QUORUM QUERY MODULE

BusinessObjects BI 4.2 Supported Platforms and Pre-Installation Instructions

Tomcat + BI Platform Single-Server Environments

BusinessObjects BI 4.2

Updated 22 November 2022

Contents

About This Document

This guide is heavily biased toward on-premises client installations as Quorum has internal processes for setting up Quorum-hosted clients.

Note: There may be some overlap between this guide and the planning document. This is intentional and for the information of those who may only see one of the two documents.

About QQM

QQM is "Quorum Query Module", one of Quorum's ad hoc querying tools that allows non-technical users to query Quorum application data easily. Most typical configurations use a read-only account so the data is protected. The Platform is designed in a way to prevent users from accidentally or intentionally changing application data.

QQM is the collective name for all of the servers, reports, and other objects contained within SAP BusinessObjects BI Platform environments.

The terms "BusinessObjects" and "Quorum Query Module" may be used interchangeably, and may be abbreviated as "BO", "BI", or "QQM". BusinessObjects may also be referred to as the "BI Platform".

QQM/BusinessObjects Support

Quorum has an OEM license agreement and support contracts with SAP that allow us to provide the BusinessObjects BI Platform at a deeply discounted rate. Contractually, Quorum is obligated to follow SAP direction on many aspects of server setup, configuration, and support in order to receive assistance from SAP. Many of these items are colored or otherwise accented in the document.

Unlike most other Quorum applications, BusinessObjects is a third party application. This has a few implications:

- Support for BusinessObjects is readily available on the Internet. While we are happy to assist as necessary, a quick web search can often help with reporting issues. On the same token, customers should not attempt to apply configuration changes to QQM servers or the BI Platform without a review from Quorum.
  Note: While Windows Updates generally do not cause issues, an in-place server upgrade on the QQM server is not permitted and will cause collateral damage leading the BI Platform to stop working.
- There are some aspects of the platform that are out of Quorum's control. There may not always be fixes for bugs in the Platform, and we may have to provide workarounds instead. Quorum can provide documentation from SAP about specific CVEs if the customer has concerns.

- Occasionally, issues will arise that Quorum cannot solve. In these cases, we may have to reach out to SAP Support for assistance. It is important to temper expectations accordingly as working with SAP Support is often a time-delay and time-consuming process.
- If a customer has deferred upgrades on a BI Platform version that has passed end-of-life, Quorum can provide only limited support for the product, as SAP will no longer support versions that have passed end-of-life. An upgrade is required.

BusinessObjects Versions and Licensing

As of this writing, Quorum supports BusinessObjects BI Platform 4.2 through SP9. Customers operating QQM servers with BI Platform 4.x or BO XI 3.x must upgrade to BI 4.2 be eligible for full support, as previous versions have passed end-of-life.

Generally, clients are provided a single BusinessObjects Edge license for BI 4.2 that allows up to 20 concurrent users. If the SoW or other customer contract provides for more concurrent users in the Quorum apps, the Quorum resource coordinating the installation effort should specify the quantity of users when requesting a license key.
Note that the license may be different in Quorum-hosted (QCloud) environments due to minor differences in hosted server configurations.

Important Note: Customers should **never** upgrade a BusinessObjects server licensed through Quorum. Additionally, customers **must not** change the license key on a BusinessObjects server licensed through Quorum or use a Quorum-provided license key on any BusinessObjects server other than those specifically designated for QQM. Performing any of these actions will likely render the systems ineligible for Quorum/QQM or SAP support as they are violations of Quorum's OEM license agreement with SAP. Generally, license keys may be used for a **single** production server and unlimited non-production servers.

Contact BI Engineering if the client requires a distributed or clustered environment. This setup comes with higher licensing costs and is not common at this time.

New Install or In-Place Upgrade

It is possible to do a fairly simple in-place upgrade to BI 4.2 SP9 from a previous version of BI 4.2. For BI 4.1 or earlier, new servers should be configured with a fresh installation.
A fresh installation is always preferred to allow for use the latest server operating systems and features. These decisions should be made during planning.

