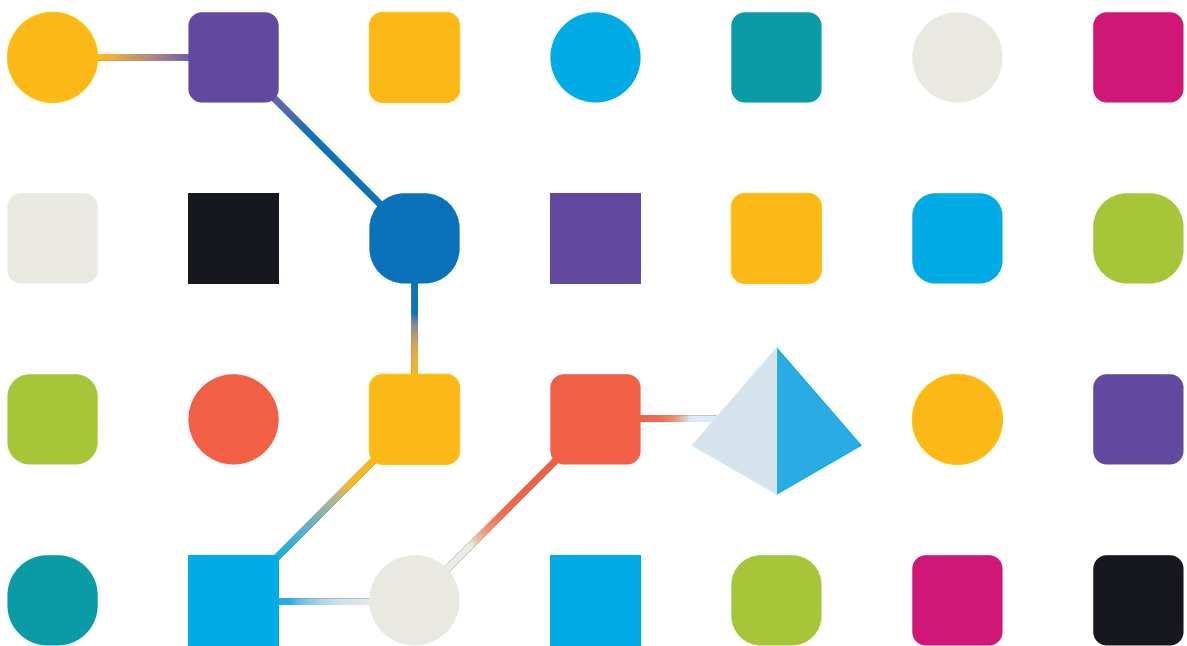




Hub 4.7

Release Notes

Document Revision: 5.0



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

Release Notes	4
Hub 4.7 – January 2023	4
Upgrade Hub and Interact	10
Upgrade Hub and Interact 4.6 to version 4.7	10
Blue Prism Data Protector Tool	18
Previous Releases	20
Hub 4.6 – June 2022	20
Hub 4.5 – November 2021	37
Hub 4.4.1 – October 2021	40
Hub 4.4 – September 2021	42
Hub 4.3 – May 2021	48
Hub 4.2 – April 2021	53
Hub 4.1 – November 2020	55
Hub 4.0 – September 2020	57


Release Notes

Hub 4.7 – January 2023

These release notes are for the 4.7 release of Blue Prism Hub.

Enhancements

The following new features and enhancements are introduced in this version of Hub.

Area	Description of Change	Reference
Installation	<p>Blue Prism Hub and its components have been updated to use:</p> <ul style="list-style-type: none"> .NET 6.0 .NET Framework 4.8 <p>Both the installer and the upgrader have been updated to reflect these prerequisites.</p> <p>For download information, see the Blue Prism Hub install guide.</p>	<p>HUB-4058 HUB-5308</p>
	<p>A security enhancement has been made to ensure encrypted connection strings are used. SQL Server must be configured to use SSL encryption, using certificates issued by a trusted certificate authority. Self-signed certificates are not sufficient to meet the requirements of this enhancement. Both the installer and upgrader have been updated to reflect this security enhancement.</p> <div style="border: 1px solid red; padding: 10px;"> <p> If you are upgrading a system where SQL Server was not configured to use SSL encryption, the connection strings for the Hub applications will need to be manually configured prior to running the upgrader. See Upgrade Hub and Interact on page 10 for more information.</p> <p>Certificates from trusted certificate authorities should be used for Production environments. However, a self-signed certificate could be used for Proof of Concept, or Development environments. It is important that the fully qualified domain name (FQDN) used by SQL Server matches the FQDN defined in the certificate. If these do not match, a connection to the database will not be established and your installation will not function correctly. For information on using and configuring self-signed certificates, see Self-signed certificates in the Blue Prism Hub installation guide.</p> </div>	<p>HUB-6630 HUB-6642</p>

Area	Description of Change	Reference
Authentication settings	<p>The Authentication settings page has been updated to include Security Assertion Markup Language 2.0 (SAML 2.0) authentication.</p> <p>SAML 2.0 authentication allows cross-domain single sign-on (SSO) and is only visible on the Authentication settings page if the Authentication Server SAML 2.0 extension has been installed on the host web server where Authentication Server is installed. The Authentication Server SAML 2.0 extension installer and the associated installation guide can be downloaded from the Digital Exchange.</p> <p>The following actions can be carried out from the Authentication settings page:</p> <ul style="list-style-type: none"> • Enable or disable SAML 2.0 authentication. • Configure SAML 2.0 provider settings. • Remove an already configured SAML 2.0 provider. • Add multiple SAML 2.0 users from a CSV file. <p>Authentication Server users configured to log in using SAML 2.0 will see the Log in using <SAML 2.0 provider name> button on the login screen, for example, Log in using Azure AD.</p>	<p>HUB-4597 HUB-5498 HUB-4958 HUB-4967 HUB-5523</p>
	<p>If a Hub administrator attempts to disable any enabled authentication types on the Authentication settings page, a check is now carried out to identify whether there are any active administrator users configured to log in using any of the other enabled authentication types. If no administrator user with a different authentication type is found, the selected authentication type cannot be disabled.</p> <p>For more information, see the Hub Administrator Guide.</p>	<p>HUB-4960</p>
Environment management	<p>All fields in the Database configuration and Database authentication sections of the Edit connection page can now be edited, however, this should only be done to prevent the loss of a connection if a parameter is incorrect, or if the database password has been changed.</p> <p>For more information, see the Hub Administrator Guide.</p>	<p>HUB-6626</p>

Area	Description of Change	Reference
Users	<p>If SAML 2.0 authentication has been enabled on the Authentication settings page and a SAML 2.0 provider has been configured, Hub administrators can add individual SAML 2.0 users on the Add users page.</p> <p>A new audit event called <i>Added SAML 2.0 user</i> has been added.</p> <p>Alternatively, Hub administrators can add multiple SAML 2.0 users at the same time from the Authentication settings page, by uploading users from a CSV file. Once uploaded, the users display on the Users page and can be edited or retired. Any users that have been created this way will have their own audit log entry that also includes details of all users who have been skipped or could not be added. It is recommended that the CSV file does not contain more than 1000 entries.</p> <p>When a SAML 2.0 provider is removed from Authentication Server, any users configured to use that provider are retired.</p> <p>For more information, see the Hub Administrator Guide.</p>	<p>HUB-4963 HUB-4959 HUB-4962 HUB-4970 HUB- 5023 HUB-4968 HUB-4969</p>

Fixes and improvements

The following fixes and minor improvements are included in this version of Hub.

Area	Description of Change	Reference
Active Directory authentication	Active Directory users can be synchronized and log into Authentication Server when their UPN contains an alias suffix that is different to the Domain Name System (DNS) name of the Active Directory domain. For example, corp.dir.company.com (DNS name) and company.com (alias suffix), where john@company.com is the UPN. Authentication Server will automatically determine available alias suffixes for the users, unless configured manually by an administrator. For more information, see Authentication Server troubleshooting .	HUB-5599
	When searching for Active Directory users or security groups to add to Authentication Server, the Search root field on the Add user and Create role pages now displays a default value, which corresponds to the Distinguished Name (DN) of the current forest root domain of the server hosting Authentication Server.	HUB-5452 HUB-5453
	Disabled Active Directory users who previously had access to the Control Room plugin are now automatically logged out of Authentication Server and redirected to the login page if they attempt to access the Control Room plugin. Previously, they were incorrectly redirected to the Welcome page.	HUB-5930
	Several performance improvements have been made when determining Active Directory group membership for a user during authentication. For more information, see Authentication Server troubleshooting .	HUB-5864
	The default value for the maximum duration that the cache stores the discovered Active Directory domains has been increased to 1440 minutes. Previously, the default was 30 minutes. For more information, see Authentication Server troubleshooting .	HUB-5855
	Email service	Additional logging has been added to Email service to log occurrences where the SMTP settings fail due to incorrect configuration in the web.config file.
General	The newtonsoft.json package used by the Hub repositories has been updated to the latest version to remove a vulnerability to insecure defaults. Authentication Server has also been updated to use the Duende IdentityServer 6.0.	HUB-2637 HUB-4016
License Manager	License Manager now correctly listens and responds to HTTP requests even when RabbitMQ is not available. Previously, License Manager did not listen for HTTP requests when RabbitMQ was not available.	HUB-4613
Login	A previous known issue where the Hub tile became inactive after logging in following an application pool recycle has been fixed.	HUB-5054
	When signing in using Authentication Server from the Blue Prism interactive client, the language selected on the Blue Prism login page is now reflected on the Authentication Server login page.	HUB-5932

Area	Description of Change	Reference
Roles and permissions	An issue has been fixed where the pagination arrows still displayed on the Roles and permissions page after adding Active Directory groups to a role if the filters used on the page resulted in an empty table.	HUB-5924
Service accounts	Service account client IDs are now set to be case sensitive. Previously, naming one client ID 'Test' and another client ID 'test' would trigger an error, whereas both can now be used at the same time without errors.	HUB-5290
	An issue has been fixed where, when filtering and selecting items on the Service accounts page, the selection was not retained once the filter had been removed.	HUB-5931
Users	An issue has been fixed on the Users page where a theme could not be selected if a user clicked the Add user button before the page had finished loading.	HUB-4824

Plugin updates

Automated Lifecycle Management (ALM)

No changes have been made to the ALM plugin in this release.

Control Room

Area	Description of Change	Reference
Schedule Manager	When editing schedules in Schedule Manager, the Repeat every interval properties are now reset to the default value when the interval type is updated. Previously, some properties retained their values when the interval type was changed.	HUB-2380

Decision

No changes have been made to the Decision plugin in this release.

Interact

For the Interact plugin improvements and fixes, see the [Interact 4.7 release notes](#).

Known issues

A list of any prominent issues with this release is maintained in the knowledge base:

- For Hub known issues, click [here](#).
- For Decision known issues, click [here](#).

