SOFTWARE. ESSENTIALLY DIFFERENT.

Installation and Upgrade Guide

Front Office 9.4

Biomni Limited, Aldwych House, 71-91 Aldwych WC2B 4HN T: +44 (0) 20 7557 4200 E: info@biomni.com

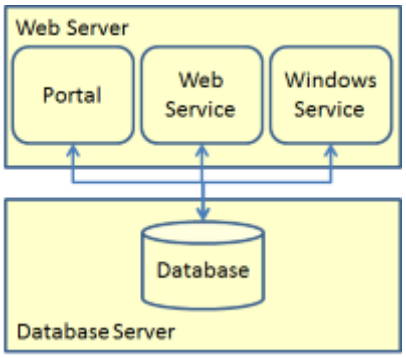
Contents

1.0 Introduction

There are four components in a Front Office installation:

1. Portal
2. Web Service
3. Windows Service
4. Database

There are several different ways the components can be distributed, but the primary focus of this guide is the two-server installation method. A Web Server hosts the portal, web service, and windows service, and a database server hosts the database; as below.



Other configurations are supported, in particular:

1. Side-by-Side installation – Multiple independent Front Office systems installed on the same hardware. This configuration is covered in detail in section 8.3.
2. Load balanced installation – A load balanced installation has a single database server and database, but multiple instances of the portal, public web service, and windows service, which provides load balancing and redundancy. This configuration is covered in detail in section 8.4.

Please visit the Biomni Community or email support@biomni.com if you have any questions about the installation process, including details of specific alternative implementation models.

2.0 Prerequisites

It is assumed that the person installing Front Office has a working knowledge of SQL Server, Windows Services, and IIS.

Front Office can be installed on a Windows Server 2012 R2, Windows Server 2016, or Windows Server 2019 platform. Detailed software requirements are given in section **Error! Reference source not found.**.

The prerequisites for each component are below.

2.1 Database

- Microsoft SQL Server 2014, Microsoft SQL Server 2016, Microsoft SQL Server 2017, Microsoft SQL Server 2019, Azure SQL database, or Microsoft SQL Server on Amazon RDS: all manual installation
- At least 5 GB free disk space for data and 2 GB for logs

2.2 Portal and Web Service

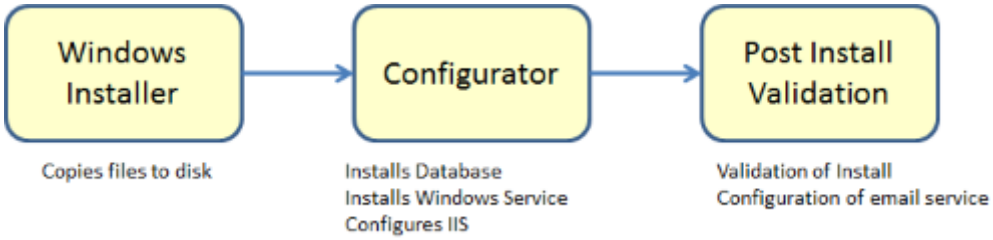
- Microsoft .NET Framework version 4.7.2: manual installation
- IIS – installed by configurator
- At least 1 GB free disk space

2.3 Windows Service

- Microsoft .NET Framework version 4.7.2: manual installation
- Access to an SMTP server
- At least 1 GB free disk space

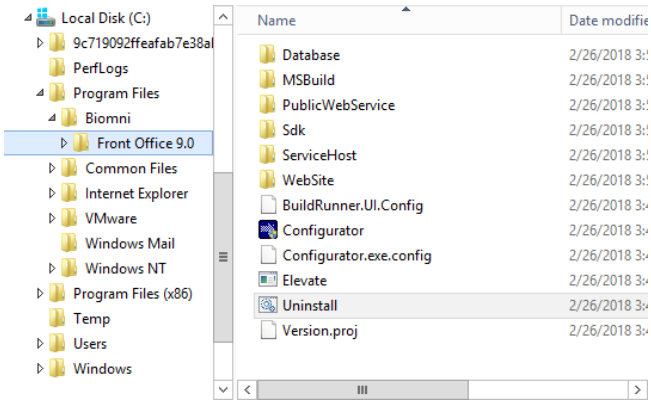
3.0 New Installation

Installing and Configuring Front Office is a three-step process:



This section focuses on the first two steps of this process. Post installation configuration of Front Office is covered in section 5.0.

The Front Office installation is packaged as a single executable, `Front Office 9.4.exe`. Double clicking on the exe launches windows installer, which copies all the relevant files onto disk. The default install location is `C:\Program Files\Biomni\Front Office 9.4`, though this can be changed. The installation produces the following folder structure; as below.



After the windows installer has run, the Configurator is launched automatically. If the configurator needs to be started manually, double click on `Configurator.exe` in the root of the installation location. The configurator is a wizard which asks for several parameters required to configure the system, such as Database name, Portal name, etc. Once these parameters have been entered the configurator configures IIS, installs the database and windows service.

