blueprint ®

Installation Guide
Blueprint

2020-11-20

blueprint

Overview

This guide walks you through the Blueprint installation process. The same process can be followed whether you are installing for the first time, or are upgrading an existing Blueprint deployment.

Activation Keys

Before you begin, ensure that you have your activation key. If you don't have one, please submit a case to Blueprint Support using the Blueprint Community at https://community.blueprintsys.com.

Ensure that your environment meets the minimum system requirements.

System requirements

Please visit our documentation site to view detailed system requirements:

https://blueprintsys.helpdocs.io/article/5669afnmex-system-requirements

Requirements for ALM integrations

There are additional requirements for environments licensed to integrate bi-directionally with ALM systems. This functionality is separate from native integrations and is facilitated by an Integration partner.

The following requirements should be met for environments licensed to integrate:

	ALM integrations server (1 Integration Server)
Hardware requirements (1000-user deployment)	2.5 GHz or faster 2 64-bit CPU cores 6 GB RAM minimum 50 GB HDD space minimum

> **Note:** If you are hosting the ALM integrations server on the same server as the web application or database, simply add the specifications above to the applicable server specifications outlined in Web application server and database server requirements.

IIS server configuration requirements

There are a number of Roles, Features and Role Services that must be enabled in the IIS *Add Roles and Features Wizard* before you can use Blueprint.

SERVER ROLES
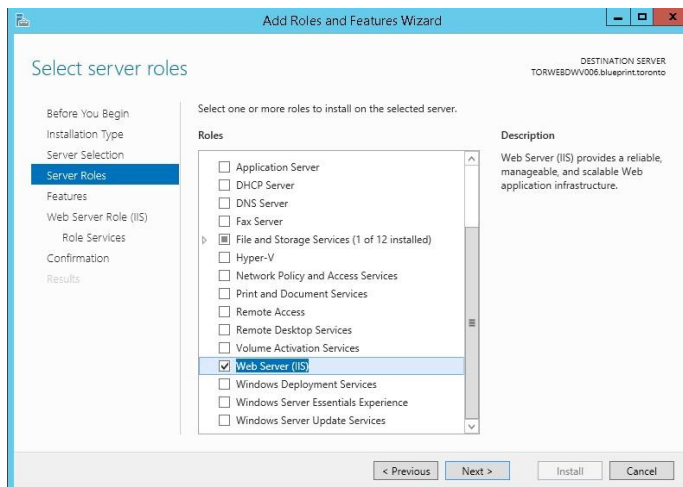
Within *Server Manager > Manage > Add Roles and Features*, the following Role must be enabled for Windows Server 2012 and Windows Server 2016:

- Web Server (IIS)
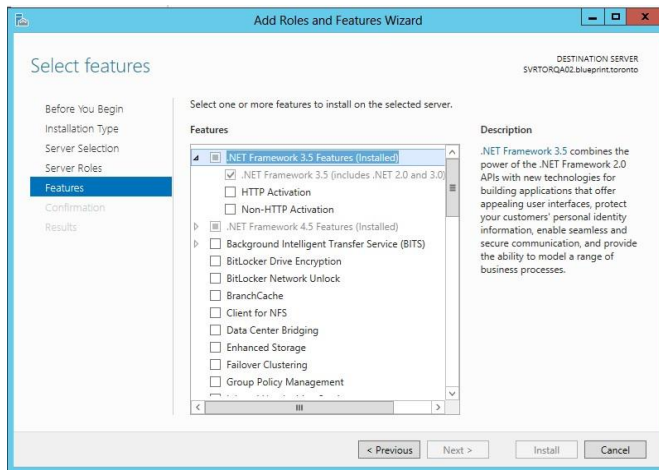
The following Features must be enabled for Windows Server 2012 and Windows Server 2016:

- .NET Framework 3.5 Features
    - .NET Framework 3.5
    - HTTP Activation
    - Non-HTTP Activation
- .NET Framework 4.5 Features
    - .NET Framework 4.5
    - ASP.NET 4.5
    - WCF Services
        - HTTP Activation
- Windows Process Activation Service
    - Process Model
    - .NET Environment 3.5
    - Configuration APIs
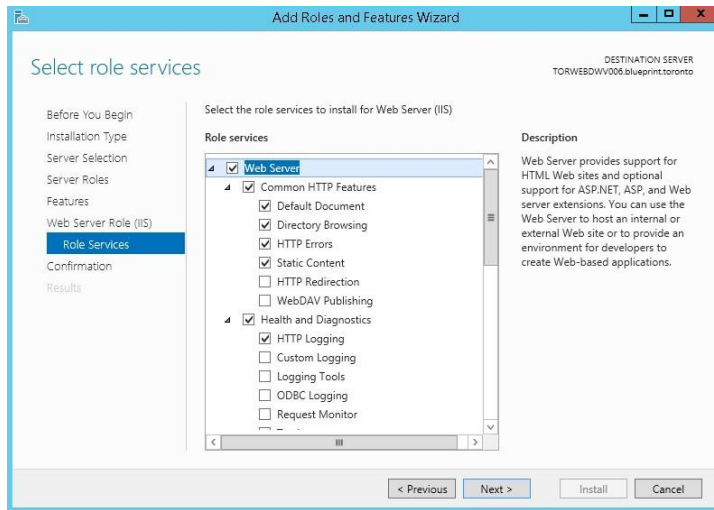
The following Role Services must be enabled for Windows Server 2012 and Windows Server 2016:

- Web Server
  - Common HTTP Features
    - Default Document
    - Directory Browsing
    - HTTP Errors
    - Static Content
    - HTTP Redirection
  - Health and Diagnostics
    - HTTP Logging
    - Request Monitor
  - Performance
    - Static Content Compression
    - Dynamic Content Compression
  - Security
    - Request Filtering
    - Basic Authentication
    - Digest Authentication
    - IP and Domain Restrictions
    - Windows Authentication
  - Application Development
    - .NET Extensibility 3.5
    - .NET Extensibility 4.5
    - ASP
    - ASP .NET 3.5
    - ASP .NET 4.5
    - ISAPI Extensions
    - ISAPI Filters

- Management Tools
  - IIS Management Console
  - IIS Management Scripts and Tools

> **Note: World Wide Web Publishing Service** must also be started within *Services* (Control Panel > Administrative Tools).

User requirements

The following diagram illustrates the Blueprint installation user requirements:
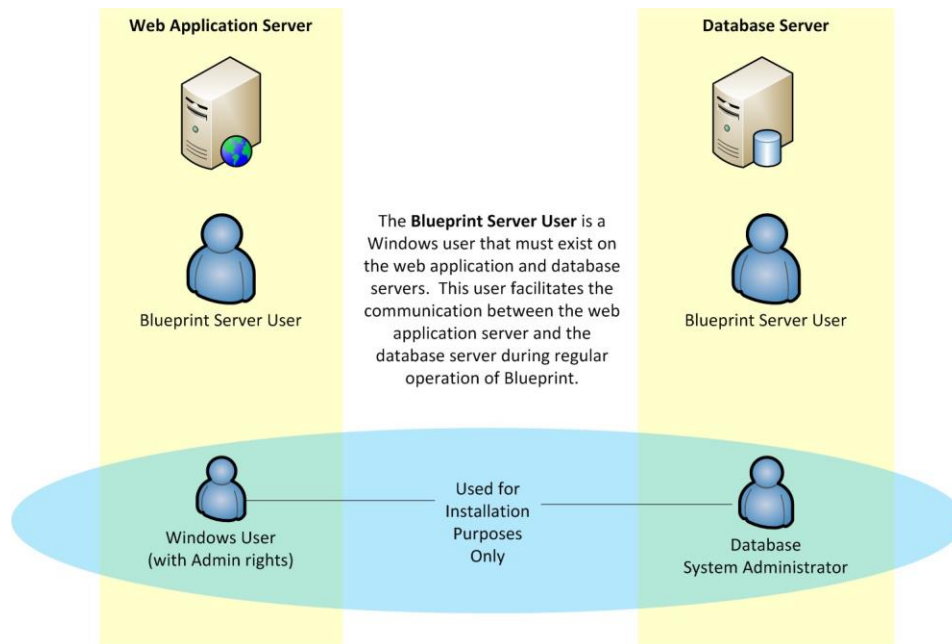
Blueprint Server User

The *Blueprint Server User* is a service account for the application pool connection from IIS to the database.

> **Note**: The Blueprint Server User is required for everyday Blueprint operation.

The following requirements must be met:

- This user account must be defined as a corporate *domain* user (that is, domain_name\username) or a local server account (that is, ApplicationPoolIdentity).
- This user account must exist on *both* the web application server and the database server.
- This user account can have standard user privileges and does not need to be an administrator. To enable Blueprint server logging, the Blueprint Server User must have **modify+read+write** permissions on the Blueprint program data folder (example: **C:\ProgramData\Blueprint Software Systems**). You can grant these permissions by including the Blueprint Server User in a group that already has access to the folder, or by granting the permissions directly to the user.

Windows User

The *Windows User* is a standard windows login which is used to install the Blueprint application. This user should have local Administrator privileges to the web application server (that is, IIS server) where Blueprint is to be installed. The *Windows User* account is required for installation purposes only, and is not used under regular operation of Blueprint.

Database System Administrator

The *Database System Administrator* is an account defined within the SQL server database. This account must have administrator privileges in order to create and update tables within the database server. This account is typically a domain account. However, if the database server is not part of a domain, then the default database administrator account is "sa" .

During installation, you must provide the credentials of this *Database System Administrator* account so the Blueprint installer can create the database and grant appropriate permissions to the *Blueprint Server User*. The *Database System Administrator* account is required for installation purposes only, and is not used under regular operation of Blueprint.

Before you begin

Enabling Semantic Search

Blueprint uses Semantic Search and requires that it is installed and enabled on the relevant SQL Server instance. Additionally, Semantic Search requires that the semantic language statistics database also be installed and registered.

