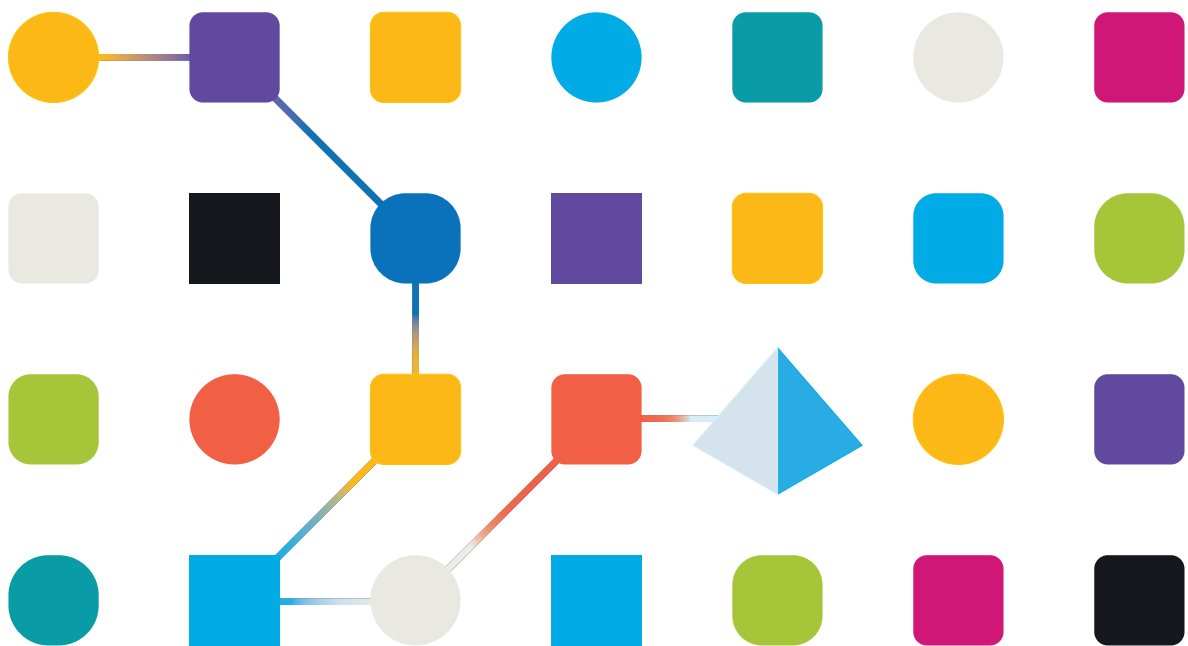




Blue Prism Hub 4.6

Administrator Guide

Document Revision: 1.0



Trademarks and Copyright

The information contained in this document is the proprietary and confidential information of Blue Prism Limited and should not be disclosed to a third-party without the written consent of an authorized Blue Prism representative. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying without the written permission of Blue Prism Limited.

© Blue Prism Limited, 2001 – 2023

“Blue Prism”, the “Blue Prism” logo and Prism device are either trademarks or registered trademarks of Blue Prism Limited and its affiliates. All Rights Reserved.

All trademarks are hereby acknowledged and are used to the benefit of their respective owners. Blue Prism is not responsible for the content of external websites referenced by this document.

Blue Prism Limited, 2 Cinnamon Park, Crab Lane, Warrington, WA2 0XP, United Kingdom.
Registered in England: Reg. No. 4260035. Tel: +44 370 879 3000. Web: www.blueprism.com

Contents

| | |
|---|----------|
| Hub | 4 |
| Intended audience | 4 |
| Administration and configuration | 5 |
| Hub restrictions | 6 |
| Settings | 7 |
| Overview | 7 |
| Platform management | 7 |
| User management | 8 |
| Profile | 9 |
| Audit | 10 |
| Environment management | 13 |
| Email configuration | 16 |
| Customization | 19 |
| Plugin management | 21 |
| Users | 24 |
| Roles and permissions | 32 |
| Registrations | 39 |
| Authentication settings | 41 |
| Service accounts | 52 |

Hub

Blue Prism brings together the principles of cloud, Robotic Process Automation (RPA) and artificial intelligence (AI) designed to automate and digitize the execution of knowledge-based work. Digital workers are deployed into business operations and work by emulating the way people use business systems, the decisions they make and the processes they follow, to augment, replace, or digitize manual work processes.

As the digital workforce landscape matures in an organization, operators and sponsors need to scale their approaches and methodologies to manage their automation investment. Management information on the digital workforce needs to be transparent across the business and intuitive to interpret, in addition best-practices need to be monitored to ensure alignment to industry standards. Blue Prism® Hub provides new and existing Blue Prism users with a productivity platform for the management of the automation lifecycle. Hub caters for the individual roles within the robotic operating model (ROM) with a set of capabilities to ensure the successful, scalable delivery of an automation strategy.

Hub has been created as a lightweight 'empty' application which is then populated by a series of plugins or features. This forms what is referred to as the plugin architecture which allows the Blue Prism team to iterate features and make them available for consumption by Hub administrators.

Each Hub instance contains a Plugin Repository page that allows administrators to view and deploy new plugins as well as update existing plugins.

Intended audience

This guide is aimed at Hub users with administrator privileges, known as Hub administrators. Hub administrators are responsible for managing the Blue Prism Hub platform, including, but not limited to:

- Managing the integration between the Blue Prism Hub platform, Blue Prism, and the Blue Prism APIs.
- Managing roles and users, including integration with Active Directory.
- Installing plugins.
- Monitoring audit logs.

As such, Hub administrators should be users who are familiar with managing IT systems, and have an understanding of enterprise software architecture and Active Directory.

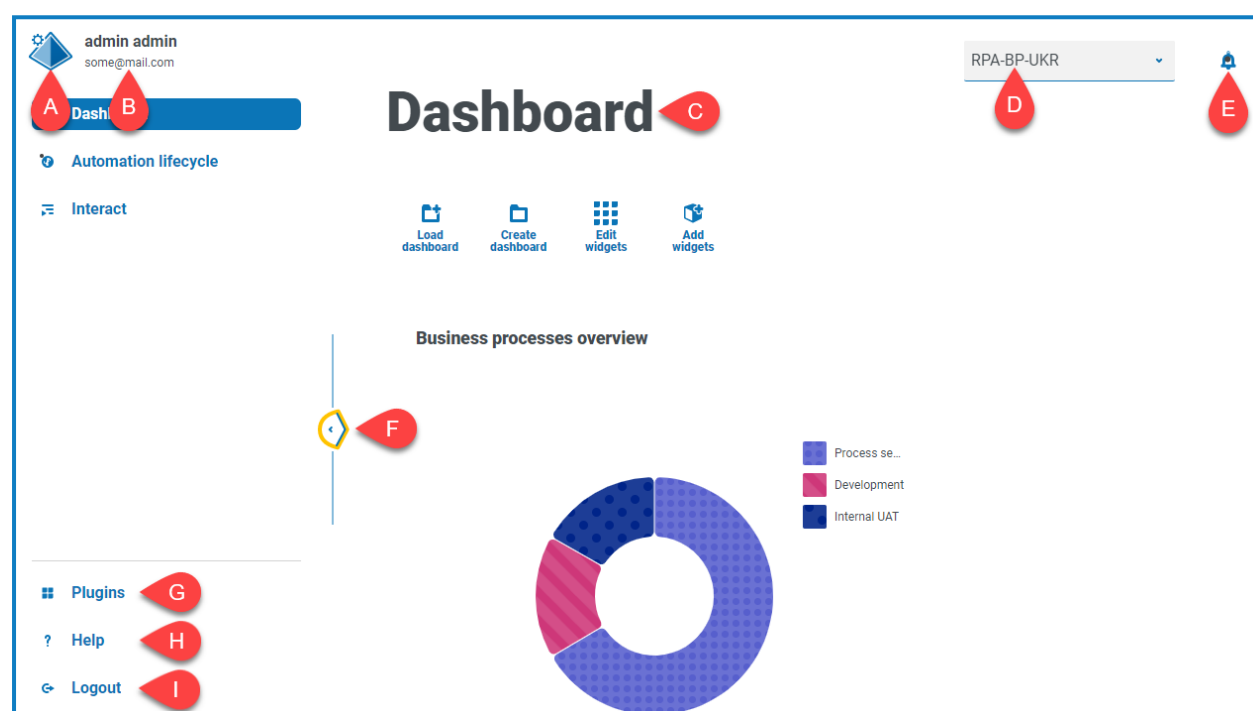
Administration and configuration

When Hub is installed for an organization, it is delivered with a main administrator role. This role is used to configure the environment with information for items such as email and connection to your RPA database.

Hub utilizes Role Based Access Control (RBAC) to ensure that users can only access functionality required to perform their role within their organization.

The top navigation bar in Hub provides access to the system settings. The settings that are available depend upon the user role. There are a number of settings which are not available to users without administrator capabilities enabled on their account, as detailed below.

The features on the top navigation bar include:



When the navigation menu on the left is expanded (as shown above), these features are shown:

- A. **Profile icon** – Defined by the user in their [profile](#). If you are:
 - A user, this provides a link to your [profile](#) page.
 - An administrator, this provides a link to the system [settings](#) from which the following can be controlled:
 - Personal profile and audit.
 - Platform management.
 - User management.
- B. **User information** – This is hidden when the navigation menu is collapsed.
- C. **Page title** – The area of the Hub user interface you are currently using.
- D. **Environment** – The currently selected environment. Environments are set up in the [environment manager](#) and can be selected here.
- E. **Notification alerts** – Notifications are created by the [Automation Lifecycle Management](#) plugin. Only notifications that you are authorized to see, or that are applicable to you, will show when you click the alert.

- F. **Toggle menu** – Opens and closes the menu. When the menu is open, the names of the menu items display. When the menu is closed, icons display for each menu item.
- G. **Plugins** – Opens the Plugins page where you can view and download available plugins.
- H. **Help** – Opens the Online Help. Right-click and select **Open link in new tab** to open in a separate browser tab.
- I. **Logout** – Logs you out of authentication server.

 If you use Interact, you will also be logged out of the Interact web application.


Hub restrictions

The following table list the restrictions enforced when using Hub.

| Item | Restriction | Related sections |
|-----------------------|--|--|
| Username | <p>Username for native users cannot exceed 25 characters in length. They can only contain Latin characters (excluding special characters), digits, periods, hyphens, and underscores. They cannot start with periods, hyphens, and underscores.</p> <p>Username for Active Directory users (their UPN) cannot exceed 255 characters in length.</p> | Users on page 24 |
| Password Restrictions | <p>Passwords must:</p> <ul style="list-style-type: none"> • Contain at least 1 upper-case • Contain at least 1 number • Contain at least 1 special character • Be at least 8 characters in length • Be different to the last five passwords • Be no longer than 32 characters | Profile on page 9 and Users on page 24 |
| Profile Image | Less than 1MB and no greater than 1920 x 1080 pixels | Profile on page 9 |
| Dashboard Widgets | Limited to 20 widgets per dashboard | Dashboards – see the Hub User Guide . |
| Brand Logo | PNG, JPEG or JPG no greater than 30KB | Customization on page 19 |

Settings


The Settings page enables you to manage Hub. You only have access to the Settings page if you are an administrator. If you are a user, you will only have access to the [Profile page](#) which opens when you click your profile icon.

