Blueprint 5.4

Upgrade Guide

3/24/2015

blueprint®

Contents

Blueprint Upgrade Guide

Overview

This *Blueprint Upgrade Guide* is applicable if you have already installed Blueprint and you want to upgrade to a newer version. If you want to install Blueprint for the first time, please refer to the *Blueprint Installation Guide*.

Important Notices

Upgrade duration

The upgrade can take up to 60 minutes for large databases.

Backing up your data

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

System Requirements

Please refer to the *Blueprint Installation Guide* for detailed information about Blueprint System Requirements.

Upgrade Steps

Step 1: Backup your data

Warning: It is strongly recommended that you backup your database before starting the upgrade.

To backup 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.

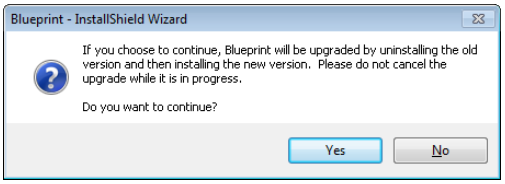
2. Backup the following data:
   - database
   - website (including the `web.config` file)

Step 2: Run BlueprintSetup.exe on the web application server

The following steps are required for both the express and manual upgrade.

1. Run **`BlueprintSetup.exe`**.

   `BlueprintSetup.exe` extracts all of the new application files and configuration utilities that are required for the Blueprint upgrade. After you launch the **`BlueprintSetup.exe`** file, the wizard detects previous installations of Blueprint on your system and asks if you wish to continue upgrading Blueprint:

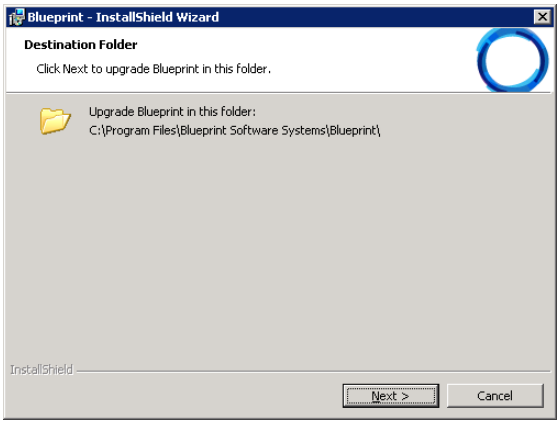
   Click **Yes** to continue. If you click **No**, the upgrade wizard is canceled.

2. The following InstallShield Wizard displays to begin the Blueprint upgrade:

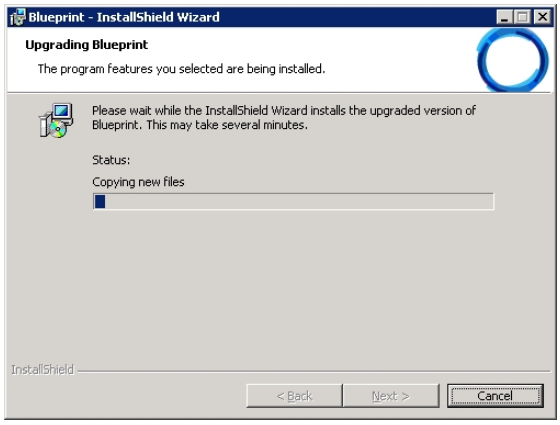
   Click **Next** to continue.

3. This screen displays the destination folder where Blueprint will be upgraded:

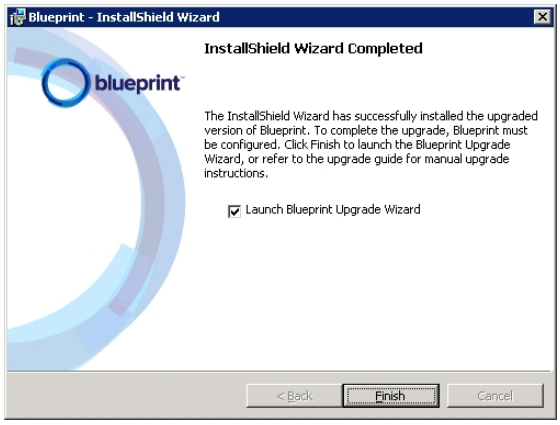
   Click **Next** to continue.

4. The next screen displays the progress as the new files are copied:



When it is finished, click **Next** to continue.