Secure development policy


Blue Prism's secure development process is a market-leading, embedded security culture, focused on delivering security excellence through four key principles:

- Education – Providing up-to-date knowledge, information, and training to the development team.
- Evaluation – Regular reviews of our products using industry standard frameworks and security tools.
- Elimination – Remove potential threats through the evaluation of standards, compliance, and performance.
- Evolution – Continued improvement of our security program, ensuring alignment with our product technologies and by reacting effectively to new and emerging threats.

Blue Prism secure development is based on OWASP ASVS, ISO 27034 and GDPR Article 25 standards and practices. For more information, see Blue Prism's [comprehensive secure development process](#).

Upgrade Hub and Interact

Upgrading Hub and Interact is a simple process that uses dedicated tools. You need to run the upgrade tools in order, starting with the version you are currently using. This section only covers upgrading from the previous release to the latest release. For the full upgrade process, see the [Blue Prism Hub and Interact Upgrade Guide](#).

 After you have completed the upgrade, advise your users to log into Hub and clear the cache by pressing **CTRL + F5**. This will refresh all web pages and ensure that any user interface changes are updated.

Upgrade Hub and Interact 4.6 to version 4.7


This upgrade updates Blue Prism Hub, Blue Prism Interact, and the supporting sites to use the following .NET components:

- .NET Desktop Runtime 6.0.9 or 6.0.10
- ASP.NET Core Runtime 6.0.9 or 6.0.10 (Windows Hosting Bundle)
- .NET Framework 4.8 – Installed by default on Windows Server 2022.

This upgrade also enforces SSL encryption requirements. For more information, see [Prerequisites below](#). It is recommended that you schedule the upgrade to take place outside of working hours.

Prerequisites


- Version 4.6 of Hub and/or Interact is installed.
- Everyone is logged out of Authentication Server.
- You have backed up all relevant databases. Although the databases are not impacted by the upgrade, it is recommended that databases are backed up before performing any upgrade.
- 2.5 GB of free disk space on the server where Hub and/or Interact are installed – This is required for the backup that is created until the installation process is complete. Remove any backups from any previous upgrades.
- SQL Server must be configured to use SSL encryption. If your organization does not already use SSL encryption (you have been running your environment without certificates for your SQL Server, or you have been using a self-signed certificate), your organization should obtain a certificate from a trusted certificate authority and import it into SQL Server to enable this. For more information, see [Microsoft's documentation](#).

 If you have not previously used SSL encryption for your SQL Server, you will need to update the connection strings in the application settings files for the Blue Prism applications before running the upgrader. For more information, see [Update application settings on the next page](#).

Certificates from trusted certificate authorities should be used for Production environments. However, a self-signed certificate could be used for Proof of Concept, or Development environments. It is important that the fully qualified domain name (FQDN) used by SQL Server matches the FQDN defined in the certificate. **If these do not match, a connection to the database will not be established and your installation will not function correctly.** For information on using and configuring self-signed certificates, see [Self-signed certificates](#) in the Blue Prism Hub installation guide.

To import the certificate into SQL Server:

1. From the Windows task bar, open **SQL Server Configuration Manager**.
2. In the SQL Server Configuration Manager, expand **SQL Server Network Configuration** and right-click **Protocols for <SqlServerInstanceName>**, and then click **Properties**.
3. In the Protocols for <SqlServerInstanceName> Properties dialog, select the **Certificate** tab, and then select or import the required certificate.
4. Click **Apply**.

 The upgrader automatically stops any running websites as part of the upgrade process. You do not need to manually stop them.

Update application settings

You only need to update the appsettings.json files for the Blue Prism applications if you have not previously been using SSL encryption for your SQL Server. You can update the application settings using the [script](#) that Blue Prism has created, or [manually](#).

To update the application settings using the script:


1. Import a certificate into SQL Server. For more information, see [Prerequisites on the previous page](#).
2. If you do not already have the Blue Prism Data Protector, download it from the [Blue Prism Portal](#) and save it to your Hub and/or Interact web server. You can remove it once this procedure is complete.
3. If you do not already have the application settings script (update-connectionStrings.ps1), download it from the [Blue Prism Portal](#) and save it to your Hub and/or Interact web server.
4. Open PowerShell as an administrator and run the update-connectionStrings.ps1 script. When prompted, enter the following information:
 - a. **installationDirectory** – Type the directory path for where Hub is installed and press Enter. For example, if the default installation location was used, the path will be C:\Program Files (x86)\Blue Prism.
 - b. **sqlSource** – Type the SQL Server name that was used during the creation of the SSL certificate and press Enter.
 - c. **dataProtectorPath** – Type the full path to the Blue Prism Data Protector and press Enter. For example, if you save it directly onto the C: drive, enter C:\BluePrismDataProtector.Console.exe.
 - d. **interactInstallationDirectory** – Type the directory path for where Interact is installed and press Enter. For example, if the default installation location was used, the path will be C:\Program Files (x86)\Blue Prism. If you have not installed Interact, do not enter any information and press Enter.

The script runs and updates the connection strings in the application settings with the new value for SQL Server.

5. Repeat the process on all machines on which Hub and/or Interact is installed.

To update the application settings manually:

1. Import a certificate into SQL Server. For more information, see [Prerequisites on page 10](#).
2. If you do not already have the Blue Prism Data Protector, download it from the [Blue Prism Portal](#).
3. Open PowerShell as an administrator in the folder where BluePrismDataProtector.Console.exe is located. You are going to use this tool to update the connection strings in the appsettings.json files. For more information on using the tool, see [Blue Prism Data Protector Tool on page 18](#).
4. On the Hub and Interact web servers, navigate to the following files and find the sections indicated in the code snippets below:

 The file paths shown below are the default installation locations. If you installed your applications to a different folder, you should navigate to that folder.

C:\Program Files (x86)\Blue Prism\Audit Service\appsettings.json

```
"ConnectionStrings": {  
  "AuditServerConnection": <Replace the string here>
```

C:\Program Files (x86)\Blue Prism\Audit Service Listener\appsettings.json

```
"ConnectionStrings": <Replace the string here>
```

C:\Program Files (x86)\Blue Prism\Authentication Server\appsettings.json

```
"ConnectionStrings": {  
  "IdentityServerConnection": <Replace the string here>  
"Storage": {  
  "Type": "Database",  
  "ConnectionString": <Replace the string here>
```

C:\Program Files (x86)\Blue Prism\Email Service\appsettings.json

```
"Database": {  
  "ConnectionString": <Replace the string here>
```

C:\Program Files (x86)\Blue Prism\File Service\appsettings.json

```
"Storage": {  
  "Type": "Database",  
  "ConnectionString": <Replace the string here>
```

C:\Program Files (x86)\Blue Prism\Hub\appsettings.json

```
"Data": {
  "Connect": {
    "ConnectionName": "Connect",
    "ConnectionString": <Replace the string here>

    "BluePrismDecision": {
      "ConnectionName": "BluePrismDecision",
      "ConnectionString": <Replace the string here>
    }
  }

  "DistributedCache": {
    "Type": "Database",
    "DefaultExpirationMinutes": 0,
    "SqlServer": {
      "ConnectionString": <Replace the string here>
    }
  }

  "Storage": {
    "Type": "Database",
    "ConnectionString": <Replace the string here>
  }
}
```

C:\Program Files (x86)\Blue Prism\IADA\appsettings.json

```
"Database": {
  "ConnectionString": <Replace the string here>
}
```

C:\Program Files (x86)\Blue Prism\Interact\appsettings.json

```
"InteractDatabases": {
  "InteractConnectionString": <Replace the string here>
}

"DistributedCache": {
  "Type": "Database",
  "DefaultExpirationMinutes": 0,
  "SqlServer": {
    "ConnectionString": <Replace the string here>
  }
}
```

C:\Program Files (x86)\Blue Prism\Interact Remote API\appsettings.json

```
"InteractRemoteDatabases": {
  "InteractConnectionString": <Replace the string here>
}

"InteractRemoteStorage": {
  "Type": "Database",
  "ConnectionString": <Replace the string here>
}
```

C:\Program Files (x86)\Blue Prism\License Manager\appsettings.json

```
"Database": {
  "ConnectionString": <Replace the string here>
}
```

C:\Program Files (x86)\Blue Prism\Notification Center\appsettings.json

```
"Database": {  
  "ConnectionString": <Replace the string here>
```

C:\Program Files (x86)\Blue Prism\Submit Form Manager\appsettings.json


```
"SubmitFormManagerDatabases": {  
  "InteractConnectionString": <Replace the string here>
```

5. For each of these files in turn:
 - a. Use the Blue Prism Data Protector Tool to decrypt the connection string and copy to a temporary text file, for example:

```
"InteractDatabases": {  
  "InteractConnectionString":  
  "CfDJ8MILtsx8cQB0rqrAat15A1aLmLP1GodofWTnhvaHwh0ryabXaXW2i-KTfsq2XTYuAzct_  
  ZXIFS3ILFv4Zu5ozmtvHv9aOLCxZjQJEUm7Ytwx8dK1Zqapywv2s5TCoi4X_9MGselkrRmbknBuQ_  
  zWE93ozrN1BUVCQNHVedkyjTTPmPnxyeIgJJdoZRbkK0upnSrJwTt95SCmvo2SLLhZZFR5e2s24smn72PKNGrg  
  a8fksbIDpaIDFwRc-i6_kkEinp5qA-FBFfIbVZzBD5ZN1dyuaC2jm7V4dxKt5tea1NP-_  
  vauczgCLBp88WdmNEe0Ew"
```

Becomes:

```
"InteractDatabases": {  
  "InteractConnectionString": "Data Source=existed-name-without-certificate;  
  Initial Catalog=Interact; User Id=sa; Pass=Pass***; Max Pool Size=500; Encrypt=False;  
  MultiSubnetFailover=True"
```

 The examples in step 4 above show the extract from the appsettings.json file to illustrate the location of the settings. The decryption and encryption is only carried out on the connection string setting, not on the settings also shown in these code examples.

Only the **Data Source** in the connection string needs to be updated. The other parameters in the connection string setting should be left unchanged. The upgrade script will make any changes that are required when run, such as updating the **Encrypt** parameter.

- b. In the copied connection string, replace the value for the **Data Source** parameter with the name from the certificate, for example:

```
"InteractDatabases": {  
  "InteractConnectionString": "Data Source=name-with-certificate; Initial  
Catalog=Interact; User Id=sa; Password=Pass***; Max Pool Size=500; Encrypt=False;  
MultiSubnetFailover=True"
```



The certificate name can be found in SQL Server Configuration Manager.

1. In SQL Server Configuration Manager, expand **SQL Server Network Configuration**, right-click **Protocols for <SqlServerInstanceName>**, and then click **Properties**.
2. In the Protocols for <SqlServerInstanceName> Properties dialog, select the **Certificate** tab. The certificate name is shown in the **Issued To** field – this displays in the format: short name followed by the common name (which is usually the FQDN). Either name can be used as the Data Source, however, if both names are present, it is recommended that the common name (FQDN) is used.
3. Optionally, for additional clarity, click **View**, and select **Subject Alternative Name**. The names are shown in the text area below the fields.