 To open the Settings page, click your profile icon. The Settings page displays if you are an administrator. The Profile page displays if you are a user.

Overview

| | |
|----------------|--|
| Profile | The Profile page enables you to change your information, display preferences and your password. For more information, see Profile on page 9 . |
| Audit | Administrators can view a history of audited system activities. For more information, see Audit on page 10 . |

Platform management

 The email and database settings are defined as part of the Hub installation and configuration process, see the [Hub installation guide](#). These are essential for normal operation.

| | |
|-------------------------------|---|
| Environment management | Administrators can add connections to Blue Prism RPA databases, manage existing connections and delete redundant RPA databases. For more information, see Environment management on page 13 . |
| Email configuration | Administrators can change the SMTP host details. Changes should be made in conjunction with your own IT Support team to ensure that the configuration and credentials match your organization's email server. For more information, see Email configuration on page 16 . |
| Customization | Administrators can customize the theme used by the Interact user interface. The theme allows the administrator to set the theme name, brand color and brand logo. For more information, see Customization on page 19 . |
| Plugin management | Administrators can view the currently installed plugins description and version number. Any updates or additional available plugins are also shown. For more information, see Plugin management on page 21 . |

User management


| | |
|--------------------------------|--|
| Users | Administrators can add, modify or retire users, and assign their access permissions and roles. For more information, see Users on page 24 . |
| Roles and permissions | Administrations can add, edit, and delete roles. For more information, see Roles and permissions on page 32 . |
| Registrations | Administrators can manage registration requests that new users have raised for access to Interact. For more information, see Registrations on page 39 . |
| Authentication settings | Administrators can enable, disable, and configure authentication settings. For more information, see Authentication settings on page 41 . |
| Service accounts | Administrators can add, edit, or delete service accounts. For more information, see Service accounts on page 52 . |

Profile


Profile settings allow you to change your information and Hub viewing preference. The profile settings you can change depend on the authentication type configured for your account. If you are a native administrator, you can change:

- Your password.
- Your profile first and last names.
- Your email address.
- Your profile picture – this displays in the profile icon. This image will only be used in Hub.
- Your Hub display theme – dark or light.

If your Hub account is configured to use Active Directory authentication, you can only change your profile picture and your Hub display theme. All other settings are managed in Active Directory and updated when you log into Hub or when manually synchronized.

 You cannot change your username, regardless of your authentication type.

For more information on authentication types, see [Authentication settings](#).


 To open the Profile page, click your profile icon to open the Settings page, and then click **Profile**.

Change your profile

1. On the Profile page, click **Edit**.

The Profile page becomes editable, indicated by the **Edit** button changing to a **Cancel** button and the fields becoming editable.

2. Update the following as required:
 - Update your first name, last name or email address.
 - Toggle the **Dark theme** on or off. By default, Hub is displayed in the light theme.
 - Click **Upload** to select your profile image. The image will be displayed within the prism icon. Images cannot be greater than 1 MB in size.
3. Click **Save** to save your changes. If you do not want to save your changes, click **Cancel**.

 The **Save** button will only become active once you have made a change to the theme setting.

Change your password

1. On the Profile page, click **Update password**.


The Update your password dialog displays.




















2. Enter your current password.
3. Enter and repeat your new password.
4. Click **Update**.

Your password is changed.

Audit

Audit enables you to view audited system activities.

 To open the Audit page, click your profile icon to open the Settings page, and then click **Audit**.

| Audit | | | | | | | | | |
|---|---|---|---|--------------------------------------|------------------|--------------------------|--|---------------------|---|
| <div> <div> Edit view</div> <div> Filter</div> <div> Save view</div> <div> Load view</div> </div> | | | | | | | | | |
|  A |  B |  C |  D | Category | Event | Audited By | IP address | Created On | Actions |
|  E | | | | b884e3ec-0cd0-423a-93b3-8780c0751503 | User management | User login |  admin | 13/01/2022 10:21:05 |  |
| | | | | ddb623a5-fbe1-47bd-a11f-5560e9e60f0a | User management | User login |  admin | 13/01/2022 09:35:26 |  |
| | | | | a8b12576-59aa-492e-96b8-786dd724e9dd | Business process | Created business process |  admin2 | 13/01/2022 09:22:59 |  |
| | | | | e95f5873-ab4e-4450-8b96-b0abd24d9f44 | User management | User login |  admin2 | 13/01/2022 09:20:42 |  |
| | | | | edca5e58-bab2-42ac-903d-36d3d6e37b71 | User management | User logout |  admin | 13/01/2022 09:20:30 |  |
| <div> <div>Rows per page</div> <div>5</div> <div>Page 4 of 138 (686 total rows)</div> <div> <div>← Previous</div> <div>Next →</div> </div> </div> | | | | | | | | | |

The Audit page provides you with the following information and functions:

- Edit view** – Define the columns that are displayed. You can then show or hide the columns using the toggle switches.
- Filter** – Filter the information that is displayed. You can turn on the [required filters](#) and enter or select the appropriate information for display, for example, you could turn on the **Category** filter and select **User management**.
- Save view** – Save your current column settings. You can enter a name for your view to make it easily identifiable when loading views.
- Load view** – Load a saved view. You can select the required view and click **Apply**.
- View log** – View the [details](#) of an audit item.
- Rows per page** – Enter a number, or use the up and down arrows, to change the number of rows seen on a page.
- Previous and Next** – Click **Previous** or **Next** to move through the pages of audit items.

View an item

- On the Audit page, select the check box for the item you want to view.
- Click **View log**.




The details of the event displays.

Use the filters on the Audit page

The filters enable you to easily find audit events based on the selected criteria.

1. On the Audit page, click **Filter** to open the Filter panel.
2. Use the toggle to turn on the required filter and complete the information to find the audit event. You can apply multiple filters at the same time.

The available filters are:

| Filter | Description |
|-----------------|---|
| Audit ID | Enter the audit identifier, or part of the identifier. |
| Category | <p>Select a category from the drop-down list. The available categories are:</p> <ul style="list-style-type: none"> • User management – Includes events related to users, such as management of users by administrators and user access information. • SMTP management – Includes changes to SMTP settings. • Role management – Includes events related to roles. • Authentication management – Includes events related to Authentication settings, such as management of the connections and syncing. • Service accounts – Includes events related to Service accounts, such as management of the accounts and key regeneration. • Business process – Includes events related to business processes, such as creating, retiring, and activating business processes. <div>  If you select a category, the options in the Event filter will be limited to only those that are in the selected category. </div> <p>If you have the following plugins installed, these additional categories are also available:</p> <ul style="list-style-type: none"> • Automated Lifecycle Management (ALM): <ul style="list-style-type: none"> • Process definitions – Includes events related to process definitions, such as the management of the definitions and the sign off workflow. • Interact: <ul style="list-style-type: none"> • Interact - Forms – Includes events related to the Interact Forms plugin, such as the management of the forms, and increasing the major version number. • Interact submissions – Includes events related to Interact, such as the end-user submission of forms and approval workflow. |
| Event | <p>Select an event from the drop-down list. This display all results for this specific audit event.</p> <div>  If you use the Category filter, the events shown in the drop-down list are limited to those for that category. </div> <div>  If you want to view all the events for a selected category, turn the Event filter off and just use the Category filter. </div> |

| Filter | Description |
|------------|---|
| Audited By | Enter a user's username or account name, or part of the name. |
| IP address | Enter the public IP address, or part of the address. |
| Created On | <p>Enter a date range:</p> <ul style="list-style-type: none">• In the first field, select the earliest date.• In the second field, select the latest date.• If required, adjust the time fields. By default, the earlier date has the time 00:00:00 and the later date has the time 23:59:59, thereby including the full day. <p>This displays any audit events during this time frame.</p> |

The information on the Audit page is immediately filtered.

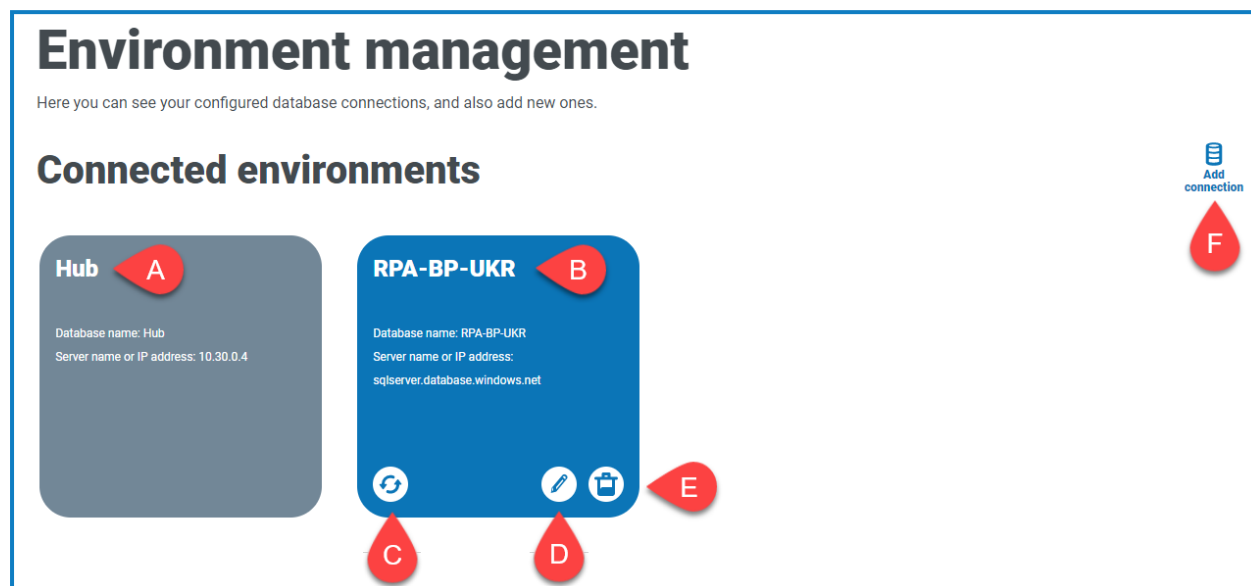


If you have set the filters but want to view the unfiltered information again, either click **Reset filters** in the panel, or turn off the required filters, or remove any settings within the filter so that it is blank.

3. Click **Close drawer** to close the filter panel.


Environment management

The environment manager displays your connected databases.



The Environment page provides you with the following information and functions:

- A. The Hub database.
- B. The Blue Prism database that was configured as part of the initial installation process.
- C. Refreshes the details of the digital workforce and queues across to Hub. Refresh the database whenever any connections are added or changed. If the database is not refreshed, you will not be able to see the digital workers or queues in that particular Blue Prism environment.
- D. Opens the Edit connection page which allows you to [edit database details](#).
- E. Deletes the database connection. See [Delete a database connection](#) for more information.
- F. Opens the Add connection dialog which allows you to configure and [add a new Blue Prism database connection](#).

 To open the Environment manager, click your profile icon to open the Settings page, and then click **Environment management**.

Add a Blue Prism database connection

1. On the Environment manager page, click **Add connection** to add an additional RPA database connection.

The Add connection page displays.

2. Enter the database connection configuration parameters.

Add connection

Once you've configured and added a connection, it will appear in your list of environments.

Environment details

Environment name *

Enter your friendly name for this environment.

Database configuration

Authentication type *

This will determine the form of authentication your database uses.

