MooD 16

Active Enterprise Installation Guide

Version 16.085

Comprising:

Business Integration Engine

Active Publisher

Notice of Copyright and Trademarks

MooD 16 Active Enterprise Server Installation Guide

® 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. 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, MooD 16, and optionally Microsoft Excel.
- **Active Publisher (AP) tier**. This comprises Active Publisher, MooD 16, Internet Information Services, and ASP.NET 4.5.

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

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 (section 2 to 10) in order. Sections 11 onwards cover particular 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 16 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. **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 server.

Internet Information Server: On the AP tier, Internet Information Server (IIS) version 7 or greater must be installed (user is prompted if an install of IIS is present, but lower than 7).

MooD: MooD 16 must be installed on both the BIE and AP tiers.

Microsoft .NET Framework: MooD 16, BIE, and AP all require Microsoft .NET Framework 4.6. This framework may already be installed, but, if not, it will be installed with the products.

Microsoft Office: On the BIE and AP tiers, Microsoft Excel 2010 or later may be required if your solution uses the Excel import synchronization activator configured to run in **Excel Native** mode.

Business Integration Engine (BIE)

Install a Database Engine

Install Microsoft SQL Server as the Database Tier

See the *MooD 16 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.

Here are some quick steps if you simply want to test connectivity or perform a local installation, rather than an installation for full deployment. Typically, customers will have a dedicated database administrator and infrastructure with multiple SQL Server instances available for use.

1. Launch the SQL Server setup program
2. Select "SQL Server Feature Installation", and click "Next"
3. In "**Feature Selection**", tick the following:
    a. "Instance Features>Database Engine Services"
    b. "Full-Text Search"
    c. Under "Shared Features", tick:
        i. "Management Tools – Basic"
        ii. "Integration Services" (only install if using SSIS packages)
4. Click "Next", until at "Server Configuration"
5. Click "Use the same account for all SQL Server services", and select "NT AUTHORITY\SYSTEM", then click "Next". (Note: Moving away from Local System Accounts).
6. Select "**Mixed Mode**" Authentication, and enter a "**sa**" password
7. Click "Add Current User", and click "Next/ Install"
8. Be sure to remember the SA password that you choose.
9. If the BIE server and SQL Server are on different machines, 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.
10. Configure SQL Server to accept TCP/IP connections;
    a. From the Start menu, open SQL Server Configuration Manager.
    b. In the right-hand panel, browse to the protocols for your SQL Server instance.
    c. In the right-hand panel, right-click **TCP/IP**.
    d. Choose **Enable**.
    e. Stop and start the SQL Server service.

Refer to your Microsoft support team for more assistance.

Install and Licence MooD 16

Perform an installation of MooD 16 (Business Architect). Right-click the MooD 16 icon on the desktop and select **Run as Administrator**; The option to install a Licence will be displayed. Ensure the option is set to make the licence available to everyone who uses this computer. The licence must also enable Active Publisher use.

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

Configure Repository Server and Create or Restore a Repository

Start MooD 16 Repository Manager, add the Database Engine Server and create or restore a repository. See the Repository Manager Guide for details. The next section gives some additional guidance for SQL Server.

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.

SQL Server

Key points and guidance for configuring a quick test repository, with the database we configured 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, when you add a server, on the **Add Server** dialog box, make sure **Security** is set to use **Native SQL 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, on the **Add Repository** dialog box, 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.
- Once 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.
- 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.

Install the Business Integration Engine (BIE)

Install the Business Integration Engine:

1. Using the MooD Media, navigate to the **MooD Active Enterprise/Business Integration Engine** folder and run the **setup.exe** file.
2. Review and accept the licence agreement.
3. Select an installation folder for BIE (the default is recommended), and ensure it is available to everyone who uses the computer.

NOTE:

- If the BIE server and Active Publisher server are on different machines, configure your firewall to open a port so that Active Publisher can connect to the BIE. By default, this is port 50016, and is configurable in the BIE's **config.xml** file.