- c. Use the Blue Prism Data Protector Tool to encrypt the new connection string and overwrite the string in the appsettings.json file with this new value.






For information on decrypting and encrypting the connection strings, see [Blue Prism Data Protector Tool on page 18](#).

6. Open IIS Manager and restart the appropriate Application Pool to ensure it uses the new connection string.
7. Repeat the process on all machines on which Hub and/or Interact is installed.

Upgrade steps

- Blue Prism Hub and Blue Prism Interact 4.7 require .NET Core 6.0 and .NET Framework 4.8. If you do not have these versions, you will need to update your Hub and/or Interact web server.

Step	Details
1	<p>Download the following components and store them in a temporary location, for example, C:\temp:</p> <ul style="list-style-type: none"> ASP.NET Core Runtime 6.0.9 or 6.0.10 (Windows Hosting Bundle) https://dotnet.microsoft.com/download/dotnet/6.0 – Select the version you require. Under ASP.NET Core Runtime, select Hosting Bundle. .NET Desktop Runtime 6.0.9 or 6.0.10 https://dotnet.microsoft.com/download/dotnet/6.0 – Select the version you require. Under .NET Desktop Runtime, select the appropriate download. .NET Framework 4.8 https://support.microsoft.com/en-us/topic/microsoft-net-framework-4-8-offline-installer-for-windows-9d23f658-3b97-68ab-d013-aa3c3e7495e0 <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p> This is installed by default on Windows Server 2022. You only need to install the .NET Framework if you are using Windows Server 2016 Datacenter or Windows Server 2019.</p> </div>
2	<p>To install the .NET dependencies, run each of the following commands using the PowerShell command prompt, waiting until each completes, before running the next command:</p> <p>For Windows Server 2016 and Windows Server 2019:</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <pre>start-process "C:\temp\dotnet-hosting-6.0.0-win.exe" /q -wait start-process "C:\temp\windowsdesktop-runtime-6.0.0-win-x64.exe" /q -wait start-process "C:\temp\ndp48-x86-x64-allos-enu.exe" /q -wait</pre> </div> <p>For Windows Server 2022 (.NET Framework is already installed by default):</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <pre>start-process "C:\temp\dotnet-hosting-6.0.0-win.exe" /q -wait start-process "C:\temp\windowsdesktop-runtime-6.0.0-win-x64.exe" /q -wait</pre> </div> <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p> Ensure the file name and file path match the files that were stored in step 1.</p> </div>
3	<p>Restart your server before installing Blue Prism Hub to ensure the components are fully installed and registered.</p>


 To watch this installation step, see our [.NET installation video](#).

- Download the Blue Prism Interact and Hub Upgrader for version 4.6 to 4.7 from the [Blue Prism Portal](#).


- Unzip the installer on the machine where Hub and Interact 4.6 are installed. It contains two files:
 - Blue Prism Interact and Hub Upgrader.exe – The upgrader executable.
 - BluePrismHubAndInteractUpdate4.7.bin – The binary file needed to upgrade to 4.7.

These files must be saved in the same directory.

- Double-click the upgrader executable to start the upgrader wizard, and on the Welcome to the Hub and Interact Upgrader screen, click **Next**.

 The upgrader checks that the prerequisite software from step 1 is installed. If it is not, the Prerequisites screen displays and you will need to close the installer and perform step 1.

- On the End-User License Agreement screen, read the End-User License Agreement and, if you agree to the terms, select the check box and click **Next**.
- On the Ready for Upgrade to 4.7 screen, click **Next** to upgrade Hub and Interact to 4.7.
- On the Completed the Blue Prism Hub and Blue Prism Interact upgrade screen:
 - When the upgrade completes successfully, click **Finish**.
 - If the installation failed, the **View Log** option will give you details of the error that was encountered. For more information, see [Troubleshooting upgrades](#).
- Repeat the process on all machines on which Hub and/or Interact is installed.

 The plugins are automatically updated to the latest version as part of the upgrade process.

Blue Prism Data Protector Tool

The Blue Prism Data Protector tool is used to decrypt and encrypt connection strings stored in the appsettings.json file. For security reasons, the connection strings are encrypted and the Blue Prism Data Protector tool allows the strings to be decrypted, so they can be altered if needed, and then encrypted again.

The BluePrismDataProtector.Console tool is a command line tool and should be used with Windows PowerShell running as an administrator.

Decrypt a connection string

To use the tool to decrypt a connection string:

1. Download the BluePrismDataProtector.Console.exe file from the [Blue Prism Portal](#) and save to a convenient location on your device.
2. Open PowerShell as an administrator in the folder where BluePrismDataProtector.Console.exe is located.

The Administrator: Windows PowerShell window displays.



If you type `.\BluePrismDataProtector.Console.exe` at the command line and press Enter, a list of possible commands will display.

3. From Windows Explorer, open the appsettings.json file that contains the string you want to decrypt and copy it. For example:

```
"HubServiceBus": {  
  "Connection": "CfDJ8LadX9spUNhMhvbXtcsxZYTHFA3m8Ty1-Z_EZ0Zn16mYfv_23Q2D2waPDTBxaz4-viN02Akk-S5C73dNjOdGHifGCxSIftwExJ304FuDXHpbNo0be-xyQt1D1-j7rosuYw",  
  "Topic": "tthtopic",  
  "Subscription": "Hub",  
}
```

4. In PowerShell, type the following:

```
.\BluePrismDataProtector.Console.exe unprotect -v "[string]" -p "[path]"
```

Where:

`[string]` = the copied string from the file

`[path]` = the path to DataProtectionKeys. Typically, C:\Program Files (x86)\Blue Prism\DataProtectionKeys

For example:

```
.\BluePrismDataProtector.Console.exe unprotect -v "CfDJ8LadX9spUNhMhvbXtcsxZYTHFA3m8Ty1-Z_EZ0Zn16mYfv_23Q2D2waPDTBxaz4-viN02Akk-S5C73dNjOdGHifGCxSIftwExJ304FuDXHpbNo0be-xyQt1D1-j7rosuYw" -p "C:\Program Files (x86)\Blue Prism\DataProtectionKeys"
```

5. Press **Enter**.

The string is decrypted and the unencrypted value displays in PowerShell.

Encrypt a connection string

To use the tool to encrypt a connection string:

1. Open PowerShell as an administrator in the folder where BluePrismDataProtector.Console.exe is located.
The Administrator: Windows PowerShell window displays.



If you type `.\BluePrismDataProtector.Console.exe` at the command line and press Enter, a list of possible commands will display.

2. In PowerShell, type the following:

```
.\BluePrismDataProtector.Console.exe protect -v "[string]" -p "[path]"
```

Where:

`[string]` = the string that you want to encrypt

`[path]` = the path to DataProtectionKeys. Typically, C:\Program Files (x86)\Blue Prism\DataProtectionKeys

For example:

```
.\BluePrismDataProtector.Console.exe protect -v "Str0ngP@$$w0rd" -p "C:\Program Files (x86)\Blue Prism\DataProtectionKeys"
```

3. Press **Enter**.

The string is encrypted and the value displays in PowerShell, for example:

```
CfDJ8LadX9spUNhMhvbXtcsxZYTHFA3m8Tyl-Z_EZ0Znl6mYfv_23Q2D2waPDTBxaz4-viNO2Akk-S5C73dNjOdGHifGCxSIftwExJ304FuDXHpbNo0be-xyQt1D1-j7rosuYw
```

4. Copy the encrypted string into the appropriate place in the appsettings.json file and save the file.
5. Open IIS Manager and restart the appropriate Application Pool to ensure it uses the new connection string.



