

QueryVision: SSO Dynamic TSOP Guide

Version 2016.1

Table of Contents

1.	OVERVIEW	1
2.	LATEST GUIDES	1
3.	SSO DYNAMIC, COGNOS, TSOPs AND JRE VERSIONS	1
4.	TSOP CONFIGURATION PROPERTIES GUIDE	2
4.1	10.1.0, 10.1.1	2
4.2	10.2, 10.2.1, 10.2.2, 11	3

1. OVERVIEW

This document provides detailed guidelines on selecting the right version of:

- **CAM_AAA_TrustedSignonJCAPSQLMulti.jar**
- **JDBC_Config_JCAPSQLSSOM.properties**

And the details on configuring both JDBC_Config_JCAPSQLSSOM.properties and QvtConfig.xml beyond what is discussed in the **QueryVision Web Parts Installation Guide**

2. LATEST GUIDES

The latest versions of this guide and the installation guide can be found on the queryvision.com web site here:

- [QueryVision SSO Dynamic Trusted Sign On Provider Guide](#)
- [QueryVision Web Parts Installation Guide](#)

3. SSO DYNAMIC, COGNOS, TSOPs AND JRE VERSIONS

QueryVision's SSO Dynamic single sign on feature requires the use of a Trusted Sign on Provider (TSOP) which is a specialized Custom Authentication Provider (CAP) written in Java to support Single Sign On (SSO).

QueryVision ships with multiple versions of **CAM_AAA_TrustedSignonJCAPSQLMulti.jar** that map to different Cognos versions and the Java JRE runtime used to run Cognos BI Servers. This is particularly important with Cognos 10.2.1 and 10.2.2 and later as you may get the following error on doing a Test of the Authentication Namespace in Cognos Configuration or in the Cognos log:

```
[ ERROR ] AAA-CFG-0008 The handler class 'TrustedSignonJCAPSQLMulti' cannot be loaded.
```

Or when attempting single sign on with the QueryVision SSO Web Part

```
Error AAA-AUT-0011 Invalid Namespace selected
```

While Cognos ships with (and installs) the most recent recommended Java runtime JRE, most versions can be configured to run with other versions. For example, Cognos 10.2.2 is supported by IBM Java versions 5.08 (1.5), 6.08, 6.10 (1.6), 7.0 (1.7), Oracle Java 7.0 (1.7), and Sun 6.0 (1.6)

To discover what versions of the JRE are supported for your Cognos version, do a web search on "*Cognos Business Intelligence Supported Software Environments*" then select your Cognos version number, then *Requirements by type: Software* and look for the Runtime Environment

The following is the selection guide to the correct folder from which to select the correct version of the following files:

- CAM_AAA_TrustedSignonJCAPSQLMulti.jar
- JDBC_Config_JCAPSQLSSOM.properties

Cognos Version	JRE Version	Trusted Sign on Provider sub folder(1)
10.1.0	1.6/6.0	10.1
10.1.1	1.6/6.0	10.1.1
10.2.0	1.6/6.0	10.2
10.2.1 and 10.2.2	1.6/6.0	10.2.1 and 10.2.2
	1.7/7.0	10.2.1 and 10.2.2
11.0	1.8/8.0	ICA 11.0

(1) This folder is part of the QueryVision Web Parts for Cognos installation and will be located here (depending on installation options):

C:\Program Files (x86)\QueryVision\QueryVision SharePoint Web Parts\Configuration\Advanced Single Signon\Trusted Signon Provider

4. TSOP CONFIGURATION PROPERTIES GUIDE

Configuration of the SSO Dynamic Trusted Sign On Provider Java component is done on the SharePoint server in QvtConfig.xml and on the Cognos server with JDBC_Config_JCAPSQLSSOM.properties.

The configuration properties and their possible values change from version to version:

4.1 10.1.0, 10.1.1

The following is an example of the JDBC_Config_JCAPSQLSSOM.properties

```
exceptionType=recoverable
cookieName=TRUSTED_SIGNON_USER
nullCookieMsg=You are not authenticated - recoverable error
capNamespace=
ntlmProcessing=true
logging=false
bcEncryptKey=94543b67dadce532e945da0eb3196bdcc8eaf2aba8ea8f6b
bcEncryptMode=enabledTimestamp
bcEncryptMaxTimeDiff=10000
```

- exceptionType – Does not apply to this version
- cookieName (default: TRUSTED_SIGNON_USER) – the name of the cookie containing the user credentials (user identity and namespace id). This name of the cookie is defined in qvtSsoDynamic.html
- nullCookieMsg (default: null) – The message to display to the user if there is no credentials in the cookie passed to the TSOP
- capNamespace (default: null) – The default namespace id to provide if a namespace id is not included in the credentials
- ntlmProcessing (default: false) – Set to true if the Cognos is using NTLM authentication (recommended setting: true)
- logging – (default: false) – is TSOP logging enabled. If true, log files of the name QvtTrustedSSO_ + timestamp + .log are saved to the Cognos installation log folder. For example: D:\Program Files\ibm\cognos\c10_64\logs

- bcEncryptKey (default: null) – this is the encryption key used to decrypt the user credentials provided in the cookie. This must match the value provided for BcEncryptionKey in the Cognos server configuration section matching the Cognos server that the TSOP is installed. See example below:
- bcEncryptMode (default: disabled) – this determines the contents of the encryption and how it is processed. This must match the value in the BcEncryption Mode value in QvtConfig.xml (see example, below). Possible values are:
 - ◇ disabled – user credentials are not encrypted
 - ◇ enabled – user credentials are encrypted using the bcEncryptKey, but are not timestamped (credentials don't expire)
 - ◇ enabledTimestamp - user credentials are encrypted using the bcEncryptKey including a timestamp. The logon credentials will expire after the time specified by bcEncryptMaxTimeDiff. This can be used to ensure credentials can't be cached or copied and used at a later time.
- bcEncryptMaxTimeDiff (default: 300) – time in seconds allowed between the time a SSO Dynamic logon request is issued by the QueryVision web parts on the SharePoint Server and the time they are received and processed by the SSO Dynamic TSOP on the Cognos Server.