5. When the InstallShield Wizard is complete, the following dialog is displayed:



Click **Finish** to complete the upgrade and launch the *Blueprint Upgrade Wizard* (recommended). If you want to complete the upgrade using the command line utilities, you can clear the **Launch Blueprint Upgrade Wizard** option.

Step 3: Finalize the Blueprint upgrade

> **Warning**: The database upgrade can take up to 60 minutes for large databases.

Choose one of the following methods to upgrade the database and finalize the Blueprint upgrade:

- Continue to the Option 1: Express Upgrade section (recommended) if you want to upgrade Blueprint database using the *Blueprint Upgrade Wizard*.
- Continue to the Option 2: Advanced / Manual Upgrade section if you want to upgrade the Blueprint database using the command line configuration utilities instead of the upgrade wizard.

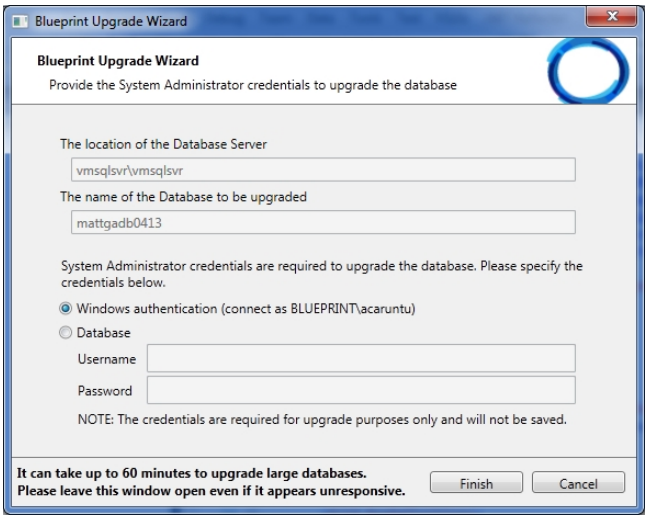
Option 1: Express Upgrade

The *Blueprint Upgrade Wizard* launches automatically unless you cleared the **Launch Blueprint Upgrade Wizard** option at the end of the InstallShield Wizard. If you need to launch the *Blueprint Upgrade Wizard* manually, run the

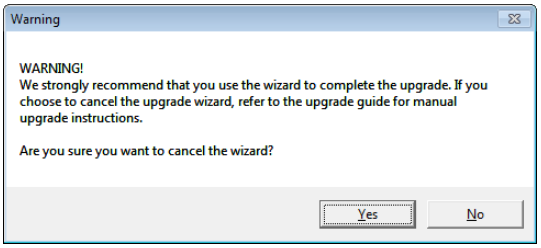
BlueprintUpgradeWizard.exe file located in the **Setup** folder. The **Setup** folder is located in the directory that you chose for installing Blueprint. For example, the default path is:

`C:\Program Files (x86)\Blueprint Software Systems\Blueprint\Setup`

The *Blueprint Upgrade Wizard* dialog is pre-populated with the location and the name of your Blueprint Database:



If you click **Cancel** at any time, the following warning is displayed:



Click **Yes** only if you want to cancel the wizard and finalize the upgrade using Option 2: Advanced / Manual Upgrade.

To finalize the upgrade using the *Blueprint Upgrade Wizard*, perform the following steps:

1. Enter the following information:
    - System Administrator Credentials: Choose whether you wish to authenticate using *Windows authentication* or *Database* authentication.

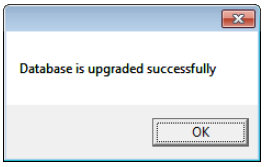
      Important: This user must be a Database System Administrator (SA). This allows the installer to create the new database and grant permissions to the database so the web application server can access the database. The SA credentials are not stored anywhere in the system. The SA user account is only required 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 wizard automatically uses the user that is currently logged in. You must ensure that the user has SA privileges on

the database server.

- **Database authentication**: If you choose database authentication, you must specify the username and password of an account that has SA privileges on the database server.

2. Click **Finish** to complete the upgrade. The following dialog is displayed after the upgrade is successful:



Option 2: Advanced / Manual Upgrade

This section explains how to upgrade the Blueprint database and finalize the upgrade using the configuration utilities (instead of using the *Blueprint Upgrade Wizard*).