If there are characters in your string which are associated with commands in PowerShell itself, you will need to add an escape character to your string so that PowerShell honors the string as intended. Such as:

- ``` and `$` will need a ``` (backtick) before the character, for example, `Str0ng`P@$`$W0rD` would need to be entered as `"Str0ng`P@`$`$W0rD"` on the command line.
- `"` will need ``` before it, for example, `P@$"W0rD` would need to be entered as `"P@`$`"W0rD"` on the command line.

These additional escape characters maintain the integrity of the string. If the resulting encrypted value is decrypted again, the value would match the original string rather than the command line version.

Previous Releases

Hub 4.6 – June 2022


This release note is for the 4.6 release of Blue Prism Hub .



Enhancements


The following new features and enhancements are introduced in this version of Hub.

Area	Description of Change	Reference
Audit	<p>The following enhancements have been made to the categories and events on the Audit page:</p> <ul style="list-style-type: none"> • Business process category: <ul style="list-style-type: none"> • Deleted Business process – This new event captures the required audit information when a business process is deleted. • Reactivated business process – This event was previously called Made active business process. • Process definitions (only applicable if the ALM plugin is installed): <ul style="list-style-type: none"> • Deleted process definition – This new event captures the required audit information when a process definition is deleted. • Owner redacted process definition – This new event captures the required audit information when the process definition owner redacts the process. • Interact - Forms category (only applicable if the Interact plugin is installed) – This category was previously called Interact. <ul style="list-style-type: none"> • Delete form – This existing event has been updated to include the deletion of form versions 0.0 and 0.1. Deleting these versions was not previously audited. • Edited form – This new event captures the required audit information when a form has been edited. • Increase major form – This event was previously called Form increase major. • Interact submissions category (only applicable if Interact is installed) <ul style="list-style-type: none"> • Form approved – Additional information is now captured in this event: the Submission id (GUID) parameter and Raised to role (role name). • Form declined – Additional information is now captured in this event: the Submission id (GUID) parameter and Raised to role (role name). • Form submitted – Additional information is now captured in this event: the Submission id (GUID) parameter and Raised to role (role name). 	<p>HUB-2902 HUB-1682 HUB-1661 INTER-175 HUB-3053 HUB-1676 HUB-1025 HUB-1298 HUB-1018</p>

Area	Description of Change	Reference
	<ul style="list-style-type: none"> • Form submitted (via API) – This new event captures the required audit information when a form has been submitted by the Interact Remote API. <p>The following audit events have been added to the Authentication management category on the Audit page:</p> <ul style="list-style-type: none"> • Native authentication enabled/disabled • Windows authentication enabled/disabled • Active Directory users created – This audits users added from Active Directory groups. • Active Directory user created – This audits users added automatically to the database without any roles or users added by assigning them to roles directly in Hub. • Updates to Active Directory users • Active Directory synchronization started • Active Directory synchronization completed • Active Directory synchronization failed • Active Directory domain added • Active Directory domain deleted • Active Directory domain updated <p>The following existing audit events have been renamed as follows:</p> <ul style="list-style-type: none"> • Made live authentication – LDAP configuration made live • Edited authentication – LDAP configuration edited • Deleted authentication – LDAP configuration deleted • Authentication synced – LDAP configuration synced • Authentication retired – LDAP configuration retired • Authentication added – LDAP configuration added <p>The Active Directory security groups associated with a role that has been created, changed, or deleted now also display when viewing the audit log for such an event. The security group entry shows the SID (Security Identifier) and DN (Distinguished Name).</p>	<p>BP-5649</p> <p>BP-5642</p> <p>BP-5498</p> <p>BP-5111</p> <p>BP-5409</p> <p>BP-5411</p> <p>BP-5419</p> <p>BP-5958</p> <p>BP-5459</p>

Area	Description of Change	Reference
Authentication settings	<p>The Authentication settings page in Hub has been updated to display all available authentication methods: native, Active Directory, and LDAP authentication. Previously, only LDAP authentication could be configured on this page.</p> <p>Hub administrators can enable/disable these authentication methods as follows:</p> <ul style="list-style-type: none"> • Native authentication is enabled by default in new environments or when upgrading Hub, however it can be disabled if there is at least one Hub administrator in the system who can sign in using LDAP or Active Directory authentication. • Both native and Active Directory authentication can be disabled if there is at least one Hub administrator in the system who can sign in using LDAP authentication. • If there are no LDAP users in the system, either native or Active Directory authentication must be enabled, and at least one Hub administrator configured to use the enabled authentication type must be kept in the system. • At least one LDAP connection must be added for LDAP authentication to be enabled. <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p> The Hub administrator(s) must be able to use the currently enabled authentication type(s). A warning displays if there is no administrator configured to sign in using the currently enabled authentication type(s).</p> </div>	<p>BP-3220 BP-4245 BP-4250 BP-5959</p>

Area	Description of Change	Reference
	<p>Authentication for Active Directory users in Hub now occurs as follows:</p> <ul style="list-style-type: none"> • Active Directory users configured in both Blue Prism and Authentication Server can now log into the Blue Prism interactive client using the Sign in using Authentication Server button on the interactive client login page. They will be directed to the Authentication Server login page where they can log in using a new Log in using Active Directory button without the need to re-enter credentials. • Active Directory users configured only in Authentication Server can log into Hub directly using the new Log in using Active Directory button if Active Directory authentication has been enabled in Hub. • Active Directory users that are not members of any Active Directory security groups or do not have any Hub roles assigned directly can still log into Hub but will be presented with a blank welcome page. This is to allow users who only have access to the Blue Prism interactive client to use Authentication Server as an authentication mechanism without accessing Hub. <div data-bbox="400 1043 1251 1137" style="border: 1px solid #00AEEF; padding: 5px;"> <p> LDAP users will still be prompted to re-enter their credentials.</p> </div>	<p>BP-5033 BP-4249 BP-6823</p>
	<p>Role management of Active Directory users in Hub is carried out by enabling at least one of the following options on the Authentication settings page:</p> <ul style="list-style-type: none"> • Allow authorization via Active Directory security group membership – One or more Active Directory security groups can be added to a Hub role. Users who are members of these security groups are automatically added to the Hub role. • Allow Active Directory users to be added directly to roles – One or more Active Directory users can be directly assigned to a Hub role. <div data-bbox="400 1563 1251 1688" style="border: 1px solid #FF0000; padding: 5px;"> <p> If you are using Interact, please see the Interact 4.6 release notes for limitations regarding Active Directory security groups and Interact.</p> </div>	<p>BP-5339 BP-4248 BP-5050 BP-5739</p>

Area	Description of Change	Reference
Active Directory domains	<p>Hub administrators can now view, add, edit, and delete Active Directory domains and associated credentials securely stored in the Authentication Server database via a new Active Directory domains page, accessible by clicking View domains on the Authentication settings page.</p> <p>Credentials are stored in the database when creating or editing an Active Directory domain. The username and password are encrypted before storage.</p> <p>For more information, see Active Directory domains.</p>	<p>BP-5408 BP-5409 BP-5411 BP-5419 BP-5410 BP-5062</p>
	<p>When searching Active Directory for users or security groups from within 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.</p> <p>The credentials stored against Active Directory domains in the Authentication Server database are used during the authentication of Active Directory users from those domains, to enable reading from the appropriate domain controller.</p> <p>The stored credentials are used in the following scenarios:</p> <ul style="list-style-type: none"> • Hub – Active Directory users from a forest that is trusted by the forest of the Windows account running the Authentication Server application pool in IIS can now log into Hub via Authentication Server. • Interact – Active Directory users from a forest that is trusted by the forest of the Windows account running the Authentication Server application pool in IIS, and who are members of Active Directory security groups assigned to Hub roles can now access the Interact application and plugin. • Hub Control Room – Active Directory users from a forest that is trusted by the forest of the Windows account running the Authentication Server application pool in IIS, and who are members of Active Directory security groups assigned to Hub and Blue Prism roles can now access the browser-based Control Room. <div data-bbox="400 1653 1251 1744" style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p> Additional configuration is required in Blue Prism, please refer to the Blue Prism 7.1 release notes (BP-6577).</p> </div>	<p>BP-5424 BP-6408 BP-6409 BP-6410</p>
Environment Manager	<p>A new Edit button has been added to the database tiles on the Environment Manager page in Settings. This opens the Edit connection page. The connection information that can be edited is limited to the new API configuration section.</p>	<p>BP-4890</p>
	<p>Users can now add API URLs to database connection configurations on the Environment Manager page. This is optional and allows users to access data via the Blue Prism API.</p>	<p>BP-4893</p>

Area	Description of Change	Reference
High Availability	The High Availability scripts have been updated for 4.6. They are available to download from the Blue Prism Portal .	HUB-3388
Installer and upgrader	The Blue Prism API screen has been removed from the installer due to these settings being moved to the Environments screen in Hub.	HUB-3011
	An enhancement has been made to apply the IIS feature Windows Authentication to the Authentication Server. If this feature is not already installed, it will be installed by the MSI.	HUB-1651 HUB-1918
	When the Hub installer or upgrader is run in Chinese, all of the screen titles now display correctly. Previously, some of the screen titles were truncated.	LOC-720
Roles and permissions	<p>If Active Directory authentication is enabled in Hub, administrators can now assign one or more Active Directory security groups to a role in Hub by retrieving security groups from the Active Directory. One or more users or security groups can be assigned to the same role.</p> <p>Active Directory users who have been assigned a Hub or Interact role from a security group, but do not have any direct roles assigned in Hub, are automatically assigned the Hub and Interact roles and their associated permissions.</p>	BP-4248 BP-5050 BP-5739
User interface	<p>The following design improvements have been made to the user interface:</p> <ul style="list-style-type: none"> • All pages in Hub now display a consistent title. • Check boxes in grids have been replaced with icons. • Rows per page selection now displays at the bottom of grids. • When entering text into a text field, the number of remaining characters allowed displays under the text field. 	HUB-2108 HUB-2110 HUB-2107 HUB-2922
	<p>The following changes have been made to the search field and filters in the following areas:</p> <ul style="list-style-type: none"> • A Username label has been added above the search field on the Users, Registrations, and LDAP> Configure user access and roles pages. • A Role name label has been added above the search field on the Roles and permissions page. • A Full name filter has been added to the filter drawer on the Users and Registrations pages. 	BP-5807

Area	Description of Change	Reference
Users	<p>A new Authentication type field has been added to the Add user page in Hub. The available options for selection are Native authentication and Windows authentication. This field only displays if both native and Windows authentication have been configured in a Hub environment.</p> <p>If Active Directory authentication has been enabled in Hub, administrators can add Active Directory users by selecting Windows authentication in the Authentication type field and searching the Active Directory. For more details, see Users.</p> <p>The validation for Hub users has also been updated as follows:</p> <ul style="list-style-type: none"> • Usernames for Active Directory users (their UPN) can now contain up to 255 characters and support the following characters: {, @, }. • Usernames for native users cannot exceed 25 characters in length and do not support the @ character. • First names for all user types can be up to 28 characters in length. 	BP-4246 BP-5049
	<p>A new Synchronize user option available for each Active Directory user record allows Hub administrators to synchronize a user's details with Active Directory. The following user details are updated: UPN, username, full name, email address, and status (active, deleted, or disabled).</p>	BP-6202
