MooD 17

Active Enterprise Installation Guide

Comprising:

Business Integration Engine

Active Publisher

Notice of Copyright and Trademarks

® MooD, MooD Smarter Decisions, Performance Activation, Synchronization Activation Technology and Knowledge Map are registered trademarks of CACI Ltd. in the United Kingdom and / or other countries.

Microsoft and Windows are trademarks of Microsoft Corporation in the USA and other countries.

Rights to all other referred trademarks or registered trademarks reside with their respective owners.

Aspects of the Enterprise Business Model, Model-Driven Data Aggregation and Business Solutions to Support Smarter Decisions are protected by International Patent and Patent Pending. These include the Meta-Architecture Framework, Panels Technologies, Auto-Explorer, Business Orchestration, the Activator mechanism, Process Driven System, Performance Activation, Model-Driven Enterprise Management, Dynamic Aggregation, Smart Columns, the Variant Mechanism, and other technologies and mechanisms implemented within MooD Business Architect and MooD Active Enterprise.

Introduction

This document guides you through the setup of the three tiers of a working Active Enterprise installation. **Active Enterprise** is the term we use to collectively describe the tiers below combined to provide a live operational web site for a MooD repository.

The three tiers and their major components are:

- **Database tier**. This comprises a database engine using SQL Server and any MooD repository.
- **Business Integration Engine (BIE) tier**. This comprises the Business Integration Engine and MooD Business Architect.
- **Active Publisher (AP) tier**. This comprises Active Publisher, MooD Business Architect, Internet Information Services, and ASP.NET 4.8.

The three tiers can run on separate machines if required, but consideration should be given to the overhead introduced by these tiers communicating over a local area network rather than locally on a single machine. A single server installation is simpler to install and enhances performance (due to not having to communicate over the network), but could introduce a performance bottleneck if the solution you are deploying places a high load on any one of the tiers, and increases the potential surface area for any cyber-attacks. Typically BIE and AP tiers are installed on the same machine, with the database isolated on another machine.

MooD Business Architect is required on the BIE/AP tiers because it provides common components, such as Repository Manager, Synchronization activators, and repository access.

Steps to Deploy Active Enterprise Server

This document covers the different ways you can install BIE and Active Publisher. It is arranged in ***tasks***. Each task brings your deployment closer to readiness and is described in its own section in this document. To successfully install Active Enterprise Server, perform the tasks in order. The appendices cover situations that might be relevant to you.

Software Requirements

Operating System:

You can install these products on the supported server and workstation operating systems listed in the MooD Release Notes. It is recommended to use the latest supported server operating system.

For demonstration purposes only, you can install these products on supported workstation operating systems (i.e. Windows 10). **NOTE:** These platforms are not suitable for live deployments.

In all cases, it is recommended that the latest service pack and patches are applied to the operating system.

Internet Information Server: On the AP tier, Internet Information Server (IIS) version 10 or greater must be installed.

MooD: MooD Business Architect must be installed before installing BIE or AP.

Dependencies: MooD Business Architect, BIE, and AP all require Microsoft .NET Framework 4.8 and the Visual C++ runtime libraries. These components may already be installed, but, if not, it will be installed with the products. Future versions of these frameworks are backward compatible, so typically can be updated as required.

Microsoft Office: On the BIE and AP tiers, Microsoft Excel 2010 or later is required only if your solution uses the Excel import synchronization activator configured to run in **Excel Native** mode. This should be enabled only by exception.

Installing the Database Tier

Basic SQL Server Installation

See the *MooD Release Notes* for a list of all supported versions of SQL Server. Using the latest supported version is recommended. All SQL Server products require the same installation choices. Over time, some of the names of features mentioned in the SQL Server installers may change. Except for the Full Text Indexing feature of SQL Server, MooD does not currently require additional components such as Microsoft SQL Server Integration Services, Reporting Services, Replication, Data Analytics with R, or artificial intelligence components, unless you are wishing to integrate with those components as part of your system design.

Here are some quick steps if you simply want to test connectivity or perform a local test installation, rather than an installation for a live deployment. Typically, customers will have a dedicated database administrator and infrastructure with multiple SQL Server instances available for use. This walk-through uses Microsoft SQL Server Express 2019 with Advanced Services, which has some limitations but can be used for production purposes for free, until a more powerful version is required.

1. Launch the SQL Server setup program.
2. Click **Custom**
3. Choose an installation folder.
4. Press **Install**. This will install the *real* setup program.
5. Once loaded, select **New SQL Server stand-alone installation**... and click **Next**.
6. After the **Product Updates** have finished scanning, press **Next**.
7. After Install Setup Files has finished working, press **Next** (unless informed otherwise by the installer).
8. In **License Terms**, if you agree to the licence, tick the box and press **Next**.
9. In **Feature Selection**, tick the following (for minimal install):
    - 9.1. In **Instance Features** > **Database Engine Services**:
        - 9.1.1. tick **Full-Text and Semantic Extractions for Search** only.
    - 9.2. Under **Shared Features**:
        - 9.2.1. Tick **Client Tools Connectivity** (should be un-tickable).
        - 9.2.2.Tick **Client Tools Backwards Compatibility**.
    - 9.3. Choose your **Instance root directory**, and press **Next**.
10. In **Instance Configuration**, rename your instance if you have a conflict, otherwise press **Next**.
11. In **Server Configuration**:

11.1. For **SQL Server Database Engine**, click choose **Browse**... and select **NT Authority\SYSTEM**

11.2. If your IT department has a group policy that prevents new accounts running services, the *pseudo* accounts like `NT Service\MSSQL$2019` will work for a while, but then suddenly stop working. You can safely alter these service accounts in the **SQL Server Configuration Manager App**. Do not use the *Services* control panel, as the SCM App also configures file permissions.

11.3. Later you need to consider using more restrictive accounts, but this step simplifies initial connection.

11.4. In **Collation**, we typically expect the server collation to be Latin1_General_CI_AS.

11.5. Press **Next**.

12. In **Database Engine Configuration**

12.1. Select **Mixed Mode** authentication and enter your own memorable password for the **sa** user.

12.2. Click **Add Current User**. Optionally add the local Administrators group too.

12.3. Optionally review **Data Directories**, **TempDB** and **Memory** settings. These may ensure that you place files in preferred locations, enable parallel processing with more than one TempDB, and prevent SQL Server from overwhelming your system memory.

12.4. Click **Install.** Then when it's finished, press **Close**.

13. Once the installation has completed, return to the setup program, and select **Install SQL Server Management Tools** (SSMS)**,** this will forward you to a Microsoft site where you can download the setup program**.** Installing SSMS is useful to help our support team diagnose issues, and for users to configure security between a repository and BIE/AP services.