Connect a Repository in Business Integration Engine (BIE)

1. It is advisable to validate the repository for publishing (but not required);
    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. It is advisable to 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**.
3. Ensure BIE service is started;
    a. Navigate to **Control Panel** > **Administrative Tools** > **Services**.
    b. Locate and start the service named **Business Integration Engine 16**.
    c. Alternatively, run this command from a command line (run "as Administrator");

    For MooD 16.082 or later:

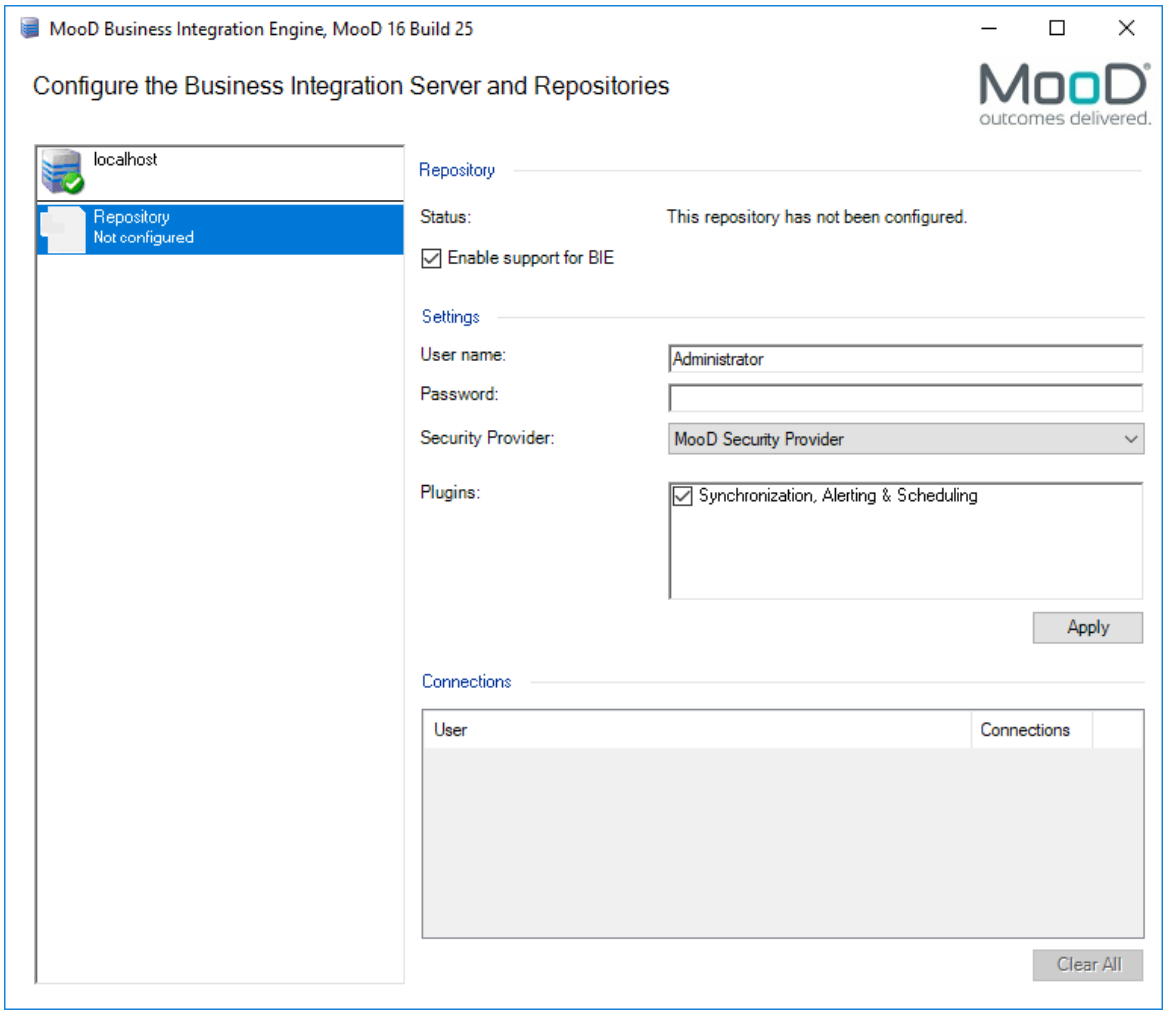
```
net start MooDBIE_16
```

    For MooD 16.076 or earlier:

```
net start bie_16
```

4. Use the BIE Manager to connect to the desired repository;
    a. Open the BIE Manager. Use **Start** > **All Programs** > **MooD 16** > **Business Integration Engine Manager**.
    b. Ensure the BIE Server and BIE Port number boxes are correct, and then click **Connect**.
    c. Select the required repository and then select **Enable support for BIE**. Enter the repository administrator username and password, choose a security provider from those installed, select the plug-in(s) you wish to enable for the repository, and then click **Apply**.