☒ SQL with SQL authentication

☐ SQL with Windows Authentication

☐ SaaS SQL

Server name or IP address *

This will be the server name or IP address of where your Blue Prism database resides.

Database name *

This will be the name of your Blue Prism database.

Timeout *

This will be the elapsed time if a connection is not found.

Database authentication

User ID *

Password *

API configuration

URL

Please enter the URL, which references your desired API.

Add connection

When all the fields are complete, the **Add connection** link is available.



You must ensure that your database password does not contain an equals sign (=) or a semi-colon (;). These characters are not supported, and will lead to issues when trying to connect to the database.

3. If required, enter the URL for the Blue Prism API in the URL field under API configuration. This URL is required if you want to use the Control room plugin. The Control room plugin is compatible with Blue Prism 7.0 or later.
4. Click **Add connection** to save the details.
The connection is created and displayed in the environment manager.
5. In the Environment manager, click the refresh icon on your new connection. This updates the information in Hub with the digital workforce and queues held in the database.

Edit database details

You can only edit the URL field under API configuration. All other fields are disabled.

1. On the Environment manager page, click the **Edit** icon on the database connection that you would like to update.

The Edit connection page displays.

2. Enter the URL under the **API configuration** section.



You must enter the full URL including the protocol, such as, http:// or https://. For example:
`https://bpapi.yourdomain.com`

3. Click **Save**.
4. In the Environment manager, click the refresh icon on your updated connection. This updates the information in Hub with the digital workforce and queues held in the database.

Delete a database connection

You can delete a connection to a database only if there are no dependencies on that database. You will not be able to delete a database if:

- Interact forms are dependent on a queue within that RPA database, for example, submitting a form to a queue.
- The ALM process definitions use objects defined within that RPA database.

You must amend the forms or process definitions to point at an alternative database to remove the dependance.

The delete function allows you to remove any databases that have accidentally been added and are not in use, for example, if the wrong database information has been added during configuration.

To delete an RPA database:

1. On the Environment manager page, click the delete icon on the database tile.
If there are no dependencies, a message displays asking you to confirm the deletion. If there are dependencies, an error message displays in the top right corner of the Hub user interface.
2. Click **Yes** to confirm the deletion.


Email configuration

Email settings allows you to change the configuration of SMTP and configure email for notifications, such as password reset requests from users. Changes should be done in conjunction with your own IT Support team to ensure that the configuration and credentials match your organization's email server.

You can configure your email settings to use one of the following authentication methods:

- Username and password
- Microsoft OAuth 2.0

Whenever you save the SMTP settings, a test email is sent to you to ensure the setup is correct. If you don't receive a test email after saving the changes, check the details and update accordingly.

 To open the Email configuration page, click your profile icon to open the Settings page, and then click **Email configuration**.

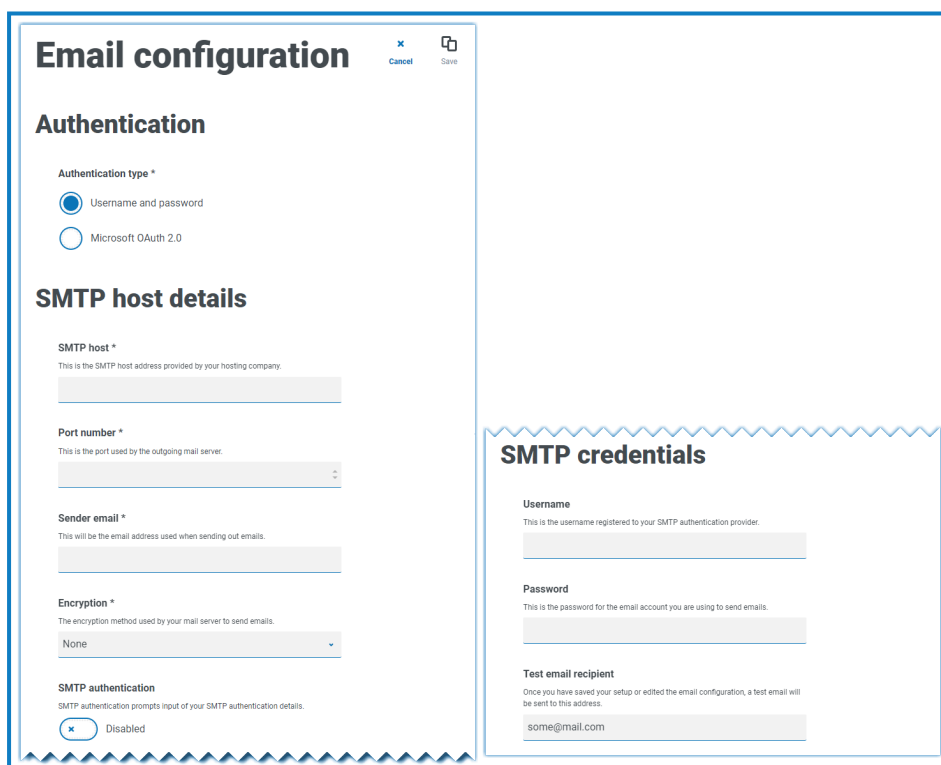
Update the email settings

The email settings are entered as part of the initial configuration of Hub. You only need to change these settings in the event of an IT infrastructure change, such as a different SMTP host, or a change to the existing host which affects these settings.

Username and password authentication

1. On the Email configuration page, click **Edit**.
2. In the Authentication section, under **Authentication type**, select **Username and password**.

The Email configuration page refreshes to display the appropriate fields:



The screenshot displays the 'Email configuration' dialog box. It features a title bar with 'Cancel' and 'Save' buttons. The main content is divided into three sections: 'Authentication', 'SMTP host details', and 'SMTP credentials'. The 'Authentication' section has two radio buttons: 'Username and password' (selected) and 'Microsoft OAuth 2.0'. The 'SMTP host details' section includes input fields for 'SMTP host', 'Port number', and 'Sender email', each with a descriptive subtitle. The 'Encryption' section has a dropdown menu currently set to 'None'. The 'SMTP authentication' section has a 'Disabled' checkbox. The 'SMTP credentials' section, which has a decorative wavy border, contains input fields for 'Username' and 'Password', and a 'Test email recipient' field with the example email 'some@mail.com'.


3. Enter the following information:

- **SMTP host** – The address of your SMTP host.
- **Port number** – The port number used by the outgoing mail server.
- **Sender email** – The email address that is used when sending emails. The email recipients will see this as the From address.
- **Encryption** – The encryption method used by the email server to send the emails.
- **SMTP authentication** – Select this if the SMTP authentication prompts for input of authentication details. If you set this to **Enabled**, the **Username** and **Password** become mandatory fields.
- **Username** – The username for the SMTP authentication.
- **Password** – The password for the account.
- **Test email recipient** – The test email will be sent to this email address. This defaults to the email address of the user who is making the changes and cannot be changed.

4. Click **Save** to save your changes.

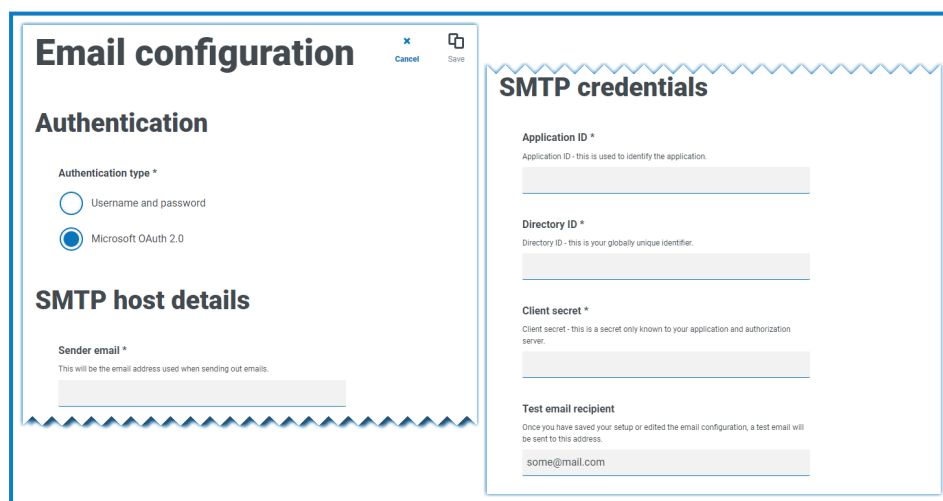
Microsoft OAuth 2.0 authentication

You can use the Microsoft OAuth 2.0 authentication service provided by Azure Active Directory to connect to the SMTP host. Your IT Support team will need to register an application in Azure AD and provide you with the Application (client) ID, Directory (tenant) ID and the client secret to complete the information in step 3. For information about finding these details in Azure AD, see the [Microsoft documentation](#).

 If you are using Microsoft OAuth 2.0, the Mail.Send permission in Azure Active Directory must be enabled. This must be configured by your IT Support team in Azure Active Directory. For more information, see [Troubleshoot a Hub installation](#) in the Blue Prism Hub Install Guide.

1. On the Email configuration page, click **Edit**.
2. In the Authentication section, under **Authentication type**, select **Microsoft OAuth 2.0**.

The Email configuration page refreshes to display the appropriate fields:



The screenshot shows the 'Email configuration' dialog box with the 'Authentication' section selected. Under 'Authentication type', 'Microsoft OAuth 2.0' is selected. The 'SMTP host details' section shows a 'Sender email' field. The 'SMTP credentials' section on the right contains fields for 'Application ID', 'Directory ID', 'Client secret', and 'Test email recipient'.

Email configuration [Cancel] [Save]

Authentication

Authentication type *

☐ Username and password

☒ Microsoft OAuth 2.0

SMTP host details

Sender email *

This will be the email address used when sending out emails.

SMTP credentials

Application ID *

Application ID - this is used to identify the application.

Directory ID *

Directory ID - this is your globally unique identifier.

Client secret *

Client secret - this is a secret only known to your application and authorization server.

Test email recipient

Once you have saved your setup or edited the email configuration, a test email will be sent to this address.

some@mail.com

3. Enter the following information:

- **Sender email** – The email address that is used when sending emails. The email recipients will see this as the From address.
- **Application ID** – This information is the Application (client) ID defined in Azure AD and will be provided to you by your IT Support team.
- **Directory ID** – This information is Directory (tenant) ID defined in Azure AD and the will be provided to you by your IT Support team.
- **Client secret** – This is the client secret as generated by Azure AD and will be provided to you by your IT Support team and controls the authentication process
- **Test email recipient** – The test email will be sent to this email address. This defaults to the email address of the user who is making the changes and cannot be changed.


4. Click **Save** to save your changes.

Customization

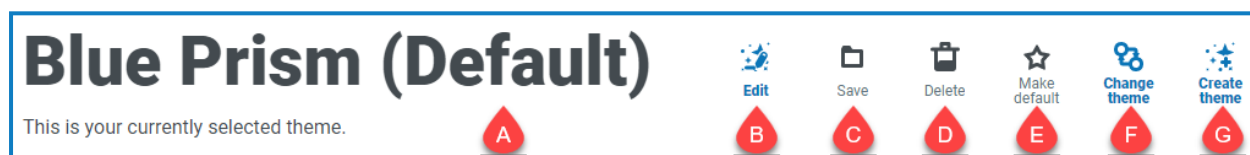
Customization settings allow you to change the appearance of the Interact user interface. You can create themes that control the following:

- **Theme name** – This is also the brand name that will appear on the user interface.
- **Brand color** – This is the color that will be used by buttons and labels in the user interface.
- **Brand logo** – This is an image that will be used as the logo on the user interface.