14. If the BIE server and SQL Server are on different machines, you may need to open a TCP port on the SQL server machine firewall so the BIE can connect to the database. For SQL Server, the default port is 1433.

15. Configure SQL Server to accept TCP/IP connections;

15.1. From the Start menu, open **SQL Server 2019 Configuration Manager**.

15.2. In the left pane find SQL Server Network Configuration, and click on the Protocols for your instance.

15.3. In the right-hand panel, right-click **TCP/IP**.

15.4. Choose **Enable**.

15.5. Stop and start the SQL Server service.

Install and Licence MooD

Perform an installation of MooD Business Architect by

- launching the **Business Architect Setup.exe** program and follow the instructions.
- Restart your computer after installation if you are asked to do so.
- Right-click the MooD icon on the desktop and select **Run as Administrator** – running as the Administrator user will ensure the licence installs for BIE and AP too.
- The option to install a Licence will be displayed automatically if one is not present.
- Ensure the option is set to make the licence available to everyone who uses this computer.
- The licence file provided by the MooD support team normally would include Business Architect plus Active Publisher and Business Integration Engine.

Note: Active Enterprise Server installations cannot be licenced via a MooD Licence Server.

Configure a Repository

- If not already open, start MooD Repository Manager
- On the **Servers** tab add the SQL Server Instance you created earlier, you can find the full syntax of patterns supported here. Typical examples are:
    - localhost – when the SQL Server is on this machine and is the default instance.
    - localhost\instancename – as above, but for a named instance of SQL Server.
    - servername – the SQL Server is on a different machine and the default instance.
    - servername\instancename – as above but with a named instance.
    - servername,portnumber – default instance on a server using a specific port.
    - servername\instancename,portnumber – as above but with a named instance.
- Add the server with your chosen authentication method.
- Create, Show, or restore a repository
- If you followed the steps to install SQL Server express mentioned previously, you can quickly use Windows Authentication to make a connection to your database.

SQL Server Notes

Key points and guidance for configuring a quick test repository, assuming you added a local SQL Server as described earlier:

- To create a database, you must have a connection to the server, and the user credentials used to connect must have at least SQL Server public role privileges.
- In Repository Manager, you can add a server, on the **Add Server** dialog box, using either **Native SQL Authentication** or **Windows Authentication**.
- Use the **Test** button on the **Add Server** dialog box to test the credentials and server name. If the test fails, check the details you have supplied.
- If you have supplied SQL Server **sysadmin** user credentials, you can create a repository immediately. By default, the **Add Repository** dialog box will include the credentials supplied on the **Add Server** dialog box.
- If you are not a **sysadmin** user, or do not have the **dbcreator** role; you could select the **Create SQL script only** checkbox and then give the script created to your database administrator (DBA). The DBA can use this script to create the repository for you. The DBA must use **sysadmin** privileges to ensure that the correct user is assigned the correct role. The SQL user used to connect to the repository must only be associated with the ***RepName*_role** database role for that database.
- If the repository has been created in SQL Server, it should be visible to Repository Manager. On the **Server** tab, select the server, and then click **Find all repositories on the selected server**. Provided you supply the correct authentication, the repository will be listed. Set it to **Show** to make it visible on the **Repositories** tab.

Configuring a Test Homepage for Active Publisher

In whatever repository you create or restore, it is advisable to locate or create some content to assist with testing the Active Enterprise setup, for example, a Home Page for Administrator; this ensures you go beyond the basic login screen when testing.

- Open the repository with Business Architect.
- Expand the **Users** node in the tree on the left.
- Right click on the **Administrator** user and click **Look Inside** to create a model for the user.
- Save the model.
- Right click on the **Administrator** user and click **Open**.
- Change the homepage to *This user's model.*
- Save and close. The repository will be ready for a login and initial homepage for the **Administrator** user.

Good housekeeping of repositories

If you have restored a large repository for an Active Enterprise installation, it's advisable to follow some normal housekeeping advice:

1. Validate the repository:
    a. In MooD Repository Manager, right click the repository, and then click **Validate**.
    b. Provide the repository administrative credentials.
    c. Select **Check & Fix errors** and then click **Next** (this may take some time).

d. If there are any errors highlighted, contact MooD International support for advice.

2. Defragment all indices (but not required);
    a. In MooD Repository Manager, right click the repository, and then click **Index Fragmentation**.
    b. Click **Defragment All** and then click **OK**.

Install the Business Integration Engine (BIE)

Installing the Business Integration Engine:

Note: MooD Business Architect must already be installed.

1. Launch the **Business Integration Engine Setup.exe**.
2. Once the setup launches, you can configure a different port or simply click **Install**.

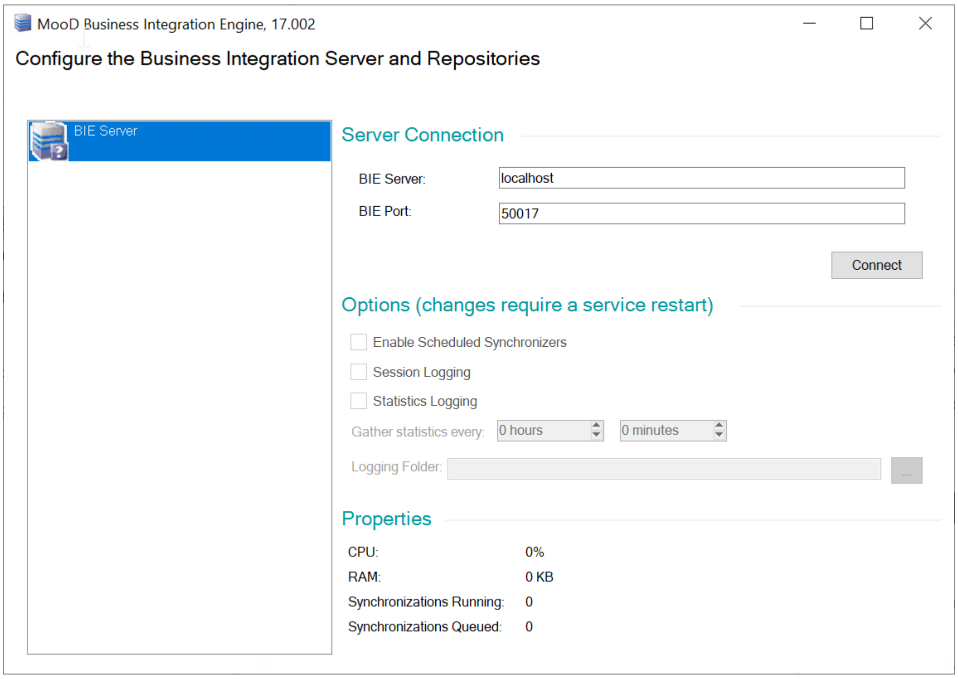
Note: If the BIE server and Active Publisher server are on different machines, you may need to configure your firewall to open a port so that Active Publisher can connect to the BIE. By default, this is port 50017, and is configurable after installation in the BIE's **config.xml** file.