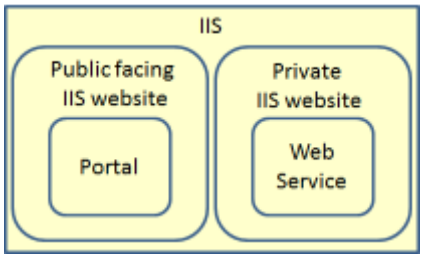
3.1 Security and IIS Configuration

It is worth thinking a bit about how IIS will be configured. Two components are installed within IIS:

1. Portal
2. Web Services

The security considerations for these two components are different. The portal needs to be visible to all users of the system, which could mean exposing the portal over the public internet. The web services provide an integration point and need only be visible to internal systems.

Therefore, the recommended configuration is to create two IIS websites for the two components. The first IIS website hosts the portal, and the second IIS website hosts the web services.



The security of the IIS websites can then be configured appropriately, restricting the visibility of the web services and not exposing them over the public internet.

3.2 HTTPS

A further level of security can be provided by configuring the websites to use HTTPS. If you want to use HTTPS, it is best to configure it before installing Front Office.

To setup an IIS Website with HTTPS:

- Import SSL Certificate into IIS
  - In a production system you need to buy an SSL certificate from a certificate provider such as Verisign. You then import the certificate into IIS, the following link describes how to do this https://technet.microsoft.com/en-us/library/cc731014(v=ws.10).aspx.
  - In a test system you can create a self-signed certificate in IIS, the following link describes how to do this https://technet.microsoft.com/en-us/library/cc753127(v=ws.10).aspx.
- Configure Website to use HTTPS
  - In IIS navigate to the Website where Front Office will be installed.
  - Right Click > *Edit Bindings*…
  - Click *Add*.
  - Select Type *HTTPS*, and choose the SSL certificate, click OK.
  - On the bindings page, choose *HTTP* and click *Remove*; accept the confirmation.

3.3 Installation Process

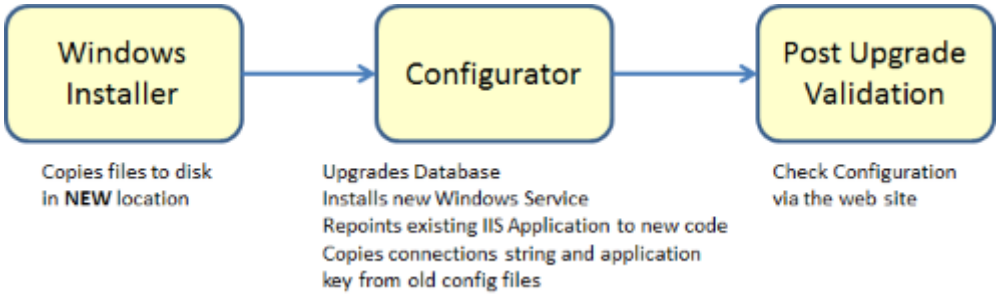
The installation process is as follows:

1. **Install** the new version of Front Office using `Front Office 9.4.exe`. Installation should be run on the web server or application server. Installation must **NOT** be run on the database server.

2. **Configurator**: click on *Install a New Front Office System*.
3. **Select Components**: leave all checkboxes checked; click *Next*.
4. **Install Web Server Features**: if you are installing the portal or web service, this page installs and configures IIS to work correctly with Front Office.
5. **New Installation Configuration Options**:
    a. Enter your Company Name.
    b. Enter the Portal Name, which will be used for the virtual directories and windows service name.
    c. Select whether to install the portal in an IIS application or directly under the root of the IIS website. This affects the URL of the website once it is installed.
    d. Select the IIS websites for the portal and web service. For security reasons, it is recommended to install the web service under a different IIS website, which is not exposed over the internet.
    e. Select a Base Currency and Language. The base currency cannot be changed after installation, so this must be carefully considered.
    f. Sample Data may also be installed, which will populate the database with preset data to showcase some of the capabilities of Front Office.
6. **Database Installer Connection**: select the credentials that the installer will use to create and build the database. The user may have either Windows or SQL Server authentication, but must have the 'sysadmin' database role. The configurator will create the database during the installation.
7. **Application Connection**: enter an application username and password. These credentials will be used to create a database login and database user, and in the connection strings for the portal, web service, and windows service. The domain policy password complexity rules are applied to the password you enter here.
8. **Application Security**: The application key is used to encrypt third party passwords in the system. If you are installing a new system, click the *Generate Key* button to create a new key. If you are installing a new component for an existing system, paste the key from the original installation into the box; for example, you are installing a second portal in a load balance system, or a second windows service for redundancy. For more information about the application key see section 5.3.
9. **Validate Installation Parameters**: performs validation to make sure that the installation parameters are correct.
10. **Confirm Options**: this screen provides a summary of what the configurator is going to create. If you are satisfied, click *Install* to begin the installation.
11. **Login**: Once the installation is complete, click the link to login, or use the link in `All Programs/Biomni/Front Office 9.4/`. Login using:
    a. **User ID:** Admin
    b. **Password:** password
    You will be forced to change the password after first login.
12. **Configuration Check**: In the portal, navigate to *Admin* > *Support* > *Configuration Check*. See section 5.0 for detailed information about checking the configuration.