For in-place upgrades, no pre-setup is required except for:

- HTTPS secure connections to tomcat may require provisioning of a server certificate by the customer's relevant Security or other IT department.

- Updating database middleware on the server (such as SQL Server ODBC and/or Oracle Client drivers) can be beneficial in some cases, especially if the Quorum app databases will be upgraded.
  Refer to the section on database setup below for a listing of supported database and middleware combinations.
- Updates to the QQM service account's configuration may be needed in Active Directory to support AD Single Sign-On in Chromium-based and other modern browsers.

System Requirements

The QQM server must be fully dedicated to BusinessObjects. No other applications or platforms (including Quorum applications, platforms, and services) may be installed on this server.
This is a strict requirement and failure to abide by this requirement renders the server ineligible for SAP support.

Note that a minimum of 100 GB of free storage space is required on the install drive. This may be the system drive or some other drive. The table below outlines the minimum and recommended system requirements for the BusinessObjects server.
The minimum requirements listed below are **not optional**, as they are the minimum requirements set forth by SAP for the system to function; failure to meet the minimum requirements renders the server ineligible for SAP support.

	Minimum Required (10 or fewer concurrent users)	Recommended (10-100 concurrent users)
Processor	1x Quad-core CPU	2x Quad-core CPU
Memory	16 GB	32 GB
Storage	100 GB available disk space	300 GB available disk space

Server Operating Systems

BusinessObjects BI 4.2 is a 64-bit product and must be installed on a server with x64 architecture.
Supported Windows Server Editions:

- Data Center Edition
- Enterprise Edition
- Standard Edition
- Web Edition

Supported Windows Server platforms:

- Windows Server 2012
- Windows Server 2012 R2

- Windows Server 2016 (BI 4.2 SP3+)
- Windows Server 2019 (BI 4.2 SP7+)

The latest Windows updates are recommended, and are required for Windows Server 2012 versions.

If a Windows Server upgrade is required, a new server must be prepared.

Never perform an in-place upgrade of Windows Server on a QQM server as it will cause irreperable collateral damage to the BI Platform.

Cloud Service Support

If a Public Cloud service will be used for hosting of the server, Quorum recommends AWS or Microsoft Azure. Installation may be completed in other Public Cloud services, but first contact Quorum for information about supported services prior to installation.

Client Operating System and Browser Support

If the application will be accessed from a client desktop rather than served via a virtualization platform on Windows Server (e.g., Citrix), the following desktop versions are supported:

- Windows 8.1 (SP5+)
- Windows 10 (SP5+)
- Windows 11 (SP9+)

Windows versions earlier than 8.1 are no longer supported.

BusinessObjects BI 4.2 continues to use the Tomcat web server platform. Chrome is our recommended browser, but the following browsers are officially supported:

- Microsoft Chromium Edge (SP8+)
- Mozilla Firefox (SP5+)
- Google Chrome (SP4+)

Notes:

- Specific browser versions are not preferred and it is expected that the latest versions will work without issue.
- Browsers not listed above are not officially supported.
- Safari is not supported, but any 32-bit Chromium-based browser is expected to work.
- Internet Explorer and NPAPI Java applications are no longer supported, including Internet Explorer mode in Edge.

For those who previously used the Java Applet report builder, the feature parity issue between the Java report panel and the HTML report panel has been eliminated and the Java web application

report builder is deprecated concurrent with Internet Explorer reaching end-of-life. In the upcoming BI 4.3 versions, the Java report builder will be removed.
As a result of the deprecation of the Java apps, it is no longer necessary to install the Java JRE on the server or client machines. The JRE compatibility matrix has been removed from this document.

Java Application Server

Tomcat 8 is the default Java Application Server through SP7. Tomcat 9 is the default Java Application Server for SP8+. IIS is **not** supported.
Tomcat is not an SAP product and limited support is available from SAP. Security or performance tuning to Tomcat by Quorum is incidental and not guaranteed.

Java components required for installation and operation of the BI Platform are included in the installer. **No Java JRE is necessary for 4.2 installations.**

In a standard QQM installation, the Tomcat platform is installed on the BusinessObjects server side-by-side with the BusinessObjects platform.