Connect a Repository in Business Integration Engine (BIE)

1. Ensure BIE service is started (if not already);
    a. Navigate to **Control Panel** > **Administrative Tools** > **Services**.
    b. Locate and start the service named **MooD Business Integration Engine 17**.
    c. Alternatively, run this command from a command line (run "as Administrator");

```
net start MooDBIE_17
```

2. Use the BIE Manager to connect to the desired repository;
    a. In the Windows taskbar, type **Business Integration Engine Manager**, and launch it.
    b. Ensure the BIE Server and BIE Port number boxes are correct, and then click **Connect**.

c. 

MooD Business Integration Engine, 17.002

Configure the Business Integration Server and Repositories

Server Connection

BIE Server: localhost

BIE Port: 50017

Options (changes require a service restart)

□ Enable Scheduled Synchronizers

□ Session Logging

□ Statistics Logging

Gather statistics every: 0 hours 0 minutes

Logging Folder:

Properties

CPU:	0%
RAM:	0 KB
Synchronizations Running:	0
Synchronizations Queued:	0

d. Select the required repository and then tick **Enable support for BIE**.

e. Enter the repository administrator username and password

f. Ensure the **Synchronization, Alerting & Scheduling** box is ticked.

g. Click **Apply**.

h. You may receive a firewall notification. If you do, and can, click **Allow**.

i. You should now see the icon be colourful, and the status message *The repository is ready*

j. The Windows Event Viewer will have extended information inside any events raised during this process. Please see the troubleshooting section of this document for specific guidance on commonly encountered issues at this stage.

Active Publisher

Install Internet Information Server (IIS)

Both IIS and ASP.NET are required by the Active Publisher tier. For further guidance on IIS installation, contact your Microsoft support team.

Windows 10 Installation

1. IIS is installed using the Turn Windows Features on or off dialog in Control Panel (in the Programs and Features section).
2. Select the 'Internet Information Services' to install IIS with default features enabled. In addition to the defaults, the following must be selected:
    a. World Wide Web Services > Application Development > ASP.NET 4.x (e.g. ASP.NET 4.5 or ASP.NET 4.7)
    b. World Wide Web Services > Common HTTP Features > Static Content
    c. Web Management Tools > IIS 6 Management Compatibility > IIS Metabase and IIS 6 configuration compatibility
3. For installations utilising Windows integrated authentication, the following is also required:
    a. World Wide Web Services > Security > Windows Authentication
4. For installations which serve Repositories which include or may include Custom Visuals, the following is also required:
    a. World Wide Web Services > Common HTTP Features > Static Content

Windows Server Installation

1. IIS is installed using the **Roles** section in the Server Manager application.
2. In the Roles Summary click Add Roles and select the Web Server (IIS) role.
3. When prompted, select **Role Service**. In addition to the defaults, the following must be selected:
    a. Web Server > Application Development > ASP.NET 4.5 (or whichever version of ASP.Net 4.x Is listed)
    b. Management Tools > IIS 6 Management Compatibility > IIS 6 Metabase Compatibility
4. For installations utilising Windows integrated authentication, the following is also required:
    a. Web Server > Security > Windows Authentication
5. For installations which serve Repositories which include or may include Custom Visuals, the following is also required:
    a. Web Server > Common HTTP Features > Static Content

Install Active Publisher

Follow the steps below to install the first instance of Active Publisher on a server. For information on installing additional instances see Installing Additional Active Publisher Instances. MooD Business Architect should be installed before Active Publisher. Normally the Business Integration Engine should also be installed on the same machine unless it has been installed elsewhere.

1. Using the MooD Media, navigate to the **MooD Active Enterprise/Active Publisher** folder and run the **Active Publisher setup.exe** file.
2. Review and accept the licence agreement.
3. During the installation you will be prompted to create an application pool in IIS. Allow this.
4. Set the (Web) **Site** and **Virtual Directory** appropriately.
    a. **Site** is simply an administrative label inside IIS for a Web Site that can contain many applications.
    b. **Virtual Directory** is used to identify an application and build up the web address for Active Publisher. For example, if you are installing on a machine called **WebServer** and install to a virtual directory called **MyApp**, you would access Active Publisher from **http://WebServer/MyApp**. Port 80 will be used as the default port for IIS. Configuration of this port is possible using the IIS Management Console.

Configure Internet Information Server (IIS)

Configure Application Pool

1. Create a new application pool. It is good practice to name application pools after the applications they will serve.
2. Note that the Active Publisher installation allows you to create an application pool during installation. If you did this, and you want to use that pool, you do not have to create a new pool. However, you should check that its settings match those of the one created here.
3. To create a new Application Pool:
    a. Open Internet Information Services (IIS) Manager (run **inetmgr.exe**).
    b. Navigate to **Application Pools** and create a new one (right click and select **Add Application Pool**). Ensure that **.NET CLR version 4.0.*xxxxx*** is selected.
    c. Give the application pool a relevant name and press **OK**.
    d. Right click on the new application pool and click **Advanced Settings**.

   e. Under **Process Model**, set **Identity** to **LocalSystem** (for now). For security reasons you may wish to move away from using LocalSystem, please contact our Support Department for information on how to do this.
   f. Set **Enable 32-bit Application** to **True**.
4. To assign Active Publisher to the new application pool:
   a. In Internet Information Services (IIS) Manager find the Active Publisher virtual directory (typically under **Sites** > **Default Web Site**).
   b. Right click the virtual directory and select **Manage Application** > **Advanced Settings**. Set the **Application Pool** to the one we just created.

Configure Integrated Authentication

1. If integrated (Windows) authentication is to be used, it must be enabled for the virtual directory.
   a. In Internet Information Services (IIS) Manager, select the Active Publisher virtual directory (under **Sites** > **Default Web Site**).
   b. In the right-hand pane, under the **IIS** heading, select **Authentication**.
   c. Right-click **Windows Authentication**, and then select **Enable**.
   d. Note that for Windows Authentication to work correctly it is necessary to disable **Anonymous Authentication** and **Forms Authentication**, which can be found in the same **Authentication** feature in IIS.