4.0 Upgrade

Upgrading Front Office is a three-step process:



This section focuses on the first two steps of the process. Post upgrade validation of Front Office is covered in Section 5.0.

An upgrade of Front Office uses the same executable as a new installation, `Front Office 9.4.exe`. Double clicking on the `exe` file launches the Windows installer, which copies all the relevant files to disk. By default, the installation location is `C:\Program Files\Biomni\Front Office 9.4`, though this can be changed. **An upgrade of Front Office puts a new set of files on the hard disk in a new location, it does not replace the existing installation.**

After the windows installer has run, the Configurator is launched automatically. If the configurator needs to be started manually, double click `Configurator.exe` in the root of the installation location. The configurator is a wizard which asks for several parameters required to upgrade the system, such as Database name, Portal name, etc. **Once these parameters have been entered, the configurator configures IIS, upgrade the database and windows service if required**.

In detail, the upgrade process is as follows:

1. **Backup** the existing database.
2. **Recovery Mode**: Set the database recovery model to Simple.
3. **Growth Settings**: For large databases (10GB plus) the upgrade may take several hours to complete. It is recommended to set file growth for both `mdf` and `ldf` files to 500MB for a balance between speed of upgrade and disk space usage.
4. **Email** (optional) : If the system should not start sending emails immediately after upgrade, deactivate emails via *Admin* > *Email Templates*.
5. **Install** the new version of Front Office using `Front Office 9.4.exe`.
6. **Configurator**: At the Configure stage, click *Upgrade a Front Office System*.
7. **Select Components**: Select the components which are installed on the server. Click *Next*.
8. **Upgrade Portal and Web Service**: Select the IIS Applications of the Portal and Web Service to upgrade. Click *Next.*
9. **Upgrade Windows Service**: Select the existing windows service to be upgraded. Click *Next.* On upgrade a new windows service will be created and the old one deleted. The connection string will be copied from the existing windows service.

10. **Upgrade Database**: Choose the database server and database to be upgraded. Select the authentication method for the upgrade (the user that the installer will use for the upgrade). The user should have the 'sysadmin' database role. It is possible to perform an upgrade with a reduced permission set, see section 8.6. Click *Next.*
11. **Application Security**: If the upgrade passes through version 8.1 then the application security page is displayed. If this is the first component upgraded, click the *Generate key* button to make a new key. If a component of this system has already been upgraded, then paste the key from the original upgrade into the input. (For example, when upgrading a second portal in a load balanced system, or a second windows service for redundancy). For more information about the application key see section 5.3.
12. **Validate Installation Parameters**: runs validation checks on the installation.
13. **Confirm Options**: This screen summarizes the parameters that have been entered. Check the details carefully. If edits are required, click the ← (back) button in the top left corner to go back though the configurator wizard. If no changes are required, click *Install* to begin the upgrade.
14. **Login**: Once the installation is complete, click the link to login, or use the link in `All Programs/Biomni/Front Office 9.4/`. Login as Admin.
15. **Configuration Check**: In the portal, navigate to *Admin* > *Support* > *Configuration Check*. See section 5.0 for detailed information about checking the configuration.
16. **Shrink** the database.
17. **Recovery Model**: Revert recovery model and file growth settings to their previous values.
18. **Email** (optional): if you disabled emails in step 4, re-enable them.
19. **Custom stored procedures**: If there are custom stored procedures in the main Front Office database, they will need to be re-created after the database upgrade. Note that it is best practice to put custom stored procedures in a separate schema or database to avoid this issue.
20. **Uninstallation**: Once you are confident that the system has upgraded correctly you may uninstall the old version via *Control Panel* > *Add or Remove Programs*. This will remove the old files on the hard disk.

5.0 Post Installation and Upgrade Validation

5.1 Configuration Check

After installation or upgrade, check that the system is configured correctly with the Configuration Check screen (*Admin* > *Configuration Check*).