    It is possible to install other security providers. See the Install a New Security Provider section on page 16 for details.



d. The repository status will change to **The repository is ready**.

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 7 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 item to install IIS with default features enabled. The following additional sub-features must also be enabled:
    a. Web Management Tools > IIS 6 Management Compatibility > IIS 6 Metabase and IIS 6 configuration compatibility
    b. World Wide Web Services > Application Development Features > ASP.NET
3. For installations utilising Windows integrated authentication, the following is also required:
    a. World Wide Web Services > Security > Windows Authentication

Windows 8.1 / 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. 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. Web Server > Security > Windows Authentication

Windows Server 2008 R2 / Windows Server 2012 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

    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

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 section 0.

Installation

1. Using the MooD Media, navigate to the **MooD Active Enterprise/Active Publisher** folder and run the **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. When you configure IIS, you can use this pool, or add additional pools.
4. Set **Site** and **Virtual Directory** appropriately. **Virtual Directory** is used to 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 **MyRepository**, you would access Active Publisher from **http://WebServer/MyRepository**. 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. Open Internet Information Services (IIS) Manager (run **inetmgr.exe**).
    a. Navigate to **Application Pools** and create a new one (right click and select **Add Application Pool**). Ensure that **.NET Framework version 4.0.*xxxxx*** is selected.
    b. Right click on the new application pool and click **Advanced Settings**. Under **Process Model**, set **Identity** to **LocalSystem**. If running on a 64-bit edition of Windows, also set **Enable 32-bit Application** to **True**. (Note, for security reasons you may wish to move away from using LocalSystem, please contact our Support Department for information on how to do this).
4. Assign Active Publisher to the new application pool.
    a. In Internet Information Services (IIS) Manager find the Active Publisher virtual directory (under **Sites** > **Default Web Site**).
    b. Right click the virtual directory and select **Manage Application** > **Advanced Settings**. Set the **Application Pool** to the one created in 1.

Configure Integrated Authentication

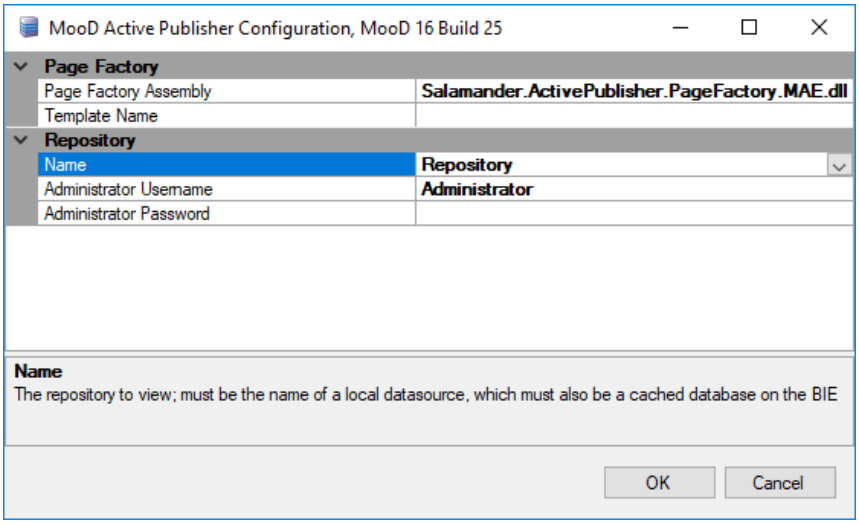
1. If integrated authentication is to be used, it must be enabled for the virtual directory.

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.

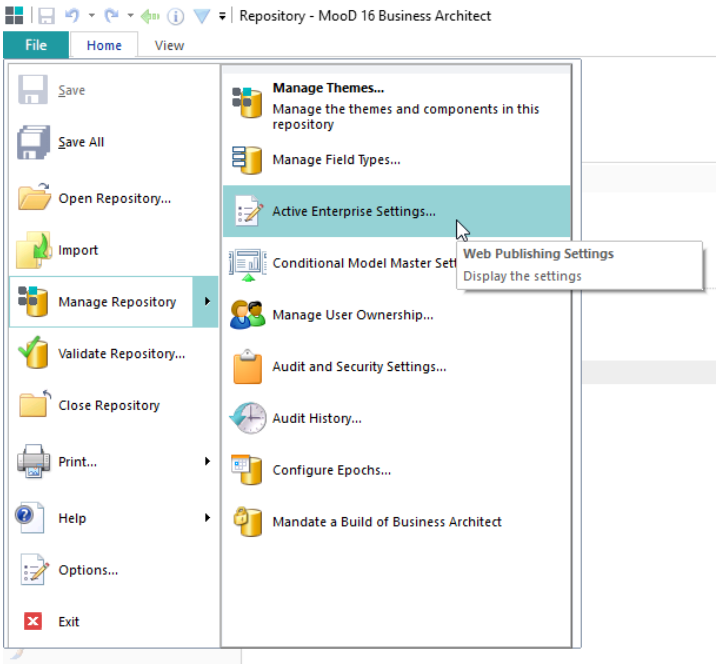
You will also need to ensure that your repository is configured to use Windows Authentication. See Section 0 Using Windows Authentication for details.