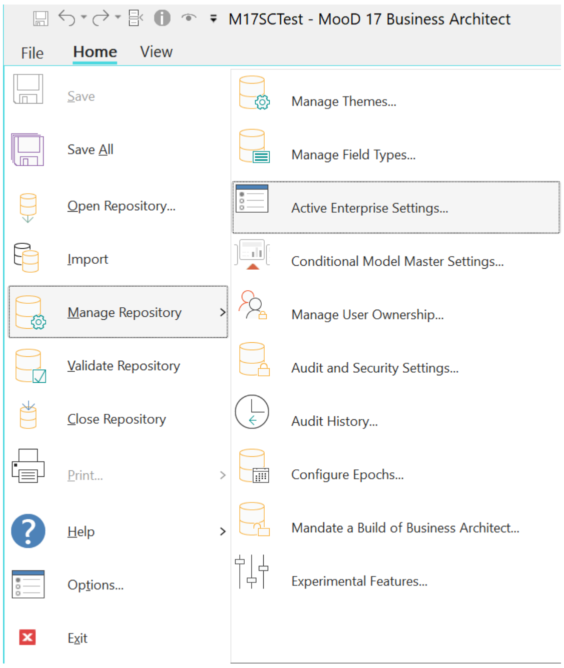
You will also need to ensure that your repository is configured to use Windows Authentication. See Using Windows Authentication.

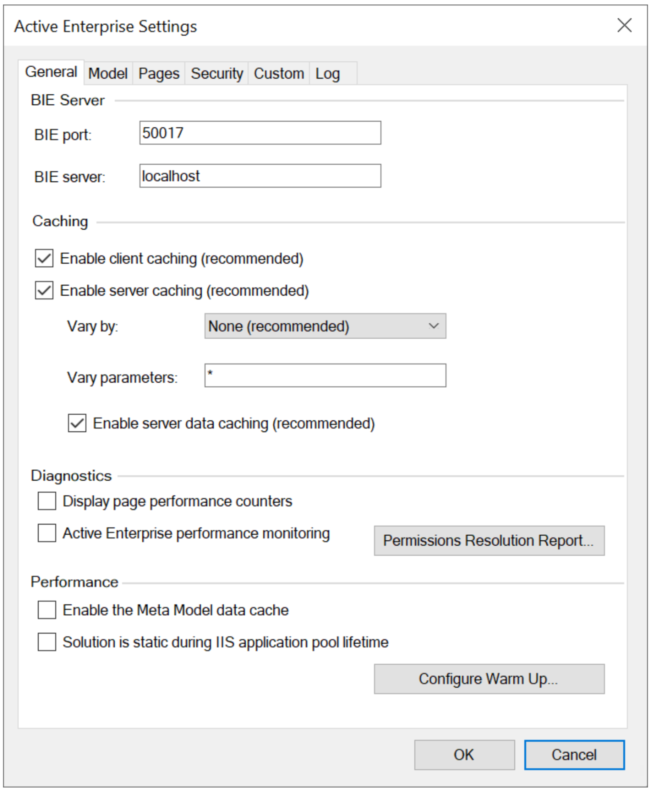
Configure Active Publisher

To tie a virtual application in IIS to a MooD repository, we need to run a small configuration tool.

1. In the folder **C:\inetpub\wwwroot\<*Your Virtual Directory*>\bin**, you will find the *application* **ConfigureActivePublisher.exe**.
2. Right-click this file and **Run As Administrator**.
3. This program modifies the **ActivePublisher.config** file in the parent folder.
4. Under **Repository**, use the **Name** drop down list to choose the repository that this Active Publisher installation will serve, and set the appropriate administrator name and password for the repository (the MooD logon not the SQL logon).

5. The remaining settings can be accessed from within Business Architect: Click File on the ribbon, under **Manage Repository**, click **Active Enterprise Settings**.





BIE Server

BIE port: 50017

BIE server: localhost

Caching

☑ Enable client caching (recommended)

☑ Enable server caching (recommended)

Vary by: None (recommended)

Vary parameters: *

☑ Enable server data caching (recommended)

Diagnostics

☐ Display page performance counters

☐ Active Enterprise performance monitoring

Performance

☐ Enable the Meta Model data cache

☐ Solution is static during IIS application pool lifetime

6. Under **BIE Server**, set the **BIE Port** and **BIE Server** settings. If the BIE is installed on the same machine, the default settings (**50017** and **localhost**) should be fine.
7. Click **OK** to accept the changes.
8. Active Publisher should detect the changed configuration and automatically restart. It can be manually restarted by entering **iisreset** from a command prompt.

You should now be able to view your repository by opening a web browser and navigating to **localhost/*NameOfApplication***. For instance http://locahost/ActivePublisher17/

Appendices

Troubleshooting

Business Integration Engine will not start

If, when starting the Business Integration Engine Service, it reports that the service could not be started, see the **MooD** application log in the Windows Event Log to find out what problems were reported. Via **Control Panel** > **Administrative Tools** > **Event Viewer** and select **Application and Services Logs** > **MooD 17**.

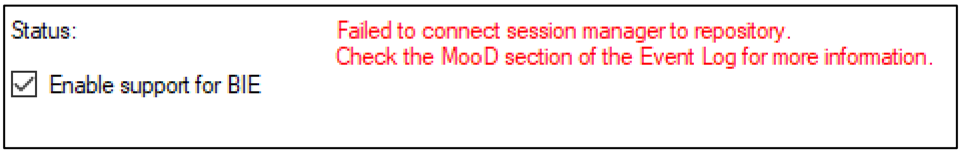
Business Integration Engine reports that it is not licensed

If, when connecting to the Business Integration Engine using the Business Integration Engine Manager, and it reports that it is not licensed, make sure that MooD Repository Manager is started as the **Administrator** user (right click the icon and choose **Run as administrator**) and reinstall the licence file for all users of the machine, and that the licence is a valid BIE licence.

Business Integration Engine cannot log in to the repository

This problem can be encountered when enabling support for BIE for a repository in MIE Manager.

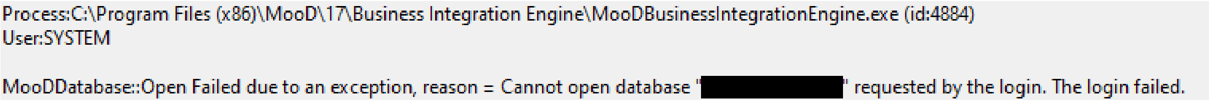
In BIE Manager, this will display as an error with text ‘Failed to connect session manager to repository.’ when applying a new connection to a repository:



Status: Failed to connect session manager to repository.
Check the MooD section of the Event Log for more information.