	<p>The option to retire or unretire a user in Hub is not available for Active Directory users using Windows authentication as this is carried out in Active Directory. An Active Directory user account is updated in Hub to reflect this once synchronization with Active Directory has occurred.</p>	BP-6226

Fixes and improvements

The following fixes and minor improvements are included in this version of Hub.

Area	Description of Change	Reference
Authentication Server	<p>Hub users are now prevented from accessing the Control Room plugin if the User login via Authentication Server option on the Security - Sign-on Settings screen in the Blue Prism interactive client has not been selected.</p> <ul style="list-style-type: none"> Automatic synchronization of user accounts between Authentication Server and the Blue Prism application server still requires user authentication via Authentication Server to be enabled, whereas service accounts are still synchronized even when user authentication via Authentication Server has not been enabled. Previously, the synchronization would incorrectly not occur if Authentication Server was not enabled in Blue Prism 	BP-3810
	<p>When an Active Directory user that has logged into Hub using Authentication Server requires a new access token, the OAuth 2.0 refresh token mechanism is used to generate a new valid access token, which will be automatically applied to that account. Any changes to permissions made while the access token is being refreshed (by default, five minutes) are now reflected when the new access token is applied to the account.</p> <p>If a user account is retired or deleted while the access token is being refreshed, the user will not be issued a new access token on refresh, and will no longer be able to access Hub.</p>	BP-6411 BP-6412
	<p>If login failures or performance issues are encountered during the login process via Active Directory, system administrators can manually configure trusted Active Directory domains that will be queried during the login process. If at least one Active Directory domain is manually configured, these settings will be used during the login process to query only the configured domain(s), rather than programmatically identifying which domains can be queried.</p> <p>The manual configuration requires adding the Active Directory domain name, forest name, and security identifier (SID) in the Authentication Server appsettings.json file for each required domain. For more information, see the Authentication Server configuration guide.</p>	BP-9497
	<p>To improve performance during login, the behavior of the cache that stores the discovered Active Directory domains can be configured by setting a refresh interval and a maximum cache duration in the Authentication Server appsettings.json file. For more information, see the Authentication Server configuration guide.</p>	BP-9654

Area	Description of Change	Reference
Email	Images are now correctly displayed in emails sent from Hub through Gmail. Previously, images such as logos were not displaying in emails sent through the Gmail service. Emails sent through Outlook were not affected.	HUB-813
Installer	Hub now installs correctly when duplicate certificates (multiple certificates with the same thumbprint) are present. Previously, the install would fail.	HUB-2205
	SQL users can now be created with a double quote (") symbol in the password. Previously, this would cause the installation fail.	HUB-1501
LDAP	When a Hub administrator synchronizes an LDAP connection in Settings > Authentication settings > LDAP for the first time after logging into Hub, the Theme filter on the Configure user access and roles page now correctly lists the available themes. This resolves the known issue present in Hub 4.5, where the available themes were not displayed.	HUB-2799 (HUB-2868)
Roles and permissions	When a Blue Prism user is mapped to the Authentication Server database, basic Hub permissions are now granted to the user so they have access to the Dashboard and Profile settings pages when they log into Hub for the first time.	BP-4810
Service accounts	It is now possible to create a new service account with the same name as a deleted one. Previously, the service account creation failed and an error message displayed.	HUB-1771
	When a user clicks the Copy to clipboard icon to copy the secret of a service account to the dashboard, a message now confirms that the secret has been copied.	BP-3793

Plugin updates

Automated Lifecycle Management (ALM)

The following improvements and fixes are included in this version of the ALM plugin.

Area	Description of Change	Reference
Process definitions	When deleting versions of a process definition, the latest version is now always deleted first. Previously, the version created first was deleted before the latest version, and an error displayed.	HUB-2061
	Members of a process definition now receive a notification when that process definition is deleted by another user, informing them of the name of the process definition and the username of the person who deleted it.	HUB-988
	It is now possible to create a new template with the same name as a deleted one. Previously, the template creation failed and an error message displayed.	HUB-2041
	Hub users can now delete templates in the following circumstances: <ul style="list-style-type: none"> • The template is not used in a process definition or exception. • The template is not locked by another user. 	HUB-1569
	When a Capture JSON file is imported into Process definitions, an <i>Else</i> choice is automatically added to the list of choices for each decision point, as an alternative option to the choices that were created in Capture. The <i>Else</i> choice is imported with a default route of <i>TBC</i> . The <i>Else</i> choice can be edited in the Edit definition page with options to either route to a step or to act as an exception. <i>Else</i> choices cannot be deleted, and will not be added if the decision point already contains 15 choices.	HUB-1593
Exceptions	When deleting versions of an exception, the latest version is now always deleted first. Previously, the version created first was deleted before the latest version, and an error displayed.	HUB-2061
	Hub users can now delete exceptions in the following circumstances: <ul style="list-style-type: none"> • The exception is not used in a process definition, a template, or another exception. • The exception is not locked by another user. 	HUB-1568
Business processes	Members of a business process now receive a notification when that process is deleted by another user, informing them of the name of the deleted business process and the username of the person who deleted it.	HUB-989
	The Business process name column now displays data in alphabetical order.	HUB-2030

Area	Description of Change	Reference
Miscellaneous	Toaster notifications now display when process definitions, business processes, exceptions, and templates are deleted.	HUB-1570
	License validation has been removed when editing: <ul style="list-style-type: none"> • Any users (or LDAP users) with the ALM role assigned to them. • Any user with Hub administrator privileges. 	HUB-3055
Wireframer	Creating actions in Wireframer is no longer case sensitive. If a user attempts to create two actions with the same name, but with different capitalization, only the first action is created and a notification displays for the second action explaining that the name is not unique. Previously, two actions were created in this scenario.	HUB-3694

Control Room

Area	Description of Change	Reference
Application	<p>The Schedules and Tasks page has been replaced by two new pages:</p> <ul style="list-style-type: none"> • Schedule Activity – Allows users to monitor the status of each environment, filter data, and create user-defined views. • Schedule Manager – Allows users to control, create, modify schedules, and manage activity with the help of user-defined views. <p>For more details, see Schedule Activity and Schedule Manager.</p> <p>The Schedules Activity and Schedule Manager pages can only be accessed by users with the scheduler permissions enabled within their Blue Prism environment. Users without the correct permissions are notified, and prompted to contact their Blue Prism system administrator.</p>	<p>HUB-2749 HUB-2750 HUB-1728</p>
	<p>Details on a user's role and permissions are now stored in the browser to ensure permissions checks are more efficiently performed in Control Room. The data is refreshed frequently for enhanced security and to ensure any permission changes are immediately applied.</p>	<p>HUB-1796 BP-5404</p>
	<p>A breadcrumb trail has been added to all pages of Control Room, providing easier navigation between features.</p>	<p>HUB-1395</p>
	<p>New refresh options have been added to all tables in Control Room to give users more control over the refresh rate of table data. Each page now includes the following options:</p> <ul style="list-style-type: none"> • Auto refresh – Defines how often the table contents will automatically refresh. It is disabled by default, but can be set to every minute, five minutes, 10 minutes, or 30 minutes. • Refresh now – Manually refreshes the table contents. If auto refresh is enabled, using this option will reset the timer. • Last updated – Displays the date and time when the table was last refreshed. 	<p>HUB-1784 HUB-3253 HUB-3252 HUB-1793</p>
	<p>Environment selection has been added to Control Room, enabling users to change environments, and API connections, from any page in Control Room. Environments must be pre-configured in Hub's Environment Manager, with a valid API URL.</p>	<p>BP-4894</p>
Schedule Activity	<p>The Schedule Activity page can now be filtered by schedule name and server name. Searches can be performed as exact matches, or by 'starts with'.</p>	<p>HUB-1701 HUB-1360</p>
	<p>Columns in the Schedule Activity table can now be sorted in ascending or descending order. The default is to show the most recent items.</p>	<p>HUB-3162</p>

Area	Description of Change	Reference
Schedule Manager	<p>The following improvements have been made to schedule cards:</p> <ul style="list-style-type: none"> • The card size has been reduced to offer a more compact view of schedule details. • Additional schedule details, such as recurrence type and expiry date, have been moved to a new View schedule details pane. Schedule cards now only include the schedule name, number of tasks, and retired status. • Longer schedule names are now truncated and displayed with an ellipsis (...) when overflowing from the schedule card. 	HUB-2751
	<p>Users can now view and edit schedule details from the Schedule Manager page. This can be achieved by clicking the ellipsis ... button on the relevant schedule card and selecting View details or Edit. Users can also access the edit view from the Details section by selecting the Edit icon in the top of the pane.</p>	HUB-1530 HUB-1531 HUB-1375 HUB-1762
	<p>Schedules can now be deleted by clicking the ellipsis (...) button on the relevant schedule and selecting Delete. This option only displays for users with the Delete Schedule permission.</p>	HUB-1723
	<p>Users can now view and edit schedule tasks by clicking the ellipsis (...) button on the relevant schedule card and selecting View tasks and sessions. Tasks can then be edited from the Tasks and sessions pane. The edit icon only displays for users with the Edit Schedule permission.</p>	HUB-1392 HUB-2158 BP-6390
	<p>Users can now add and edit scheduled sessions by clicking the ellipsis (...) button on the relevant schedule card and selecting View tasks and sessions. Scheduled sessions can then be added by selecting the ellipsis button on the task and clicking Add session, and edited by selecting the edit icon. The edit icon only displays for users with the Edit Schedule permission.</p>	HUB-1731 HUB-2125 HUB-2127
	<p>Users can now configure start-up parameters when editing scheduled sessions from the Tasks and sessions pane. For improved usability, start-up parameters also include the relevant parameter type.</p>	HUB-1408 HUB-2464
	<p>Users can now delete a schedule's tasks and sessions from the Tasks and sessions pane. This is accessed by clicking the ellipsis (...) button on the relevant schedule card and selecting View tasks and sessions. The delete icon only displays for users with the Delete Schedule permission.</p>	HUB-1732 HUB-1733
	<p>Schedules can now be cloned by clicking the ellipsis (...) button on the relevant schedule, and selecting Clone. This option only displays for users with the Create Schedule and Edit Schedule permissions. When cloning a schedule, users can configure the details of the new schedule, and choose to retire the existing schedule if required and they have the relevant permissions.</p>	HUB-2307 HUB-2308 HUB-2969

Area	Description of Change	Reference
	A schedule that is running can now be stopped via Schedule Manager by clicking the ellipsis (...) button on the relevant schedule, and selecting Stop . This option only displays for users with the Edit Schedule permission.	HUB-2880
	Users can now edit the repeat configuration for schedules and define the parameters required for each recurrence type. This feature includes schedules that run once, minutely, hourly, daily, weekly, monthly, and annually.	HUB-1702
	Users can now retire and unretire schedules via the schedule cards. This can be achieved by clicking the ellipsis (...) button on the relevant schedule and selecting Retire or Unretire . These options only display for users with the Edit Schedule, Retire Schedule, and Create Schedule permissions.	HUB-1822
	The error message displayed when attempting to retire an already retired schedule has been improved to be clearer. Previously, the message only contained an error code.	HUB-1452
	An issue has been resolved where duplicate validation error messages displayed when attempting to configure a schedule with an expiry time before the start time. Now, only one error message displays.	HUB-2375
Sessions	The Sessions table has been updated to display warnings on any sessions with the warning status. A status calculation query has been added to the table, ensuring that sessions with the warning status are correctly highlighted to users.	BP-2665
	The Sessions table has been re-sized to improve usability and the visual presentation of the table data.	HUB-2761
	Calculation stages are now displayed as expected in session logs. Previously, calculation stages displayed fully capitalized in the Stage type column.	HUB-1453