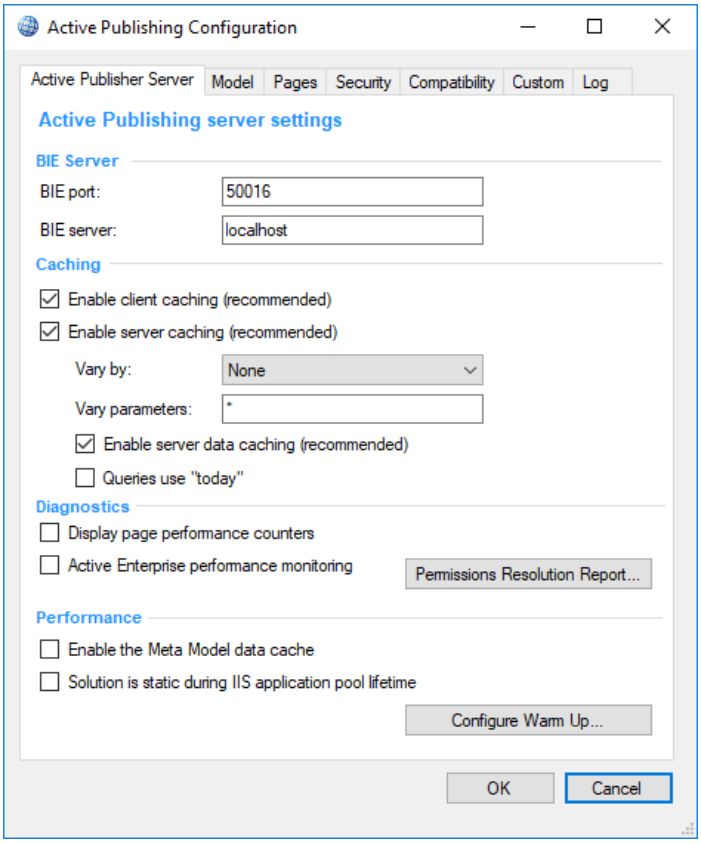
Configure Active Publisher

1. In the folder **\inetpub\wwwroot\<*Virtual Directory*>\bin**, you will find the application **ConfigureActivePublisher.exe**. Double-click this to run the Active Publisher configuration tool (note that this program modifies the **ActivePublisher.config** file in the parent folder).



2. 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).
3. The remaining settings can be accessed from within Business Architect. Click File on the ribbon, under **Manage Repository**, click **Active Enterprise Settings**.





4. Under **BIE Server**, set the **BIE Port** and **BIE Server** settings. If the BIE is installed on the same machine, the default settings (**50016** and **localhost**) should be fine.
5. Click **OK** to accept the changes.

6. 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/ActivePublisher16/

Appendices

Troubleshooting

Installing Active Publisher does not complete

If, when installing Active Publisher, the installer appears to complete before rolling back and failing with the message “The installer was interrupted before MooD 16 Active Publisher could be installed”, check that the **correct version** of **ASP.NET** is installed with IIS. For Windows 8+/Server 2012+, **ASP.NET 4.x** (e.g. ASP.NET 4.5) is required.

Business Integration Engine will not start

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

Business Integration Engine reports that it is not licensed

If, when connecting to the Business Integration Engine using the Business Integration Engine Manager, 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.

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.

Install a New Security Provider (optional)

The security providers are pluggable additions to Business Integration Engine and Active Publisher that control how the web users log into the Active Publisher website, and control the view and edit permissions on the content.

They are fully pluggable, and installation instructions should be included with the appropriate installation files. Contact your distributer or MooD International support for further details.