Verify that Semantic Search is installed

Query the `isFullTextEnabled` property of the `SERVERPROPERTY` function:

```
SELECT SERVERPROPERTY('IsFullTextInstalled');
GO
```

If the returned value is "`1`", Semantic Search is installed, and you can skip the next section. If the returned value is "`0`", proceed to the next section.

Installing Semantic Search

If the returned value is "`0`" and not installed, go to your SQL Server setup page, and enable the *Full-Text and Semantic Extractions for Search* option in the *Features* section.

Once this has been done, proceed to the next section.

Verify that the semantic language statistics database is installed

Query the catalog view `sys.fulltext_semantic_language_statistics_database`:

```
SELECT * FROM sys.fulltext_semantic_language_statistics_database;
GO
```

If the returned value is information about the database, this means it is installed, and the Semantic Search functionality is fully enabled. You have completed this procedure and can skip the next section. If the returned value is "`0`", proceed to the next section.

Installing the semantic language statistics database

This section summarizes how to install, attach, and register the semantic language statistics database.

1. Download the appropriate installer package from the Microsoft Download Center:

    - SQL Server 2014: https://www.microsoft.com/en-US/download/details.aspx?id=42296

    - SQL Server 2016: https://www.microsoft.com/en-us/download/details.aspx?id=52681

2. Run the **SemanticLanguageDatabase.msi** installer package.
3. Move the extracted MDF database file and LDF log file to the desired location.
4. Remove the read-only permission setting for the MDF file.

ATTACHING THE DATABASE

Attach the database to your SQL Server instance using Management Studio, or by calling CREATE DATABASE with the FOR ATTACH syntax:

```
CREATE DATABASE semanticsdb
    ON ( FILENAME = 'C:\Microsoft Semantic Language
Database\semanticsdb.mdf' )
    LOG ON ( FILENAME = 'C:\Microsoft Semantic Language
Database\semanticsdb_log.ldf' )
    FOR ATTACH;
GO
```

By default, the name of the database is semanticsdb.

REGISTERING THE DATABASE

Call the stored procedure sp_fulltext_semantic_register_language_statistics_db, providing the name assigned to the database when you attached it in the previous step (by default, semanticsdb):

```
EXEC sp_fulltext_semantic_register_language_statistics_db @dbname =
N'semanticsdb';
GO
```

For more information about setting up Semantic Search, please refer to https://docs.microsoft.com/en-us/sql/relational-databases/search/install-and-configure-semantic-search.

Choosing a Message Broker Service

By default, application messaging is managed by SQL Server's Service Broker feature and requires no further configuration. For larger Blueprint deployments, it is recommended that RabbitMQ is used instead. During the installation process, the Blueprint Configuration Wizard gives the option to provide information about your RabbitMQ server.

If you plan on using RabbitMQ in place of Service Broker, ensure it is installed and running before installing Blueprint.

Installation information can be found at the RabbitMQ downloads and installation page.

Installing Blueprint from a previous version

This section is applicable if you have already installed Blueprint and you want to upgrade to a newer version.

Backing up data from a previous deployment

It is strongly recommended that you back up your Blueprint data prior to starting the upgrade.

To back up your data before performing an upgrade:

1. Stop the Blueprint application pool and Blueprint web site.

   > **Note**: Your Blueprint application pool and Blueprint web site may have different names, depending on what you chose during installation.

2. Stop any installed components, including:

   - Job services
   - the HP ALM application pool and web site (formerly known as HP QC)

   > **Note:** This step only applies if any job services or the HP ALM web site have been installed.

3. Back up the following data:

   - Blueprint database
   - Blueprint website, including:
       - the **web.config** files
           - Blueprint web.config
           - AdminStore web.config
           - FileStore web.config
           - AccessControl web.config
           - ConfigControl web.config
       - logging configurations (**Logging.config** files for the above config files)
       - any customized logo files (for example, **customlogo.png**)
       - any custom dictionary files (**dictionary.dct**)
   - **JobExecutorService** folder. This includes the **BluePrintSys.RC.JobExecutor.exe.config** for each job service that has been installed. It also includes the **BluePrintSys.RC.JobExecutor32.exe.config** if you have configured 32-bit job services to support HP Quality Center

Determining your upgrade path

Your upgrade path depends on which version of Blueprint you are currently using:

- **7.3 and later:** Proceed to next section to begin installing the latest version of Blueprint.
- **7.2:** Since the installation process was redesigned for version 7.3, you first will need to uninstall Blueprint from the *Programs and Features* Control Panel. After Blueprint has been uninstalled, proceed to the next section and perform a new installation.
- **7.1 or earlier:** You will first need to upgrade to version 7.2. The specific steps and amount of downtime required to complete this process depend on aspects of your environment such as the size of your database, the database server version, and which specific version of Blueprint you are using. Contact Technical Support to get more information on the scope of the upgrade process.

Post-upgrade steps

After upgrading, to ensure graphical assets in some features (such as Impact Analysis) are updated correctly, it is recommended that your end users clear their browser cache and log in again.
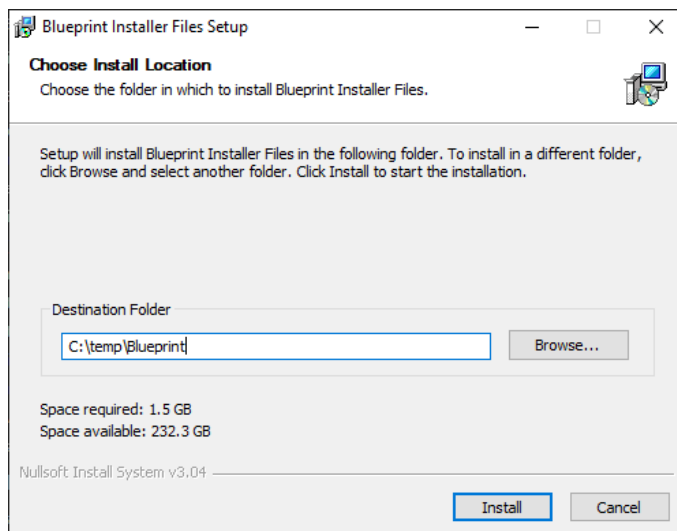
Installing Blueprint

- Step 1: Extract the installation files
- Step 2: Create the Blueprint settings file
- Step 3: Install Blueprint
- Step 4: Activate Blueprint
- Step 5: Blueprint instance setup
- Step 6: Blueprint client setup

Step 1: Extract the installation files

The recommended installation procedure is to use the Blueprint Configuration Wizard to create a Blueprint settings file that will be used with an installation script.

Run the `BlueprintInstallerFiles` executable file to extract the installer files.

The following Installer Files Setup Wizard appears:

> **Note**: The file extraction location should be different from the where Blueprint will be installed.

Click **Install** to extract the files.

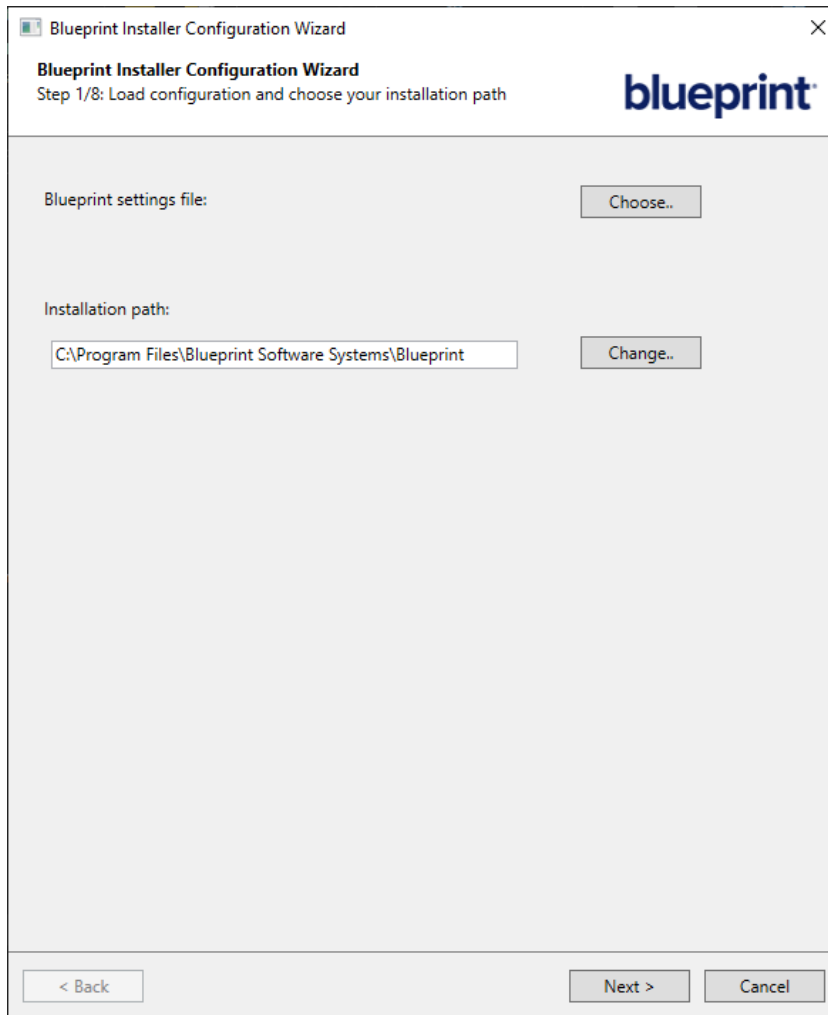After this process is complete, click **Close**.

Step 2: Create the Blueprint settings file

Next, you will use the configuration wizard to create a configuration file that is used to install Blueprint:

- In File Explorer, navigate to the directory where you ran the `BlueprintInstallerFiles` executable file.
- Run the `BlueprintSys.RC.Installer.Configuration.Wizard.exe` file to begin configuring your Blueprint installation.