You can create multiple themes which can be applied dependent upon the user, providing a different look and feel depending on who logs in. The default theme is automatically selected when creating a user, however, this can be changed.

 To open the Customization page, click your profile icon to open the Settings page, and then click **Customization**.

When you open the Customization page, the default theme displays:



This provides you with the following information and functions:

- A. Name of the currently displayed theme.
- B. [Edit](#) – Edit the theme that is currently displayed.
- C. [Save](#) – Save any changes you have made. This icon is only active when you are editing a theme.
- D. [Delete](#) – Delete the currently displayed theme. This icon is only active if you have more than one theme.
- E. [Make default](#) – Set the currently displayed theme to be the default for the system. This icon is only active if the current theme is not the default.
- F. [Change theme](#) – Select which theme you want to display on the page.
- G. [Create theme](#) – Create a new theme.

Edit and save a theme


1. On the Customization page, click **Edit theme**.

The Theme page becomes editable, indicated by the **Edit theme** button changing to a **Cancel** button and the **Reset** buttons becoming active.

2. If required, change the theme **Name**.


As you type, the Create theme title also changes.

3. If required, change the **Primary color** by clicking the color bar. You can:

- Select a color using the sliding bar.
- Enter a value using the text boxes. You can click on the  icon to toggle between the different types; RGB, HSL or Hex.

4. If required, click **Upload** to change the logo to a file of your choice.

5. Click **Save** to save your changes. If you do not want to save your changes, click **Cancel**.

 The **Save** button will only become active once you have made a change to theme setting.

Delete a theme

1. With the theme you want to delete shown on the screen (see [Change the theme below](#)), click **Delete**.

A message displays asking you to confirm the deletion.


2. Click **Yes** to delete the theme.

Set a new default theme

1. With the theme you want to use shown on the screen (see [Change the theme below](#)), click **Make default**.

(Default) appears next to the theme name and a notification appears confirming the change. The theme change will be seen in Interact.

Change the theme

 The **Change Theme** icon changes the theme that you are currently viewing. If you want to make changes to the theme itself, you need to [edit](#) the theme.

1. On the Customization page, click **Change theme**.

A list of available themes displays.

2. Click the theme you want to view.

The selected theme displays.

3. Close the list to return to the main tools.

Create a new theme


1. On the Customization page, click **Create theme**.

The Create theme page displays.

2. Enter the theme **Name**.

As you type, the Create theme title also changes.

3. Click the **Primary color** bar to change the color. You can:

- Select a color using the sliding bar.
- Enter a value using the text boxes. You can click on the  icon to toggle between the different types; RGB, HSL or Hex.

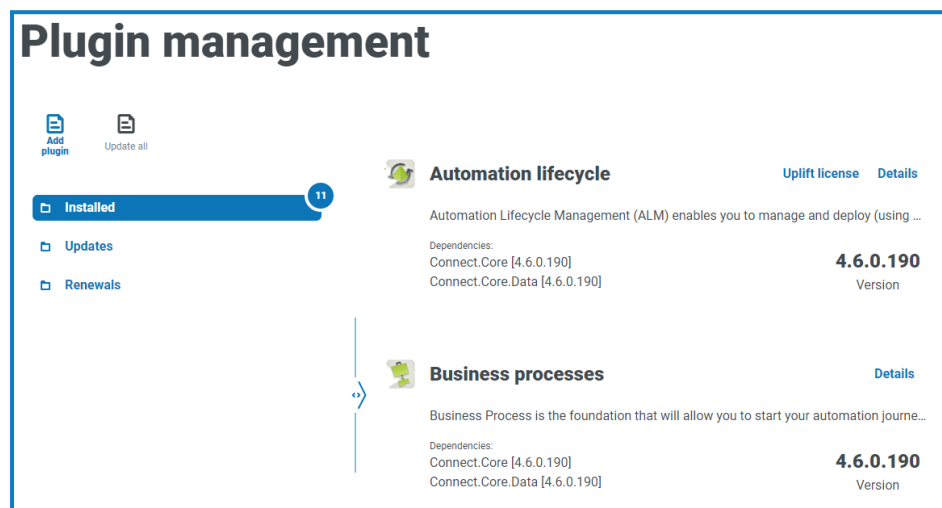
4. Click **Upload** to change the logo to a file of your choice.

5. Click **Create theme** to save your new theme.

Plugin management

Plugin management displays the details of the installed plugins, some of these are available by default during the installation process. You can manage your existing plugs, update them and add new plugins.

Plugins are the heart of Hub and are self-contained features that can be individually installed and customized to provide information about your automated processes. Some plugins also provide development tools to assist in the building of automations.



To open the Plugin management page, click your profile icon to open the Settings page, and then click **Plugin management**.

View installed plugins

When you open Plugin management, the currently installed plugins are displayed. The plugin name, an extract from the description and the version numbers are shown. To view:

- More information about a plugin, click **Details**.
- Information about any updates, click **Updates**. Note that this feature is not currently available for Hub on-premises.
- Information about any upcoming or pending license renewals, click **Renewals**. If any plugins require a license renewal, a number is shown next to the **Renewals** link showing the number of updates. If no number is shown, there are no renewals.

Add a plugin

When a plugin is installed, the website will automatically restart. It is therefore essential that the installation of plugins is performed out of hours or during maintenance windows.

1. On the Plugin management page, click **Add plugin**.
The Open dialog displays to enable you to find a local file.
2. Navigate to, and select, the plugin file and click **Open**.
The plugin file uploads and installs. The website automatically restarts to complete the installation.

Update plugins

When an update is available, a number appears next to the **Updates** link.

This functionality is only available for Hub on-premises installations immediately following an upgrade. The on-premises version is unable to check for updates online between upgrades.

1. On the Plugin management page, click **Updates**.
The potential updates display showing details of the new version.
2. Click **Update all** to update all the plugins.
A message displays confirming the plugins have been updated.
3. Click **OK**.
The site restarts.

Uplift license

The **Uplift license** option is only available when there has been an update to the licensing model used by a plugin between released versions. It enables you to load a new license for your plugin outside of the normal renewal period.

1. On the Plugin management page, click **Installed**.
The installed plugins display.


The screenshot displays the 'Installed' tab of the Blue Prism Hub plugin management interface. It lists three installed plugins: 'Automation lifecycle', 'Business processes', and 'Forms'. Each plugin entry shows its description, dependencies (Connect.Core [4.3.0.142] and Connect.Core.Data [4.3.0.142]), and the version number 4.3.0.142. There are links for 'Uplift license' and 'Details' for each plugin. The left sidebar shows 'Installed' as the selected tab, with 'Updates' and 'Renewals' also visible.

2. Click **Uplift license** for the required plugin. In the example above, the option appears for Automated lifecycle.

The Renew license key panel displays.

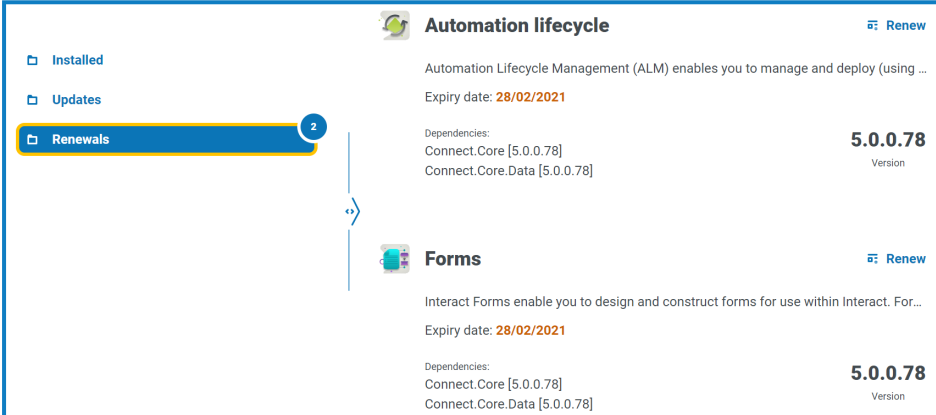
3. Upload a valid license and click **Finish** to apply.

Renew plugins

 You are given 14 days notice before the license is due to expire.

1. On the Plugin management page, click **Renewals**.

The expiring plugins display.



| Plugin Name | Expiry Date | Version | Action |
|----------------------|-------------|----------|--------|
| Automation lifecycle | 28/02/2021 | 5.0.0.78 | Renew |
| Forms | 28/02/2021 | 5.0.0.78 | Renew |

2. Click **Renew** next to the required plugin.
3. Upload a valid license and click **Finish** to apply.

Users

User settings allow you to manage user accounts in Hub based on their authentication type. This can be Native authentication for native users, or Windows authentication for Active Directory users. You are also able to set the user's access to Hub and Interact and their roles within these. Before you configure users, it is recommended that [user roles](#) are configured.

The Users page displays a list of existing users. You can click on a user to view their information. If only native authentication has been configured in your environment, the Authentication type field is hidden.

ALM Approver

User details

Authentication type *
Native authentication

Username *
ALM_approver

First name *
ALM

Last name *
Approver

Email address *
alm_approver1@noreply.com

Theme *
Blue Prism (Default)

Assign roles and privileges

Select permission(s) *

☒ Hub
☐ Hub administrator
☐ Interact
☐ Approver

Hub roles
Automation Lifecycle Management

Interact roles



To open the Users page, click your profile icon to open the Settings page, and then click **Users**.

Find users

The Users page includes two methods for finding users:

- **Search** by username – This is located above the list of users. Start typing a user's name to filter the search results, the list dynamically filters as you enter more characters.
- **Filters** – The filters enable you to easily find a specific user or types of users based on the selected criteria. Click **Filter** to view and use the filters. By default, the filters are set to show you only the 'live' users and not the retired users. If you want to see all the users, turn off the **Live** filter. For more information, see [Use the filters on the Users page on page 30](#).

Add users

Add a native user

1. On the Users page, click **Add user**.

The Add user section displays.

Add user

User details

Authentication type *
Native authentication

Username *

First name *

Last name *

Email address *

Theme *
Blue Prism (Default)

Assign roles and privileges

Select permission(s) *

☐ Hub
☐ Hub administrator
☐ Interact
☐ Approver


Hub roles

Interact roles

Create user

2. Enter the user's details:

- **Authentication type** (if displayed) – Select **Native authentication**.

 This field only displays if both native and Windows authentication have been configured in your environment. If only native authentication has been configured, the added user is a native user by default.

- **Username** – Enter a username for the user.
- **First name** – Enter the user's first name.
- **Last name** – Enter the user's last name.
- **Email address** – Enter the user's email address.
- **Theme** – The default theme is automatically selected. You can select a different theme for the user. See [Customization on page 19](#) for more information about themes.