5.1.1 Server Tab

- **Windows Service:** Shows the status of windows services which are pointing at the Front Office database. Each windows service writes heartbeat information into the database every 5 minutes. If the database has not received a heartbeat within 7 minutes the service will be highlighted in red.
- It is possible to configure the system with multiple windows services pointing at a single database, a configuration useful for redundancy. Each windows service writes three records into the windows service table, so if for example there are two windows services, six records will be displayed.
  After upgrade the table may contain records for services that no longer exist. To remove these records, click the *Clear All* button. This clears the entire table, but active services will insert new records when they next update their heartbeat.
  Section 5.2 describes checking the configuration of the windows service on the server where it runs.
- **Database**: Shows the database version and most recent database change. These fields are useful in support scenarios.
- **Web Server:** The critical field is the Web Root Address. This should be the URL of the home page of Front Office, as seen by a user of the system. This setting is used when constructing emails with hyperlinks into Front Office.
- **Public Web Service:** If the Public Web Service URL is incorrect the web page will display an error message.
- **Table:** The table at the bottom of the page shows the version numbers, connection strings, and application encryption status of all the components in the system. All the version numbers and connection strings must match, if they do not an error message is displayed. If the application key is incorrect, the application encryption status will indicate this, and an error will be displayed.

5.1.2 Base Settings Tab

- **Check that the base settings** for Front Office are appropriate:
  - System Language
  - System Time Zone – choose a time zone which will be an acceptable default for most users.
  - Country Code.

  Base system currency is also shown, however this is set at installation time and must not be changed after a request has been raised, as this will cause major data issues.
- **Image Upload**: Click the image button to open the Image Manager. When correctly configured, the Image Manager should list a folder named `UploadedImages`. Select the `UploadedImages`

folder and click the *Upload* button. Browse to an image file and upload, if successfully uploaded the image should appear on the right-hand side of the Image Manager dialog.

5.1.3 Email Tab

- **Configure SMTP settings** for outbound email by clicking *Edit SMTP Settings*. On upgrade these settings should be migrated forward, though it is still worth checking that they are correct.
- **Review core email addresses** for the system.
- **Send test email**: Click on the *Send Test Email* button to send a test email from the Front Office system. For the email to be sent successfully a windows service must be running, the email task must be enabled, and the SMTP settings must be correct.
- **Check the Email Queue**: Queued emails can be viewed via the Email Queue button. The email queue will show any error encountered whilst sending the email. When the email is sent successfully it is removed from the queue.

5.2 Windows Service

After an installation or upgrade, it is advisable to check that the windows service is running correctly on the server where it is installed:

1. Open *Event Viewer* and navigate to the *Application Log*.
2. Find messages with a Source of 'DirectaService9.4$FrontOffice'. The name may vary slightly - the naming convention is 'DirectaService9.4$<SiteName>', where <SiteName> is the name of the portal.
3. If the windows service has logged any errors, then it is possible there is a configuration problem. Examine the detail of the error.

There are two common types of configuration problems which can occur with the windows service:

1. Windows service cannot connect to the database. The windows service checks connectivity to the database defined in the config file. If the service cannot connect, it will log an error in the windows event log.
2. Windows service and database at different versions. The windows service is tied to a specific version of the Front Office database. So, for example, a Front Office 9.1 service will work with a Front Office 9.1 database, and a 9.0 service will work with a 9.0 database. If the service detects that it is pointing at a database which is a different version of Front Office, it will log an error in the windows event log and shut down.

5.3 Application Key

An application key is created during the configuration of the portal. The application key is used to encrypt third party passwords which are stored in the database; for example, the passwords for adapters and integration settings. The application key is not used for encryption of user login passwords. The application key is stored in an encrypted section of the config file for the portal, public web service, and windows service.

The application key is critical to the correct operation of the system. If the application key is lost it will not be possible to recover the third-party passwords. Logging on will be unaffected but passwords for adapters and integration settings will need to be re-entered.

In practice there are two ways the application key could be lost.

1. The web server fails.
2. The website is uninstalled.

To mitigate the first issue, a backup of the web server should be kept. For the second scenario, if, for example, the web server needs to be moved to a different physical machine, the application key should be copied from the config file on the old server and the new website installed using the application key. Test that the new server is working correctly and verify that there is a valid backup of the server. Once complete, uninstall the website from the old server.

The application key, as well as the database connection strings, are stored in an encrypted section of the config files for the components. There are two helpers to decrypt and encrypt the config files:

- `<Install Location>\MsBuild\ConfigEncrypt.bat`
- `<Install Location>\MsBuild\ConfigDecrypt.bat`

The files which are encrypted / decrypted are:

- `<Install Location>\WebSite\web.config`
- `<Install Location>\PublicWebService\web.config`
- `<Install Location>\ServiceHost\DirectaSvcHost.exe.config`

6.0 Applying a Service Pack

The Front Office Service Pack updates a single Front Office instance to the latest service pack release. Details of the service pack changes can be found in the `Front Office 9.4 Service Pack Contents.pdf` file.

There are two different methods to apply a Service Pack, depending upon whether the original installation was via the Windows installer (`exe`) method, or the `zip` file (manual) method.