The following is an example of a Cognos Server configuration in QvtConfig.xml for SSO Dynamic:

```
<LogicalName>w28r2ent208</LogicalName>
<DisplayName>C10.2.2 Server on w28r2ent208</DisplayName>
<Authentication>SSODynamic</Authentication>

<BcEncryptionKey>54d9796d20c891b5bfe0c8d0b59df4a7d643a70d0de36dab</BcEncryptionKey>
<BcEncryptionMode>enabledTimestamp</BcEncryptionMode>
```

4.2 10.2, 10.2.1, 10.2.2, 11

The configuration properties have evolved for 10.2 and later for JDBC_Config_JCAPSQLSSOM.properties. There are no changes for QvtConfig.xml

- **exceptionType** is functional in this version
- **nullCookieMsg** has been renamed to **missingCredentialsMessage**
- **errorCaption** and **errorPostscript** have been added
- **logging** (T/F) has now become **loggingLevel** and is functionally different
- **capNamespace** has been renamed to **defaultNamespaceID**

The following is an example of the JDBC_Config_JCAPSQLSSOM.properties

```
exceptionType=Unrecoverable
cookieName=TRUSTED_SIGNON_USER
missingCredentialsMessage=Missing Credentials Message
errorCaption=An Error Caption
errorPostscript=An Error Postscript
defaultNamespaceID=NamespaceXX
ntlmProcessing=true
loggingLevel=INFO
bcEncryptKey=94543b67dadce532e945da0eb3196bdcc8eaf2aba8ea8f6b
bcEncryptMode=enabledTimestamp
```

`bcEncryptMaxTimeDiff=10000`

- `exceptionType` (default: unrecoverable, possible values: Unrecoverable, UserRecoverable) – Cognos CAPs can through unrecoverable or recoverable exceptions. UserRecoverable allows Cognos to challenge the user for user id and password if the SSO authentication fails.
 - `cookieName` (default: TRUSTED_SIGNON_USER) – the name of the cookie containing the user credentials (user identity and namespace id). This name of the cookie is defined in `qvtSsoDynamic.html`
 - `missingCredentialMessage` (default: "User Credentials missing") – The message to display to the user if there is no credentials in the cookie passed to the TSOP
 - `errorCaption` (default: "QueryVision Authentication Error: ") – this permits customization of the error message that the user sees. This is put at the beginning of all error messages on exceptions.
 - `errorPostscript` (default: ". Please contact your Cognos Administrator") – this permits customization of the error message that the user sees. This is put at the end of all error messages on exceptions.
 - `defaultNamespaceID` (default: null) – The default namespace id to provide if a namespace id is not included in the credentials
 - `ntlmProcessing` (default: false) – Set to true if the Cognos is using NTLM authentication (recommended setting: true)
 - `loggingLevel` – (default: OFF) – this allows logging of TSOP processing. The following are the currently used logging levels. Note that logging at INFO level includes ERROR and DEBUG includes INFO and ERROR etc.
 - ◇ OFF – no logging
 - ◇ ERROR – errors and exceptions are logged
 - ◇ INFO – logs configuration information and user credential
 - ◇ DEBUG – all processing is logged
- Log files are named `QvtTrustedSSO_ + timestamp + .log` are saved to the Cognos installation log folder. For example: `D:\Program Files\ibm\cognos\c10_64\logs`
- `bcEncryptKey` (default: null) – this is the encryption key used to decrypt the user credentials provided in the cookie. This must match the value provided for `BcEncryptionKey` in the Cognos server configuration section matching the Cognos server that the TSOP is installed. See example below:
 - `bcEncryptMode` (default: disabled) – this determines the contents of the encryption and how it is processed. This must match the value in the `BcEncryption Mode` value in `QvtConfig.xml` (see example, below). Possible values are:
 - ◇ disabled – user credentials are not encrypted
 - ◇ enabled – user credentials are encrypted using the `bcEncryptKey`, but are not timestamped (credentials don't expire)
 - ◇ enabledTimestamp - user credentials are encrypted using the `bcEncryptKey` including a timestamp. The logon credentials will expire after the time specified by `bcEncryptMaxTimeDiff`. This can be used to ensure credentials can't be cached or copied and used at a later time.

- bcEncryptMaxTimeDiff (default: 300) – time in seconds allowed between the time a SSO Dynamic logon request is issued by the QueryVision web parts on the SharePoint Server and the time they are received and processed by the SSO Dynamic TSOP on the Cognos Server.

The following is an example of a Cognos Server configuration in QvtConfig.xml for SSO Dynamic:

```
<LogicalName>w28r2ent208</LogicalName>  
<DisplayName>C10.2.2 Server on w28r2ent208</DisplayName>  
<Authentication>SSODynamic</Authentication>
```

```
<BcEncryptionKey>54d9796d20c891b5bfe0c8d0b59df4a7d643a70d0de36dab</BcEncryptionKey>
```

```
<BcEncryptionMode>enabledTimestamp</BcEncryptionMode>
```