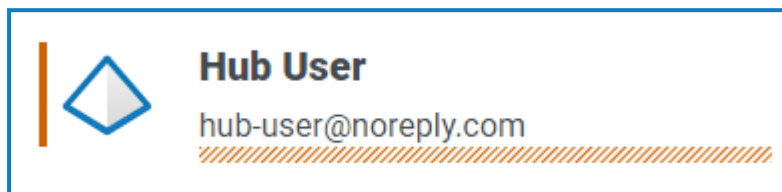
3. Select the permissions for the user:

- **Hub** – Select this check box for standard Hub users and administrators.
- **Hub administrator** – Select this check box to give administrator permissions to the user role. You must select **Hub** before this option becomes available.
- **Interact** – Select this check box to enable the user to be assigned Interact Forms. See the [Interact user guide](#) for more information.
- **Approver** – Select this check box to give approval rights for Interact to the user role. You must select **Interact** before this option becomes available.

4. Select the roles for the user:


- **Hub roles** – Select the Hub roles required for the user. If the required role has not yet been created, you can edit the user at a later date to assign new roles.

If the user is created without a Hub role, the user is underlined in the user list to indicate that the user setup has not been completed, for example:



The user will be able to log in to Hub, but they will not be able to perform any tasks as they will not have access to any plugins.

- **Interact roles** – Select the Interact roles required for the user. If the required role has not yet been created, you can edit the user at a later date to assign new roles. You can select more than one role.


 Users can also be added to roles from the [Roles and Permissions](#) page.

5. Click **Create user**.

The Create password dialog displays.

6. Select one of the password options:

- **Send the user a password update email** – This sends the user an email prompting them to enter a password on login using a link.
- **Manually update the user's password** – This enables you to set a password for the user.

 Passwords must obey the restrictions within Hub. For more information, see [Hub restrictions on page 6](#).

7. Click **Continue**.

- If you have selected to send the user a password update email, click **Finish** in the confirmation dialog.
- If you have selected to set a password for the user, set a password and click **Create**.

The new user displays in the list of users.

Add an Active Directory user

To add an Active Directory user, Windows authentication must be configured for your environment and Active Directory authentication must be enabled on the Authentication settings page. For more information, see [Authentication settings on page 41](#).

You can add an Active Directory user by following the steps below or by adding an Active Directory security group to a role where users who are members of the security role are automatically added to Hub when they sign in for the first time. For more information, see [Add Active Directory security groups to a role on page 34](#).

1. On the Users page, click **Add user**.

The Add user section displays.

2. In the **Authentication type** field, select **Windows authentication**.
3. Click **Search Active Directory**.

The Search Active Directory drawer opens.



Before searching for users in Active Directory, ensure that a username (UPN) and email address are populated for them in Active Directory.

4. Enter the search root for the Active Directory user you want to add. This is the distinguished name of the root location, for example, dc=bvdevops,dc=co,dc=uk.

You can also use wildcard search and apply search filters based on:

- **CN** – The Common Name attribute contains names of an object. If the object corresponds to a person, it is typically the person's full name.
- **UPN** – A User Principal Name is the name of a system user in an email address format. A UPN consists of the user name (logon name), separator (the @ symbol), and domain name (UPN suffix), for example, john.doe@domain.com.
- **SID** – A Security Identifier is a unique, immutable identifier of a user, user group, or other security principal. A security principal has a single SID for life (in a given domain) and all properties of the principal, including its name, are associated with the SID.

- Once you have entered the search criteria, click **Search**.

When searching Active Directory for users or security groups in Hub, the credentials stored against the domain in the Authentication Server database are used. If no stored credentials are found, queries that require additional authentication will be executed under the context of the Windows account running the Authentication Server application pool in IIS.

The available users display. You can scroll down to view all retrieved users.

Search Active Directory Reset filters Close drawer

Search root
dc=bpdevops,dc=co, dc=uk

Filter by Text matches (* available)

None

Search

- CN=azureuser,CN=Users,DC=bpdevops,DC=c...
- domainadmin@bpdevops.co.uk**
CN=domainadmin,CN=Users,DC=bpdevops,...
- domainuser@bpdevops.co.uk**
CN=domainuser,CN=Users,DC=bpdevops,DC...
- CN=Guest,CN=Users,DC=bpdevops,DC=co,D...

Apply

- Select the user you want to add and click **Apply**. You can only select one user at a time. Previously added users show as grayed out and cannot be selected.
- On the Add a user page, select the permissions and roles for the new user (see [Steps 3 and 4 in the Add a native user section](#)) and click **Create user**.

The new user displays in the list of users.


Active Directory users' credentials are managed in Active Directory so you do not need to create a password for the user. These users can log into Hub using single sign-on by selecting the **Log in using Active Directory** option on the login page.

Edit users

1. On the Users page, select the required user and click **Edit**.
2. Change the information as required.

If the user is:

- a native user, you can change the information as required.
- an Active Directory user, you can only change their roles and permissions. All other details are managed in Active Directory.

 You cannot change their username.

3. Click **Save** to apply your changes.

Synchronize an Active Directory user


1. On the Users page, select the required Active Directory user.
2. Click **Synchronize user**.

The following details of an Active Directory users are refreshed: UPN, username, full name, email address, and status (active, deleted, or disabled).

Retire native users

1. On the Users page, select the required user and click **Retire**.

A message displays asking you to confirm.

 You can use the **Live** filter to filter the user list for retired users. See [Find users on page 24](#).

2. Click **Yes**.

The user is retired and the **Retire** icon is replaced with the **Make live** icon. You can use this to reinstate the user if required. The user is also underlined in the user list to indicate they are retired.

Unlock native users

If a user enters their password incorrectly five times, they will be locked out of the system for three hours. Alternatively, you can unlock their account for them.

1. On the Users page, select the required user and click **Unlock**.

A notification message displays confirming the user has been successfully unlocked.

 You can use the **Locked** filter to filter the user list for locked users. See [Find users on page 24](#).

Change password for native users

Native users can change their own password using the Profile page (for more information, see [Profile on page 9](#)). If a user has forgotten their password, they can use the **Forgot password** link on the login page. However, you can change their password if needed. For example, you may need to do this in the scenario where a user was an Interact Approver and they have left your organization and there are outstanding forms to be approved in Interact by them. Depending upon your organization's policy, you could access their account and process these.

1. On the Users page, select the required user and click **Change password**.

The Change password screen displays.

2. Enter a new password for the user in both fields. The password must meet the character restrictions, however, the restriction regarding password reuse is not applied. For more information, see [Hub restrictions on page 6](#).
3. Click **Submit**.



A notification message displays confirming the user's password has been changed.


Use the filters on the Users page

The filters enable you to easily find a specific user or types of users based on the selected criteria.

1. On the Users page, click **Filter** to open the Filter panel.
2. Use the toggle to turn on the required filter and complete the information to find the user. You can apply multiple filters at the same time.

The available filters are:

| Filter | Description |
|----------------------|---|
| Full name | Enter the user's full name, or part of their full name. |
| Email address | Enter the user's email address, or part of their email address. |
| Locked | Select the locked status of the user from the drop-down list; the options are: <ul style="list-style-type: none">• Locked – Displays all the users who have had their accounts locked.• Unlocked – Displays all the users with unlocked accounts. |
| Live | Select the live status of the user from the drop-down list; the options are: <ul style="list-style-type: none">• Live – Displays all the users who have active log in credentials.• Retired – Displays all the users who have been retired by the administrator and can no longer log in. <div> By default, the Live filter is already turned on. You can turn this off if you want to view all the users.</div> |
| Setup status | Select the setup status of the user from the drop-down list; the options are: <ul style="list-style-type: none">• Setup correctly – Displays all the users who are correctly setup within Hub, that is, they have completed user credentials and assigned roles.• Needs action – Displays all the users who's user accounts are not correctly configured, for example, they may be missing their roles. |
| Domain | Enter the name of a domain, or part of a name. This matches against the domain names that are specified in the Authentication settings page, and displays any users that were imported into Hub from the matching domain. <div> If you have entered part of a domain name, the results display for all partial matches. There maybe users from other domains as well as the one you intended.</div> |

| Filter | Description |
|-------------------------|--|
| Connection name | <p>Enter the name of a connection, or part of a name. This matches against the connection names that are specified in the Authentication settings page, and displays any users that were imported into Hub using the matching connection.</p> <div>  If you have entered part of a connection name, the results display for all partial matches. There maybe users from other connections as well as the one you intended. </div> |
| Access | <p>Select the access level of the user from the drop-down list. These are based on the permissions level given to the user; the options are:</p> <ul style="list-style-type: none"> • Hub – Access to Hub. • Interact – Access to Interact. • Approver – Access to Interact with approver permissions. |
| Hub role(s) | Enter the name of the role, or part of the role name. This searches against any roles that have Hub set as the role type. |
| Interact role(s) | Enter the name of a role, or part of the role name. This searches against any roles that have Interact set as the role type. |
| Themes | Select the theme from the drop-down list. The users who have the selected theme are displayed. |

The information on the Users page is immediately filtered.



If you have set the filters but want to view the unfiltered information again, either click **Reset filters** in the panel, or turn off the required filters, or remove any settings within the filter so that it is blank.

3. Click **Close drawer** to close the filter panel.

Roles and permissions

Roles and permissions allow you to create roles and assign permissions to specific areas of Hub or Interact to these roles. Before you [configure users](#), it is recommended that user roles are configured. If roles are not configured, users will be able to log on but, without a role assigned, they will get a limited display and no access to features or functionality.

The Roles and permissions page displays a list of existing roles. There are predefined roles automatically created as part of the Hub installation process. These are indicated by a blue tick, for example, the Hub Administrator role. These automatically created predefined roles are locked and cannot be changed or deleted, although you can add users to them. You can click on a role to view the permissions.

Roles and permissions

Filter Create role

Role name

Automation Lifecycle Manag...
Hub ✓

Hub Administrator
Hub ✓

Human Resources
Interact

Hub Administrator


Edit Save Delete

Role information

Role name *
Hub Administrator

Role type *
☒ Hub
☐ Interact

Role description

 To open the Roles and permissions page, click your profile icon to open the Settings page, and then click **Roles and permissions**.

Find roles


The Roles and permissions page includes two methods for finding roles:

- **Search by role name** – This is located above the list of roles. Start typing the name of a role to filter the search results, the list dynamically filters as you enter more characters.
- **Filters** – The filters enable you to easily find a specific role or roles with specific permissions based on the selected criteria. Click **Filter** to view and use the filters. For more information, see [Use the filters on the Roles and permissions page on page 37](#).

Add roles

Based on the authentication type and settings configured for your environment on the [Authentication settings](#) page, there are several ways of adding users to the role you are creating:

- If native authentication is enabled, you can [add native users directly to a role](#).
- If Active Directory authentication is enabled, you can:
 - [Add Active Directory users directly to a role](#) – **Allow Active Directory users to be added directly to roles** must be enabled on the Authentication settings page.
 - [Add Active Directory security groups to a role](#) – The **Allow authorization via Active Directory security group membership** must be enabled on the Authentication settings page.

