.

User Input Security

AIPCORE-1120 - support for MongoDB for Java

NoSQL injections for applications using MongoDB for Java can now be detected. Results are provided via the rule **8418 - Avoid NoSQL injection**.

AIPCORE-1057 - Name of rule changed - Sensitive cookie in HTTPS session without 'Secure' attribute (8240)

The rule **Sensitive cookie in HTTPS session without 'Secure' attribute (8240)** has been renamed as **Avoid using unsecured cookie (8240)**.

AIPCORE-1040 - SpringMVC technology - total checks less than failed checks (violations)

A bug causing the total number of checks to be reported as lower than the total number of failed checks (i.e. violations) for Applications containing SpringMVC technology has been fixed therefore improving accuracy.

AIPCORE-1028 - Improvement to Avoid HTTP response splitting (7740) rule

The rule **Avoid HTTP response splitting (7740)** computed by the User Input Security has been improved: the full path of related violations is now computed thus improving bookmark accuracy.

AIPCORE-1025 - java.io.ObjectInputStream methods handled

java.io.ObjectInputStream methods are now automatically taken into account.

AIPCORE-1010 - Improvement to SpringMVC regression introduced in 8.3.16

During the analysis of an application using Spring MVC, a blackbox is generated by the **SpringMVC extension**, however, this blackbox was ignored during a User Input Security analysis. As a result, some violations were not found. This bug has been fixed improving accuracy.

AIPCORE-993 - Support for CWE-601: URL Redirection to Untrusted Site ('Open Redirect')

Support has been introduced for **CWE-601: URL Redirection to Untrusted Site ('Open Redirect')**.

AIPCORE-641 - Avoid log forging vulnerabilities (8044) - total checks less than failed checks (violations)

A bug causing the total number of checks to be reported as lower than the total number of failed checks (i.e. violations) has been fixed therefore improving accuracy.