This wizard will not perform any system changes but will create a configuration file that will be used later in the installation process.

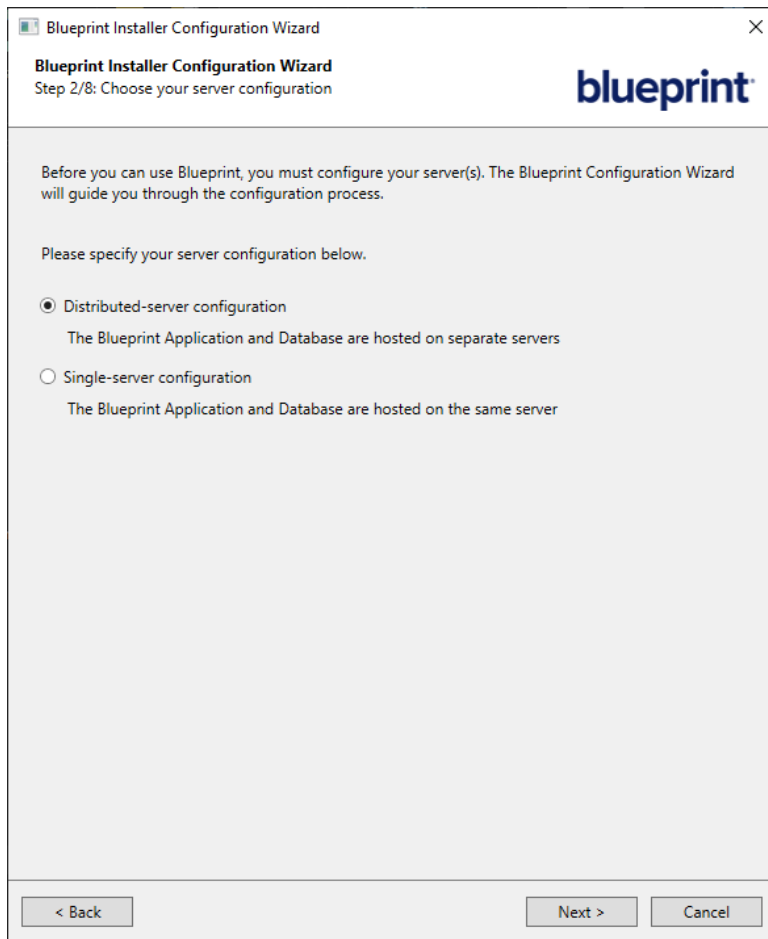In the first wizard dialog, enter the Blueprint **Installation path**:

The Blueprint Configuration Wizard dialog allows you to choose your desired configuration:

Note: You can also use a previously created **Blueprint settings file** as a starting point in the wizard.

Select one of the following options and then click **Next**:

- **Distributed-server configuration**: This option allows you to host the Blueprint application and database on separate servers. This is the typical configuration.
- **Single-server configuration**: This option allows you to host the Blueprint application and database on the same server.

Application Configuration

The Application (IIS AppPool and Site) configuration dialog looks like this:

Complete the following fields and then click **Next**:

- **Specify the Site name**: Define the name of the main Blueprint IIS Site. Example: Blueprint

- **Port Number**: Define the port number of the main Blueprint IIS Site. Example: 8080

- **Auxiliary services port Number**: Define the port number used by the Blueprint Auxiliary site. Example: 9101

- Specify the Binding Type:

    - **Use HTTP Binding Host Name**: Optionally specify a name for the HTTP binding if you want to run Blueprint over HTTP.

    - **Manually replace the HTTP binding with HTTPS**: Select this checkbox if you want to run Blueprint over HTTPS instead of HTTP.

        > **Note:**This option requires that you manually create one or more HTTPS bindings for the primary website in IIS Manager, then remove the original HTTP binding. You can also use both HTTP and HTTPS bindings; see Supporting HTTP and HTTPS bindings in the Appendix.

- Specify the Application Pool Identity:
  - **Built-in Account**: Selecting this account means the Blueprint application pools in IIS will run with the `ApplicationPoolIdentity` Identity. Note that the option to use the local account is only available for single-server installations.
  - **Custom Account**

  > **Note**: The Custom Account refers to the user account that was outlined in the User Prerequisites section of this document. Example: acme\rrunner.

  - **Username**: Specify the name of the Blueprint Server User account that has appropriate permissions on both the application and database servers. During the installation, you will be prompted for the password.

HP ALM Legacy Support

The *Blueprint Application Configuration Wizard* dialog gives you the option of enabling legacy support for versions 12 and earlier of HP ALM:

Configure HP ALM legacy support or deselect **Enable HP ALM legacy support**.

Specify the account to run Blueprint Windows services:

- **Windows Services Account**: If you choose *Windows Services Account* authentication, enter your Blueprint credentials.
- **Local System**
- **Local Service**
- **Network Service**

> **Note**: This account must have access to the database server on which the Blueprint database will be installed. The local account options are only available for single-server installations.

Database Configuration

The Database configuration dialog looks like this:

Complete the following fields and then click **Next**:

- Database installation settings: For new installations, choose whether to install all Blueprint databases as a single database.

  The default distributed-database option accommodates a large deployment that will have many users contributing to many large projects. It can maintain performance by allowing databases to be deployed on different servers.

  A single database is simpler to maintain but is less scalable in performance compared to the distributed-database option.

  > **Important**: This option is available only for new installations, and pre-existing database deployments cannot be changed during upgrade installations. Distributed databases cannot be merged, and single databases cannot be separated.

- **Provide the location of the Database Server**: The database server must be provided in the following format: [server_name]\[instance_name]

Example: DBSERVER\INSTANCE01

- **Specify the name of the Database**: The database must not already exist.

  Example: Blueprint

- System Administrator Credentials: Choose whether you wish to authenticate using *Windows authentication* or *Database* authentication.

> **Important**: This user must be a Database System Administrator (SA). This allows the installer to create the new database and grant permissions to the database so the web application server can access the database. The SA credentials are not stored anywhere in the system. The SA user account is only required for installation purposes and is not used during normal operation of the application. During normal operation of Blueprint, the Blueprint Server User account (example: acme\rrunner) is used to facilitate communication between the web application and database servers.

- **Windows authentication**: If you choose windows authentication, the installation script will automatically use the user that is currently logged in when the script is run. You must ensure that the user has SA privileges on the database server.
- **Database authentication**: If you choose database authentication, specify the username of an account that has SA privileges on the database server. The password will be requested at the time of installation.

AdminStorage Configuration (Distributed-Server and Distributed-Database Configuration)

If you are performing a distributed-server and distributed-database configuration, you have the option of setting up the AdminStorage database on another server. The AdminStorage configuration dialog looks like this:

By default, the AdminStorage database is set up on the same server defined in the previous wizard dialog. You can click **Next** to accept this, or you can first click Set a different server for AdminStorage database and complete the following fields:

- **Provide the location of the AdminStorage Database Server**: The database server must be provided in the following format: [server_name]\[instance_name]
  Example: DBSERVER2\INSTANCE01
- System Administrator Credentials: Choose whether you wish to authenticate using *Windows authentication* or *Database* authentication.

> **Important**: This user must be a Database System Administrator (SA). This allows the installer to create the new database and grant permissions to the database so the web application server can access the database. The SA credentials are not stored anywhere in the system. The SA user account is only required for installation purposes and is not used during normal operation of the application. During normal operation of Blueprint, the Blueprint Server User account (example: acme\rrunner) is used to facilitate communication between the web application and database servers.

- **Windows authentication**: If you choose windows authentication, the installation script will automatically use the user that is currently logged in when the script is run. You must ensure that the user has SA privileges on the database server.
- **Database authentication**: If you choose database authentication, specify the username of an account that has SA privileges on the database server. The password will be requested at the time of installation.

Message Broker Configuration

By default, application messaging is managed by the SQL Server Service Broker, and requires no further configuration.
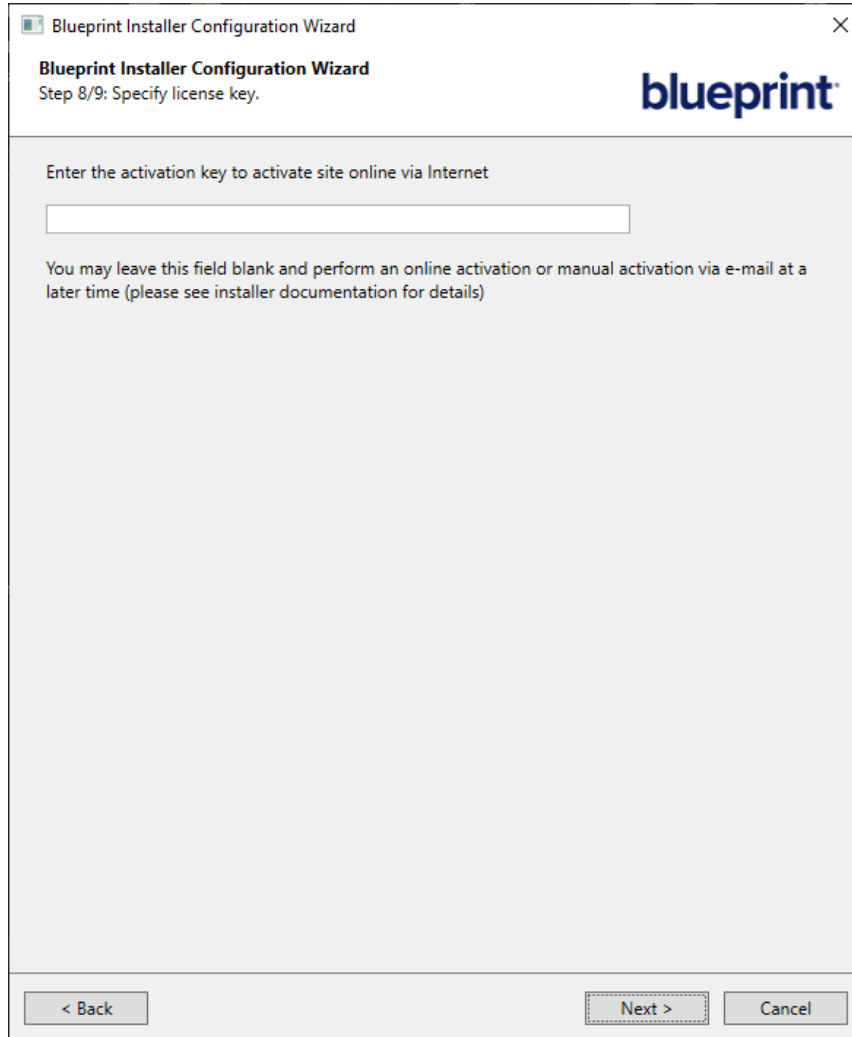
If you have an existing RabbitMQ installation that you would like you use instead, provide the host, virtual host, and username of an administrator account:

blueprint®

Activation Key Entry

If you wish to activate Blueprint immediately upon installation, and you have an activation key, you can enter it now:

Note: Multiple keys can be entered as comma-separated values.