☑ Enable support for BIE

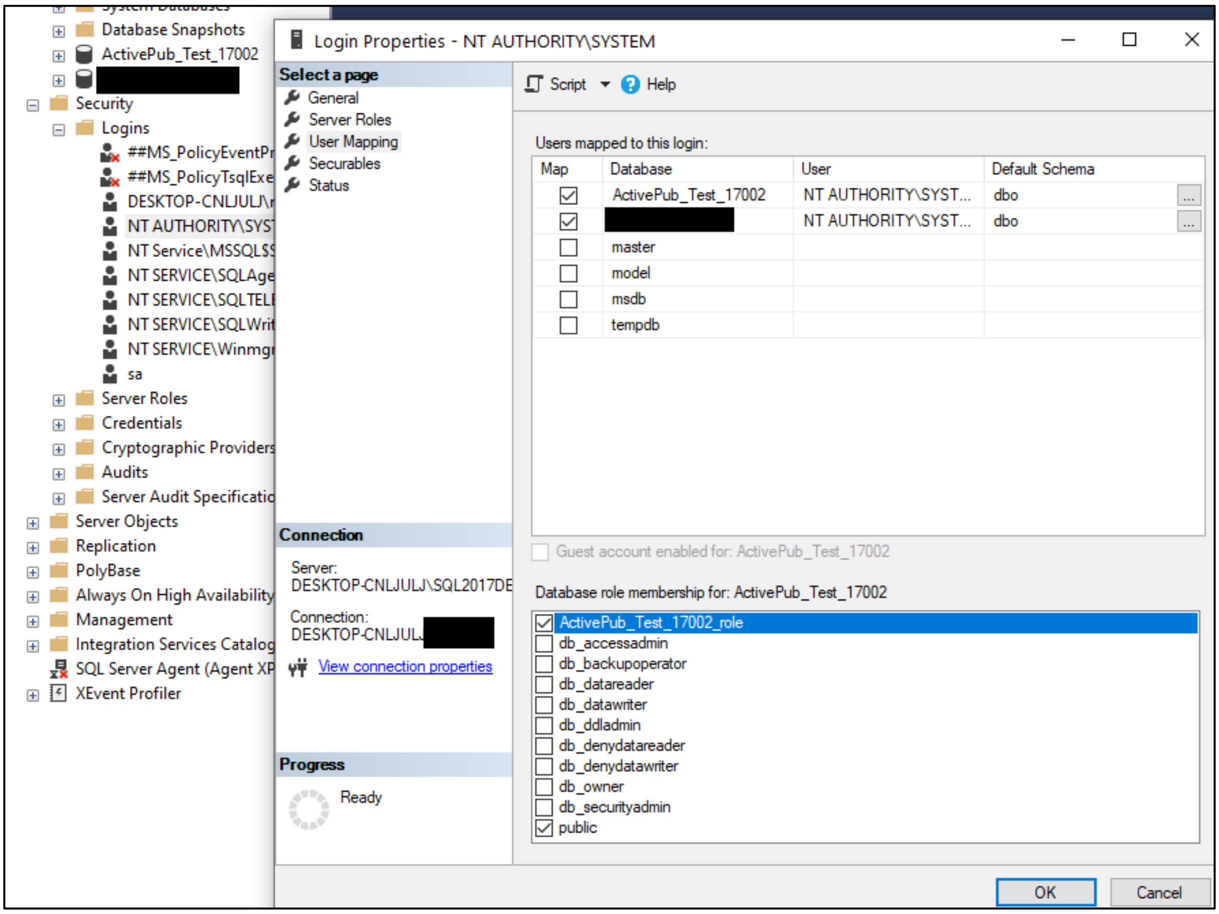
In this circumstance, you should look in the Windows Event Logs for MooD 17 for further information. If the error is due to BIE being unable to login to the repository you will see an error in the Event Logs similar to that below:



```
Process:C:\Program Files (x86)\MooD\17\Business Integration Engine\MooDBusinessIntegrationEngine.exe (id:4884)
User:SYSTEM

MooDDatabase::Open Failed due to an exception, reason = Cannot open database "[redacted]" requested by the login. The login failed.
```

The solution to this is to grant the SQL Server Role “<repositoryName>_role” to the user under which the BIE service runs. This can be done via a UI in SSQL Server Management Studio.



Server: DESKTOP-CNLJULJ\SQL2017DE

Connection: DESKTOP-CNLJULJ[redacted]

Users mapped to this login:

Map	Database	User	Default Schema
☑	ActivePub_Test_17002	NT AUTHORITY\SYST...	dbo
☑	[redacted]	NT AUTHORITY\SYST...	dbo
□	master		
□	model		
□	msdb		
□	tempdb		

□ Guest account enabled for: ActivePub_Test_17002

Database role membership for: ActivePub_Test_17002

- ☑ ActivePub_Test_17002_role
- □ db_accessadmin
- □ db_backupoperator
- □ db_datareader
- □ db_datawriter
- □ db_ddladmin
- □ db_denydatareader
- □ db_denydatawriter
- □ db_owner
- □ db_securityadmin
- ☑ public

More detailed instructions for this step are available in the ‘Active Enterprise – moving away from LocalSystem’ document.

Active Publisher cannot access database

If, when accessing Active Publisher from the web browser, there is an error (either in the browser or in the Event Log) indicating a database error e.g.:

The database reported a problem. If the problem re-occurs try re-starting MooD. Otherwise, contact the administrator of the repository

The problem may be that the IIS Application Pool does not have permission to access the database. In this circumstance please follow the steps (above) to grant the <repositoryName>_role to the Application Pool user or follow the more detailed instructions in the ‘Active Enterprise – moving away from LocalSystem’ document.

Cannot log in to an Active Published Repository

If, when trying to log into an Active Published repository using a username and password, you are always returned to the login page, make sure that **Forms Authentication** is enabled for the site.

If, when trying to log into an Active Published repository using integrated login, it doesn't work, make sure that **Windows Authentication** is enabled for the site.

Trying to connect to Active Published Repository gives 404.2 error

If you receive an HTTP Error 404.2 – Not Found message when trying to connect to an Active Published Repository, IIS must be configured to allow ASP.NET v4.0 sites.

Open IIS Manager (InetMgr.exe) and in the **Connections** panel, select the topmost option. In the right-hand pane, under the **IIS** heading, select **ISAPI and CGI Restrictions**. Make sure any rows that are related to ASP.NET v4.0 are **Allowed**. Right-click any rows that are not allowed and click **Allow** to change this.

See the **MooD Release Notes** in the Business Architect installation folder for more troubleshooting information.

Installing Additional Active Publisher Instances

It is possible to run multiple Active Publisher web sites each as its own Virtual Application in IIS, but all sharing a single Business Integration Engine installation. However, the original installer should not be used for this purpose, instead you can:

Adding a new Active Publisher Instance

1. Enable this repository with the BIE Manager.
2. Then use Windows File Explorer to copy the existing Active Publisher installation folder and give it an appropriate name, for example copy **C:\InetPub\wwwroot\ActivePublisher** to **C:\InetPub\wwwroot\ActivePublisher2**.
3. Convert the new Active Publisher folder into an application.
    a. Open Internet Information Services (IIS) Manager (run **inetmgr.exe**).
    b. Right-click the folder and select **Convert to Application**.