Installing Additional Active Publisher Instances

It is possible to run multiple Active Publisher web sites using a single Business Integration Engine installation, up to a recommended maximum of six repositories per server (depending upon the size and complexity of the data and web pages, and the user usage patterns).

Adding a new Active Publisher Instance

1. Follow the steps in section 6 to cache the repository in BIE.
2. 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:

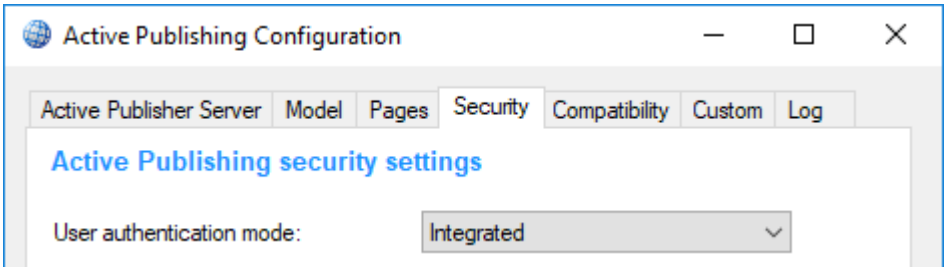
```
<sessionState cookieName="ActivePublisherSession2" mode="InProc"
stateConnectionString="tcpip=127.0.0.1:42424"
sqlConnectionString="data source=127.0.0.1;Trusted_Connection=yes"
cookieless="false" timeout="20" regenerateExpiredSessionId="true" />
```

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

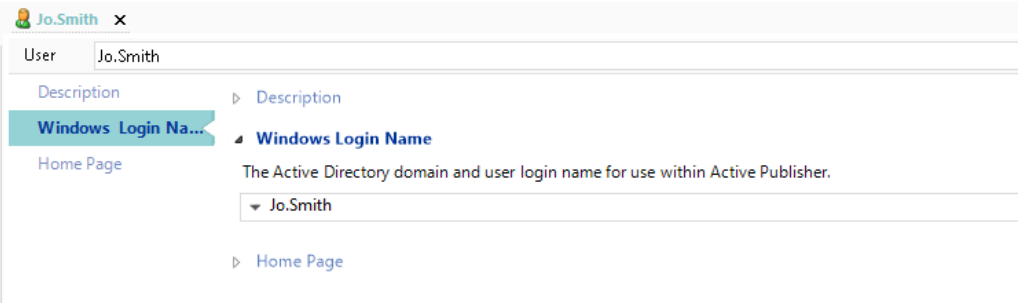
Using Windows Authentication

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. On the ribbon, on the **Web** tab, click **Settings**.
3. In the **Active Publishing Configuration** dialog box, click the **Security** tab.
4. Set **User Authentication Mode** to **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 **Windows Login Name** setting.



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 BIE performance and reduce BIE synchronization execution recycling where large models or matrices are used.

The following registry keys can be created under

[HKEY_LOCAL_MACHINE\SOFTWARE\Salamander\Business Integration Engine\16]

- **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 keys can be created under

[HKEY_LOCAL_MACHINE\SOFTWARE\Salamander\Active Publisher\16]

- **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 solution (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.

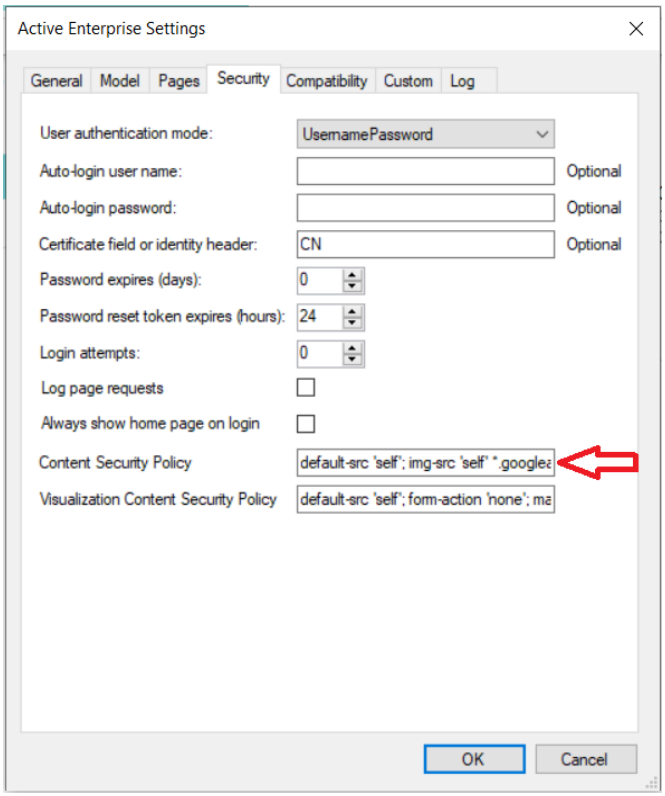
Within: `<system.webServer><httpProtocol><customHeaders>`

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

With version 16.085 the specification of this policy has been moved to within the solution.