6.1 Applying a Service Pack to an exe Installation

1. Log into the web server as Administrator.
2. Copy the Service Pack onto the web server.
3. Run `Front Office 9.4.xxxx Service Pack.msp`.
4. For each load balanced web server repeat steps 1 to 3.
5. Login to Front Office as a supervisor and check that the site loads correctly; this step updates the database with any changes. Once the update is complete the site is presented ready for use. If any problems updating the database are found, an error will be displayed on the home page, with a reference to the Error Log (available via the *Admin* > *Support* menu).

6.2 Applying a Service Pack to a zip (Manual) Installation

1. If the Front Office Service has been installed, the service should be stopped (*Biomni Front Office Service 9.4* in services).
2. Copy the contents of the `Front Office 9.4.xxxx Service Pack for Manual Install` folder over the Front Office 9.4 site, but first unblock the zip file before uncompressing by right clicking on *Properties* > *Unblock*.
3. Restart the *Biomni Front Office Service 9.4 service*.
4. Login to Front Office as a supervisor and check that the site loads correctly; this step updates the database with any changes. Once the update is complete the site is presented ready for use. If any problems updating the database are found, an error will be displayed on the home page, with a reference to the Error Log (available via the *Admin* > *Support* menu).

6.3 Applying a Service Pack when Windows Service is Running on a Separate Server

If running a separate application server for the Biomni Front Office Service, the service pack must also be applied to this installation.

7.0 Uninstallation

To uninstall a Front Office system:

1. Navigate to *Control Panel* > *Programs and Features*
2. Locate the Front Office System to be uninstalled
3. Click *Remove*

The uninstallation process will remove the windows service, the portal, and the public web service, which are pointing at the installation location. It will then delete the software from the hard disk and the start menu shortcut. The uninstallation will NOT delete the database, this must be done manually.

If you have installed Front Office with the zip file (manual installation):

1. In Windows Explorer, navigate to the root installation folder.
2. Double click on the `uninstall.bat` file and follow the instructions. This will uninstall the web components and windows service. It will **not** delete the database.
3. In Windows explorer, delete the root installation folder.

8.0 Appendices

8.1 Appendix A – Software Requirements

It is recommended that the latest service pack should always be used for all software.

8.1.1 Server Operating System

The following operating systems are supported:

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

8.1.2 SQL Server

The following versions of SQL Server are supported:

- SQL Server 2014
- SQL Server 2016
- SQL Server 2017
- SQL Server 2019
- Azure SQL database
- Microsoft SQL Server on Amazon RDS

8.1.3 Client Browsers

The following client browsers are supported:

- Internet Explorer 11
- Edge
- Firefox
- Chrome
- Safari

8.2 Appendix B – Customizing Image Upload

Image upload is configured automatically. By default, uploaded images are stored at: `C:\inetpub\Biomni\Images`. This section describes how to change this storage location:

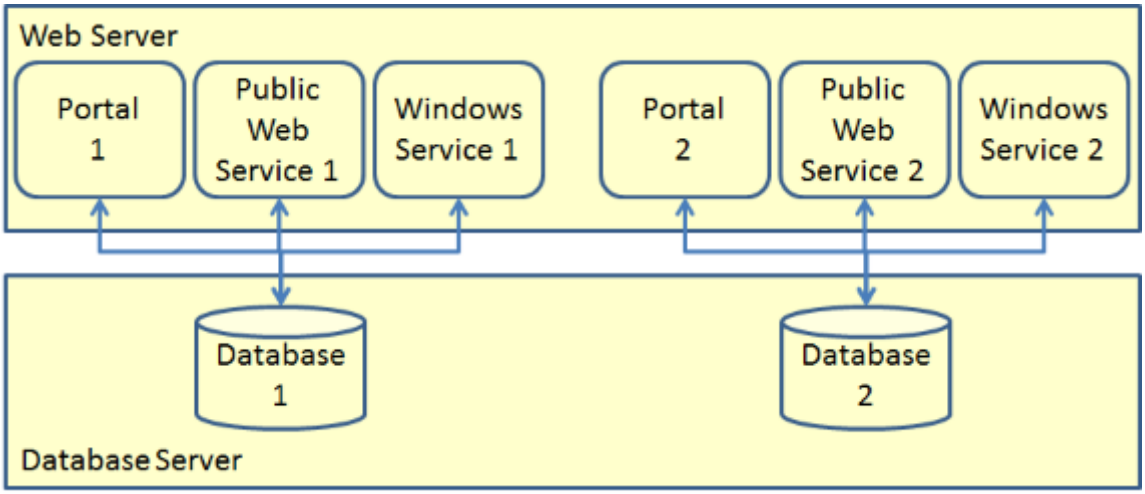
- Launch Internet Information Services (IIS) Manager.
- Navigate to the *Front Office* Application.
- Expand the view and locate the *UploadedImages* virtual directory.
- Right click *Manage Virtual Directory* > *Advanced Settings*.
- In the 'physical path' text box, enter a path to where the virtual directory will exist on disk. This path is where any uploaded images will be stored. The path can either be a path on the local server; for example, `c:\uploadedimages`; or a UNC share; for example, `\\myshare\uploadedimages`.
- By default, the connection to the physical directory is set to be 'pass-through authentication'. If a UNC Share was chosen click *Physical Path Credentials*, followed by *Specific User*, and enter the required credentials.
- In either scenario, the connecting credentials will require read and write access to the physical location.