	Error handling has been improved when a user attempts to navigate to an invalid session log parameter. Users are now redirected to the Sessions log page and informed by a toast message that the parameter does not exist.	HUB-1455
Digital Worker Health	Users are now able to filter resources by retired status on the Digital Worker Health page. The default configuration is to display only unretired resources. For more details, see Digital Worker Health .	HUB-1754
Work Queues	The Work Queues table has been re-sized to improve usability and the visual presentation of the table data.	HUB-2759 HUB-2760
Dashboard	The calculations used by the Monthly utilization diary have been improved to more accurately convert hours of activity and inactivity into percentages.	HUB-1721
	The Utilization heatmap has been updated to introduce a more expansive color palette, with a color scale representing values from zero to 60, enabling users to more easily understand utilization data at a glance.	HUB-2967

Decision

The release notes for Decision are split into:

- [Decision Model Service](#) – covering any changes to the model service. This is supplied either as a container or as an msi (from this release). The model service is a prerequisite for running the Decision plugin.
- [Decision plugin](#) – the user interface used to generate the Decision models. This is available as a plugin in Blue Prism Hub.

Decision Model Service

Area	Description of Change	Reference
Container	The Decision container has been updated to return the version label (currently 1.1.1), which is now displayed in the Decision plugin.	DCN-243
Installer	The Decision Model Service is now available as a Windows service, as well as the Docker container introduced in 4.5. The Windows service can be installed using the Decision Model Service MSI available on the Blue Prism Portal . For more information, see the Decision install guide .	DCN-559

Decision Plugin

Area	Description of Change	Reference
Define, Train and Calibrate	The model accuracy now displays on the Teach tab of the Train page. This value will change as each new sample is created and the model is trained.	DCN-660
	The samples that are used on the Ask tab of the Calibrate page are now in a collapsed section. To see the samples or rules used by the prediction, the user can click on the Show references used link to expand the section.	DCN-587
	A message now displays if samples are created for all possible combinations informing the user that no more samples are required.	DCN-274
	The Weight column is no longer displayed on the Ask tab of the Calibrate page as this column was redundant.	DCN-711
	The numerical combo-box and slider fields have been changed to a numerical field. Users can now enter numbers directly into the field. In addition, the validation messages have been updated. The updates impact the : <ul style="list-style-type: none"> • The Rules tab, Initialize tab and the Teach tab on the Train page. • The Ask tab on the Calibrate page. This resolves a previous known issue.	DCN-485 DCN-616

Area	Description of Change	Reference
Export and Import	Decision now supports the import and export of models. This new functionality enables models to be easily transferred between development and production environments. The models include all the information that is needed to run them, including the variables, the training, and the calibration, along with the version number of the model service used. Exported models are encrypted using base64.	DCN-561 DCN-562 DCN-625 DCN-612
Library	<p>The following enhancements have been made to the Decision Library page:</p> <ul style="list-style-type: none"> Filters have been added. These can be accessed by clicking the Filter icon and enable users to filter models by identification number, name, or a date range for when models were created or edited. The inline icons have been removed from the individual model rows and now display along the top of the Library page, with new icons for new functionality. A check box has been added to each row in the Selected column instead. This enables users to carry out an action on multiple models at the same time. Users can now delete multiple models at the same time by using the Selected check box and clicking Delete. The Use count column has been renamed to Total predictions. The version of the model service that was used to create the model is now displayed. Users can update their models to use the latest model service. 	DCN-568 DCN-565 DCN-434 DCN-593 DCN-588 DCN-590
Prediction history	<p>The prediction history has been enhanced:</p> <ul style="list-style-type: none"> Information now displays in the main screen in place of the Library and not on an overlay screen. Filters have been added. These can be accessed by clicking the Filter icon and enable users to filter the prediction history by correlation ID, model result, and time stamp. 	DCN-529 DCN-567 DCN-346
User Interface	<p>The following overall improvements have been made to the user interface:</p> <ul style="list-style-type: none"> The plugin name is now displayed as Decision rather than Blue Prism Decision, and this is also reflected in the path shown at the top of each page. Label changes have been made to be more intuitive or more accurately reflect the functionality shown. Helpful tooltips have been added. Where available, these are shown by a question mark ? icon. When a user clicks the ?, further information is shown. 	DCN-453 DCN-434 DCN-113 DCN-602

For more information, see the [Decision User Guide](#)

Interact

For the Interact plugin improvements and fixes, see the [Interact 4.6 release notes](#).

Known issues

A list of any prominent issues with this release is maintained in the knowledge base:

- For Hub known issues, click [here](#).
- For Decision known issues, click [here](#).
- For Interact known issues, click [here](#).

Secure development policy

As part of our secure development policy, Blue Prism products are evaluated against the following security standards:

- OWASP Top 10 –The security vulnerabilities that pose the most risk to applications development. For more information, see the [OWASP website](#).
- SANS CWE Top 25 – The most common software security vulnerabilities found throughout the software development industry. For more information, see the [SANS website](#).
- Federal Information Processing Standard (FIPS) Publication 140-2 – U.S. government standard that defines minimum security requirements for cryptographic modules in information technology products.
- Payment Card Industry Data Security Standard (PCI DSS).
- Health Insurance Portability and Accountability Act (HIPAA).
- Federal Information Security Management Act (FISMA).

A compliance highlight summary report is available upon request via Product Support.

Hub 4.5 – November 2021

This release note is for the 4.5 release of Blue Prism Hub .

Enhancements

The following new features and enhancements are introduced in this version of Hub.

Area	Description of Change	Reference
Audit	<p>Hub administrators are now able to change passwords for other administrators. Additionally, a new Change password event type has been added to the User Management audit category in the Hub Audit area. When a password change occurs, the Hub administrator can view:</p> <ul style="list-style-type: none"> • The username of the user who performed the change • The username of the user whose password has changed • The date the event happened • The IP address of the computer where the change was made • The category of the event that happened 	HUB-1312 HUB-1522
High Availability	<p>Blue Prism Hub has been enhanced to support high availability infrastructures. Multiple instances of your Blue Prism Hub servers can be used with your organization's load balancers, RabbitMQ clusters and SQL Server clusters, thereby improving the availability of your Blue Prism environment to your users.</p> <p>For more information, see the High Availability configuration guide.</p>	HUB-1164
Installer and Upgrader	<p>The following enhancements have been made to the Hub installer and the Hub and Interact Upgrader:</p> <ul style="list-style-type: none"> • Localization – The user can now select the language on the first screen in the wizard. For a list of supported languages, see Localization. • Blue Prism Decision Setup – A new optional screen has been added to the Hub Installer to allow the user to enter a Blue Prism Decision URL and certificate. • Blue Prism Decision SQL configuration – An additional screen appears after the Decision URL is configured. This new screen enables the database for Decision to be configured. • Blue Prism API URL screen – A Skip button has been added to allow the user to skip the API URL setup and proceed to the next part of the wizard. <p>For more information, see the Hub install guide or the upgrade guide.</p>	HUB-2443

Fixes and improvements

The following fixes and minor improvements are included in this version of Hub.

Area	Description of Change	Reference
Hub Roles	If a Hub user is assigned to a Hub administrator role, they now have access to the Hub Settings page. Previously, if a user with Hub permission was assigned to a Hub administrator role, they were denied access to the Hub Settings page.	HUB-2374

Plugin updates

Automated Lifecycle Management (ALM)

The following improvements and fixes are included in this version of the ALM plugin.

Area	Description of Change	Reference
Wireframer	Wireframe action names are no longer case sensitive to ensure the action name is unique. If two actions are given the same name, one in uppercase and the other in lowercase, an error message now displays and only the first of the two actions is created. Previously, two separate actions were created.	HUB-2913

Control Room

No changes have been made to the Control Room plugin in this release.

Decision – New in Hub 4.5

Blue Prism® Decision provides Blue Prism users with the ability to train and deploy intelligent machine-learning decision-making models within their Digital Workforce, without requiring any data science expertise. Blue Prism Decision's simple and intuitive user interface allows users to:

- **Define a model** – Add a title, description, decision type, and decision variables.
- **Train the model** – Use active learning based on defined input variables specified by the model service, without needing any data science knowledge to produce statistically accurate machine-learning models.
- **Calibrate the model** – Review model inputs and outcome predictions, and overwrite model decisions if required.

Blue Prism Decision is a new license-controlled plugin available in 4.5. For more information, see [Decision](#) in the online help.

Interact

For the Interact plugin improvements and fixes, see the [Interact 4.5 release notes](#).

Known issues

A list of any prominent issues with this release is maintained in the knowledge base:

- For Hub known issues, click [here](#).
- For Decision known issues, click [here](#).
- For Interact known issues, click [here](#).

Secure development policy

As part of our secure development policy, Blue Prism products are evaluated against the following security standards:

- OWASP Top 10 –The security vulnerabilities that pose the most risk to applications development. For more information, see the [OWASP website](#).
- SANS CWE Top 25 – The most common software security vulnerabilities found throughout the software development industry. For more information, see the [SANS website](#).
- Federal Information Processing Standard (FIPS) Publication 140-2 – U.S. government standard that defines minimum security requirements for cryptographic modules in information technology products.
- Payment Card Industry Data Security Standard (PCI DSS).
- Health Insurance Portability and Accountability Act (HIPAA).
- Federal Information Security Management Act (FISMA).

A compliance highlight summary report is available upon request via Product Support.

Hub 4.4.1 – October 2021

This release note is for the 4.4.1 release of Blue Prism Hub delivered in an on-premise configuration.

Control Room

The following improvements and fixes are included in this version of the Control Room plugin.

Area	Description of Change	Reference
Application	An issue with dashboard widgets on the Control Room dashboard has been fixed. Widgets now display data and filters work as intended. In Hub version 4.4 this issue caused widgets to display no data, and applying a filter to a widget would display a blank page.	HUB-2447

Known issues

A list of any prominent issues with this release is maintained in the knowledge base, click [here](#) for more information.

Secure development policy


As part of our secure development policy, Blue Prism products are evaluated against the following security standards:

- OWASP Top 10 –The security vulnerabilities that pose the most risk to applications development. For more information, see the [OWASP website](#).
- SANS CWE Top 25 – The most common software security vulnerabilities found throughout the software development industry. For more information, see the [SANS website](#).
- Federal Information Processing Standard (FIPS) Publication 140-2 – U.S. government standard that defines minimum security requirements for cryptographic modules in information technology products.
- Payment Card Industry Data Security Standard (PCI DSS).
- Health Insurance Portability and Accountability Act (HIPAA).
- Federal Information Security Management Act (FISMA).

A compliance highlight summary report is available upon request via Product Support.

Upgrade from 4.4.0 to 4.4.1

Blue Prism has made the latest plugin files available on the Blue Prism portal. These enable a Hub administrator to update the plugins from 4.4.0 to 4.4.1, thereby restoring the use of the Control Room widgets.

 You must be a Hub administrator to update the plugin files. You should update the plugins during a system maintenance period, when no other users are logged in, as the system will restart as part of the process.

To update 4.4.0 to 4.4.1:

1. Download the 4.4.1 Hub plugin package from the Blue Prism portal and unzip it to a folder on your computer.
2. In Hub, click your profile icon to open the Settings page and click **Plugin Management**.
The Plugin management page displays.
3. Click **Add plugin**.
The Open dialog displays to enable you to find a local file.
4. Navigate to the folder from step 1, select all the plugin files which you have unzipped from the plugin package and click **OK**.
A notification message displays indicating that the files have been uploaded successfully.