> **Note**: If you finalized the upgrade using the *Blueprint Upgrade Wizard*, you are NOT required to run the configuration utilities. The configuration utilities are run automatically when you complete the upgrade using the *Blueprint Upgrade Wizard*. You are only required to run the configuration utilities manually if you decide to perform a manual upgrade instead of using the Wizard.

The configuration utilities are located in a folder called **`Setup`**. The **`Setup`** folder is located in the directory that you chose for installing Blueprint. For example, the default path is:

`C:\Program Files (x86)\Blueprint Software Systems\Blueprint\Setup`

> **Tip**
>
> You can type the following command to view more information about the command parameters:
>
> `blueprintdbcmd.exe /help`

Manual Upgrade Steps

> **Warning**: The upgrade can take up to 60 minutes for large databases.

To upgrade the database:

1. Run the following command:

   > **Important**: The command must be run with Administrator privileges.

   ```
   blueprintdbcmd.exe /object DB /command UPGRADE /catalog Blueprint
   /datasource DBSERVER\INSTANCE01 /integratedsec FALSE /userid dbadmin
   /password "pAssw0rd"
   ```

2. Stop and then restart 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.

Step 4: 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 artifacts
- 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 one of the following registry values:
   - On 32-bit computers:
     Set the **`HKEY_LOCAL_MACHINE\Software\Microsoft\Silverlight\AllowElevatedTrustAppsInBrowser`** registry value to **0x00000001**.
   - On 64-bit computers:
     Set the **`HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Silverlight\AllowElevatedTrustAppsInBrowser`** registry value 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 Customer Portal.
3. Add the **`publicBlueprintCertificate.cer`** certificate to the Trusted Publishers Store.

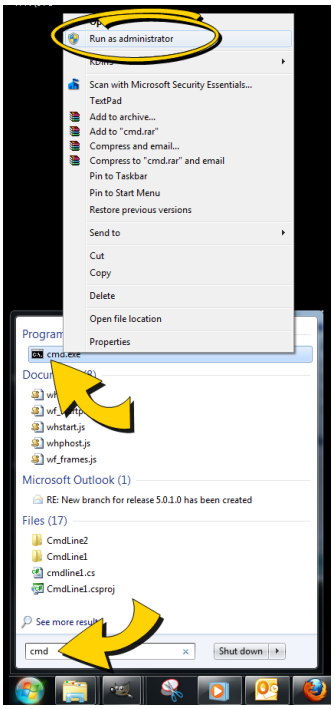
   To learn more about adding a certificate through Group Policy, please refer to the Microsoft documentation that explains how to deploy certificates by using group policy (http://technet.microsoft.com/en-us/library/cc770315(v=ws.10).aspx).

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:

    - For 64-bit operating systems:

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

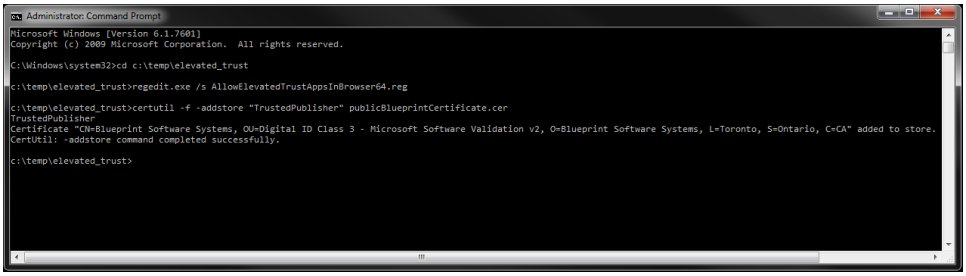
- For 32-bit operating systems:

```
regedit.exe /s AllowElevatedTrustAppsInBrowser.reg
```