Generate Blueprint Setup File

Click **Finish** to generate the configuration file:
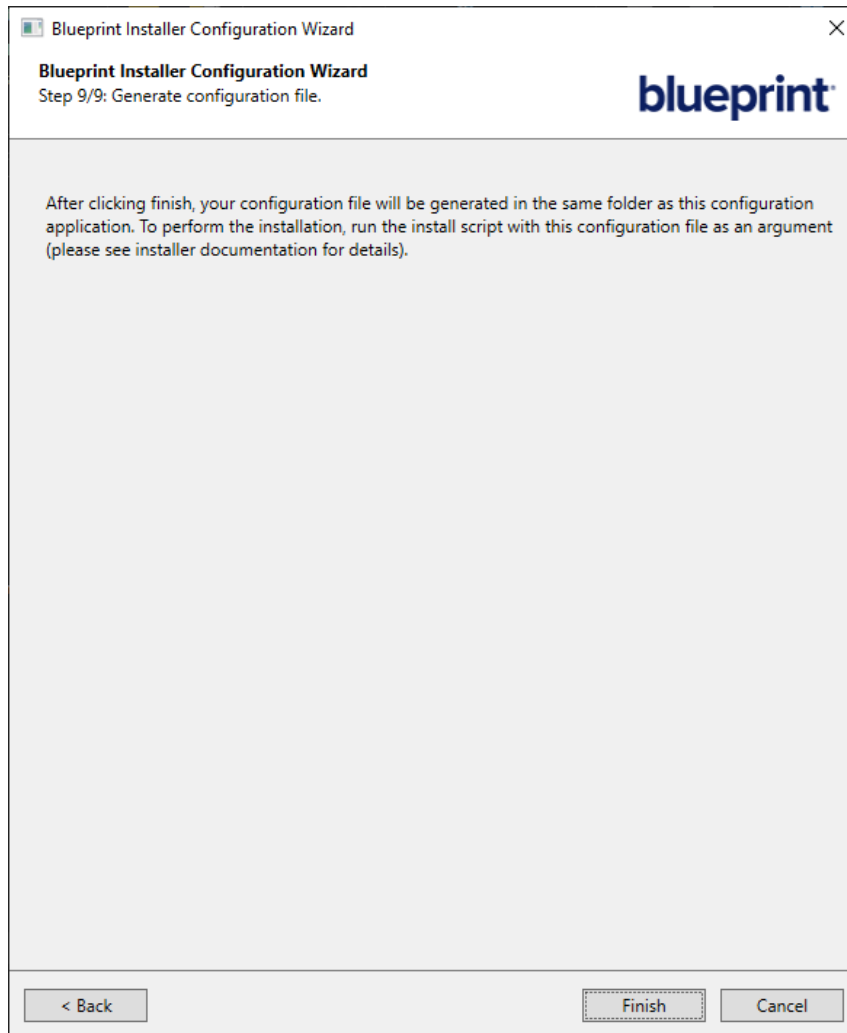
The file will be created in the same folder as the
BlueprintSys.RC.Installer.Configuration.Wizard.exe file:
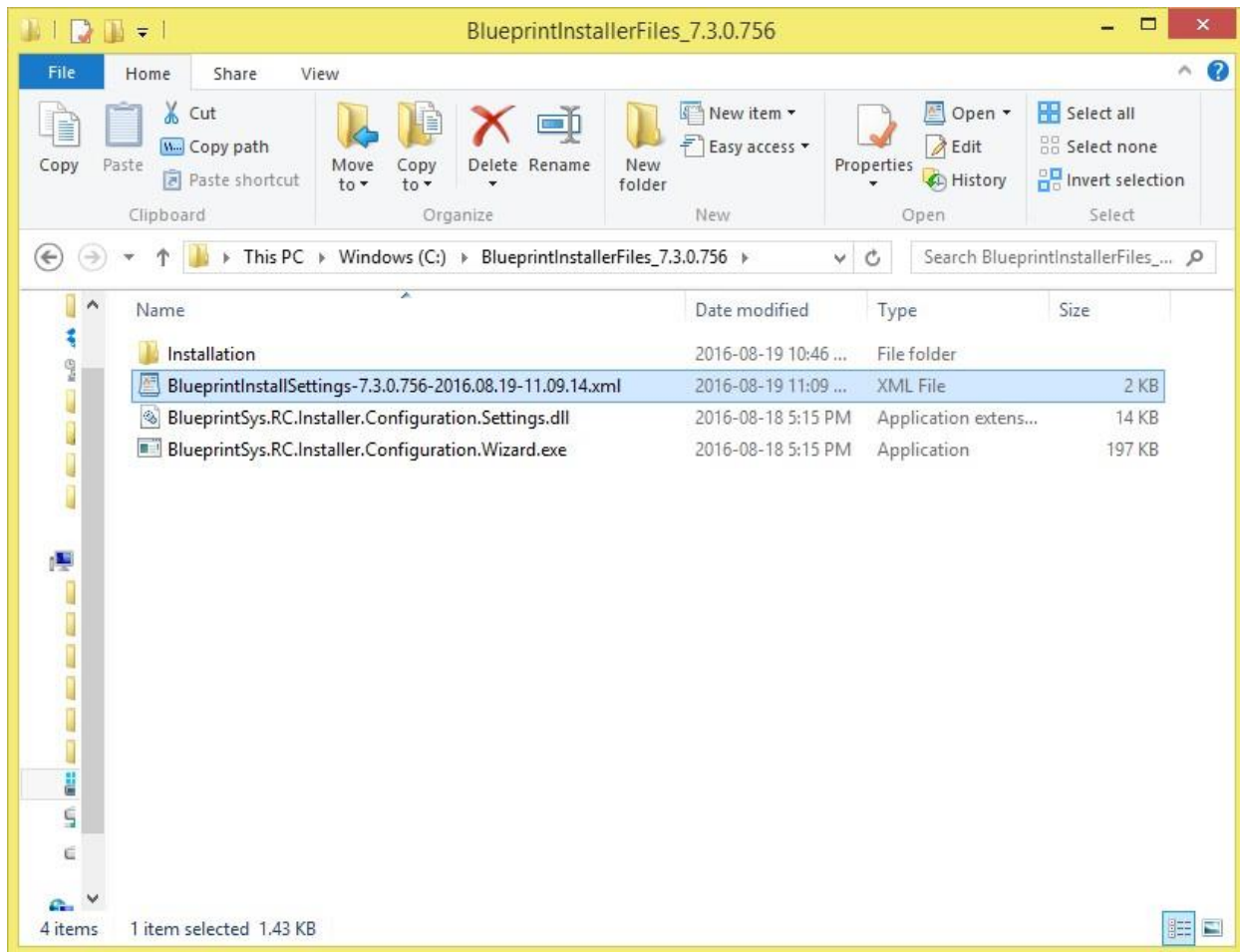
The file name uses the following template: `BlueprintInstallSettings-<VER>-<TIME>.xml`, where `VER` is the Blueprint version being installed, and `TIME` is the date and time stamp when the file was created.

Step 3: Install Blueprint

Next, install Blueprint by running the installation script. This script will use the Blueprint setup file you created using the configuration wizard.

In Windows PowerShell (run as an administrator), navigate to the folder where the configuration file was created and run the following command:

```
.\Installation\Installer\Install-Blueprint.ps1 -
BlueprintInstallSettingsPath .\BlueprintInstallSettings-<VER>-<TIME>.xml
```

For example:

```
.\Installation\Installer\Install-Blueprint.ps1 -
BlueprintInstallSettingsPath .\BlueprintInstallSettings-8.3.0.756-
2017.12.22-11.09.14.xml
```

The settings in the configuration file will be validated. During this process, you will be prompted for various administrator account passwords that are required to install Blueprint (such as the application server, and database server).

> **Note:** There are optional parameters that can be used when running the installation script. See Blueprint Installation Script Parameters in the Appendix for more information.

Once the validation process is successful, installation will begin. (If any validation issues are encountered, the process will stop, and specific errors will be displayed.)

> **Note:** Semantic Search must be installed and enabled on the SQL Server instance, and a dependent semantic language statistics database must also be installed, attached, and registered. If these components are not present, you will be warned during the installation process. These are not required for the installation to continue; the Full-Text Search feature will be used instead, with a diminished experience. Although these components can be set up after installation, it is recommended that they are already present. For more information, see "Enabling Semantic Search" in this guide.

Replace HTTP Binding with HTTPS

If you want to run Blueprint over HTTPS instead of HTTP, after installation, you will need to manually create one or more HTTPS bindings for the primary website in IIS Manager, then remove the original HTTP binding. See Supporting HTTP and HTTPS bindings in the Appendix for more information.