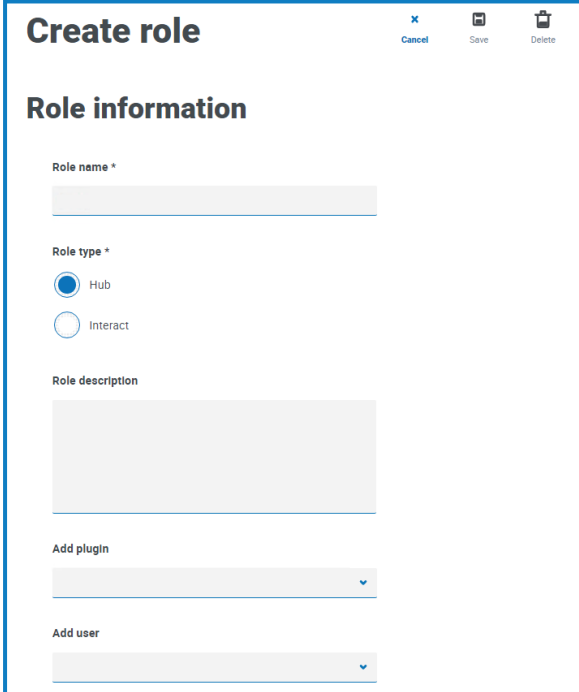
 If you are using Interact with Active Directory, be aware that some actions in the Interact Web API Service do not support the use of security groups. All actions support Active Directory users being directly assigned to Interact roles. For more information, see the [Interact Web API Service user guide](#).

Add users directly to a role

1. On the Roles and permissions page, click **Create role**.

The Create role section displays. If the environment is configured to allow [adding Active Directory security groups to roles](#), this page displays three tabs: Role information, Security groups, and Summary.

Example page when AD security groups cannot be added to roles:



Create role [Cancel] [Save] [Delete]

Role information

Role name *

Role type *

☒ Hub

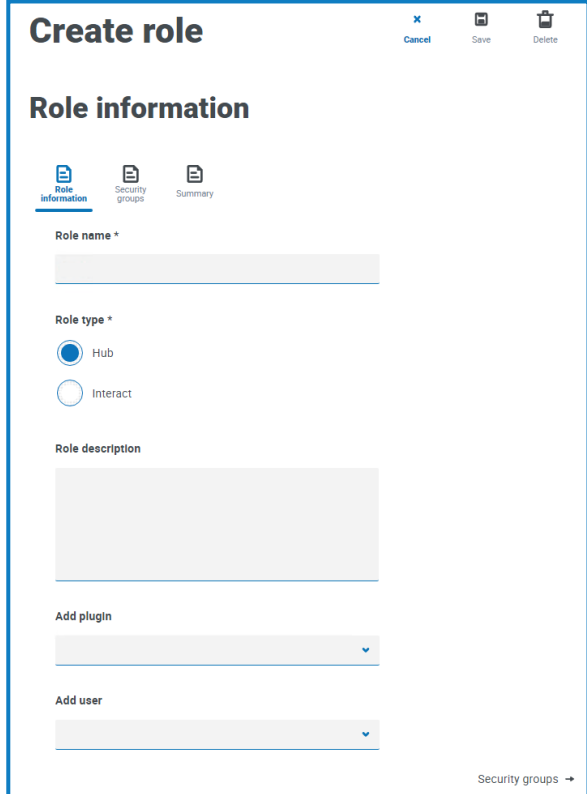
☐ Interact

Role description

Add plugin

Add user

Example page when allowing AD security groups to be added to roles:



Create role [Cancel] [Save] [Delete]

Role information

[Role information] [Security groups] [Summary]

Role name *

Role type *

☒ Hub

☐ Interact

Role description

Add plugin

Add user

Security groups →

2. Enter a role name and select whether it applies to **Hub** or **Interact**.
3. If required, enter a description.

4. Select the items that you want the role to have access to. If you have selected:
 - **Hub**, select the required plugins from the **Add plugin** drop-down list.
 - **Interact**, select the required forms from the **Add forms** drop-down list.

You can select more than one item from the list.

5. Select the users that will be assigned this role from the **Add user** drop-down list. The list only displays users who have appropriate privileges, for example, if the role is for Interact, it will only display Interact users and not Hub users. See [Users on page 24](#) for more information on user permissions.



Users can also be added to roles from the [Users](#) page.

6. Click **Save** to create the role.

Add Active Directory security groups to a role



If you are using Interact with Active Directory, be aware that some actions in the Interact Web API Service do not support the use of security groups. All actions support Active Directory users being directly assigned to Interact roles. For more information, see the [Interact Web API Service user guide](#).

1. On the Roles and permissions page, click **Create role**.
The Create role section displays.
2. In the Role information tab, enter a role name and select whether it applies to **Hub** or **Interact**.
3. If required, enter a description.
4. Select the items that you want the role to have access to. If you have selected:
 - **Hub**, select the required plugins from the **Add plugin** drop-down list.
 - **Interact**, select the required forms from the **Add forms** drop-down list.

You can select more than one item from the list.

5. Click **Security groups**.

6. Search for security groups by entering the distinguished name of the root location, for example, dc=bpdevops, dc=co, dc=uk.

DevOps - Forms

Role information

Role information | **Security groups** | Summary

Search root
dc=bpdevops,dc=co,dc=uk

Filter by: None | Filter value:

Reset filters | Search

Rows per page: 10

| Name | Type | PATH | Select group |
|-------------------------------------|---------------------------|---|--------------------------|
| Access Control Assistance Operators | Security Group (Built-in) | CN=Access Control Assistance Operators,C... | <input type="checkbox"/> |
| Account Operators | Security Group (Built-in) | CN=Account Operators,CN=Builtin,DC=bpde... | <input type="checkbox"/> |
| Administrators | Security Group (Built-in) | CN=Administrators,CN=Builtin,DC=bpdevop... | <input type="checkbox"/> |

← Role Information | Summary →

You can apply search filters based on CN (Common Name), UPN (User Principal Name) or SID (Security Identifier); or use wildcard search, for more information, see [Add an Active Directory user on page 27](#).

You can also scroll down the page, click **Next** or **Previous** to navigate between multiple pages of security groups, or move between the Role information and Summary tabs.

7. Select the group(s) you want to add to the role and click **Save**.

The added security groups display as part of the role information. All users who are members of the added security groups will be automatically added to the role and will have an account created in Hub when they sign in for the first time.

DevOps - Forms

Role information

Role name *

DevOps - Forms

Role type *

☒ Hub

☐ Interact

Role description

Plugins

Forms

Users


(domainuser@bpdevops.co.uk) domainuser domainuser

Security groups

Administrators


Edit roles

1. On the Roles and permissions page, select the required role and click **Edit**.
2. Change the information as required, including adding or removing users and/or security groups.

 You cannot change the role type. If you are editing a role that displays a blue tick, you can only amend the users assigned to the role.

3. Click **Save** to apply your changes

Delete roles

 You cannot delete a role that displays a blue tick. This is a role that was automatically created when installing Hub or a plugin.

1. On the Roles and permissions page, select the required role and click **Delete**.

A message displays asking you to confirm.

2. Click **Yes**.


The role is deleted and a confirmation notification displays.

Use the filters on the Roles and permissions page

The filters enable you to easily find a specific role based on the selected criteria.

1. On the Roles and permissions page, click **Filter** to open the Filter panel.
2. Use the toggle to turn on the required filter and complete the information to find the required role. You can apply multiple filters at the same time.

The available filters are:

| Filter | Description |
|-----------------------|---|
| Type | Select the role type from the drop-down list. The options are: <ul style="list-style-type: none">• Hub – Displays the roles which have Hub set as the role type.• Interact – Displays the roles which have Interact set as the role type. |
| Description | Enter a term or word to search against the text in the Role description. |
| Hub plugins | Enter the name, or part of the name, of the Plugin that you want to search against. For example: <ul style="list-style-type: none">• Automation lifecycle – Displays all roles which have access to ALM.• Forms – Displays all roles which have access to Interact Forms.• Business process – Displays all roles which have access to the Business process plugin.• Control Room – Displays all roles which have access to Control Room. |
| Interact forms | Enter the name, or part of the name, of the Interact Form that you want to search against. |
| Users | Enter a user's username, or part of their username, to find the roles that are associated with that user. <div> If you have entered part of a username, the roles display for all partial matches. These may be for other users as well as the one you intended.</div> |

The information on the Roles and permissions page is immediately filtered.



If you have set the filters but want to view the unfiltered information again, either click **Reset filters** in the panel, or turn off the required filters, or remove any settings within the filter so that it is blank.

3. Click **Close drawer** to close the filter panel.


Registrations

The Registrations page enables you to manage registration requests that new users have raised for access to Interact.

Users can request an Interact user account from the registration page:

<https://{hostname}/#/user-registration>

The Registrations page displays the submitted registration requests, which you can approve or deny.

 To open the Registrations page, click your profile icon to open the Settings page, and then click **Registrations**. A numerical value is shown against the Registrations option on the Settings page if there are outstanding requests.

Approve a request

The user will need to be assigned a role before they will be able to access any forms in Interact. You can either do this as part of the approval process, as shown below, or you can approve the request and then [edit the user](#).

1. On the Registrations page, select the user and click **Edit**.
2. Select the required role from the drop-down list. This is the only field you can edit.
3. Click **Save**.
4. Click **Approve**.

The user is removed from the registrations list and displays on the [User](#) page. The user receives an email providing a one-time use link to complete registration by entering a password and they can then access Interact.

Reject a request

1. On the Registrations page, select the user and click **Deny**.

The access request is rejected and the user details are removed from the list.

Use the filters on the Registrations page

The filters enable you to easily find a specific user based on the selected criteria.

1. On the Registrations page, click **Filter** to open the Filter panel.
2. Use the toggle to turn on the required filter and complete the information to find the user. You can apply multiple filters at the same time.

The available filters are:

| Filter | Description |
|-------------------------|--|
| Full name | Enter the user's full name, or part of their full name. |
| Email address | Enter the user's email address, or part of their email address. |
| Interact role(s) | Enter the name of a role, or part of the role name. This searches against any roles that have Interact set as the role type. |

The information on the Registrations page is immediately filtered.




If you have set the filters but want to view the unfiltered information again, either click **Reset filters** in the panel, or turn off the required filters, or remove any settings within the filter so that it is blank.

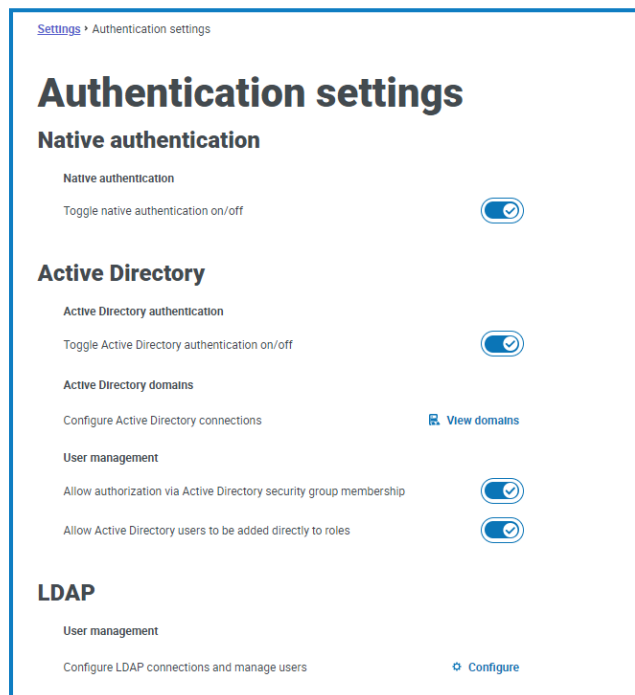
3. Click **Close drawer** to close the filter panel.

Authentication settings

You can configure your organization's authentication settings using the following options:

- Native authentication
- Active Directory authentication
- LDAP

 To open the Authentication settings page, click your profile icon to open the Settings page, and then click **Authentication settings**.




