

Changes or new features - 8.3.3

On this page:

- [Technology support changes](#)
- [Installation and deployment](#)
 - [Renamed WAR files](#)
 - [SAML authentication mode](#)
 - [Supported Platforms](#)
 - [Upgrade - removal of the CAST Update Tool \(CUT\)](#)
 - [CastGlobalSettings.ini](#)
- [Engineering Dashboard](#)
 - [Risk Model colour](#)
 - [Critical Violation icon](#)
 - [Change Language option](#)
- [Health Dashboard](#)
 - [New columns for drill down from tiles](#)
 - [Change Language option](#)
- [User Input Security \(dataflow\)](#)
 - [Security for Java extension](#)
 - [Automatic Blackboxing](#)
 - [Improved Common Weakness Enumeration support](#)
- [CAST Management Studio](#)
 - [CLI](#)
 - [PurgeVersion](#)
- [CAST Delivery Manager Tool](#)
 - [New Package Alerts tab](#)
- [CAST Architecture Checker](#)
 - [Checking links to objects outside the application boundary](#)
 - [CLI](#)
- [CAST Transaction Configuration Center](#)
 - [Change to the way non-contributing End Points are handled](#)
- [CAST System Views](#)



Summary: CAST AIP 8.3.3 introduces a number of features and changes as listed below.

Technology support changes

Please see [Technology coverage changes in CAST AIP 8.3.x](#) for more detailed discussion of this subject.

Installation and deployment

Renamed WAR files

Continuing with the dashboard re-naming modifications made in CAST AIP 8.3.2 (see [Changes or new features - 8.3.2](#)), the WAR files have now been renamed as follows:

Previous name	New name
CAST-AAD.war	CAST-Health.war
CAST-AED.war	CAST-Engineering.war
CAST-AAD-AED.war	CAST-Health-Engineering.war

Please ensure that you take note of this and modify any WAR deployment routines you may have. See also:

- [Installing and configuring the Health Dashboard](#)
- [Installing and configuring the Engineering Dashboard](#)

SAML authentication mode


The following CAST AIP web applications now support user authentication over **SAML**:

- [CAST AIC Portal](#)

- [Health Dashboard](#)
- [Engineering Dashboard](#)
- [CAST-RestAPI](#)

Supported Platforms

Windows Server 2016 is now supported for use with CAST AIP, CAST Delivery Manager Tool and CAST dashboards. Please see [Supported Platforms](#) for more information.

 Windows Server 2016 is **only supported** by CAST when installed in **Desktop Experience mode**(i.e. with a GUI).

Upgrade - removal of the CAST Update Tool (CUT)

The CAST Update Tool (CUT.exe) and its command line counterpart (CUT-CLI.exe) have been removed from the CAST AIP setup and are no longer installed. All upgrade actions are to be performed with [CAST Server Manager](#) or the [upgrade batch file](#).

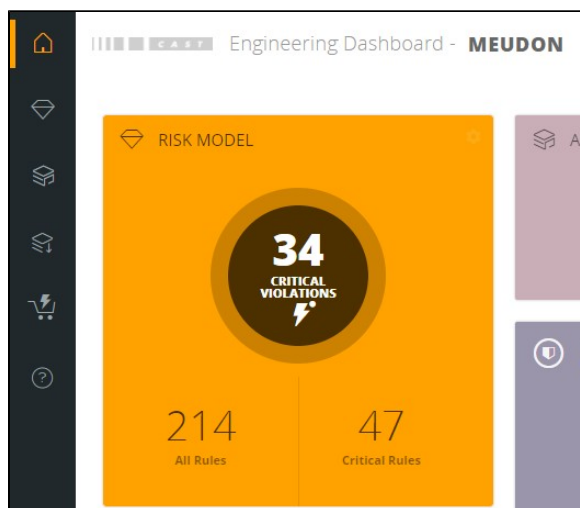
CastGlobalSettings.ini

The [CastGlobalSettings.ini](#) file has been cleaned up to remove references to an obsolete environment variable "%ALLUSERSPROFILE%\Application Data". This has been replaced with the variable "%PROGRAMDATA%". There is no impact to end users.