Once the `UploadedImage` virtual directory has been created, it can be verified in the portal in the Configuration Check pages.

- Login to the portal as Admin
- *Admin* > *Configuration Check* > *Base Settings*.
- Click the image button.
- When configured correctly the Image Manager should list a folder named `UploadedImages`
- Select the `UploadedImages` folder and click the *Upload* button.
- Browse to an image file and upload, if successfully uploaded the image should appear on the right-hand side of the image manager dialog.

8.3 Appendix C – Side-by-Side Installation

A side-by-side installation has multiple independent Front Office systems installed on the same hardware.



Due to technical limitations of the Windows installer technology, only a single instance of Front Office can be installed with the windows installer (`exe`) method. However, Front Office can also be installed from a `zip` file, which is available from the Download website.

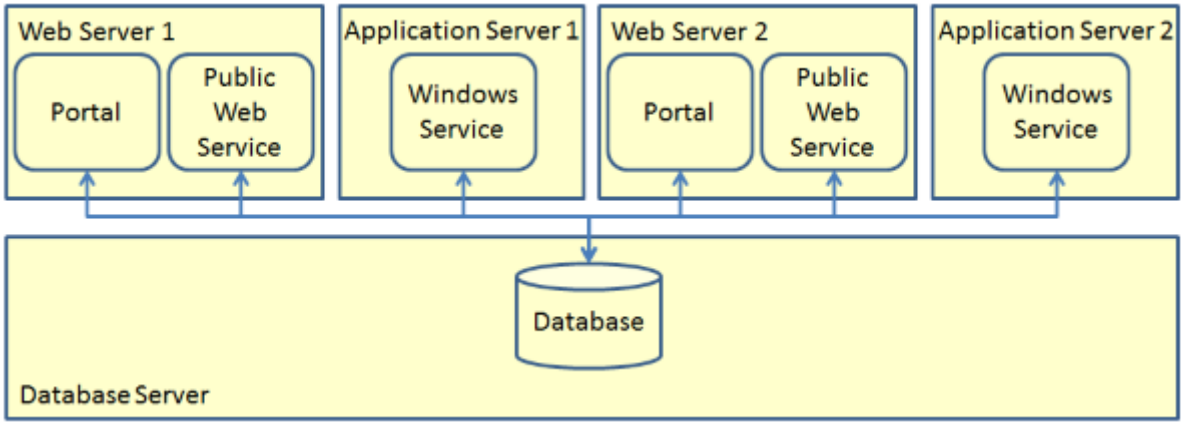
1. Create a folder on the web server where Front Office is being installed.
2. Copy the Front Office install `zip` file into this location. Unblock the file before uncompressing it, right click the file and select *Properties*, then *Unblock*.
3. Extract the file to this location.
4. Double click on `Configurator.exe` to run the configurator.
5. Follow the on-screen instructions.

To uninstall a Front Office installed from a zip file:

1. In Windows Explorer, navigate to the root installation folder.
2. Double click on `uninstall.bat` and follow the instructions. This will uninstall the web components and windows service. It will **not** delete the database.
3. In Windows explorer, delete the root installation folder.

8.4 Appendix D – Load Balanced Installation

A load balanced installation has a single database server and database, but multiple instances of the portal, web service, and windows service, which provide load balancing and redundancy.



It is possible to run the installation on any web server or application server. The installation process copies all the required files onto the server. The components to install or upgrade can be selected at the Configurator stage; for example, if configuring an application server which will host the windows service, simply choose to configure only the windows service.

When creating a load balanced installation, all the components must be installed with the same application key. On the first installation of the system, generate a new application key. On subsequent installations, copy the application key rather than generate a new key. The application key is explained in more detail in section 5.3.

When configuring a load balanced installation, the machine key must be manually configured for both the portal and public web service on both web servers. The machine key should be the same for both IIS applications on both web servers. To manually configure the machine key:

- In IIS, navigate to the FrontOffice application then *Machine Keys*
- Untick *automatically generate machine key*
- Untick *automatically generate validation key*
- Click *Generate Keys*
- Click *Apply*
    - The `web.config` file is updated with a machine key section containing the generated values.
- Repeat the process for the WebService application, but rather than generating keys use the previous values.
- Repeat the process on the second webserver, but rather than generating keys use the same values as used on the first web server.

When upgrading, the machine keys are copied forward to the new IIS applications, so this process should only be necessary on first install.