4. Configure IIS for the new application. Perform the steps in Configure Internet Information Server.
5. Configure the new Active Publisher instance. Follow the steps in Configure Active Publisher.

Separating Cookie Settings

For a user to be able to simultaneously log into multiple Active Publisher instances on the same domain, you must configure each instance to use a separate pair of cookies for session management and authentication.

1. For each Active Publisher instance, make the following changes.
    a. Navigate to the root of the Active Publisher folder and open the **Web.config** file.
    b. Modify the **name** attribute of the **forms** element to an instance-specific value, for example:

```
<forms timeout="20" name="ActivePublisher2" loginUrl="Login.aspx"
protection="All" />
```

    c. Add a **cookieName** with an instance-specific value to the **sessionState** element, for example:

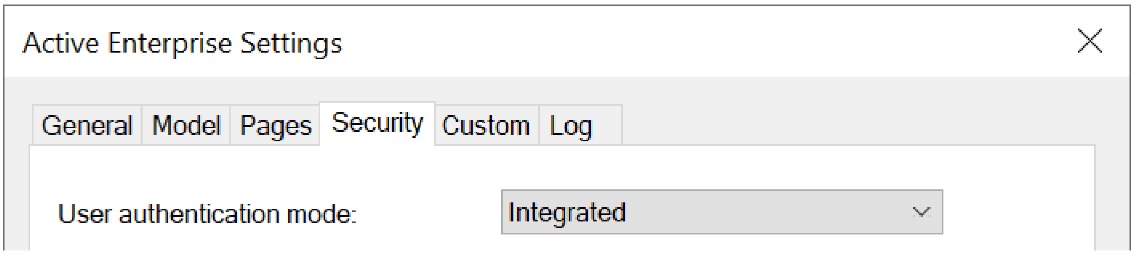
```
<sessionState cookieName="ActivePublisherSession2" mode="InProc"
stateConnectionString="tcpip=127.0.0.1:42424"
sqlConnectionString="data source=127.0.0.1;Trusted_Connection=yes"
cookieless="false" timeout="20" regenerateExpiredSessionId="true" />
```

Note that each **name** and **cookieName** setting must be unique both within and across all **Web.config** files.

Using Windows Authentication

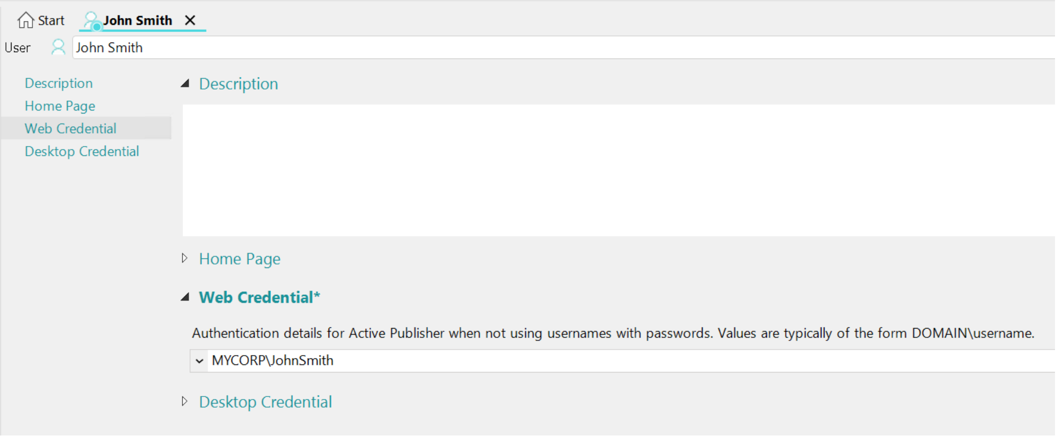
Provided IIS has been configured to allow the use of Windows Authentication (see section Configure Integrated Authentication) you can configure a repository so that users can use their Windows Authentication to log in. How to do this is covered here.

1. Open the repository in Business Architect and navigate to any model.
2. Go to **File**->**Manage Repository**->**Active Enterprise Settings**...
3. Click the **Security** tab.
4. Set **User Authentication Mode** to **Integrated**.



User authentication mode: Integrated

5. Click **OK**.
6. You must now associate the correct Windows login name with each user in the **Users** theme. To do this, in Business Architect's Explorer Bar, under **Themes**, under **Users**, open the user's definition window and set the **Web Credential** field.



User John Smith

Web Credential*

Authentication details for Active Publisher when not using usernames with passwords. Values are typically of the form DOMAIN\username.

MYCORP\JohnSmith

The user should now be able to use their Windows Authentication to log into the MooD Active Enterprise site.

Other authentication methods

It is possible to use other methods (besides the IIS provided Forms Authentication and Windows Authentication) of authenticating the web user with MooD Active Enterprise, such as:

- Certificate
- Header Variable
- Server Variable

These methods are usually reliant on other environmental factors or components (such as a reverse proxy to make an authentication challenge) and therefore will only be applicable to particular deployments.

MooD Support can provide information on how to configure the Repository and IIS instance if one of these authentication methods is required.

Authentication methods other than those specified above have been implemented on MAE deployments. If there is a particular authentication mechanism which you need to use, please discuss this with your account manager.

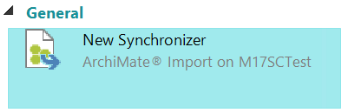
Advanced Configuration

Business Integration Engine

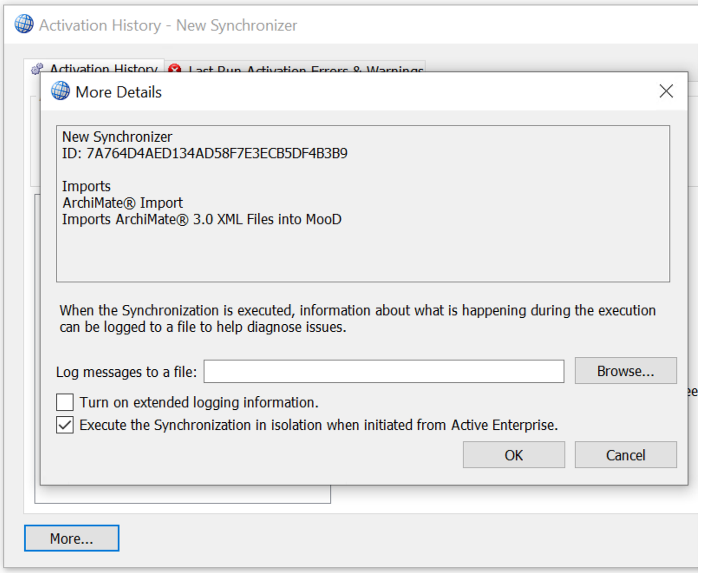
The **Config.xml** file in the BIE install location can be edited to turn on performance monitoring, out of process model publishing, and set the memory usage threshold before recycle or maximum number of Synchronization threads.