Native authentication

Native authentication is enabled by default on the Authentication settings page in new environments or when upgrading Hub.

To enable or disable native authentication:

1. Use the slider to toggle to the required position:
 - Cross indicates off
 - Tick indicates on
2. Click **OK** to accept the confirmation message.

 You can only disable native authentication if there is at least one Hub administrator in the system who can sign in using one of the other authentication methods.

You can add native users on the [Add user](#) page and they can log into Hub by entering their username and password.


Active Directory authentication

Active Directory authentication can only be enabled on the Authentication Settings page if the server hosting Authentication Server is a member of an Active Directory domain.

To enable or disable Active Directory authentication:

1. Use the slider to toggle to the required position:
 - Cross indicates off
 - Tick indicates on
2. Click **OK** to accept the confirmation message.

Once enabled, you can add Active Directory users on the [Add user](#) page and they can log into Hub directly using the **Log in using Active Directory** option.

 This does not apply to LDAP users who will still be required to enter their credentials.

Active Directory user management

If Active Directory authentication has been enabled on the Authentication settings page, you must select how to manage access for Active Directory users in Hub by enabling at least one of the following options on the Authentication settings page:


- **Allow authorization via Active Directory security group membership** – Enables Active Directory security groups to be added to Hub roles. Users can be assigned to multiple Hub roles by being a member of any Active Directory security groups associated with those roles.
- **Allow Active Directory users to be added directly to roles** – Enables Active Directory users to be directly assigned to Hub roles. Users can be assigned to multiple Hub roles.

For details on how to assign Active Directory users and security groups to roles, see [Roles and permissions on page 32](#).


 Watch [this video](#) for an overview of Active Directory integration with Authentication Server.

Active Directory domains

The Active Directory domains page allows you to view, add, edit, and delete Active Directory domains and associated credentials stored in the Authentication Server database.

 To open the Active Directory domains page, click your profile icon to open the Settings page, click **Authentication settings** and then click **View domains**.

| Active Directory domains | | |
|--------------------------|-----------------------|--|
| | | <div><div><div>A</div><div>B</div><div>C</div></div><div><div>+</div><div>✎</div><div>🗑</div></div><div><div>Add</div><div>Edit</div><div>Delete</div></div></div> |
| Domain name | Domain DN | Selected (0) |
| bpdevs.co.uk | DC=bpdevs,DC=co,DC=uk | <input type="checkbox"/> |
| bpqas.co.uk | DC=bpqas,DC=co,DC=uk | <input type="checkbox"/> |

 You only need to add new Active Directory domains for multi-forest environments with one-way trust relationships. For more details, see [Trust relationships between domains on page 44](#).

The Active Directory domains page provides you with the following information and functions:

- A. **Add** – [Add](#) a new Active Directory domain.
- B. **Edit** – [Edit](#) the details of an existing Active Directory domain. You can only edit one domain at a time.
- C. **Delete** – [Delete](#) one or more Active Directory domains.

Add a domain

1. On the Active Directory domains page, click **Add**.

The Add domain page displays.

2. Enter a domain name.

This must be the fully qualified domain name (FQDN) using the format subdomain.domain.com or domain.com.

3. Enter the username and password for the domain. Usernames must be in the format username@domain.co.uk or DOMAIN\username. The credentials must be requested from a system administrator beforehand.

Active Directory domain credentials are stored in the database and are encrypted before storage. The credentials stored for each domain must be that of an Active Directory service account. The service account password must not expire, the service account must not be a user account, and should follow [Active Directory service account best practices](#).

Settings > Authentication settings > Active Directory domains > Add domain

Add domain

Domain name *

Domain names must be fully qualified domain names in the format subdomain.domain.com or domain.com, for example, blueprism.com.

bpqas.co.uk

Username *

BPQAS\bpqasadmin

Password *

Add

4. Click **Add**.

The domain name and credentials are validated against the Active Directory domain controller and the added domain displays in the domains list.

Edit a domain

1. On the Active Directory domains page, select a domain and click **Edit**.
You can only select one domain at the time.
2. Change the information as required. If you want to edit the domain name, you must delete this domain and create a new domain.
3. Click **Save** to apply your changes.

Delete domains

1. On the Active Directory domain, select the required domain(s) and click **Delete**.
A message displays asking you to confirm the deletion.
2. Click **Yes** to delete the selected domain(s) or **No** to cancel.

Trust relationships between domains

For multi-forest environments, trust relationships must be configured between domains. These can be two-way or one-way to the domain that should be trusted.

For example:

- In a one-way trust between Domain A and Domain B, users in Domain A can access resources in Domain B. However, users in Domain B cannot access resources in Domain A.
- In a two-way trust, Domain A trusts Domain B and Domain B trusts Domain A. This means that authentication requests can be passed between the two domains in both directions.

Two-way trusts do not require the user to provide domain credentials if the Authentication Server application pool user has relevant read access to the domain that the user belongs to. In these examples, the web server hosting Authentication Server would reside in Domain B. Two-way trusts require credentials to be provided when the user need to query a trusted domain using an account different to the Authentication Server application pool user. One-way trusts require a domain with credentials to be created.

The following trust types are supported:

- External
- Parent-child
- Tree-root
- Forest

LDAP

The LDAP page allows you to configure a Lightweight Directory Access Protocol (LDAP) connection to an organization's Active Directory environment.

To open the LDAP page, click your profile icon to open the Settings page, click **Authentication settings** and then click **Configure** under the LDAP section.

LDAP

[Edit view](#) (A)
 [Filter](#) (B)
 [Save view](#) (C)
 [Load view](#) (D)
 [Add new](#) (E)

| Live | LDAP server | Base DN | Domain | Number of user imports | Last sync | Synced by | Actions |
|------|--------------|---------------------------|-----------------|------------------------|---------------------|-----------|--|
| Live | 20.40.108.71 | DC=thoughtonomy-qa,DC=com | thoughtonomy-qa | 1 | 14/04/2021 08:03:47 | admin | Edit (F) Re-sync (G) Retire (H) Delete (I) |

Rows per page: 5 (J)
 Page 1 of 1 (1 total rows)
 [Previous](#)
[Next](#) (K)

The LDAP page provides you with the following information and functions:

- A. **Edit view** – Define the columns that are displayed. You can then show or hide the columns using the toggle switches.
- B. **Filter** – Filter the information that is displayed. You can turn on the [required filters](#) and enter or select the appropriate information for display, for example, you could turn on the **Domain** filter and enter the domain name.
- C. **Save view** – Save your current column settings. You can enter a name for your view to make it easily identifiable when loading views.
- D. **Load view** – Load a saved view. You can select the required view and click **Apply**.
- E. **Add new** – Add a [new connection](#).
- F. **Edit** – [Edit the selected connection](#) details.
- G. **Re-sync** – [Re-sync the users](#) with Hub. You need to do this if new users are added to Active Directory.
- H. **Retire/Re-instate** – A tick icon allows you to make a retired connection active, and a cross allows you to retire a connection. See [Retire and reinstate an application](#) for more information.
- I. **Delete** – [Delete the selected connection](#). You can only delete a retired connection.
- J. **Rows per page** – Enter a number, or use the up and down arrows, to change the number of rows seen on a page.
- K. **Previous and Next** – Click **Previous** or **Next** to move through the pages.

Add a new connection

If you add more than one LDAP connection into Hub which contain the same users (such as name, email address, and domain), duplicate users will be created which could lead to login issues. When synchronizing the users in the procedure described below, ensure that you only select the users that you require to prevent duplicate users from being imported.

1. On the LDAP page, click **Add new**.

The Create authentication connection page displays.

Create authentication connection

Configuration

Connection name *
Enter your friendly name for this connection.

Domain *
Enter the domain of the LDAP server.

LDAP server *
Enter the name of the server where LDAP is hosted, this can be an IP address or fully qualified DNS hostname.

Port number *
Enter the LDAP server port.
389

☒ Encrypt port

Base DN *
This is the point from where a server will search for users.

Time out *
Enter the seconds for which the system caches the LDAP server response result.
10

Query bind

Username *
Enter the username for logging to the LDAP server.

Password *
Enter the password for logging to the LDAP server.

Attributes

Username *

First name *

Last name *

E-mail *

Test username *
Enter a username that resides in the LDAP server, if all the values of the attributes appear then you successfully have setup authentication.

Lookup user

Create authentication connection

2. Complete the Configuration fields:

- **Connection Name** – A name that you want the connection to be known as.
- **Domain** – The name of the domain you are connecting to, for example “bp”.

Do not use the fully qualified domain name (FQDN) of your domain. You must use the short name format.

- **LDAP Server** – The hostname of the LDAP server, for example blueprism-srv1.local.
- **Port Number** – The port number it operates on, by default this is port 389.
- **Encrypt port** – Select this option if you want to encrypt the port. If you use port 636 (the LDAPS port), you should turn on this option.
- **Base DN** – The starting point within the Active Directory where the system begins to look for users, for example dc=blueprism, dc=local.

3. Complete the Query Bind fields:

- **Time Out** – The timeout period in seconds that the system will wait to get a response from the Active Directory server.
- **Query Bind Username** – An Active Directory user that has access to the organization's LDAP system.
- **Query Bind Password** – The password for the Active Directory user.

4. Complete the Attributes fields. The purpose of this section is to map the Active Directory attributes to the Hub fields. The text entered in these fields must match named attributes within the user profile in Active Directory. You can use the Active Directory Users and Computers (ADUC) tool to find the user attributes by selecting a user and then clicking the **Attribute Editor** tab to view the mapping of attributes to values.
 - **Username** – The Active Directory attribute name for the username, for example, 'SAMAccountName'.
 - **First Name** – The Active Directory attribute name for the user's first name, for example, 'givenname'.
 - **Last Name** – The Active Directory attribute name for the user's last name, for example, 'sn'.
 - **E-mail** – The Active Directory attribute name for the user's email, for example, 'mail'.
5. To test that everything is set up correctly, enter the username in the **Test Username** field and click **Lookup User**. The text entered in the **Test Username** field must match the text format of the Active Directory Attribute. For example, if the username is set to:
 - 'SAMAccountName', then the test data is likely to be in the format domain\user.
 - 'name', then the test data is likely to be in the format user.


The associated information will be retrieved and populated in the corresponding Attributes fields, for example:

6. Click **Create authentication connection**.

A notification message displays confirming the connection is successful and you are prompted to import users.

- Click **Yes** to synchronize now. Alternatively, you can select **No** and synchronize later using the process in [Synchronize Active Directory users on the next page](#).


A message displays indicating the number of users found.

 When importing a large number of users (for example, tens of thousands), the database transaction log files for the databases AuthenticationServerDB, HubDB and InteractDB will increase in size. If the size of the transaction log file of any of these three database is restricted by either a maximum file size that is too small or the file is not permitted to increase in size, the import may fail. It is therefore recommended that you enable the autogrow setting for the database transaction log files and set the growth setting to 1024 MB, whilst ensuring a sufficient maximum size is set to prevent the import from failing. For more information on autogrowth, see [Microsoft's documentation](#).

- Click **Proceed**.

A list of users display. These have not yet been imported to Hub as you need to configure the permissions and roles for the required users.

- Select a user to import and assign the appropriate Hub roles and/or any Interact responsibilities.

 If you configure a user to have a Hub Administrator role, they will have access to all the plugins and features of Hub, including the ability to create new Database and LDAP connections and other security features so it is important to assign this role with care.