8.5 Appendix E – Install and Configure Reporting

The Reporting feature is a licensed option. Please either email info@biomni.com or contact the support team at https://community.biomni.com/ to find out more information.

The files needed to setup reporting are in `Front Office 9.4 Reports.zip`.

8.5.1 Architecture

Reports are hosted by an instance of SQL Server Reporting Services (SSRS) in SQL Server, which does not need to be the same server that hosts the Front Office database. The reports are setup in a folder in SSRS to isolate connection strings and customizations for different installations of Front Office.

The Front Office portal uses a web service to connect to SSRS to get the report definitions. Access to the reports can be configured for different user groups. Finally, when the reports are viewed, Front Office connects to SSRS using a web service to run and display the reports.

8.5.1 Prerequisites

- SQL Server Reporting Services (SSRS) 2014 or 2016, 2017, or 2019 (preferred) is required to run Front Office reports; the Front Office database itself does not need to run on the same version or the same server.
- Reporting is not supported in Azure SQL or AWS RDS environments.

8.5.2 Installing Reports in SQL Server Reporting Services

A license that allows Reporting is required for this feature.

Note: There have been user interface changes between versions of SSRS. These instructions focus on the SQL Server Reporting Services 2017 UI but the same can be achieved in other supported versions.

1. Copy `Biomni.Directa.Reporting.SupportCode.V1.dll` to the `[SQL Server installation directory]\Reporting Services\ReportServer\bin` directory.

   By default this will be:

Version	Path
2019	`%ProgramFiles%\Microsoft SQL Server Reporting Services\SSRS\ReportServer\bin`
2017	`%ProgramFiles%\Microsoft SQL Server Reporting Services\SSRS\ReportServer\bin`
2016	`%ProgramFiles%\Microsoft SQL Server\MSRS13.MSSQLSERVER\Reporting Services\ReportServer\bin`

Version	Path
2014	`%ProgramFiles%\Microsoft SQL Server\MSRS12.MSSQLSERVER\Reporting Services\ReportServer\bin`

2. Ensure Reporting Services is configured using Reporting Services Configuration Manager, in particular the Web Service URL, Database (click Change Database to create the database), and Web Portal. The Web Service URL virtual directory should be titled 'ReportServer' and the Web Portal URL should be 'Reports'. Click *Apply* on these screens to create the corresponding site.
3. Set the Reporting Services Session Timeout.
   Open SQL Server Management Studio as an Administrator, connect to 'Reporting Services'. Right click the server > *Properties*, select the *Advanced* page, set *SessionTimeout* to at least the Front Office session timeout.
   Note: Front Office session timeout is in minutes, reporting services is in seconds.
4. On the report server machine run a browser as Administrator and navigate to: `http://localhost/Reports`.
5. Create a folder; for example, `FrontOffice`. This is where the reports will be installed. The purpose of the sub folder is to isolate connection strings and report customizations for different installations of Front Office.
6. The Front Office reports adapter requires a domain account to connect to the report server.

   The account can be any domain account and requires no special rights, although it is important that the password will not change or expire. This account will be used as the Security credentials that the Front Office Adapter uses to run the reports (this will be setup in a later step).

   Drill into the folder created above, click *Manage Folder* and select the *Security* tab. You should see that *BUILTIN\Administrators* has the *Content Manager* role. Click *Customize Security* then *Add group or user*. Enter the domain user account Front Office will use to access the reports into *Group or user* and assign the *Content Manager*.
7. The report server needs to connect to the Front Office database to retrieve data to build the reports. The report server can use the same SQL Server credentials to connect to the database as the portal, which are set when Front Office is installed.

   In the `FrontOffice` folder create a new data source called 'FrontOffice'.
   - Set the connection string to the Front Office database; for example, `"Server=(local);Database=FrontOffice;"`
   - Set the username and password under *Using the following credentials* to the same credentials the Front Office portal uses to connect to SQL Server.
   - Click *Test connection* then, if successful, click *Apply*.
8. In the `FrontOffice` folder upload the reports (`.rdl` files) from `Front Office 9.4 Reports.zip`.
9. Click on … (three dots) for each report, select *Manage*, choose the *Data sources* tab, and browse to the FrontOffice Data Source you created above (this may already be selected).
10. Test the reports executed on the report server by clicking on each report.