Step 4: Activate Blueprint

If you provided a key when running the Blueprint Configuration Wizard, the installation script performs online activation.

If you elected to not provide a key, or connectivity was disabled when running the installation script, you will see the following message if you navigate to the Blueprint URL (example: http://localhost:8080/):

The application cannot be run without a valid license. Please contact your Administrator.

You must activate Blueprint using one of the following methods:

- Online activation via internet (recommended)
- Manual offline activation via Email

Complete the following steps to activate your Blueprint software online:

1. Launch the Blueprint Activation Wizard.

   The **BlueprintActivationWizard.exe** file is in a folder called **Setup**. The **Setup** folder is in the directory that you chose for installing Blueprint. For example, the default path is:

   `C:\Program Files\Blueprint Software Systems\Blueprint\Setup`

   The *Blueprint Activation Wizard* looks like this:
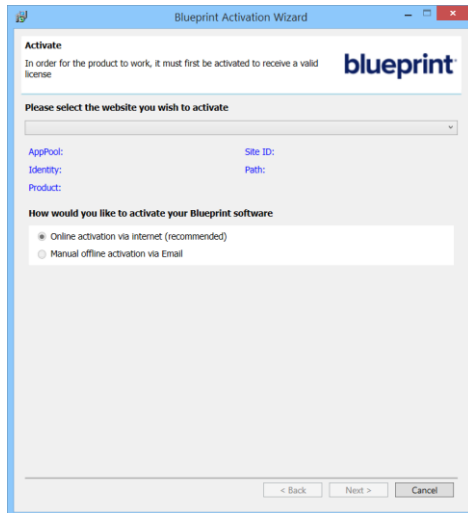
2. Select the website you want to activate by selecting an option from the drop-down list. The drop-down list only displays Blueprint sites.
3. Select the **Online activation via internet** option.
4. Click **Next**.

   The *Online Activation* screen appears:

5. Type your activation key into the space provided.
6. Click **Submit**.

A Success dialog appears after Blueprint is activated. Click **OK** to close the dialog.

7. Click **Done** to close the Blueprint Activation Wizard.

To verify that Blueprint was activated successfully, navigate to the Blueprint URL (example: http://localhost:8080/). If the software was activated successfully, you will see a login screen instead of the error message.

Continue to to setup the Blueprint instance.

Activating Blueprint using manual offline activation

Complete the following steps to activate your Blueprint software offline:

1. Launch the Blueprint Activation Wizard.

   The **BlueprintActivationWizard.exe** file is in a folder called **Setup**. The **Setup** folder is in the directory that you chose for installing Blueprint. For example, the default path is:

   `C:\Program Files\Blueprint Software Systems\Blueprint\Setup`

   The *Blueprint Activation Wizard* looks like this:
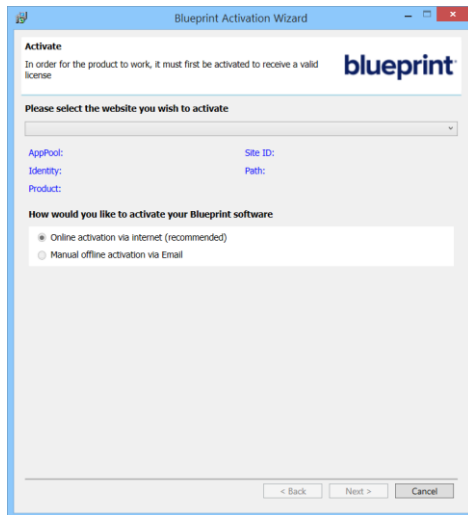
2. Select the website you want to activate by selecting an option from the drop-down list. The drop-down list only displays Blueprint sites.
3. Select the **Manual offline activation via Email** option.
4. Click **Next**.

   The *Offline Activation* screen appears:
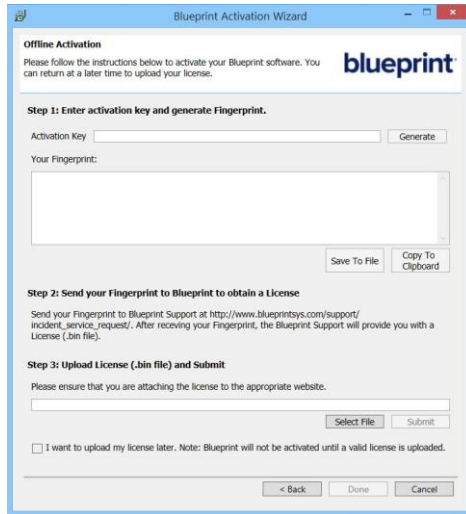
5. Type your activation key into the space provided.
6. Click **Generate**.

    A fingerprint is generated and displayed in the **Your fingerprint** field.

7. Send the generated fingerprint to Blueprint Support at https://community.blueprintsys.com/

    > **Tip**: Click **Save To File** or **Copy To Clipboard** so you don't have to type out the fingerprint manually.

    The Blueprint support team will provide you with a license (`.bin` file) after receiving your fingerprint. To close the Activation Wizard while waiting for your license file, click the **I want to upload my license later** option and then click **Done**.

    > **Note**: Blueprint is not activated yet.

8. After you have received your license (`.bin` file) from the Blueprint support team via Email, you must return to the *Offline Activation* screen to complete the activation. To return to the *Offline Activation* screen, launch the Blueprint Activation Wizard, select a Blueprint site, select the **Manual offline activation via Email** option and then click **Next**.

9. Click **Select File**.
10. Locate and select the `.bin` license file.
11. Click **Submit**.

    A Success dialog appears after Blueprint is activated. Click **OK** to close the dialog.

12. Click **Done** to close the Blueprint Activation Wizard.

To verify that Blueprint was activated successfully, navigate to the Blueprint URL (example: http://localhost:8080/). If the software was activated successfully, you will see a login screen instead of the error message.

Continue to Step 4 to setup the Blueprint instance.

Step 5: Blueprint instance setup

Complete the following steps to set up your Blueprint instance:

1. Open your browser and navigate to the URL where Blueprint is installed. For example: `http://blueprintsys.net`.

2. Log in to Blueprint:

   1. Enter the following credentials and click **Login**.

      - User Name: admin
      - Password:

        Will be given to users

   2. Read the EULA and click **I Agree** if you agree to the terms and conditions. You cannot continue until you accept the EULA.

3. Change the **admin** account password.

   1. Open the **Admin Portal** by clicking the gear on the top right
   2. Open the **User Management** section on the left-hand panel.
   3. Click **Users**.
   4. Click the **admin** user in the table.
   5. Click the **Change Password** button located at the top right of the window.
   6. Type the new password in the appropriate fields and click **OK**.
   7. Remain in the Instance Admin Portal, and proceed to the next step

4. Create a new user for administration purposes and assign instance admin rights to the new user:

   > **Note**: We recommend creating a new user account for administration purposes so the **admin** account remains intact as a backup administration account. For example, if you create a new account called **administrator**, and then later accidentally revoke instance administration privileges from the **administrator** account, you can reapply those permissions using the **admin** account.

   1. Return back to **User Management** > **Users.**
   2. Create a new Database user by clicking **Add Database User** on the top right of the window.
   3. Enter the information for your new administrator user.
   4. Set **Instance Administrator Role** to **Default Instance Administrator**.
   5. Click **Save and Assign Groups**.

5. Log off Blueprint using the **Logout** link located in the upper right corner of the application.
6. Log on to Blueprint using the new user that you created (example: administrator).
7. (Optional) Setup active directory integration. Refer to the *Instance Administration Guide* for more information.

   To configure default active directory integration:

   1. Open the *Instance Administration Console*.
   2. Click **Active Directory Settings**.
   3. Select the **Enable Active Directory Integration** option.
   4. Select the **Use default connection on identity** option.

> **Note**: The default connection only works if your Blueprint Server User (example: `acme\rrunner`) is a member of the active directory and the Blueprint Application Server is also a member of the active directory.

5. Optionally select the **Synchronize Active Directory groups and users** option to ensure user details and group membership in Blueprint reflect changes in Active Directory.

   If synchronization is enabled, configure the **Frequency** and time the operation will begin.

   Synchronization for the weekly and monthly options occur on the first day of the week or month, respectively.

   > **Note**: It is recommended that you schedule synchronization to a time when a minimum number of users will be working with Blueprint.

6. Click **Save**.

To configure custom active directory integration:

1. Open the *Instance Administration Console*.
2. Click **Active Directory Settings**.
3. Select the **Enable Active Directory Integration** option.
4. Select the **Use custom Active Directory integration** option
5. Click the **Add** button.
6. Specify the active directory information on the rightmost side of the screen:

   - **Setting Name**: Choose a name for this active directory server so you can easily identify it in the list.
   - **Bind User**: Defines the user name of a user that has access to read from the active directory server. This user name must be the SamAccountName of the Bind User (not the common name, as per RC2010).

     > Note: The Bind User must be specified like this: **[DomainName]\[UserName]**. Example: **BPTEST\root**

   - **Bind Password**: Defines the password of the Bind User.
   - **Active Directory Authentication URL**: Defines the authentication URL of the active directory server. Example: `LDAP://bpsdc-neo.blueprint.toronto/DC=blueprint,DC=Toronto`

7. Optionally select the **Synchronize Active Directory groups and users** option to ensure user details and group membership in Blueprint reflect changes in Active Directory.

   If synchronization is enabled, configure the **Frequency** and time the operation will begin.

   Synchronization for the weekly and monthly options occur on the first day of the week or month, respectively.

   > **Note**: It is recommended that you schedule synchronization to a time when a minimum number of users will be working with Blueprint.

8. Click **Save**.

8. (Optional) Setup federated authentication if you want to enable Blueprint's single sign-on capabilities.

9. (Optional) Setup the Email Settings (SMTP) if you want to enable notifications.