5. Click the refresh icon on your browser window to refresh the Plugin management page.
The **Update all** icon activates and a number is shown indicating the number of plugins to be updated.
6. Click **Update all**.
A message displays informing you of the update progress followed by a list of installed plugins.
7. Click **OK** on the Installed plugins screen to restart the site.
A Restating site message displays; this may display for a few minutes. Following the restart, the plugins display with a version number in the format 4.4.1.x, such as 4.4.1.2.
The updated system is now ready to use.

Hub 4.4 – September 2021

This release note is for the 4.4 release of Blue Prism Hub delivered in an on-premise configuration.

Enhancements

The following new features and enhancements are introduced in this version of Hub.

Area	Description of Change	Reference
Application	<p>The following improvements have been made to the user interface:</p> <ul style="list-style-type: none"> • Fields can no longer be edited when the submission process is in progress. • When editing or selecting information, a yellow border now displays around the field in focus. • Drop-down lists have been replaced with combo boxes. Starting to type the name of an item into the text field filters the displayed options to only show items that match the text. 	<p>INTER-56 HUB-1557 HUB-1714</p>
Audit	<p>The following categories and events have been added to the Audit page:</p> <ul style="list-style-type: none"> • Business process <ul style="list-style-type: none"> • Created business process • Made active business process • Retired business process • Process definitions (only applicable if the ALM plugin is installed) <ul style="list-style-type: none"> • Created process definition • Removed process definition • Increase major – audit logging for increasing the process definition major version • Sign off started • Sign off process definition • Redacted process definition • Sign off finished • Interact (only applicable if the Interact plugin is installed) <ul style="list-style-type: none"> • Created form • Removed form • Form increase major - audit logging for increasing the form major version <p>Audit functionality has been added to support all these events.</p>	<p>HUB-1117</p>
User Management	<p>It is now possible to create a new user in the Users area when Interact is not connected.</p>	<p>HUB-944</p>
Security	<p>To improve security, optional Single Socket Layer (SSL) settings have been added for applications that use RabbitMQ.</p>	<p>HUB-74</p>

Fixes and improvements

The following fixes and minor improvements are included in this version of Hub.

Area	Description of Change	Reference
Application	An issue has been fixed where Hub continually attempted to reload while displaying the "Something went wrong" error message. The issue was caused by an incorrect token refresh and was reported in environments that use Windows Authentication to authenticate with the SQL Server.	HUB-1201
	An issue has been fixed where, after applying an ALM license and rebooting the system, Hub and Interact could not be accessed. When Hub was selected from the selection screen displayed after logging in, an <i>HTTP Error 502.5 - ANCM Out-Of-Process Startup Failure</i> message was observed; where as Interact appeared as unavailable on the selection screen. Blue Prism Hub and Blue Prism Interact can now be accessed without experiencing these issues.	DS-597 HUB-2300 IADA-102
Audit	A minor adjustment has been made to the Edit view pane on the Audit page. The filter category/column heading previously labeled Date time has been changed to Created On for consistency.	HUB-1127
Authentication Server	A header style error has been fixed on the Authentication Server login page, where changing the width of the browser window to 992px or less caused the language drop-down list to become disabled.	HUB-1223
Environment Management	An issue has been resolved where the user was unable to add a new environment to the Hub Environment management page following a previous failed attempt. This was due to the environment data not being cleared from connected databases after the failed attempt.	HUB-1356

Area	Description of Change	Reference
Installer	<p>The following changes have been made to the Hub Installer:</p> <ul style="list-style-type: none"> • New fields have been added to the Prerequisites 2 – RabbitMQ screen: Virtual host and Protocol. • The Distributed Cache SQL connection screen has been removed. • The File Service SQL connection configuration screen has been added. This creates a new File Service database for the storage of files, rather than storing the files in a folder system on the server hard disk. <p>For more information, see the Hub install guide.</p>	<p>HUB-1515 HUB-1516 HUB-1654</p>
	<p>The installation no longer fails if the machine has no internet access or has an incompatible version of the PowerShell SqlServer module is installed on the machine. Previously, the installation would fail if the column encryption script was run in an offline environment.</p>	<p>HUB-2020</p>
	<p>Host names for all sites can now be custom host names and use mixed case characters (uppercase and lowercase).</p> <p>Previously, if the initial part (application name) of the default host name was changed during installation and mixed case characters were used, a 500 error was displayed when certain pages in Hub were accessed, for example, Email configuration page, Audit page, and when uploading a license.</p>	<p>HUB-906</p>
LDAP	<p>Hub can now synchronize with more than 10,000 Active Directory users. Previously, Hub was restricted by the default limit set within MaxTempTableSize on the LDAP server.</p>	<p>HUB-1538</p>
SMTP	<p>SMTP host names with more than three symbols can now be entered into the SMTP host field.</p>	<p>HUB-1222</p>
Settings	<p>An issue with the Customization page has been fixed, where attempting to save a theme with incorrectly formatted text in the Name field resulted in the system endlessly attempting (and failing) to validate the name, instead of displaying an error message.</p>	<p>HUB-1134</p>
	<p>On the Add connection page, the Database authentication header on the Add connection page no longer displays on the form when SQL with Windows Authentication is selected.</p>	<p>HUB-1163</p>
	<p>When creating new roles in Hub, all names must now be unique. It is no longer possible to give a Hub role and an Interact role the same name.</p>	<p>HUB-2036</p>
Service accounts	<p>A new permission has been added to service accounts: Interact Remote API. This enables service accounts to be created that can be used when setting up the Interact Remote API with other Blue Prism products.</p>	<p>HUB-1564</p>

Plugin updates

Automated Lifecycle Management (ALM)

The following improvements and fixes are included in this version of the ALM plugin.

Area	Description of Change	Reference
All	The user interface has been further refined to improve usability and readability when modifying process definitions, wireframes, exceptions, and templates. For more information about the user interface. See the ALM user guide	HUB-1093
Business processes	A new Delete button has been added to enable the user to retire business processes. A business process can only be deleted by the business process owner, and it cannot be deleted if it has a process definition or an Interact Form associated with it. For more information, see ALM – Business processes .	HUB-895
	When sorting data in the Name and Stage progression columns of the Business processes overview page, the first click now sorts the data alphabetically and the second click sorts in reverse alphabetical order. Previously, the sorting was incorrectly applied the opposite way around.	HUB-1159

Area	Description of Change	Reference
Process definitions	<p>JSON files exported from Blue Prism Capture versions 1.0, 2.0, and 2.1 can now be imported into ALM. This enables ALM users to quickly and efficiently generate a process definition without manually documenting the steps.</p> <p>The user can:</p> <ul style="list-style-type: none"> • Add up to 15 custom choices per decision step to be added to the process definition. • Drag and drop steps and sections to rearrange them in the process definition. • Move sections and steps directly above or below a specified section or step in the process definition. • Upload missing images manually if any fail to import automatically. • Opt to have any applications that are not already listed in ALM to be automatically added to the Applications page on import. <p>The following items are included in the import:</p> <ul style="list-style-type: none"> • Capture notes. • A Custom action option has also been added in the Action type drop-down list when creating an Action step in a process definition. • Click hold, Click release, Key press, and Triple click actions. <p>For more information, see Upload a JSON file.</p>	HUB-593
	<p>Process definitions can now be deleted. A process definition can only be deleted by the process definition document owner, and it cannot be deleted if it is locked for editing by another user. For more information, see Delete a process definition.</p>	HUB-896
	<p>A new filter called Sign off status has been added to the Process definitions page. This filter enables users to view only those process definitions where sign-off has been started but not yet completed.</p>	HUB-496
	<p>Auditing of process definition workflow events has been added. For information about the events within the Process definition category, see Audit page.</p>	HUB-1117
	<p>The maximum number of characters in the Element name field has been increased from 50 to 75.</p>	HUB-638
	<p>An issue on the Edit definition page has been resolved, where the thumbnail image did not display correctly in the action steps.</p>	HUB-1234
Wireframer	<p>Clicking the Send report button no longer results in an error and opens the correct page.</p>	HUB-1227
	<p>An issue has been fixed where the incorrect notification displayed when the user set up traditional SMTP settings and clicked Send report. The correct notification now displays.</p>	HUB-1171

Control Room

No changes have been made to the Control Room plugin in this release.

Interact

For the Interact plugin improvements and fixes, see the [Interact 4.4 release notes](#).

Known issues

A list of any prominent issues with this release is maintained in the knowledge base, click [here](#) for more information.

Secure development policy

As part of our secure development policy, Blue Prism products are evaluated against the following security standards:

- OWASP Top 10 –The security vulnerabilities that pose the most risk to applications development. For more information, see the [OWASP website](#).
- SANS CWE Top 25 – The most common software security vulnerabilities found throughout the software development industry. For more information, see the [SANS website](#).
- Federal Information Processing Standard (FIPS) Publication 140-2 – U.S. government standard that defines minimum security requirements for cryptographic modules in information technology products.
- Payment Card Industry Data Security Standard (PCI DSS).
- Health Insurance Portability and Accountability Act (HIPAA).
- Federal Information Security Management Act (FISMA).

A compliance highlight summary report is available upon request via Product Support.


Hub 4.3 – May 2021

This release note is for the 4.3 release of Blue Prism Hub delivered in an on-premise configuration.

Enhancements

The following new features and enhancements are introduced in this version of Hub.



Area	Description of Change	Reference
Control Room	<p>A new plugin has been added to Hub; Control Room. This plugin can only be used with Blue Prism version 7.0 or later, and it complements the Control Room features in the Blue Prism interactive client.</p> <p>The new Control Room provides dashboards and data views that allow users to view and manage Blue Prism activity for all their environments. Control Room has four plugin features that complement the existing Blue Prism interactive client functionality:</p> <ul style="list-style-type: none"> • Work Queues – Monitor the status of work queue items and track queue activity. • Schedules and Tasks – View and monitor schedules and tasks. • Sessions – View, filter, and organize session activity in each environment. • Digital Worker Health – View and monitor the Digital Workers in each environment. <p>The Control Room plugin also introduces a number of widgets which can be used on the Dashboard to graphically view the data.</p>	BP-131 BP-1581

Area	Description of Change	Reference
Installer	<p>The following new features have been added to the Hub installer:</p> <ul style="list-style-type: none"> Authentication Server SQL configuration and IIS setup – The Identity Management Server (IMS) has been renamed to Authentication Server. In addition, the Authentication Server facilities enhanced integration to utilize the new features in Blue Prism 7.0, such as service accounts (using centralized authentication for selected components of the Blue Prism platform) and the Control Room plugin. <div data-bbox="424 584 1251 678" style="border: 1px solid #0070C0; padding: 5px; margin: 10px 0;">  The Authentication Server screens in the installer replace the IMS screens that were present in earlier versions. </div> Email Service SQL configuration – Email configuration now supports Microsoft OAuth 2.0 authentication as well as the existing username and password authentication method. To support this, a new screen has been added to the installer to configure the database for the Email Service. Email Service IIS setup – In earlier releases, Email Service was called Email Sender. The installer screen has been updated with this name change. The default website name has also changed, however, the default URL still remains as email.local. Blue Prism API URL – A new screen has been added to the installer to capture the URL for the Blue Prism API. The URL is required to use the new Control Room plugin with Blue Prism 7.0, otherwise, the screen can be left blank. 	<p>HUB-867 HUB-947 BP-2895</p>
Localization	<p>Support for two languages, Russian and Portuguese (Brazilian), has been removed. English will now be displayed for users who have selected these languages in their browser settings, or using the language drop-down on the login page in earlier versions of Hub.</p>	<p>BP-3601</p>