Engineering Dashboard

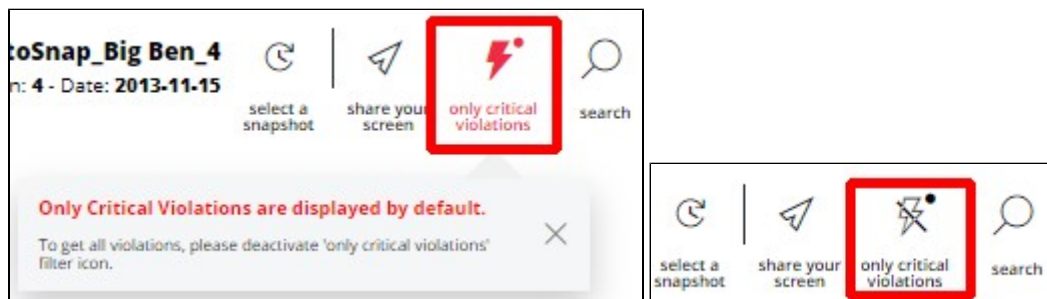
Risk Model colour

The colour used for the Risk Model view and tile has changed from red to yellow:



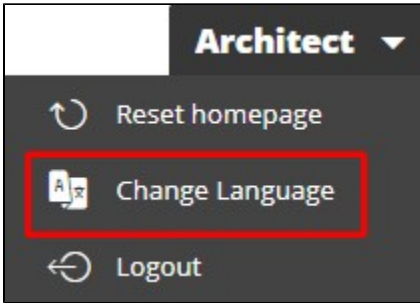
Critical Violation icon

The **Critical Violation** toggle icon has been redesigned - there is no change to the behaviour of this toggle icon. See [Engineering Dashboard](#) for more information.



Change Language option

Improvements have been made to the Change Language option:



- To view a new language in the **Change Language option**, it is now only necessary to define a new locale folder and a translation file. The dashboard will automatically detect the locale and offer the language.
- Language change is specific to the browser. Therefore if the browser cache is emptied, the language will reset to whatever the default is.
- Ability to set a default language now added to the **ced.json** file.

See:

- [Engineering Dashboard](#)
- [HD-ED - Dashboard localization](#)
- [ED - Dashboard wide configuration options in json](#)



Note only **English (en_US)** and **Chinese (zh_CN)** are supported locales. All other locales that are added will not be displayed.

Health Dashboard

New columns for drill down from tiles

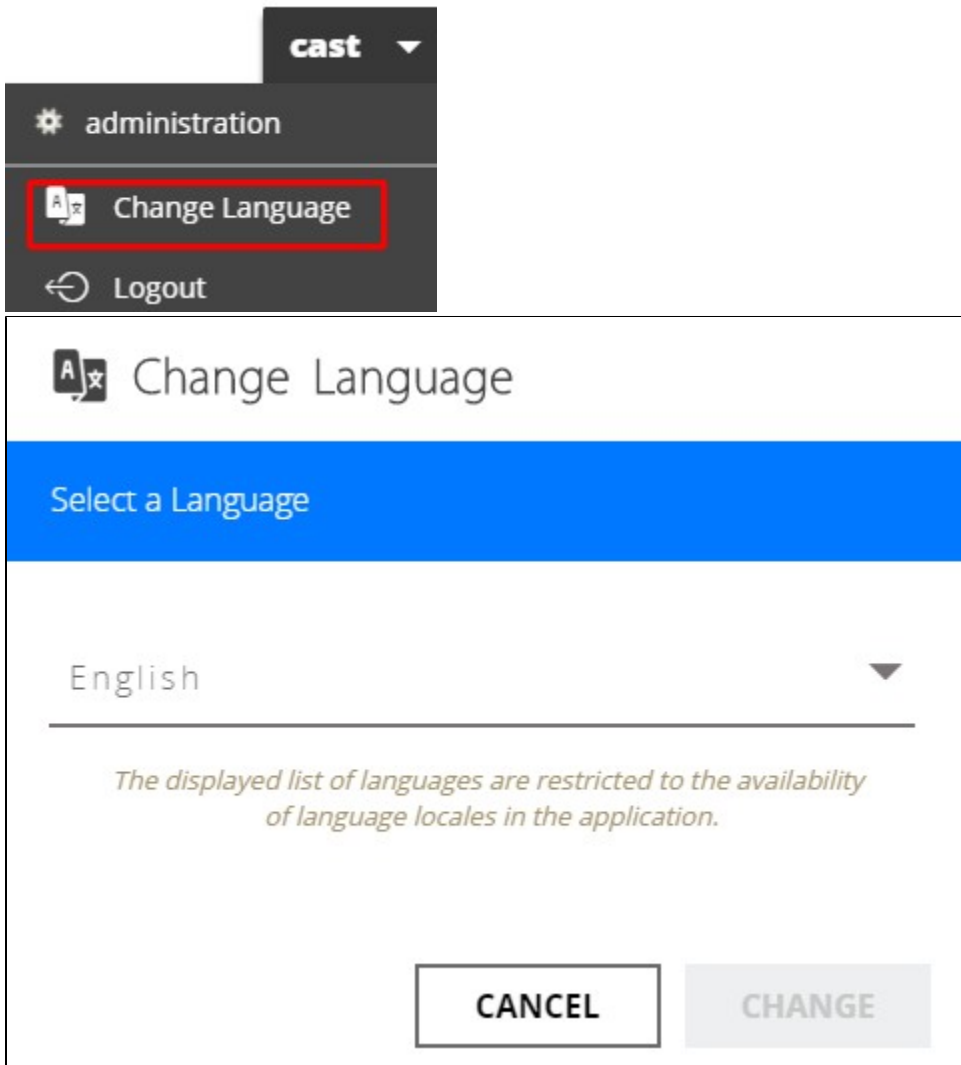
The columns displayed when drilling down from Health Measure tiles, Top Critical Rules, Technologies Overview tiles have been redesigned:



It is now also possible to force the "% Compliance" column to display "% Failed". See [HD - Dashboard wide configuration options in json](#) in the **app-navigation.json** section.

Change Language option

The top user menu now has an additional drop down menu item called "Change Language". This allows a user to change the language of the text items in the dashboard, providing an administrator has configured the language:



- To view a new language in the **Change Language option**, it is only necessary to define a new locale folder and a translation file. The dashboard will automatically detect the locale and offer the language.
- Language change is specific to the browser. Therefore if the browser cache is emptied, the language will reset to whatever the default is.
- Ability to set a default language is managed in the **cmp.json** file.

See:

- [Health Dashboard](#)
- [HD-ED - Dashboard localization](#)
- [HD - Dashboard wide configuration options in json](#)



Note only **English (en_US)** and **Chinese (zh_CN)** are supported locales. All other locales that are added will not be displayed.

User Input Security (dataflow)

Improvements to the [User Input Security feature](#) have been added in this release.

Security for Java extension

A new extension called [Security for Java](#) is available for [download](#) and [installation](#) - this extension automatically generates **JEE** specific **bytecode** (also known as "CASTIL") for the **User Input Security** feature. It provides more accurate results than the bytecode that was previously generated by the analyzer and CAST highly recommends that this extension is used if you are intending to perform User Input Security checks as part of your source code analysis.

Automatic Blackboxing

The User Input Security feature will now automatically generate blackbox methods **on the fly** during the analysis process for **all methods which do not have a body**, i.e. all code that is deemed to be "external" to the application boundary. This includes the majority of assemblies for which no source code can be found (framework assemblies, third-party JARs/assemblies, internal frameworks without source code etc.). It is still possible to manually create blackbox methods if necessary.

Improved Common Weakness Enumeration support

The following CWE are now supported:

- Trust Boundary Violation (CWE-501)
- Sensitive Cookie in HTTPS Session Without 'Secure' Attribute (CWE-614)
- Use of hard-coded credential (java, C#, VB.Net languages) (CWE-798)

CAST Management Studio

CLI

PurgeVersion

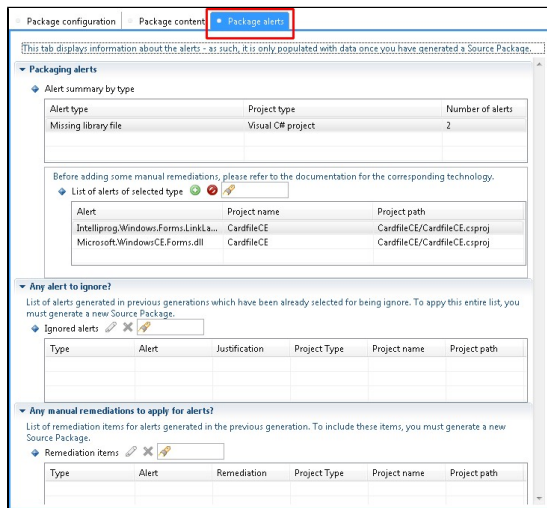
A new option called **PurgeVersion** has been added to enable you to automate the deletion of a Version whose extracted source code has already been deleted, i.e. the version is present in the "Delivery without source code" section of the CAST Management Studio GUI. See [Automating CAST Management Studio tasks](#) for more information.

CAST Delivery Manager Tool

New Package Alerts tab

The CAST Delivery Manager Tool now has a new tab called **Package Alerts** that is present for some package types:

Click to enlarge



This tab contained three panels:

- **Packaging alerts** > was previously available in the **Package Content** tab. An **ignore** button has been added enabling you to ignore an alert (the ignored alert will be listed in the new panel **Any alert to ignore?**)
- **Any alert to ignore?** > this is a new panel not previously available. It lists all alerts that have been manually ignored from the **Packaging Alerts** tab.
- **Any manual remediations to apply for alerts?** > was previously available in the **Package Configuration** tab.

See also [How do I fine-tune my Version](#) in [Onboarding an Application in CAST AIP](#).