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

```
certutil.exe –f –addstore “TrustedPublisher” publicBlueprintCertificate.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.

Appendix

Configuration utility command reference

> **Tip**
>
> You can type the following commands to view more information about the command parameters:
>
> `blueprintwebcmd.exe /help`
>
> `blueprintdbcmd.exe /help`

Web Application Server Configuration Parameters

Parameter	Description	Default	Example
/object	Defines the object type of the command. This parameter can be set to one of the following values: ■ SITE ■ APPPOOL ■ DBCONFIG		
/command	Defines the command to perform. This parameter can be set to one of the following values: ■ LIST ■ ADD ■ DELETE ■ START ■ STOP		
/wsname	Defines the name of the site.	Blueprint	BlueprintWS
/wsid	Defines the ID of the site.		25
/port	Defines the port number used for the site.		8080
/dir	Defines the location of the Blueprint installation.		C:\Program Files (x86)\Blueprint Software Systems\Blueprint\Web
/apppoolname	Defines the name of the application pool.	Blueprint	BlueprintAP
/datasource	Defines your database and instance names.		DBSERVER\INSTANCE01
/catalog	Defines the name of the database.	Blueprint	

Parameter	Description	Default	Example
/integratedsec	Defines whether or not Windows security is used. This parameter can be set to one of the following values: ■ TRUE ■ FALSE If /integratedsec is set to FALSE, you must specify a /userid and /password.		
/userid	Defines the username of the Service Account/Application Pool user.		
/password	Defines the password of the Service Account/Application Pool user.		

Database Server Configuration Parameters

Parameter	Description	Default	Example
/object	Defines the object type of the command. This parameter can be set to one of the following values: ■ SERVER ■ DB ■ USER		
/command	Defines the command to perform. This parameter can be set to one of the following values: ■ LIST ■ ADD ■ INIT ■ UPGRADE		
/datasource	Defines your database and instance names.		DBSERVER\INSTANCE01
/catalog	Defines the name of the database.	Blueprint	BlueprintDB
/integratedsec	Defines whether or not Windows security is used. This parameter can be set to one of the following values: ■ TRUE ■ FALSE If /integratedsec is set to FALSE, you must specify a /userid and /password.		
/userid	Defines the username of the *Database System Administrator* user. This parameter is only required if /integratedsec is set to FALSE.		
/password	Defines the password of the *Database System Administrator* user. This parameter is only required if /integratedsec is set to FALSE.		
/nuseridentity	Defines the username of the *Blueprint Server User*.		acme\rrunner

Maintaining the Blueprint database

For best performance, we recommend that you perform routine maintenance on the Blueprint database. For more information, login to the Blueprint Customer Portal (http://portal.blueprintsys.com) and refer to *Knowledge Base Article 1046, How to perform routine maintenance on the Blueprint database*.

Setting up a new database

Warning: Be careful completing the steps below. If you run the re-initialize command on an existing database, you will lose all data!

1. Create the new database:

```
blueprintdbcmd.exe /object DB /command ADD /datasource
DBSERVER\INSTANCE01 /catalog BlueprintDB /integratedsec FALSE /userid
dbadmin /password "pAssw0rd"
```

2. Add security:

```
blueprintdbcmd.exe /object USER /command ADD /datasource
DBSERVER\INSTANCE01 /catalog BlueprintDB /integratedsec FALSE
/nuseridentity "acme\rrunner" /userid dbadmin /password "pAssw0rd"
```

3. Initialize the database:

```
blueprintdbcmd.exe /object DB /command INIT /datasource
DBSERVER\INSTANCE01 /catalog BlueprintDB /integratedsec FALSE /userid
dbadmin /password "pAssw0rd"
```

Pointing the web application server to a different database

Complete the following steps if you want the web application server to point to a different database:

1. Make sure the new database is setup. Learn more about setting up a new database.
2. Run the connection string command, using the new database name and location as parameters. For example:

```
blueprintwebcmd.exe /object DBCONFIG /command SET /datasource
DBSERVER\INSTANCE01 /wsname BlueprintWS /integratedsec TRUE /catalog
BlueprintDB
```

Clearing database contents and re-initializing the database

Warning: The steps below will result in data loss!

1. Backup your data!
2. Run the database initialization command. For example:

```
blueprintdbcmd.exe /object DB /command INIT /datasource
DBSERVER\INSTANCE01 /catalog BlueprintDB /integratedsec FALSE /userid
dbadmin /password "pAssw0rd"
```

Moving the application to a new web application server

The steps below may be required if a server is being decommissioned and you want to move the application to a new web application server.

1. Run the MSI installation on the new web application server.
2. Proceed with the configuration of the application (using the Blueprint Configuration Wizard or the Advanced/Manual installation steps).

   Warning: Do NOT proceed with the installation of the database.

3. Run the connection string command.
   For example:

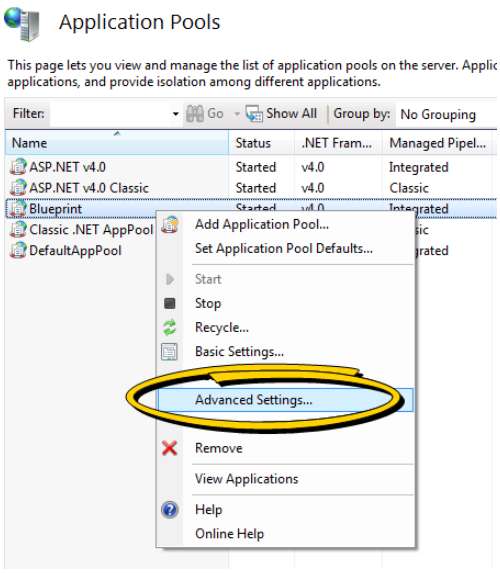
```
blueprintwebcmd.exe /object DBCONFIG /command SET /datasource
DBSERVER\INSTANCE01 /wsname BlueprintWS /integratedsec TRUE /catalog
BlueprintDB
```

Changing the Blueprint Server User of the Blueprint application

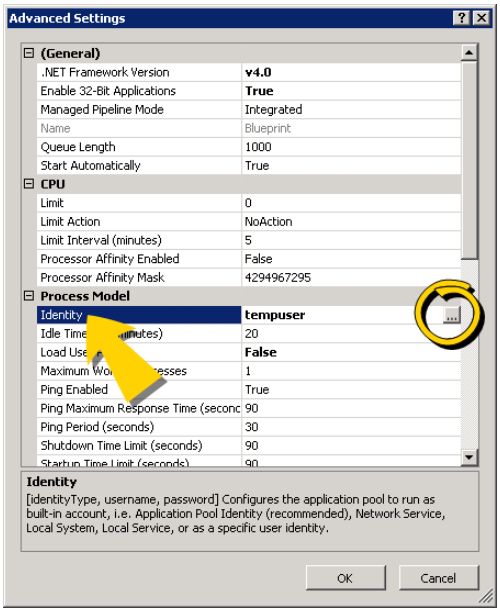
You can use the steps below to change the Blueprint Server User of the Blueprint application. For example, complete the steps below if you installed Blueprint using a temporary account as the Blueprint Server User (example: tempuser) and now you want to change the Blueprint Server User to a different user (example: acme\rrunner).

1. Add the new user to both the web application server and the database server. The user must exist on both servers with the same user name.
2. Change the `Identity` of your Blueprint application pool by performing the following steps:
   1. Open *Internet Information Services (IIS) Manager* on the web application server that is hosting Blueprint.
   2. Right-click your Blueprint application pool and select **Advanced Settings**:

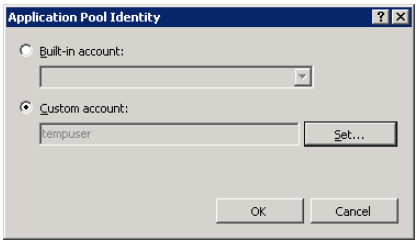
      Note: The Application Pool is named **Blueprint** in the example image below. The name, however, depends on the name that was chosen during the installation of Blueprint.



3. On the *Advanced Settings* dialog, select **Identity** and then click the ellipsis button.



The *Application Pool Identity* dialog appears:



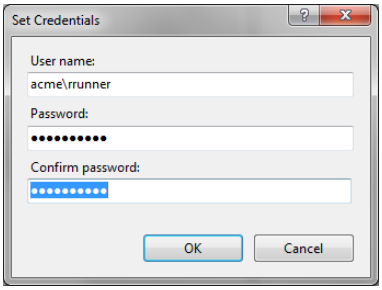
4. Select one of the following options:

   - **Built-in account**: Allows you to use the Built-in account for the Blueprint Server User. The ApplicationPoolIdentity built-in account in IIS is created as **IIS APPPOOL\<AppPoolName>** in

SQL.

> **Note**: The Built-in account should only be used for single-server installs, where the datasource is always localhost.

- **Custom account**: Allows you to set a specific user account for the Blueprint Server User. Click the **Set** button to open the *Set Credentials* dialog. Enter the user name and password for the new user, and then click **OK** to save the changes.



3. Run the Blueprint database utility command to set the user. You must specify the new user using the `/nuseridentity` parameter:

   - If you chose the **built-in account** option:

     ```
     blueprintdbcmd.exe /object USER /command ADD /datasource
     LOCALHOST /catalog <database> /integratedsec TRUE /nuseridentity
     "IIS APPPOOL\<AppPoolName>"
     ```

     Example:

     ```
     blueprintdbcmd.exe /object USER /command ADD /datasource
     LOCALHOST /catalog BlueprintDB /integratedsec TRUE /nuseridentity
     "IIS APPPOOL\BlueprintAP"
     ```

   - If you chose the **Custom account** option:

     ```
     blueprintdbcmd.exe /object USER /command add /datasource <db_
     server>\<instancename> /catalog <database> /integratedsec TRUE
     /nuseridentity <new_user_id>
     ```

     Example:

     ```
     blueprintdbcmd.exe /object USER /command ADD /datasource
     DBSERVER\INSTANCE01 /catalog BlueprintDB /integratedsec TRUE
     /nuseridentity "acme\rrunner"
     ```

Changing the spell check dictionary language

Blueprint allows you to change the spell check dictionary language so users can leverage Blueprint's spell checking capabilities even if they write requirements in a different language. After a dictionary has been selected and

configured, all Blueprint users on that particular instance will automatically utilize that particular dictionary for their spell checking needs. Users can disable spell checking, but they cannot configure the dictionary.