10. Create projects.

11. Add users to Blueprint.

12. Create license groups.

13. Grant access to projects by creating project role assignments.

Step 6: Blueprint client setup

Configuring elevated trust in-browser

Blueprint must be configured to run with elevated trust in-browser before you can use some advanced features, such as:

- screen capture capabilities
- pasting images into diagrams
- Visio integration, such as importing and exporting diagrams
- rich text table integration with other applications

Elevated trust in-browser can be configured manually on each client machine, or the configurations can be pushed to Windows computers in a centralized manner.

Using group policy to push the elevated trust-in browser configurations to Windows computers in a centralized manner

The recommended way to configure Blueprint to run with elevated trust in-browser is to use Group Policy. Group Policy allows IT Administrators to push configurations to Windows computers in a centralized manner.

For overview information about Group Policy, refer to Microsoft's Group Policy documentation at: http://technet.microsoft.com/en-us/windowsserver/bb310732.aspx.

To configure Blueprint to use elevated trust in-browser, your Group Policy configuration must do the following:

1. Set the following registry value:

   `HKEY_LOCAL_`
   `MACHINE\Software\Wow6432Node\Microsoft\Silverlight\AllowElevatedTrustApp`
   `sInBrowser`
   should be set to
   0x00000001.

   To learn more about setting a registry value through Group Policy, please refer to the Microsoft documentation that explains how to configure a registry item at: http://technet.microsoft.com/en-us/library/cc753092.aspx.

2. Download the elevated trust in-browser package from the Blueprint Community.

blueprint®

3. Add the `publicBlueprintCertificate2020.cer` certificate to the Trusted Publishers Store.

   To learn more about adding a certificate through Group Policy, please refer to the Microsoft documentation that explains how to deploy certificates by using group policy (http://technet.microsoft.com/en-us/library/cc770315(v=ws.10).aspx).

Manually configuring a computer to run with elevated trust in-browser

To configure Blueprint to run with elevated trust in-browser, perform the following steps on each client:

1. Download the elevated trust in-browser configuration files.
2. Unzip the package and note the directory where the files are located.
3. Run `cmd.exe` as Administrator.

   1. Click the Windows **Start** menu and type **cmd.exe** into the search bar.

   2. Right-click the **cmd.exe** program that appears under the Programs heading and then select **Run as administrator**:
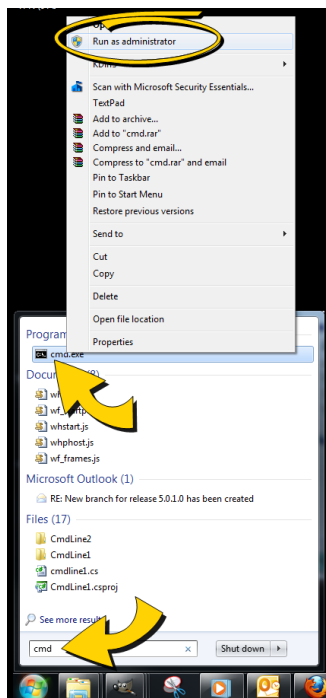
   3. When the confirmation dialog appears, click **Yes**.

      The `cmd.exe` application launches with Administrator privileges:

4. Use the `cd` command to navigate to the folder where you unzipped the files.

   For example:

   ```
   cd c:\temp\elevated_trust
   ```
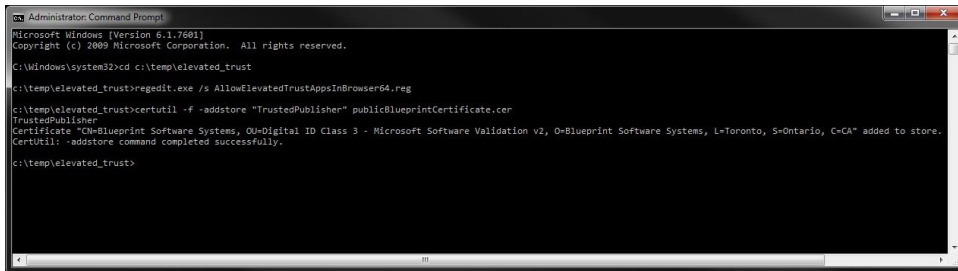
5. Enter the following commands to allow elevated trust to run on your local machine:

```
regedit.exe /s AllowElevatedTrustAppsInBrowser64.reg
```

6. Run the following `certutil` command to apply the Blueprint public certificate:

```
certutil.exe -f -addstore "TrustedPublisher"
publicBlueprintCertificate2017.cer
```

Here is an example of the commands run on a 64-bit operating system:

7. Restart your web browser for the changes to take effect.

Blueprint installation is complete, but there are further setup steps that should be performed by the Blueprint administrator.

Post-install steps for Blueprint instance administrators

Instance administration tips

Project Templates

You may want to consider creating one or more new project(s) in a folder called Templates. Then, you can create new projects using those templates. Project templates provide an efficient way to setup project groups and roles once, rather than configuring the project roles and groups every time you create a new project. Consider looking at the existing Project Templates first, as they model the recommended structure for any of your future projects.

Access Rights

Use groups when you create project role assignments instead of including individual users. For example, whenever a new user requires *write* access to the **Getting Started** project, all you need to do is add the new user to Blueprint and then add the user to the **All Authors** group. The new user will immediately have access to all projects that include the **All Authors** group in a project role assignment.

Supporting HTTP and HTTPS bindings

Open **<BlueprintInstallation>\Web\web.config** and locate the following:

```
<service name="BluePrintSys.RC.Service.RIAServices.ContentDomainService">
    <endpoint address="" binding="webHttpBinding"
bindingConfiguration="streamBinding"
contract="BluePrintSys.RC.Service.RIAServices.ContentDomainService" />
    <!-- This should only be enabled for IIS hosted web site that contains
https site binding -->
    <!--<endpoint address="" binding="webHttpBinding"
bindingConfiguration="securedStreamBinding"
contract="BluePrintSys.RC.Service.RIAServices.ContentDomainService"/>-->
<service>
```

- By default, only HTTP is supported (that is, the "streamBinding" node is uncommented, and the "securedStreamBinding" node is commented).
- When only HTTPS is supported uncomment "securedStreamBinding" and ensure "streamBinding" is commented.
- Uncomment both nodes to support both HTTP and HTTPS.

Setting up federated authentication

Refer to the *Instance Administration Guide* for more information.

To configure your identity provider for Blueprint federated authentication, ensure the following requirements are met:

- The **Entity ID** must be set to:

  > `<Blueprint_URL>/Login/SAMLHandler.ashx`

  where <Blueprint_URL> is your main Blueprint URL.

  > **Example**
  >
  > For Blueprint cloud customers, the **Entity ID** will look something like this:
  >
  > **https://acme.blueprintcloud.com/Login/SAMLHandler.ashx**
  >
  > For Blueprint on-premise customers, the **Entity ID** will look something like this:
  >
  > **https://blueprint.acme.com/Login/SAMLHandler.ashx**

- The **POST Endpoint** must be set to:

  > `<Blueprint_URL>/Login/SAMLHandler.ashx`

  where <Blueprint_URL> is your main Blueprint URL.

- A **Username** attribute must be included in the SAML response (that is, the token).

  Blueprint reads the username from the **Username** attribute in the token (not the Subject). The name of this attribute must be **Username**. The username can be in the format you want, but must match the usernames as created in Blueprint. Valid options are regular usernames, Windows/AD account names (DOMAIN\user), e-mail addresses, Distinguished Names, or x509 Subjects.

  The SAML response must contain the identity provider certificate (x509).

To enable Blueprint federated authentication:

1. Open the *Instance Administration Console*.
2. Click **Federated Authentication Settings**.
3. Select the **Enable Federated Authentication** option.
4. Set your federated authentication settings:

   - Click **Replace certificate** to upload your Identity Provider Certificate. The certificate must be in DER format.

     > **Important**: Certificates have an expiry date. Make sure you replace your certificate before it expires or users will be unable to access Blueprint.

   - **Login URL**: Defines your Identity Provider Login Service URL. This is the URL that Blueprint navigates to when the user clicks the Go button on the login screen. At this time, the Identity Provider returns a authentication token to Blueprint to authenticate the user.

     Example: https://idp.domain.com/adfs/ls/

   - **Logout URL**: Defines the URL to navigate to after a user clicks the Logout button in Blueprint. This

behavior is not applicable if a user is logged in with fallback authentication.

- **Error URL (optional)**: If a token error occurs, the user is redirected to the specified URL. The specific error is included as a GET parameter in the URL.

  If an **Error URL** is not provided, Blueprint displays the token errors in the popup window.

- **Login Prompt (optional)**: Defines the login text that appears on the login screen when Federated Authentication is enabled:

The default text is:

Login with Corporate Credentials

- **Customize electronic signature prompt (optional)**: Defines the text that appears on the electronic signature message when Federated Authentication is enabled. If you require signatures for the review process, users are asked to confirm their identity in order to approve or reject an artifact. When federated authentication is enabled, users will be able to use this federated identity to sign off.

5. If Active Directory integration is enabled, and for federated authentication your identity provider is configured to only pass on a username, select **Allow SSO User Authentication without a Domain Name** and list all domain names:

   - Click **Add**, then click the newly created line and enter the domain.
   - Do not include the backslash. For example, when entering to account for "DOMAIN\username", only enter "domain".
   - Domains will be applied in the order they are listed.

6. Click **Save**.

Setting up email notifications

Email settings are required in Blueprint if you want to take advantage of Blueprint notifications. Blueprint notifications provide your users with information and reminders at key moments. Notifications can help users stay up-to-date with project developments. There are two types of notifications you can enable: review notifications and email integrated discussions notifications. For more information about notifications, see the *Instance Administration Guide*.

Setting up review notifications

Perform the following steps if you want to enable review notifications and configure the associated settings:

1. Open the *Instance Administration Console*.

2. Click **Configure Instance** > **E-mail Settings** on the ribbon (*Instance Admin* tab, *Instance* group).

3. Select the **Enable Review Notifications** check box to enable review notifications.Enter your e-mail credentials in the *Email Credentials* section:

   - **E-mail Address**: Defines the e-mail address that will appear in the **From** address for all e-mail notifications.
   - **User Name**: Defines the user name of the e-mail account.
   - **Password**: Defines the password of the user.