If a solution-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 solution-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.



Note that following any modification to the Content-Security-Policy it is a good idea to test the site, particularly pages which include uploads, external visualizations or XHTML panels to ensure that they still function correctly. The Content-Security-Policy may need modification if it is blocking some required functionality.

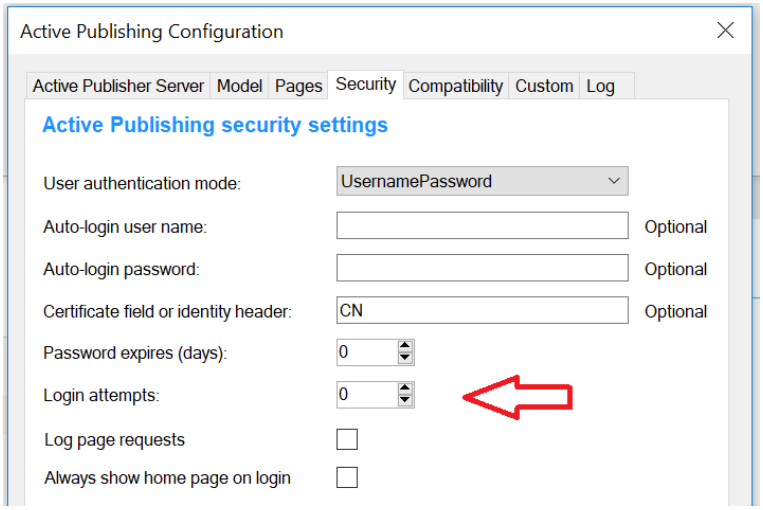
Hardening of the solution

Various changes can be made to a solution to ensure it is more secure.

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.

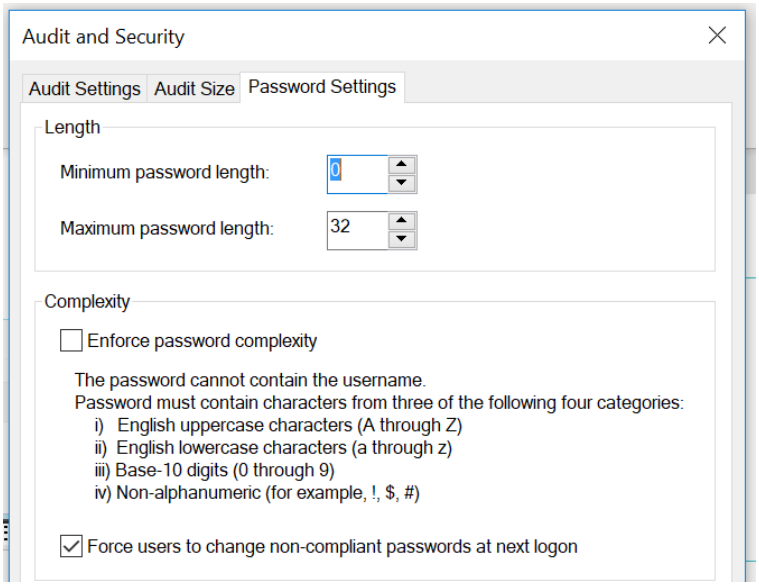
Do this in Business Architect in Active Publisher Settings on the Security tab:



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:



Setting password complexity is currently considered to be of less value than password length, but may be required by the customer's security standards.

Ensure the permissions model is robust

The permissions model 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.

Using 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 (n.b. 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/

Note:

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

As such, please ensure that you have:

- a version of the 32bit SQL Server Native Client Driver that supports TLS (greater than 2009.100.6537.00 - found in ODBC Data Source Administrator 32bit)
- At least .NET 4.5.2
- SQL Server 2016 or above.

Tip: Confirm that your Web Server, Sql Server and desktop clients have the appropriate versions of the SQL Native Client Driver.

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.

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