CAST Architecture Checker

Checking links to objects outside the application boundary

Architecture Checker can report violations between two Layers even when objects inside the targeted Layer not only are external, but also belong to a module external to the Application being checked. The only constraint is that the objects inside the Layer from which the Dependency towards the targeted Layer is issued, must belong to a module internal to the Application. For example, it is possible to check for links which reach objects belonging to a .NET assembly outside of the Application boundary, provided these links start from objects in a module which is internal to the Application (even though these latter objects can be external).

CLI

The CAST Architecture Checker now has a CLI mode that can be used to run a **check model** action (equivalent to the same action in the GUI). See [Automating CAST Architecture Checker tasks](#) for more information.

CAST Transaction Configuration Center

Change to the way non-contributing End Points are handled

To avoid having empty transactions, if a transaction has non-contributing End Points then their DET value is considered as a contribution to the transaction. In previous releases of CAST AIP some of these End Points had a DET value of **0**, and as a consequence these transactions were considered as empty.

To avoid this situation, starting from CAST AIP 8.3.3, where transactions ONLY have non-contributing End Points, the minimum DET of the transaction is set to **1**. The impact of this is that after upgrade to CAST AIP 8.3.3, some of the transactions which were empty before may now become valid. This can happen with the predefined list of End Points delivered in CAST AIP, when the following End Points are reached and they are the only one reached by the transaction:

Click to enlarge

Description	DET	Contribute	Activ...	U...	Package
Standard End Point - Net - Microsoft.Office.Interop...	0	0	ACTIVE	•	Base_DotNet
Standard End Point - Net - System.Console	0	0	ACTIVE	•	Base_DotNet
Standard End Point - Net - System.Data	0	0	ACTIVE	•	Base_DotNet
Standard End Point - Net - System.DirectoryServic...	0	0	ACTIVE	•	Base_DotNet
Standard End Point - Net - System.Drawing	0	0	ACTIVE	•	Base_DotNet
Standard End Point - Net - System.Linq	0	0	ACTIVE	•	Base_DotNet
Standard End Point - Net - System.Net	0	0	ACTIVE	•	Base_DotNet
Standard End Point - Net - System.Reflection	0	0	ACTIVE	•	Base_DotNet
Standard End Point - Net - System.Security.Crypto...	0	0	ACTIVE	•	Base_DotNet
Standard End Point - Net - System.ServiceModel	0	0	ACTIVE	•	Base_DotNet
Standard End Point - Net - System.Text	0	0	ACTIVE	•	Base_DotNet
Standard End Point - Net - System.Xml	0	0	ACTIVE	•	Base_DotNet
Standard End Point - Java - com.ibm.jms	0	0	ACTIVE	•	Base_Java
Standard End Point - Java - com.sun.jndi.toolkiturl	0	0	ACTIVE	•	Base_Java
Standard End Point - Java - com.sun.jndi.url	0	0	ACTIVE	•	Base_Java
Standard End Point - Java - com.sun.msv	0	0	ACTIVE	•	Base_Java
Standard End Point - Java - java.net	0	0	ACTIVE	•	Base_Java
Standard End Point - Java - java.nio	0	0	ACTIVE	•	Base_Java
Standard End Point - Java - java.security	0	0	ACTIVE	•	Base_Java
Standard End Point - Java - java.util.Properties	0	0	ACTIVE	•	Base_Java
Standard End Point - Java - java.util.queue	0	0	ACTIVE	•	Base_Java
Standard End Point - Java - java.util.zip	0	0	ACTIVE	•	Base_Java
Standard End Point - Java - javax.jms	0	0	ACTIVE	•	Base_Java
Standard End Point - Java - javax.xml.stream	0	0	ACTIVE	•	Base_Java
Standard End Point - Java - org.apache.commons...	0	0	ACTIVE	•	Base_Java
Standard End Point - Java - sun.net.telnnet	0	0	ACTIVE	•	Base_Java
Standard End Point - Web - External URL	0	0	ACTIVE	•	Base_Web

CAST System Views

Two previously undocumented CAST System Views (CSV) for the Dashboard Service schema have now been documented. Please see [CAST System Views - Dashboard Service](#) for more information:

- CSV_OBJECTS_STATUSES
- CSV_VIOLATION_STATUSES

In addition, both CAST System Views listed above contained column names that had typographical errors. These typographical errors have been fixed by adding new columns spelt correctly. The existing column names containing the spelling errors will remain and are now deprecated, therefore, please update any scripts or queries that use the existing column names:

- CSV_OBJECTS_STATUSES
 - SNAPHOT_ID replaced by SNAPSHOT_ID
 - OBEJCT_TECHNO_TYPE_ID replaced by OBJECT_TECHNO_TYPE_ID
- CSV_VIOLATION_STATUSES
 - SNAPHOT_ID replaced by SNAPSHOT_ID