In this configuration, the HTTP and/or HTTPS ports should be open to client machines. Most typically these will be 80 (HTTP) and 443 (HTTPS) for client connections to the web platform, but these may be changed during setup. Additionally, by default, BI Platform components communicate using ports 6400 to 6410, so these should be open to client machines.

Central Management Server (CMS) Repository and Audit Database Requirements

Database connections must be created to allow the BusinessObjects server to communicate with the database servers. Quorum recommends SQL Server for the CMS repository and Audit databases, but Oracle may be used as well. Azure SQL Server may be used with SP8+ provided that the QQM/BO server can connect to the Azure SQL Server database. The latest version of the specific driver to be used is recommended.
Note that this matrix applies to all database connections from BusinessObjects, not just the CMS and Audit databases.

Database Platform Support for Windows Server

Platform	Version	BI Version	Database Connector
Microsoft SQL Server	2008 R2 SP1	All 4.2	ODBC Driver for SQL Server (WDAC 6)
	2012	All 4.2	SQL Server Native Client 11.0
	2014	All 4.2	Microsoft ODBC Driver 13
	2016	SP4+	
	2017	SP6+	
	2019	SP8+	Microsoft ODBC Driver 17
Oracle	11g R1, 11g R2	All 4.2	Oracle Client 11g R1, 11g R2
	12c	All 4.2	Oracle Client 12c
	12c R2	SP5+	
	18c	SP7+	Oracle Client 18c
	19c	SP7+	Oracle Client 19c
Sybase SQL Anywhere	16	All 4.2	Sybase SQL Anywhere ODBC Driver 16
	17	SP4+	Sybase SQL Anywhere ODBC Driver 17

Notes:

- SQL Anywhere may be installed as part of the BusinessObjects installation. If using this option, no QQM database configuration is required. This is not recommended for SOX compliance requirements as this database is self-contained and is not user-serviceable.
- Starting with SQL Server Native Client 11.0, High-Availability Cluster Listeners are supported.
- Officially-supported SQL Server drivers are listed, but the latest version of SQL Server Native Client 11.0 is known to work, as well.
- "SQL Server" driver is not compatible with SSL or High Availability Listeners.
- Oracle ODBC drivers are not supported and will cause database querying issues.

Note: For SQL Server ODBC connections, Microsoft ODBC Driver 13 is preferred. For Oracle connections, Oracle ODBC is **not** supported and is known to cause server or report issues.

QQM Database Configuration

General

- Two databases or schemas should be created per QQM server on the **production database server**, regardless of the QQM environment. These databases directly affect the functionality of the BusinessObjects platform and are server-specific.
- Regular nightly or weekly backups for both UAT and Production kept for 60-90 days at minimum are strongly recommended. These should be proximately synchronized with BusinessObjects server backups.
- These two databases or schemas should never be refreshed or modified.

- These two databases are specific to an instance of the BI Platform and may only be used by a single BI Platform installation. Except in an environment specifically configured for clustering, attempting to install a second BI Platform using the same databases will cause irreparable damage to both the existing and the new installations.

SQL Server

1. The QQM server must have the appropriate 32-bit and 64-bit ODBC driver installed.
2. Two databases (per QQM server) should be created on the **production** database server, regardless of the QQM environments.
3. It is recommended that database names include the text “QQM_REPO” and “QQM_AUDIT” (respectively) along with notations that make these databases easily identifiable. These names are recommendations only and Company DB naming guidelines may be followed instead. These designations should be recorded in project documentation.
4. Recommended sizing is 1 GB minimum for each database.
5. These databases should be set to Latin1_General_CI_AI collation.
6. The database logins should have full rights to their respective databases. Specifically, they must be granted and maintain db_owner role.
7. The databases should be blank. The installer will set up the table structure.
8. Database login information should be provided to the user setting up the server. If database login information ever changes, the server will stop functioning properly until login information is updated on the server.
9. 64-bit System DSNs should be created in the Windows ODBC Administrator tool. Quorum may perform this step using the login information provided.