4. Enter your outgoing mail server settings and preferences:

   - **Server IP / Hostname**: Defines the IP address or hostname of your SMTP server.
   - **Port**: Defines the port number of your SMTP server.
   - **Enable SSL**: Defines whether or not the SMTP server requires SSL.
   - **Authenticated SMTP**: Defines whether or not SMTP authentication is required. If authentication is required, select this option and enter a valid user name and password.

     - **User Name**: Defines the user name of a user with access to the SMTP server. This user name can be different from the user name provided in the *Email Credentials* section.

       > **Note**: The SMTP user name is sometimes, but not always, the e-mail address of the user. The format of the user name is dependent on the server configuration.

     - **Password**: Defines the password of the user.

5. Click **Save**.

   > **Tip**: You can click the **Send Test E-mail** button to verify that e-mails can be sent successfully.

Setting up e-mail integrated discussions

Perform the following steps to enable and configure e-mail integrated discussion settings:

1. Open the *Instance Administration Console*.

2. Click **Configure Instance** > **E-mail Settings** on the ribbon (*Instance Admin* tab, *Instance* group).

3. Select the **Allow projects to enable discussions via E-mail** check box to enable e-mail-integrated discussions.

> **Note:** By default, e-mail integrated discussions are set to only allow users to mention Blueprint registered users.
>
> To change this setting: click **Edit Settings**. Next, click **All users** to allow any user outside of Blueprint to contribute via e-mail to discussions.
>
> To restrict this setting to a subset of e-mail domains: ensure **Specify domains** is enabled, enter the domains you want to allow in e-mail integrated discussions and click **OK**.

4. Enter your e-mail credentials in the *Email Credentials* section:

   ■ **E-mail Address**: Defines the e-mail address that will appear in the **From** address for all e-mail notifications.

   ■ **User Name**: Defines the user name of the e-mail account.

   ■ **Password**: Defines the password of the user.

5. Enter your incoming mail server settings and preferences:

   ■ **IMAP/POP**: Defines the protocol of the incoming email server.

   ■ **Server IP/Hostname**: Defines the IP address or hostname of your IMAP/POP server.

   ■ **Port**: Defines the port number of your IMAP/POP server.

   ■ **Enable SSL**: Defines whether or not the IMAP/POP server requires SSL.

   > **Tip**: You can click the **Test Connection** button to verify that e-mail integrated discussions can be delivered successfully.

6. Enter your outgoing mail server settings and preferences:

   ■ **Server IP / Hostname**: Defines the IP address or hostname of your SMTP server.

   ■ **Port**: Defines the port number of your SMTP server.

   ■ **Enable SSL**: Defines whether or not the SMTP server requires SSL.

   ■ **Authenticated SMTP**: Defines whether or not SMTP authentication is required. If authentication is required, select this option and enter a valid user name and password.

      ■ **User Name**: Defines the user name of a user with access to the SMTP server. This user name can be different from the user name provided in the *Email Credentials* section.

      > **Note**: The SMTP user name is sometimes, but not always, the e-mail address of the user. The format of the user name is dependent on the server configuration.

   ■ **Password**: Defines the password of the user.

7. Click **Save**.

Next, enable the e-mail integrated discussions setting within *Project Settings* (Project Administration).

Adding users to Blueprint

Refer to the *Instance Administration Guide* for more information.

Adding all Active Directory users

Complete the following steps to add all Active Directory users to Blueprint:

> **Important**: You can only add Windows users if Active Directory integration is enabled.

1. Click **Manage Users And Groups** > **Users** on the ribbon (*Instance Admin* tab, *Instance* group).
2. Click **New** > **New Windows User** on the ribbon (*Instance Admin* tab, *Manage Items* group).
3. Click the **Find** button to display all Active Directory users.

> **Note**: If Active Directory integration is enabled, the Location is automatically populated so you can access the Active Directory.

4. Type `Ctrl-a` to select all users and then click **OK**.

Adding a database user in Blueprint

Complete the following steps to add a single database user to Blueprint:

1. On the *Users* tab, click **New** > **New Database User** on the ribbon (*Instance Admin* tab, *Manage Items* group).
2. Enter the user information on the right side of the window.
3. Click **Save**.

Creating license groups

Refer to the *Instance Administration Guide* for more information.

A license group is an instance-level group that allows you to control the type of license that a user consumes while logged into Blueprint. From a licensing perspective, Blueprint users are known as Authors, and have universal capabilities. An individual user's privileges within a given project are determined by their project-role assignments.

> **Important**: Users must be added to an *Author* or *Collaborate* license group before they can take advantage of most Blueprint features. Users that are not added to an *Author* or *Collaborate* license group are limited to accessing Blueprint artifacts by URL.

Complete the following steps to create an **All Authors** group that is designated as an *Author* license group:

1. Click **Manage Users And Groups** > **Groups** on the ribbon (*Instance Admin* tab, *Instance* group).
2. Click **New** > **Database Group** on the ribbon (*Instance Admin* tab, *Manage Items* group).
3. Enter the group information:

   - **Name**: Set this field to **All Authors**.
   - **Description**: Specify a description for the group.
   - **Email**: Specify an email address for the group.
   - **Scope**: This field must be left blank. License groups cannot have an associated Scope.
   - **License Group?**: Enable this option so the group is a license group.
   - **License Type**: Change this option to **Author**.

4. Click the **Add** button to add members to the group. Type `Ctrl-a` to select all users, and then click **OK**.

5. Click **Save**.

Repeat the steps above to create an **All Contributors** group, but set the **License Type** to **Collaborate**.

Creating projects

Refer to the *Instance Administration Guide* for more information.

Complete the following steps to create the **Getting Started** project.

> **Note**: The purpose of the Getting Started project is to provide a location for users to experiment with Blueprint features and complete the tutorials in the Getting Started Guide.

1. Click the **Projects** button on the ribbon.

2. Right-click the *Blueprint* item on the left side of the window and select **New Folder**.

3. Specify the following folder information:

   - **Name**: Getting Started
   - **Description**: Folder containing getting started project(s).

4. Click **Save**.

5. Expand the *Blueprint* item on the left side of the window, right-click **Getting Started**, and select **New Project**.

6. Specify the project information:

   - **Name**: Getting Started
   - **Description**: Project for users to learn Blueprint using the Blueprint Getting Started Guide.
   - **Location**: This should be set to /Blueprint/Getting Started/
   - **Select Source**: Empty Project

7. Click **Save**.

8. Click the **Launch Project Administration** button. This button is located in the lower-right area of the window. The *Project Administration Console* is displayed.

Granting access to projects

Refer to the *Project Administration Guide* for more information.

> **Note**: From a licensing perspective, Blueprint users are known as Authors, and have universal capabilities. An individual user's privileges within a given project are determined by their project-role assignments.

Complete the following steps to configure the **Getting Started** project so the **All Authors** group can modify the project.

1. Create an Authors role.

   1. In the *Project Admin Console*, click **Manage Access** > **Project Roles** on the ribbon (*Project Admin* tab, *Project* group)
   2. Click the **New** button on the ribbon (*Project Admin* tab, *Actions* group).
   3. Specify the role information:

- **Name**: Authors
- **Description**: This role has read, edit, trace, and comment privileges.
- **Privileges**: Place a checkmark beside **Read**, **Edit**, **Trace**, and **Comment**.

    4. Click **Save**.

2. Assign the **Authors** role to the **All Authors** group for the **Getting Started** project.

3. Assign the **Authors** role to the **All Authors** group for the **Getting Started** project.

    1. In the *Project Admin Console*, click **Manage Access** > **Project Role Assignments** on the ribbon (*Project Admin* tab, *Project* group)

    2. Click the **New** button on the ribbon (*Project Admin* tab, *Actions* group) and then click the *Groups* tab after the dialog appears.

    3. Select the **All Authors** group and click **OK**.

    4. Specify the project role assignment information:

- **Identity**: Group : All Authors
- **Role**: Authors
- **Scope**: Project

    5. Click **Save**.

Configuration reference

Blueprint Installation Script Parameters

The following parameters can be used with the Blueprint installation script (`Install-Blueprint.ps1`).

Parameter	Description
-DontAskForDatabaseMigrationConfirmation	Perform database migration during installation without prompting for confirmation.
-InstallDatabaseOnly	Only create or migrate the Blueprint databases.
-InstallJobExecutorsOnly	Only install the Blueprint JobExecutor Windows Services.
-InstallSiteOnly	Only install the Blueprint site. Can be used in conjunction with -InstallDatabaseOnly, -InstallJobExecutors, -InstallPacksOnly, and -InstallWindowsServicesOnly to install some, but not all, Blueprint components.
-InstallWindowsServicesOnly	Only install the Windows Services (such as the Blueprint services and image rendering service).
-SkipValidation	Skip the validation phase of the installation (not recommended).
-ValidateOnly	Only perform the validation phase of the installation, without making any changes to the system.

During installation, you are prompted for various administrator account passwords that are required to install Blueprint. The following parameters can be used to bypass prompts by providing passwords as parameter values. After installation, these passwords are not retained.

Note that if the password includes a dollar sign ($), use single quotation marks.

Password-Prompt Bypass Parameter	Description
-AppPoolPassword	Provides the password for the application pool identity (the account specified in Step 3/8 of the Blueprint Installation Configuration Wizard).
-WindowsServiceAccountPassword	Provides the password for the Windows Service account (the account specified in Step 4/8 of the Blueprint Installation Configuration Wizard).
-BlueprintDatabasePassword	Provides the password for the Blueprint database system administrator account (the account specified in Step 5/8 of the wizard).