- Repeat for all required users.


- Click **Save access and roles**.

Only the users that have had their roles and permissions defined are saved and the [Users page](#) displays with the new users shown.

Edit a connection

- On the LDAP page, select the **pencil** icon for the required connection.
- Edit the information as required. You can not change the domain, LDAP server, port number or base DN.
- Click **Save**.

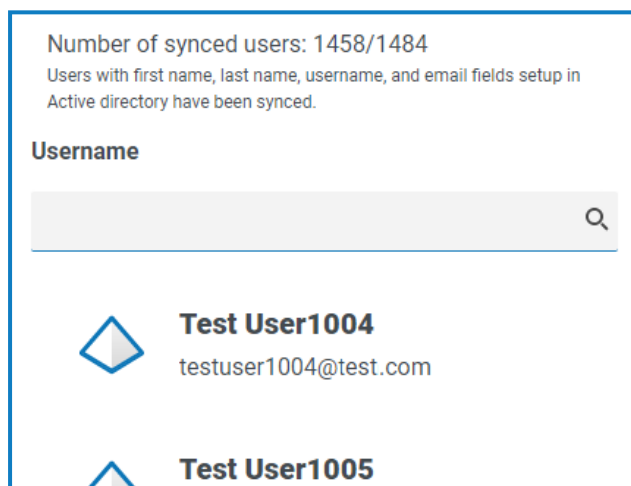
Synchronize Active Directory users

 When importing a large number of users (for example, tens of thousands), the database transaction log files for the databases AuthenticationServerDB, HubDB and InteractDB will increase in size. If the size of the transaction log file of any of these three database is restricted by either a maximum file size that is too small or the file is not permitted to increase in size, the import may fail. It is therefore recommended that you enable the autogrow setting for the database transaction log files and set the growth setting to 1024 MB, whilst ensuring a sufficient maximum size is set to prevent the import from failing. For more information on autogrowth, see [Microsoft's documentation](#).

When additional users are added to Active Directory, those users must be synchronized with Hub.


1. On the LDAP page, click the **re-sync** icon in the row for the required connection.


A message displays above the list of users showing the number of synced users (those with valid information in Active Directory – first name, last name username and email) against the total number of users found. Only synced users are displayed in the list. You will need to configure the permissions and roles for the required users.




Number of synced users: 1458/1484
Users with first name, last name, username, and email fields setup in Active directory have been synced.

Username

 **Test User1004**
testuser1004@test.com


 **Test User1005**

 For more information about the Active Directory Attributes that supply Hub with the first name, last name username and email, see [Add a new connection on page 46](#). Hub will only sync users which have information in all the mapped attributes.

2. Select the required user to add to the Hub user base, assigning the appropriate Hub roles and/or any Interact responsibilities.
3. Repeat for all required users.
4. Click **Save access and roles**.

Only the users that have had their roles and permissions defined are saved and the [Users page](#) displays with the new users shown.

Retire and reinstate a connection

 Retiring a connection does not affect the status of the associated users – users can still log in and use the applications. All users associated with an LDAP connection can be retired by [deleting the connection](#).

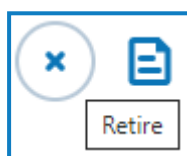
1. On the LDAP page, select the **retire/re-instate** icon for the required connection.

If the connection is:

- Live, the **retire/re-instate** icon displays as a cross.
- Retired, the **retire/re-instate** icon displays as a tick.

2. To retire a connection:

- a. Click the cross.

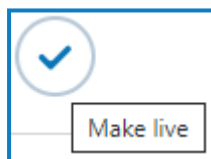


A message displays asking you to confirm.

- b. Click **Yes**.

The connection is retired and the cross changes to a tick.

3. To make a retired connection live, click the tick.



The connection is instantly reinstated and the tick changes to a cross.

 You can use the **Live** filter to filter the list for retired connections.

Delete a connection

You can only delete a [retired connection](#).

1. On the LDAP page, select **Delete** (the trash can) for the required connection.

A message displays asking you to confirm.

2. Click **Yes**.


The connection is deleted and all users associated with it are retired.

Use the filters on the LDAP page

The filters enable you to easily find a specific connection or similar connections based on the selected criteria.

1. On the LDAP page, click **Filter** to open the Filter panel.
2. Use the toggle to turn on the required filter and complete the information to find the required connection. You can apply multiple filters at the same time.

The available filters are:

| Filter | Description |
|-------------------------------|---|
| Live | Select the status of the connection from the following options: <ul style="list-style-type: none">• Live – Displays the active connections; those that have not been retired.• Retired – Displays the connections that have been retired by an administrator. |
| Connection name | Enter the full or partial name of a connection. |
| LDAP Server | Enter the hostname of the server, or part of the server hostname. |
| Base DN | Enter the Base DN, or part of the Base DN to match against. |
| Domain | Enter the full or partial name of a domain. |
| Number of user imports | Enter a numerical range: <ul style="list-style-type: none">• In the first field, enter the lowest number of imports.• In the second field, enter the highest number of imports. This displays any connections that have imported users within that range. |
| Last sync | Enter a date range: <ul style="list-style-type: none">• In the first field, select the earliest date.• In the second field, select the latest date.• If required, adjust the time fields. By default, the earlier date has the time 00:00:00 and the later date has the time 23:59:59, thereby including the full day. This displays any connections that have synced during this time frame. |
| Synced by | Enter a user's username, or part of their username. <div> If you have entered part of a username, the results display for all partial matches. These may be for other users as well as the one you intended.</div> |

The information on the LDAP page is immediately filtered.



If you have set the filters but want to view the unfiltered information again, either click **Reset filters** in the panel, or turn off the required filters, or remove any settings within the filter so that it is blank.

3. Click **Close drawer** to close the filter panel.

Service accounts

The Service accounts page allows you to manage the authenticated application accounts.

Service accounts are used by applications that need to get access tokens for their own use rather than on behalf of a user. These access tokens can then be used to make authenticated requests to APIs. The APIs that service accounts can get access tokens for are:

- **Authentication Server API** – A service account must be created for any applications that integrate with the Authentication Server API. For more details, see the [Authentication Server configuration guide](#).
- **Blue Prism API** – A service account must be created for any third-party applications that integrate with the Blue Prism API. For more details, see the [Blue Prism API install guide](#).
- **Decision API** – A service account must be created for Blue Prism to use the Decision models that have been trained and calibrated in the Decision plugin. For more details, see the [Blue Prism Decision install guide](#).
- **Interact Remote API** – A service account must be created for any applications that integrate with the Interact Remote API, such as the Blue Prism interactive client. For more details, see the [Interact Web API Service user guide](#).

To open the Service accounts page, click your profile icon to open the Settings page, and then click **Service accounts**.

The Service accounts page provides you with the following information and functions:

- Edit view** – Define the columns that are displayed. You can then show or hide the columns using the toggle switches.
- Filter** – Filter the information that is displayed. You can turn on the [required filters](#) and enter or select the appropriate information for display, for example, you could turn on the **Permissions** filter and select **Blue Prism API**.
- Save view** – Save your current column settings. You can enter a name for your view to make it easily identifiable when loading views.
- Load view** – Load a saved view. You can select the required view and click **Apply**.
- Regenerate secret** – [Create a new secret](#) for an existing service account.
- Add account** – [Add](#) a new service account.
- Edit account** – [Edit](#) the details of an existing service account.
- Delete account(s)** – [Delete](#) one or more service accounts.
- Rows per page** – Enter a number, or use the up and down arrows, to change the number of rows seen on a page.
- Previous and Next** – Click **Previous** or **Next** to move through the pages of service accounts.

Add a service account

1. On the Service accounts page, click **Add account**.
2. Enter a unique ID for the client application and a friendly name for the client in the Authentication Server database.
3. Under **Permissions**, select the appropriate option:
 - **Blue Prism API** – The service account secret is used to get an access token to authenticate with the Blue Prism API.
 - **Authentication Server API** – The service account secret is used to make authenticated requests to the Authentication Server API.
 - **Interact Remote API** – The service account secret is used to get an access token to authenticate with the Interact Remote API.
 - **Decision API** – The service account secret is used to get an access token to authenticate with the Decision Web API.
 - **Director API** – This permission does not have a function. It is reserved for future functionality.
4. Click **Create service account**.

Settings > Service accounts > Add a service account

Add a service account

ID *
Client ID which uniquely identifies the client application to the identity provider.

Auth_Server

Name *
Client name in the Authentication Server database.

Authentication Server

Permissions
The API(s) to which the client has access.

☐ Blue Prism API

☒ Authentication Server API

☐ Interact Remote API

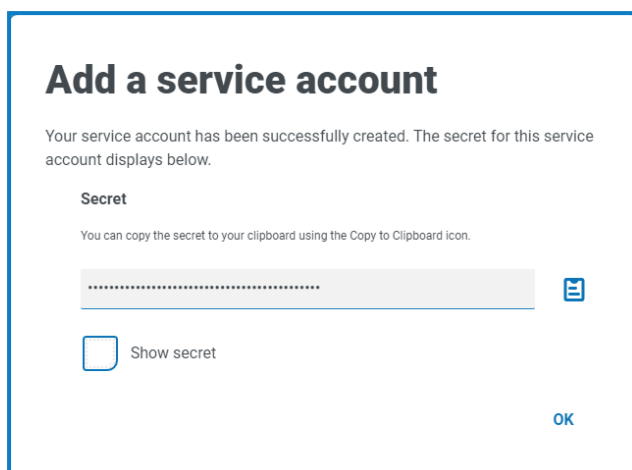
☐ Decision API

☐ Director API

Create service account

The Add a service account dialog displays with a generated secret, which will be used to get the access token to the selected API(s).

- Click the Copy to Clipboard icon to copy the generated secret to your clipboard.



- Click **OK** to close the dialog.

The Service accounts page displays with the newly created account.


Regenerate secret

If you have misplaced a previously generated secret for an existing service account, you can generate a new secret.

- On the Service accounts page, select the required service account and click **Regenerate secret**.
The new secret for the service account displays.
- Click the Copy to Clipboard icon to copy the generated secret to your clipboard.
- Click **OK** to close the dialog.

Edit a service account

- On the Service accounts page, select the required service account and click **Edit account**.
- Change the information as required.

 You cannot change the client ID for a service account.

- Click **Save** to apply your changes.

Delete service accounts

- On the Service accounts page, select the required service account(s) and click **Delete account(s)**.
A message displays asking you to confirm the deletion.
- Click **Yes** to delete the selected account(s) or **No** to cancel.

Use the filters on the Service accounts page

The filters enable you to easily find a specific service account based on the selected criteria.

1. On the Service accounts page, click **Filter** to open the Filter panel.
2. Use the toggle to turn on the required filter and complete the information to find the service account. You can apply multiple filters at the same time.

The available filters are:

| Filter | Description |
|----------------------|--|
| Friendly Name | Enter the service account name, or part of a name. |
| ID | Enter the service account identifier, or part of the identifier. |
| Permissions | Select the appropriate permission level option. You can select more than one option. If you do not select any permission levels, all levels are included on the Service accounts page. |

The information on the Service accounts page is immediately filtered.



If you have set the filters but want to view the unfiltered information again, either click **Reset filters** in the panel, or turn off the required filters, or remove any settings within the filter so that it is blank.

3. Click **Close drawer** to close the filter panel.