- **monitor-performance="true"** – turns on the performance monitors in BIE so that **perfmon** can be used to monitor the performance of the service (by default this is off).
- **memory-usage-threshold="<*percentage*>"** – sets the percentage threshold of used process memory to get to before the BIE synchronization execution recycles (the default is 90%).
- **maximum-threads="<*number*>"** – sets the limit of Scheduled or MAE manually triggered synchronizations which are run concurrently. This can help overall system performance especially where BIE and AP are on the same machine. The default is 5 times the number of processor cores. This may need to be tuned according to the needs of the solution and hardware.

- **in-process-model-publisher=”false”** – tells Synchronizations that are publishing models or matrices to do this in a separate process. This can help reduce BIE synchronization execution recycling and spread memory load, where large models or matrices are used. (Default is true). **Note** –you may find that configuring specific Synchronizers to execute completely in their own isolated process solves your problem. This setting is inappropriately tucked away inside the History window of a Synchronizer.



New Synchronizer
ArchiMate® Import on M17SCTest



Activation History - New Synchronizer
Activation History
Last Run Activation Errors & Warnings
More Details

New Synchronizer
ID: 7A764D4AED134AD58F7E3ECB5DF4B3B9

Imports
ArchiMate® Import
Imports ArchiMate® 3.0 XML Files into MooD

When the Synchronization is executed, information about what is happening during the execution can be logged to a file to help diagnose issues.

Log messages to a file:

□ Turn on extended logging information.

☑ Execute the Synchronization in isolation when initiated from Active Enterprise.

The following registry keys can be manipulated:

[HKEY_LOCAL_MACHINE\SOFTWARE\Salamander\Business Integration Engine\17]

- **DisableSynchronizationTimers=<true|false>** – Causes BIE to skip checking for scheduled synchronizations.
- **SATThreadPoolSize=<*number*>** - Limits the number of Scheduled or MAE manually triggered synchronizations which are run concurrently. This can help overall system performance especially where BIE and AP are on the same machine. Default is 5 times the number of processor cores. Note: The value of **SATThreadPoolSize** needs to be tuned according to the needs of the solution and hardware. This overrides anything set in the **Config.xml**.

Active Publisher

The following registry keys can be manipulated:

[HKEY_LOCAL_MACHINE\SOFTWARE\Salamander\Active Publisher\17]

- **Upload Folder=<*Share*>** - (note the space between **Upload** and **Folder**). If using the file upload control and the BIE and AP are on different machines, you must specify a shared location for AP to store the uploaded file and from which BIE will pick up the file.

Hardening Active Enterprise Installations

This section describes changes which can be made to the **web.config** file to harden an installation against malicious attack.
Comments on these changes can also be found within the web.config file.

httpRuntime Modifications

Please retain the 'false' value for enableVersionHeader; this prevents the ASP.Net version from being disclosed in a response header.

```
<httpRuntime … enableVersionHeader="false" …/>
```

The execution timeout (how long to wait for a request in seconds) can be modified using the executionTimeout attribute:

```
<httpRuntime … executionTimeout="1200" …/>
```

The maximum request length can be set to enable the upload of large files. This may be necessary if the solution allows the upload of files for Synchronizer execution, or if users can add Images to Formatted Text fields via the web. The value is in Kb:

```
<httpRuntime … maxRequestLength="20480" … />
```

Enforce SSL protection for cookies

Important - only make this change if your installation is using SSL/https, otherwise it will disable login altogether. Do NOT make this change if you only support http.

Add the attribute and value `requireSSL="true"` to the `<forms>` element
e.g. from:

```
<forms timeout="20" name="ActivePublisher" loginUrl="Login.aspx"
protection="All"/>
```

to:

```
<forms timeout="20" name="ActivePublisher" loginUrl="Login.aspx"
protection="All" requireSSL="true"/>
```

By setting **requireSSL="true"**, the **secure** cookie property is set. This determines whether browsers should send the cookie back to the server. With the **secure** property set, the cookie is sent by the browser only to a secure page that is requested using an HTTPS URL. For details, see http://msdn.microsoft.com/en-us/library/1d3t3c61(v=VS.80).aspx.

Set the `requireSSL` attribute on the `<httpCookies>` element to be `"true"` e.g. from:

```
<httpCookies requireSSL="false" httpOnlyCookies="true" />
```

to:

```
<httpCookies requireSSL="true" httpOnlyCookies="true" />
```

This secures the BIE cookie so the cookie is sent by the browser only to a secure page that is requested using an HTTPS URL. For details, see http://msdn.microsoft.com/en-us/library/ms228262(v=VS.80).aspx.

Applying secure headers

Headers can be added to all responses using the `<system.webServer><httpProtocol><customHeaders>` element in the Web.config file.

Various headers are added or removed in this section in the default state of the Active Publisher web.config file. These all pertain to security and should not be modified unless a specific need is identified.

HSTS header – be very careful

If HTTPS is being used exclusively, you can also configure a Strict-Transport-Security header, with an appropriate max-age value (in seconds) to ensure that the site is always connected-to using SSL. **However**, this header will cause all connections to the specified Domain to be connected-to using SSL, and can cause denial of service if other applications under the same domain do not support SSL. So be extremely careful when implementing this on a customer's domain. This header may be best left to a customer's Web Application Firewall.

Manage the Content-Security-Policy in the repository (MooD v16.085 and above only)

In versions of MooD prior to 16.085 the Content-Security-Policy was applied to Active Publisher as an additional custom header which was specified in the web.config file e.g.

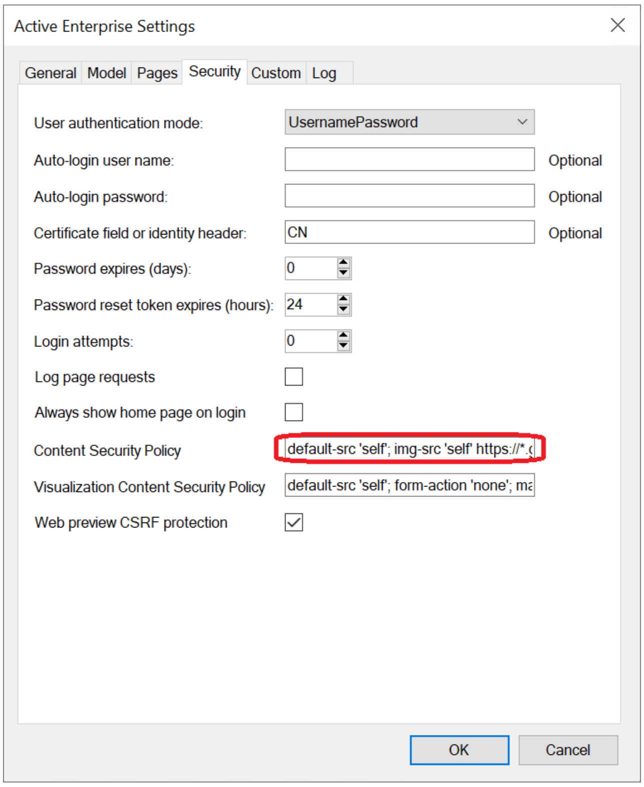
Within: `<system.webServer><httpProtocol><customHeaders>`

```
<add name="Content-Security-Policy" … />
```

With version 16.085 the specification of this policy is now stored within the repository, making it portable when restoring a .bak file.