Oracle

1. QQM server must have a compatible version of Oracle Client installed including the relevant Oracle Client database connector. Both 32-bit and 64-bit versions are required and should be installed at C:\Oracle.
2. One database with two schemas (per QQM server) should be created on the **production** database server, regardless of the QQM environments.
3. It is recommended that schema names include the text “QQM_REPO” and “QQM_AUDIT” (respectively) along with notations that make these schemas and databases easily identifiable. These names are recommendations only and Company DB naming guidelines may be followed instead. These designations should be recorded in project documentation.
4. Recommended sizing is 1 GB minimum for each schema.
5. If Oracle TNSNames are used, update the tnsnames.ora files on the server (or at the path dictated by the environment variable) with the connection information.

6. Schema logins require full rights to their respective schemas, including CONNECT, SELECT_CATALOG_ROLE, and RESOURCE.
7. The schemas should be blank. The installer will set up the table structure.
8. Schema login information should be provided to the user setting up the server. If this schema login information ever changes, the server will stop functioning properly until login information is updated on the QQM server.

Adobe Flash Support for Dashboards

Dashboards support is considered to be end-of-life as of BI 4.2 SP8, as Internet Explorer and Flash have reached EOL.

Microsoft .NET Framework

Microsoft .NET Framework must be installed on the BusinessObjects server. At least one of the following versions is required:

- .NET Framework 4.6.2 (BI 4.2 SP5+)
- .NET Framework 4.7.1 (BI 4.2 SP6+)

Earlier versions of .NET Framework are known to work, but are no longer officially supported because they have passed end-of-life.

Virtualization Support

Virtualization is officially supported in BusinessObjects BI 4.2. The following platforms are preferred:

- Citrix XenApp 7.5 on Windows Server 2012
- Citrix XenApp 7.6 on Windows Server 2012 (SP3+)
- Citrix XenApp 7.11, 7.12, 7.15 on Windows Server 2016 (SP5+)

Other virtualization platforms may be supported. Contact Quorum for assistance.

Active Directory Requirements

Typical setup includes an Active Directory Service Account. BusinessObjects will log into its server as this account and will use it to communicate with Active Directory to synchronize and authenticate users. Setup also includes at least 3 Active Directory security groups. These groups will facilitate control of user access to QQM.

Active Directory Service Account Setup and Configuration

- Create an Active Directory Service Account. This account's password should not expire. If the password expires, the server will stop functioning. If the password is changed, the server will stop functioning until it is updated in several locations.
- This account should be assigned a service (SPN) for BusinessObjects.
- For each QQM server that will use this Service Account, two additional services (SPNs) must be assigned.
- There are multiple ways to add these services. The command line method is outlined below. Other methods are possible if preferred, such as using the Attribute Editor in the AD Users and Computers snap-in or using a script in PowerShell.
- Unlike the repository and audit databases, AD service accounts may be reused among BI Platform environments.

Register the Services with a Command Line Using the SETSPN Tool

These instructions demonstrate how to add Service Names using the SETSPN utility through a command line. For the purposes of this example, the Service Account name will be QQM_SVC on the domain qdev.net. The QQM servers will be QQMUAT on qdev.net and QQMPRD on qdev.net. For a third server, and additional pair of HTTP commands would be required, but not an additional BOCMS service.
These steps must be performed by a Domain Administrator.

1. Open a command line on any machine on the network.
2. Add the Service Names by issuing the following commands:

   SETSPN -S BOCMS/QQM_SVC.QDEV.NET QQM_SVC
   SETSPN -S HTTP/QQMUAT.QDEV.NET QQM_SVC
   SETSPN -S HTTP/QQMUAT QQM_SVC
   SETSPN -S HTTP/QQMPRD.QDEV.NET QQM_SVC
   SETSPN -S HTTP/QQMPRD QQM_SVC

   The commands are in the following format:
   - SETSPN -S BOCMS/[SERVICE_ACCOUNT].[FULLY_QUALIFIED_DOMAIN] [SERVICE_ACCOUNT]
   - SETSPN -S HTTP/[SERVER_NAME].[FULLY_QUALIFIED_DOMAIN] [SERVICE_ACCOUNT]
   - SETSPN -S HTTP/[SERVER_NAME] [SERVICE_ACCOUNT]

3. As you enter each command, SETSPN will respond with a message to let you know that the SPN was registered. Verify that you have entered them correctly. (Note that there is only one forward-slash and no colon after "HTTP".)
   If you get a message stating that a duplicate SPN was found, verify that it is assigned to the

correct service account. If not, refer to steps 6 and 7 below for deleting an SPN from a service account. Once removed from the incorrect account, repeat the command to add it to the correct account.