8.5.3 Configuring Reports in Front Office

1. In Front Office go to *Admin* > *Support* > *Configuration Check* and click on the *Reporting* tab.
2. Set the 'Reporting Services Folder' to the name of the folder created above by clicking *Edit*.
3. Create a 'Reporting Services' Adapter by clicking the Adapter link or icon.
    - Click *New*.
    - Set the Web Service URI to the 'Report Server Web Service URL' in 'Reporting Services Configuration Manager' for the server the reports were uploaded to; for example, `http://localhost/ReportServer`.
    - Set the 'Authentication Mode' to Windows Authentication.
    - Set User Name and Password to the domain account that was given the 'Content Manager' role on the reporting services folder created above.
    - Click *OK*.
4. Ensure the following:
    - There are no errors displayed. If errors are found, view them in *Admin* > *Support* > *Error Log* and see the 'Security' and 'Resources' sections below for further details; or search for the error message on the Internet.
    - The reports expected are listed in *Reports & Data sources*.
    - The data source for each report is correct.
5. In Front Office navigate to *Admin* > *Organization* > Report and click *Refresh Reports*. The reports from the folder created above should now be listed.
   NB: This step will need to be repeated when new reports are added, or modifications made.
6. Click on each individual report in the list to configure user group access as required.
7. Test each report by clicking on the *Reports* menu item in the top bar, selecting a report and viewing it. It is recommended that a Microsoft browser be used to ensure all functionality is available.

8.5.4 Security

If the reports do not work some security settings for the network configuration may need to be adjusted. Consider the following:

- If the error "*The HTTP request is unauthorized with client authentication scheme 'Negotiate'. The authentication header received from the server was 'NTLM'.*" is found it may be necessary to modify the `rsreportserver.config` file to allow the appropriate authentication method.
    - The `rsreportserver.config` file can be found in `[SQL Server installation directory]\Reporting Services\ReportServer\`
        - For example, `%ProgramFiles%\ Microsoft SQL Server Reporting Services\SSRS\ReportServer\rsreportserver.config` for SQL Server 2017.
    - Add <RSWindowsNegotiate/> to <AuthenticationTypes>.

      Note: In some cases it may also be necessary to add the RSWindowsKerberos element. More information is available: https://docs.microsoft.com/en-us/sql/reporting-services/security/configure-windows-authentication-on-the-report-server
- Try changing the Service Account to 'Network Service' or 'Virtual Service Account' in Reporting Services Configuration Manager.

8.5.5 Adapter Configuration

The report server name in the Web Service URI should use the 'Full computer name' or IP address. The 'Full computer name' can be found in the machine properties.

The username may need to use the UPN format rather than the old Windows 2000 format; for example, user.name@full.domain.name.com, rather than domain\user.name. This may not be essential or available in all network configurations but is the most reliable, if available.

8.5.6 Report Styling

Reports are unaffected by Front Office styles; the style is set in the report. Therefore, consideration should be given to applying any Front Office style customization to the reports.

8.5.7 Report Localization and Personalization

To assist with localization and personalization, Front Office automatically populates extra parameters with data for the user / system running the report, if the parameters exist on the report. To receive the benefit of these parameters, they should be added as hidden parameters with the names below. If they are not present on the report, Front Office will not attempt to populate them.

- Directa_UserId
- Directa_UserEmailAddress
- Directa_UserTimeZoneKey
- Directa_UserTimeZoneDisplayName
- Directa_SystemTimeZoneKey
- Directa_SystemTimeZoneDisplayName
- Directa_UserCurrencyCode
- Directa_UserCurrencyBeforeSymbol
- Directa_UserCurrencyAfterSymbol
- Directa_SystemCurrencyCode
- Directa_SystemCurrencyBeforeSymbol
- Directa_SystemCurrencyAfterSymbol

In addition to these custom parameters, the built in User!Language property is populated with the Front Office user's culture code. The report Language property can be set to this property to allow consistent localization if required.

`Biomni.Directa.Reporting.SupportCode.V1.dll` may be referenced to provide consistent formatting and conversion. Specifically, there are some methods to help with conversion of dates to and from time zones.

8.6 Appendix F – Installing Database with Reduced Permission Set

When upgrading the database, it is necessary to choose a database login to perform the database upgrade. The simplest choice is to use a user who has the 'sysadmin' role.

However, if your DBA is unwilling to grant the sysadmin role to you, you can do a database upgrade with a reduced permission set. This appendix describes the process.

The SQL script below creates a Login 'UpgradeUser' which is suitable for upgrading the database:

1. Run the script in SQL Management Studio to create a login and user suitable for upgrading the database.
2. When you run the configurator and are selecting the database to upgrade, choose Authentication Mode 'SQL' and enter the following values:
    a. DB User: UpgradeUser
    b. DB Password: password
3. Once installation is complete, you can disable or delete the 'UpgradeUser' since it is only used during the upgrade process.

```
-- Create a login for upgrading the database
use master
Create Login UpgradeUser WITH PASSWORD = 'password', Check_Policy = OFF
GO

-- Make a database user for the login
-- and give them db_owner role on the target database
USE FrontOffice
CREATE USER UpgradeUser FOR LOGIN UpgradeUser
GO
ALTER ROLE db_owner ADD MEMBER UpgradeUser
GO

-- Allow ownership of database to be transferred to sa.
-- The sa login can be disabled as per good dba practice,
-- and everything will still work ok.
use master
GRANT IMPERSONATE ON LOGIN::sa to UpgradeUser
```