If a specific Content-Security-Policy has been applied in the web.config file, please extract this policy and save it in the 'Content-Security-Policy field on the Security tab of the Active Enterprise Settings for the repository in Business Architect. Then remove the `<add name="Content-Security-Policy" … />` element form the web.config file.

If no specific Content-Security-Policy has been applied in the web.config file, then please remove the `<add name="Content-Security-Policy" … />` element form the web.config file. The default Content-Security-Policy will then be applied, and can be modified if necessary, in the Active Enterprise Settings for the Repository.



User authentication mode: UsernamePassword

Auto-login user name: Optional

Auto-login password: Optional

Certificate field or identity header: CN Optional

Password expires (days): 0

Password reset token expires (hours): 24

Login attempts: 0

Log page requests □

Always show home page on login □

Content Security Policy default-src 'self'; img-src 'self' https://*;(

Visualization Content Security Policy default-src 'self'; form-action 'none'; ma

Web preview CSRF protection ☑

Note that following any modification to the Content-Security-Policy it is a good idea to test the site, particularly pages which include uploads, custom visualizations or Generic HTML panels to ensure that they still function correctly (open F12/Developer tools in your Web Browser and watch the console for CSP related errors). The Content-Security-Policy may need modification if it is blocking some required functionality.

Hardening Tips

Various changes can be made to a repository, SQL Server, Web Site, and associated infrastructure to ensure it is more secure, here are a few suggestions.

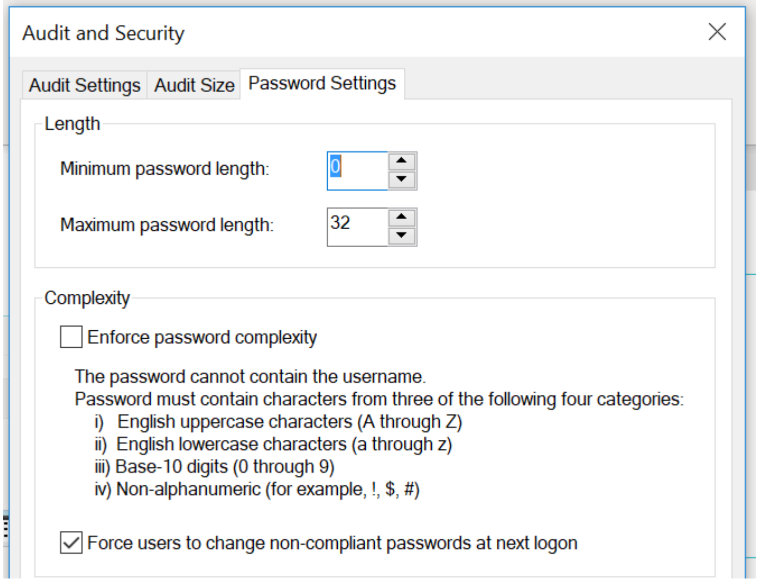
Setting a maximum number of login attempts

Setting a maximum number of password attempts should be considered mandatory as it provides protection against brute-force style password attacks.

Do this in Business Architect in Active Enterprise Settings on the **Security** tab.

Set password length and complexity

Setting a minimum length for the password is also good practice. This can be done in Business Architect using the Audit and Security Settings, Password Settings tab:



Length

Minimum password length: 0

Maximum password length: 32

Complexity

□ Enforce password complexity

The password cannot contain the username.
Password must contain characters from three of the following four categories:
i) English uppercase characters (A through Z)
ii) English lowercase characters (a through z)
iii) Base-10 digits (0 through 9)
iv) Non-alphanumeric (for example, !, $, #)

☑ Force users to change non-compliant passwords at next logon

Setting password complexity is currently considered to be of less value than password length, but may be required by the customer's security standards. However, using Integrated security (Windows Authentication), is even better.

Ensure the permissions model is robust

The permissions model in Business Architect should be properly utilised to ensure that users cannot access functionality or data which is inappropriate for their group.

Whilst menus can be populated to display limited subsets of pages to more restricted users, that in itself does not prevent a user from accessing a page. Unless the permissions model restricts viewing of an element or model, any user who can get the URL to a particular model will be able to access the model from a browser.

Ensure appropriate password complexity on existing accounts

Ensure that Administrator and solution builder accounts are properly secured by applying a password of appropriate length and complexity.

Use TLS 1.2 or 1.3

On June 30, 2018, the PCI Data Security Standard (DSS) required that all websites needed to be on TLS 1.1 or higher. Thus you may need to disable TLS 1.0 to update the security of your Active Enterprise, SQL Server and Business Architect environments.

Please refer to these articles (information in linked articles may be out of date):

https://www.globalsign.com/en/blog/disable-tls-10-and-all-ssl-versions

https://caniuse.com/tls1-3

You can make the necessary changes by editing the registry to disable the protocols, see this article as an example for disabling TLS1.0.

https://windowsreport.com/how-to-disable-tls-1-0/

These settings will not only affect Web Sites, but also the communication between Active Publisher and SQL Server, and Business Architect and SQL Server.

Moving away from Local System Accounts

Using MooD Active Enterprise with the *LocalSystem* identity in Internet Information Services (IIS) is a fast way to prove a basic installation works. But this can leave your server open to emerging vulnerabilities.

Production deployments normally create a unique service account in Active Directory and:

- Ensure it has a strong password
- Ensure the password does not expire (otherwise services suddenly stop working).
- Reduced permissions on the domain.
- Ensure it has no RDP access.
- Use this account in SQL Server, Business Integration Engine and the IIS App Pool.
- Ensure group policy does not overwrite accounts which are permitted to run in services (i.e. add this account to the allowed service accounts).
- Tip: Always use **SQL Server Configuration Manager** to change SQL Server accounts.
- You may need to allow your App Pool account activation permissions to the MooDModelPublisherProxy 17 service, via DCOMCNFG – See the MooD release notes.

Contact our support department for more information on how to configure alternative accounts to minimize the risk of system vulnerabilities.