The default language is **en-US (Enlish - United States)**.

To change the spell check dictionary language:

1. Locate the dictionary file that you want to use.

   The dictionary files (**dictionary.dct**) for each supported language are available in the following folder:

   C:\Program Files (x86)\Blueprint Software Systems\Blueprint\Web\Dictionary\Languages

2. Overwrite the active (default) dictionary file with the desired dictionary file.

   The active (default) dictionary file is stored here:

   C:\Program Files (x86)\Blueprint Software Systems\Blueprint\Web\Dictionary\default\dictionary.dct

> **Example**
>
> If you want your users to utilize a French spell check dictionary, copy this file:
>
> **C:\Program Files (x86)\Blueprint Software Systems\Blueprint\Web\Dictionary\Languages\fr-FR (French - France)\dictionary.dct**
>
> and use it to overwrite this file:
>
> **C:\Program Files (x86)\Blueprint Software Systems\Blueprint\Web\Dictionary\default\dictionary.dct**

The new spell check dictionary becomes effective immediately. If a client was already using Blueprint prior to the dictionary update, the new spell check dictionary becomes effective after the client browser cache is cleared.

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 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**.
3. Select the **Enable Federated Authentication** option.
4. Set your federated authentication settings:
   - Click **Replace** 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

5. Click **Save**.

Setting up email notifications

E-mail 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.

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

Perform the following steps if you want to configure e-mail settings and enable notifications in Blueprint:

1. Open the *Instance Administration Console*.
2. Click **Manage** > **E-mail Settings** on the ribbon (*Instance Admin* tab, *Instance* group).
3. Enter your SMTP server settings and preferences:

    - **Enable Notifications**: Defines whether or not e-mail notifications are enabled. This option must be selected to enable notifications in Blueprint.
    - **Server IP / Hostname**: Defines the IP address or hostname of your SMTP server.
    - **Port**: Defines the port number of your SMTP server.
    - **Sender E-mail**: Defines the e-mail address that will appear in the From address for all e-mail notifications.
    - **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 username and password.

        - **User Name**: Defines the user name of a user with access to the SMTP server.

            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.

4. Click **Save**.

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

Adding users to Blueprint

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

- 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.

  - Click **Manage Users And Groups** > **Users** on the ribbon (*Instance Admin* tab, *Instance* group).
  - Click **New** > **New Windows User** on the ribbon (*Instance Admin* tab, *Manage Items* group).
  - 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.

  - Type **`Ctrl-a`** to select all users and then click **OK**.
- Complete the following steps to add a single database user to Blueprint:
  - On the *Users* tab, click **New** > **New Database User** on the ribbon (*Instance Admin* tab, *Manage Items* group).
  - Enter the user information on the right side of the window.
  - 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. A user's effective access in Blueprint is the intersection of their project role assignment and their license.

> **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 **Contribute**.

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 Admininistration** 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**: A user's effective access in Blueprint is the intersection of their project role assignment and their license.

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.
    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**.