4. After all applicable SPNs are registered, verify by issuing the following command at any command prompt on the network:

   SETSPN -L QQM_SVC

5. You will be presented with a list of SPNs for the service account. Note that the above changes may take time to appear if there is latency in AD propagation among domain controllers.
6. If you discover any typos or errors, remove the erroneous Service Names by issuing the same command that you used to register the SPN, switching in a "-D" switch in place of the "-S" switch, for example:

   SETSPN -D HTTP/QQMUAT.QDEV.NET QQM_SVC

7. The Service Name will be removed. You can then enter the correct name by issuing the proper command as in previous steps.

Active Directory Service Account Configuration (Continued)

After the Service Names have been added, there are two more settings that must be adjusted in Active Directory properties for the Service Account.

1. Open the Active Directory tool and locate the Service Account. Open its properties.
2. Go to the Account tab.
3. In the Account options list box, verify that "Use Kerberos DES encryption types for this account" is unchecked.
4. Go to the Delegation tab.
   If the Delegation tab is missing, the service account has no services (SPNs) assigned. Refer to the previous section to add the appropriate services, then return to this section.
5. Select the second option, "Trust this user for delegation to specified services only". This is a heightened security requirement for SSO in the supported browsers.
6. Click the Add button, look up the service account, and add all of the previously created service names (SPNs) to the specified services selection.

Active Directory Service Account Setup on the QQM Server

The Active Directory Service Account must be granted certain rights on the QQM server:

- The Service Account must be a local administrator on the server. Add the Service Account to an AD group that is part of the local Administrators group on the server, or by add the

Service Account individually to the local administrators group on the server. Quorum can complete this step if appropriate access to the server is granted.
    - If a separate AD group is not assigned to the local Administrators group on the server is done using the Computer Management snap-in (Run compmgmt.msc).
    - Expand the trees to System Tools > Local Users and Groups > Groups.
    - Open the Administrators group properties and add the Service Account.
- The Service Account must have the authority to act as part of the operating system in order to log users in with AD Single Sign-On. Add the Service Account to this policy as provided by client's GPO management or by adding the Service Account name to the Act as part of the operating system local policy on the server. Quorum can complete this step if this Policy is not restricted by GPO.
    - This is done using the Local Security Policy snap-in (Run secpol.msc).
    - Expand the trees to Local Policies > User Rights Assignment.
    - Open the Act as part of the operating system policy and add the Service Account.

Active Directory Groups for QQM

Active Directory groups are created in the client's AD environment and mapped to representative levels of access in QQM. In a broad sense, there are three QQM access levels with the following permissions:

VIEWERS	View	Edit	Save	Refresh	Delete	Export Data	Print	Send	Schedule	Create New
Favorites	No access to create reports or save to Personal/Favorites folder									
Public	Yes	No	No	Yes	No	Yes	Yes	Yes	No	No
USERS	View	Edit	Save	Refresh	Delete	Export Data	Print	Send	Schedule	Create New
Favorites	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Public	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes	No
SUPERUSERS	View	Edit	Save	Refresh	Delete	Export Data	Print	Send	Schedule	Create New
Favorites	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Public	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Generally, three groups are created, one for each of the access levels. Suggested naming convention is:

- QQM_SuperUsers
- QQM_Users

- QQM_Viewers

These may be re-used in all environments. However, if different access is required for each environment, create three groups per environment. Suggested naming convention is:

- QQM_UAT_SuperUsers
- QQM_UAT_Users
- QQM_UAT_Viewers
- QQM_PRD_SuperUsers
- QQM_PRD_Users
- QQM_PRD_Viewers

If different access is required per application (for example, if client wants Land and TIPS to be separate), create three groups per application. For example:

- QQM_LAND_SuperUsers
- QQM_LAND_Users
- QQM_LAND_Viewers
- QQM_TIPS_SuperUsers
- QQM_TIPS_Users
- QQM_TIPS_Viewers

After QQM setup, client may move users to these groups as desired.
Please note:

- Each user should be in only one AD group (per server/per application). If a user is in multiple groups, denied rights will supercede granted or unspecified rights and unusual behavior may occur.
- The server will update access against Active Directory on a set schedule (usually hourly) and when a user attempts to log in. AD changes that take time to propagate across domain controllers may take time to be reflected in the BI Platform as well.
- If a user's account is disabled, the user will not be able to log in.
- If a user is removed from QQM AD groups or a user is deleted from Active Directory, the user (and all of the user's personal folder, inbox, and personal category content) may be deleted from the server automatically.
- WARNING: If an AD user's DN/username or OU string changes (e.g., user is updated due to a last name change from marriage, etc.), the user may be deleted and recreated in BusinessObjects with the new username and all of the user's existing content in Personal Folders and Inbox will be lost. If this situation is encountered, copy the user's personal content to be preserved to a public folder first, then copy it back to the new user folder once the username is updated. Contact Quorum for assistance if needed.

HTTPS – Secure Connections with TLS

Quorum may now configure the web front-end to use TLS v1.2 with a standard list of cyphers (see below). This usually isn't needed but may be completed if customer's IT policy requires. Here are some notes about the process:

- As directed by Quorum's Security Engineer, TLS 1.0 and 1.1, as well as SSL 2.0 and 3.0 should be disabled on the BusinessObjects servers, but Quorum *will not* do this for client-hosted installations.
- For on-premises client installations, client *must* provide the signed certificate chain (including private key) as a *.pfx keystore in PKCS12 format along with the password, or install relevant certificates and in the Windows Root Certificate store on the server.
- Previously, BusinessObjects was configured to use port 8080 for HTTP requests. New BI 4.2 installations are configured to use the standard HTTP and HTTPS ports of 80 and 443, meaning the port will no longer need to be explicitly specified in the URL. This port is customizable, but firewall rules should be updated accordingly. If other ports are used, they must be specified in the URL as before (e.g., https://qqmdev.qdev.net:8443/). *Note that Quorum cannot provide support for specific network and firewall services and appliances.*
- The HTTP port will be configured to redirect to the HTTPS port and only secure connections will be enabled.

As of this writing, this is the Quorum security standard cyphers list as directed by the Security Engineer:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256

Pre-Installation Summary and Checklist

There are several steps that must be completed before the installation begins.

1. Depending on how the installation will be done, provision resources and access for the user or consultant performing the installation. Refer to the planning guide for suggestions.
2. Set up a supported server or VM. Reference the server supported platforms and the hardware requirements section above.
3. Set up the QQM databases as outlined above in the database information section. Provide the database login information to the consultant or user performing the installation.
4. Update the tnsnames.ora file (Oracle) or create 64-bit System DSNs in ODBC (SQL Server). Quorum may perform this step if login and connection information are provided.
5. Turn off Internet Explorer Enhanced Security Configuration on the server (IE ESC). This may be done in the Server Manager. Initial configuration in the Central Management Console is best performed in Internet Explorer and IE ESC will interfere with the CMC.
6. Disable any antivirus programs on the server for the duration of installation. This is required.
7. Set up the Active Directory Service Account for QQM, using the AD Service Account setup section as a reference. Provide the installing consultant or user with the account and login information.
8. Set up the Active Directory groups as provided in the AD group setup section and add the installing consultant or user's AD account to the SuperUsers group for testing purposes.
9. Transfer the QQM installation and configuration files to the server. Quorum may facilitate this using sFTP or client's preferred file transfer method.
   NOTE: The installation and configuration packages total 6-12 GB in size. Transfer will take a lot of space and may take a lot of time, depending on connection. HTTP transfers are not recommended.
10. Transfer the relevant certificate files or install the certificate in the store on the server.
11. If email is to be used, provide SMTP server information as well as a login if applicable, and configure antivirus and/or the mail server to allow outgoing emails from the QQM server from the application running as the AD service account.