Password-Prompt Bypass Parameter	Description
-AdminStorageDatabasePassword	Provides the password for the Admin Store database system administrator account (the account specified in Step 6/9 of the wizard).
-BlueprintMessagingPassword	Provides the password for the messaging service user account (the account specified in Step 7/9 of the wizard).

Script parameter examples

The following example tests the referenced settings file to ensure the installation will run correctly:

```
.\Installation\Installer\Install-Blueprint.ps1 -
BlueprintInstallSettingsPath .\BlueprintInstallSettings-7.3.0.756-
2016.08.19-11.09.14.xml -ValidateOnly
```

The following example installs only the Blueprint sites, and excludes the database and job services creation:

```
.\Installation\Installer\Install-Blueprint.ps1 -
BlueprintInstallSettingsPath .\BlueprintInstallSettings-7.3.0.756-
2016.08.19-11.09.14.xml -InstallSiteOnly
```

The following example installs only the Blueprint sites, and bypasses the prompt for the application pool identity password:

```
.\Installation\Installer\Install-Blueprint.ps1 -
BlueprintInstallSettingsPath .\BlueprintInstallSettings-7.3.0.756-
2016.08.19-11.09.14.xml -AppPoolPassword Password -InstallSiteOnly
```

The following example installs only the Blueprint databases, and bypasses the prompts for the database administrator passwords (the first of which includes dollar signs):

```
.\Installation\Installer\Install-Blueprint.ps1 -
BlueprintInstallSettingsPath .\BlueprintInstallSettings-7.3.0.756-
2016.08.19-11.09.14.xml -InstallDatabaseOnly -BlueprintDatabasePassword
'Pa$$word' -AdminStorageDatabasePassword Password
```

Web.config reference

Note: Before upgrading Blueprint, we recommend backing up the `web.config` file. None of your existing customizations are preserved during the upgrade process. The backup file can be used as a reference to make changes to the new version of `web.config` after upgrading.

Blueprint web.config

The Blueprint `web.config` file contains many Blueprint web application settings, most of which should not be edited in common configuration scenarios. The following table identifies Blueprint settings that are commonly configured as well as their possible values:

Section	Parameter name	Default value	Description

`<appSettings>`
 	
`  <add key="UseLegacyDomainName">`
	value	false	The `UseLegacyDomainName` key indicates the domain name section. You can use the original parsing algorithm to determine the domain name.
			
			There is no need to change the default value in most circumstances. However, if you have problems integrating Blueprint with LDAP, you may need to change the value to `TRUE`. Please contact Blueprint Support before changing this value.

`<appSettings>`
 	
`  <add key="ExcelImportArtifactLimit">`
	value	500	This section defines the amount of artifacts that a user can import from Microsoft Excel at a time.
			
			Note: We do not recommend changing this value unless it is necessary.

Section	Parameter name	Default value	Description
`<appSettings>` `<add key="LdapGetTimeout">`	value	300	Indicates how many seconds it takes for LDAP retrieval to time out. By default, the LDAP retrieval timeout is `300` seconds (recommended). The value can be changed. The minimum value it can be changed to is `30` and the maximum is `600`.
`<appSettings>` `<add key="QCMaxRetries">`	value	30	This section defines the maximum number of connection re-attempts that will be made when connection to HP Quality Center initially fails. By default, the value is `30` (recommended). To change the value, the following tag must be manually added to the `<connectionString s>` section first: `<add key="QCMaxRetrie s" value="">` The minimum value it can be changed to is `3` and the maximum is `60`.

Section	Parameter name	Default value	Description
`<appSettings>` `<add key="QCDelayInSeconds">`	value	30	This section defines the delay between connection re-attempts that will be made when connection to HP Quality Center initially fails. The delay is measured in seconds. To change the value, the following tag must be manually added to the `<connectionStrings>` section first: `<add key="QCDelayInSeconds" value="">` The recommended value is 5. The minimum value it can be changed to is 5 and the maximum is 60.
`<appSettings>` `<add key="AccessControl">`	value	None	Indicates the location of the auxiliary AccessControl service.
`<appSettings>` `<add key="ConfigControl">`	value	None	Indicates the location of the auxiliary ConfigControl service.

`<connectionStrings>`
  `<add connectionString>`
	connectionString	`metadata=res://*/Models.Instance.csdl|`
		
		`res://*/Models.Instance.ssdl|`
		`  res://*/Models.Instance.msl;`
		
		`provider=System.Data.SqlClient;`
		`  provider connection string=`
		`    "data source=BlueprintDevDB;`
		`  Initial Catalog=Blueprint;`
		`  Integrated Security=True;`
		
		`MultipleActiveResultSets=True;`
			The connection string that points to the Blueprint database.

Blueprint AdminStore web.config

The AdminStore service is the interface to administration functionality and logins. Its **web.config** file's settings likely do not require editing in typical deployment scenarios, with the exception of the following connection parameters:

Section	Parameter name	Default value	Description
`<appSettings>` `<add key="AccessControl">`	value	http://localhost:9101/svc/accesscontrol/	The URL for the auxiliary AccessControl service.
`<appSettings>` `<add key="ConfigControl">`	value	http://localhost:9101/svc/configcontrol/	The URL for the auxiliary ConfigControl service.

`<connectionStrings>`
    `<add name="AdminStorage">`
	connectionString	`data source=BlueprintDevDB;`
		`    initial catalog=Blueprint_AdminStorage;`
		`    integrated security=True;`
		`    min pool size=4;`
		`    max pool size=128;`
		`    load balance timeout=2;`
		`    packet size=16384;`
		`    connectretrycount=3;`
		`    connectretryinterval=3;`
		`    MultipleActiveResultSets=True;`
			The connection string that points the AdminStore service to the AdminStorage database.

`<connectionStrings>`
    `<add name="RaptorMain">`
	connectionString	`data source=BlueprintDevDB;`
		`    initial catalog=Raptor;`
		`    integrated security=True;`
		`    min pool size=4;`
		`    max pool size=128;`
		`    load balance timeout=2;`
		`    packet size=16384;`
		`    connectretrycount=3;`
		`    connectretryinterval=3;`
		`    MultipleActiveResultSets=True;`
			The connection string that points the AdminStore service to the Blueprint database.

Blueprint FileStore web.config

The FileStore service is the interface to files accessed from Blueprint. Its **`web.config`** file's settings likely do not require editing in typical deployment scenarios, with the exception of the following storage and connection parameters:

Section	Parameter name	Default value	Description
`<appSettings>` `<add key="FileChunkSize">`	value	1	The chunk size for files stored in the FileStorage database, in megabytes. The recommended value is the default of `1`.

Section	Parameter name	Default value	Description

`<appSettings>`
 	
  `<add key="ConfigControl">`
	value	http://localhost:9101/svc/configcontrol/	The URL for the auxiliary ConfigControl service.

`<connectionStrings>`
 	
  `<add name="FileStoreDatabase">`
	connectionString	`data source=BlueprintDevDB;`
		  `initial catalog=Blueprint_`
		`FileStorage;`
		  `integrated security=True;`
		  `min pool size=4;`
		  `max pool size=128;`
		  `load balance timeout=2;`
		  `packet size=16384;`
		  `connectretrycount=3;`
		  `connectretryinterval=3;`
		  `MultipleActiveResultSets=True;`
			The connection string that points the FileStore service to the FileStorage database.

`<connectionStrings>`
 	
  `<add name="FileStreamDatabase">`
	connectionString	`data source=BlueprintDevDB;`
		  `initial catalog=Raptor;`
		  `integrated security=True;`
		  `min pool size=4;`
		  `max pool size=128;`
		  `load balance timeout=2;`
		  `packet size=16384;`
		  `connectretrycount=3;`
		  `connectretryinterval=3;`
		  `MultipleActiveResultSets=True;`
			The connection string that points the FileStore service to the Blueprint database.
			
			The use of the Blueprint database is a fallback, for files not found in the FileStorage database. This scenario applies in cases where Blueprint is upgraded to v7.0, but the FileStore Migration Utility has not been run.

Auxiliary AccessControl web.config

The AccessControl service handles sessions and authentication. Its `web.config` file's settings likely do not require editing in typical deployment scenarios, with the exception of the following timeout and connection parameters:

Section	Parameter name	Default value	Description

`<appSettings>`
 	
`<add key="SessionTimeoutInterval">`
	value	1200	Interval to remove terminated sessions from the database (in seconds).
			
			This value overrides the `<add key="SessionLifetimeInterval" />` section in the Blueprint `web.config` file. (Note that the latter is measured in minutes.)

`<appSettings>`
 	
`<add key="ConfigControl">`
	value	http://localhost:9101/svc/configcontrol/	The URL for the auxiliary ConfigControl service.

`<connectionStrings>`
 	
`<add name="AdminStorage">`
	connectionString	`data source=BlueprintDevDB;`
		`    initial catalog=Blueprint_`
		`AdminStorage;`
		`    integrated security=True;`
		`    min pool size=4;`
		`    max pool size=128;`
		`    load balance timeout=2;`
		`    packet size=16384;`
		`    connectretrycount=3;`
		`    connectretryinterval=3;`
		
		`MultipleActiveResultSets=True;`
			The connection string that points the AccessControl service to the AdminStorage database.

Auxiliary ConfigControl web.config

The ConfigControl service handles configuration settings and logging. Its **web.config** file's settings likely do not require editing in typical deployment scenarios, with the exception of the following:

Section	Parameter name	Default value	Description

`<connectionStrings>`
 	
`<add name="AdminStorage">`
	connectionString	`data source=BlueprintDevDB;`
		`    initial catalog=Blueprint_AdminStorage;`
		`    integrated security=True;`
		`    min pool size=4;`
		`    max pool size=128;`
		`    load balance timeout=2;`
		`    packet size=16384;`
		`    connectretrycount=3;`
		`    connectretryinterval=3;`
		`    MultipleActiveResultSets=True;`
			The connection string for the AdminStorage database.