SMTP	<p>The Email configuration page has been enhanced to support Microsoft OAuth 2.0 authentication with SMTP, as well as the existing username and password authentication method. Any changes to the SMTP settings are audited and can be seen on the Audit page.</p>	<p>HUB-713</p>
User management	<p>The Users page has been enhanced:</p> <ul style="list-style-type: none"> Only live users (those that are not retired) are displayed by default. Retired users can be viewed by changing the setting under the Live filter. All users can be viewed by turning off the Live filter. On the Users page, an administrator can view a user's information and click the new Change password icon to change their password. An administrator cannot change another administrator's password. 	<p>HUB-865</p>

Fixes and improvements

The following fixes and minor improvements are included in this version of Hub.

Area	Description of Change	Reference
ALM	<p>The Uplift License option has been added to the Plugin management page to enable administrators to upgrade the ALM license from an earlier version to a version that is compatible with 4.3.</p> <p>This resolves the previously documented known issue where a warning message was permanently displayed on some pages in the system indicating that the ALM license limit had been exceeded.</p>	HUB-722
	<p>The creator of a process definition can now assign their own access level. Previously, they were defaulted to be the owner of the process definition and this could not be changed. They can now select to be a Contributor or a Viewer, however, the process definition can not be saved unless there is at least one owner.</p>	HUB-866
Audit	<p>Two columns in the Audit page have been renamed:</p> <ul style="list-style-type: none"> • Username is now Audited by – to reflect that the audit records can also be created by system components and not just users. • Date time is now Created on – to clearly define the purpose of this column. 	BP-2935
Environment	<p>An enhancement has been made so that Hub now also supports connections to multiple RPA databases that reside on the same server, that is, they have the same server IP or hostname. Previously, multiple databases could only be connected as long as they were on different servers to each other. The connection is configured through the existing Environment management page.</p>	HUB-723
	<p>Database connections can no longer be edited on the Environment management page. Connections can still be added, refreshed and deleted.</p>	HUB-932

Area	Description of Change	Reference
LDAP	<p>The importing of Active Directory users into Hub has been fixed. Previously, when importing Active Directory users into Hub, if any of the Active Directory user accounts were missing one of the mapped attributes defined in the Hub authentication settings, the import would fail for all users.</p> <p>The import now displays a counter with the number of valid users against the total number of users found, and displays the list of valid users so that the administrator can select the required users to synchronize with Hub.</p> <p>In addition, an enhancement has been made to introduce detailed LDAP logging. This can be turned on by updating the appsettings.json file in the Application Server folder. Under lms > Logging > LogLevel, add the line:</p> <pre>"ImsServer.IntegrationServices.Services.LdapConnectionService": "Debug"</pre> <p>Once this change has been made, refresh the Application Pool.</p> <div data-bbox="347 887 1275 1077" style="border: 1px solid #0070C0; padding: 5px;"> <p> For:</p> <ul style="list-style-type: none"> • a new install, the Application Pool will be called Authentication Server. • an upgraded system, the Application Pool will be called IMS. </div>	HUB-718
	<p>If a user who has been imported into Hub using LDAP clicks the Forgot password link, they are no longer sent an email enabling them to reset their password within Hub. Previously, this email was sent, and, if a user went through the process, it created a native user account in addition to their LDAP account.</p> <p>Users who have been synced into Hub using LDAP use their Active Directory domain password to log into Hub. If they need to reset their password, they should do so using Windows.</p>	HUB-1152
Licensing	<p>The error messages that display when uploading an invalid license file for a plugin have been improved. If an administrator uploads an invalid file type, or a license file that is too large, using the Renew license key functionality, a more informative message will display.</p> <div data-bbox="347 1576 1275 1632" style="border: 1px solid #0070C0; padding: 5px;"> <p> Only .lic files under 100Kb are accepted.</p> </div>	HUB-841
Plugins	<p>When a user clicks a plugin in the Plugins repository, they now see an overview of the plugin with a link to learn more about the product, which opens the online help. The plugin downloads are available below the overview.</p>	HUB-972 HUB-1063
SMTP	<p>A change has been made to ensure that emails are sent according to the encryption method selected. For SMTP configurations using the Username and password authentication method, the encryption method can be set to None or SSL-TLS. Previously, Hub was attempting to send emails over SSL regardless of the encryption setting.</p>	HUB-717

Known issues

A list of any prominent issues with this release is maintained in the knowledge base, click [here](#) for more information.

Secure development policy

As part of our secure development policy, Blue Prism products are evaluated against the following security standards:

- OWASP Top 10 –The security vulnerabilities that pose the most risk to applications development. For more information, see the [OWASP website](#).
- SANS CWE Top 25 – The most common software security vulnerabilities found throughout the software development industry. For more information, see the [SANS website](#).
- Federal Information Processing Standard (FIPS) Publication 140-2 – U.S. government standard that defines minimum security requirements for cryptographic modules in information technology products.
- Payment Card Industry Data Security Standard (PCI DSS).
- Health Insurance Portability and Accountability Act (HIPAA).
- Federal Information Security Management Act (FISMA).

A compliance highlight summary report is available upon request via Product Support.

Hub 4.2 – April 2021

This release note is for the 4.2 release of Blue Prism Hub delivered in an on-premise configuration.

Enhancements

The following new features and enhancements are introduced in this version of Hub.

Area	Description of Change
Application	<p>The Hub user interface has been redesigned.</p> <p>The help has been updated to reflect the changes, see the Hub user guide. The help can also be accessed from the link in the side navigation in Hub.</p>
Configuration	<p>An RPA database with no dependencies can now be removed from Hub.</p> <p>For more information, see Environment management.</p>
Installer	<p>The following new features have been added to the Hub installer:</p> <ul style="list-style-type: none"> • Notification Center SQL configuration and IIS setup – The Notification Center is required to enable the new notification functionality within Interact. • License Manager SQL configuration and IIS setup – Control of the licenses has been moved from within Hub into the new License Manager. The benefit of this is that Interact can still be accessed even if Hub is unavailable. Previously, if Hub was unavailable, Interact would be too. • SignalR IIS setup – This has been taken out of the Interact installer and moved into the Hub installer.
Licensing	<p>A new website (License Manager) has been created to handle license tasks. The advantage this provides is that if Hub is offline, users can still access Interact. Previously, Hub handled license tasks and if Hub was offline, Interact was unavailable too. The new website is installed and configured using the Hub installer.</p> <p>Hub now displays warnings if all the licenses have been used. For example, if all the ALM licenses have been assigned, a message is displayed against the users and/or roles:</p> <div style="border: 1px solid blue; padding: 10px; margin: 10px 0;"> <p>Automation Lifecycle restriction: 3/0</p> <p>WARNING: You are in breach of your license, please remove users, remove the ALM plugin or get in contact with your Accounts Manager for more information</p> </div>
Localization	<p>The IMS login page and Hub now display in the language compatible with the user's language settings set in their browser. If the user has an unsupported language selected in their browser settings, English is used as the default. If required, the user can manually change the language they want to use from the drop-down list on the login page.</p>
Supported software	<p>Hub now supports the use of Azure SQL Database.</p>

Fixes and improvements

The following fixes and minor improvements are included in this version of Hub.

Area	Description of Change
Audit	<p>The following event options have been added to the Audit page:</p> <ul style="list-style-type: none"> • Forms submitted • Forms declined • Forms approved <p>The Digital Worker category has been removed from the Audit page, this also removes the following event options:</p> <ul style="list-style-type: none"> • Edited Digital Worker Log • Retired Virtual Worker Log • Made Live-Virtual Worker Log
Configuration	<p>The following fields have been removed or replaced:</p> <ul style="list-style-type: none"> • The SMTP host field in the email configuration has been modified to remove the restrictive validation that was in place. Your organizations SMTP hostname can now be entered and accepted by the field. • The IADA URL field has been removed from the database connection information accessed from the Environment manager. • The Create a password for user check box has been removed from the Create user page. Instead, a new Create password dialog displays upon completing the new users details and clicking Create user. From this, the administrator can selected whether to create a password or send the user a password update email.
User Interface	<p>The level of visual customization has been reduced. UI customization is now restricted to:</p> <ul style="list-style-type: none"> • Theme name • Brand color • Brand logo <p>For more information, see Customization.</p>

Known issues

A list of any prominent issues with this release is maintained in the knowledge base, click [here](#) for more information.

Hub 4.1 – November 2020

This release note is for the 4.1 release of Blue Prism Hub delivered in an on-premise configuration.

Upgrading

The Blue Prism Interact and Hub Upgrader can be downloaded from the customer portal. This easy-to-use tool will upgrade 4.0 to 4.1. For more information, see [Upgrade Hub and Interact 4.0 to version 4.1](#).

Enhancements

The following new features and enhancements are introduced in this version of Hub.

Area	Description of Change
Authentication	Active Directory Authentication using LDAP can now be used to leverage the advantages of single sign-on. Once this connection has been established, users will be able to use their corporate logins to sign into Hub or Interact. This removes the need for the Hub Administrator to set up local users.
Installer	<p>The following enhancements have been made to the Hub installer:</p> <ul style="list-style-type: none"> • Server Manager roles and features automatically install – This requires VMs to restart after the installation; the choice can be made to restart immediately or later. • Customer ID is now entered through a new screen, rather than manually updating the customerid key in the appsettings.json file after installation. • Enhanced SQL screens: <ul style="list-style-type: none"> • Test connection button – This ensures that the information entered establishes a successful SQL connection. The installation cannot progress to the next step without a successful connection. • Inherited values from the previous SQL screen – This prevents the user from having to enter the same SQL information across multiple screens.
Tools	<p>A new tool has been added for encrypting and decrypting of connection strings.</p> <p>For security reasons the appsettings.json files for all the web sites are encrypted. If changes are needed to the configuration settings in this file, the encrypting/decrypting console application allows the file to be decrypted and then encrypted again.</p> <p>See Blue Prism Data Protector Tool for more information.</p>

Fixes and improvements

The following fixes and minor improvements are included in this version of Hub.

Area	Description of Change
Authentication	Previously, if Windows Authentication was selected within the Hub Database settings, the username and password fields were still available. These fields are now unavailable if the Windows Authentication option is selected, which reduces the likelihood of any potential SQL errors.
Installer	The following improvements have been made to the Hub installer: <ul style="list-style-type: none">• The installer has been renamed to Blue Prism Hub from Blue Prism Base.• Increased maximum number of users – Previously the maximum pool size used the default value. The maximum pool size has now been set to 500, thus allowing more users.• Legal and visual enhancements:<ul style="list-style-type: none">• The End-User License Agreement (EULA) has been reformatted.• The publisher name has been updated to "Blue Prism Limited" throughout the installer.

Known issues

A list of any prominent issues with this release is maintained in the knowledge base, click [here](#) for more information.

Hub 4.0 – September 2020

This release note is for the 4.0 release of Blue Prism Hub delivered in an on-premise configuration.

Enhancements

The following new features and enhancements are introduced in this version of Hub.

Area	Description of change
Plugins	<p>The following enhancements have been made to Hub's plugin repository:</p> <ul style="list-style-type: none"> • Differentiating all, free and licensed plugins drop-down • Differentiating all, free and licensed plugins label • Enter license file modal • Renew plugin license tab • Renew license modal
	<p>The following enhancements have been made to Hub's plugin expiry functionality:</p> <ul style="list-style-type: none"> • A warning now displays when a plugin is about to expire • When a plugin license expires, the following can no longer be accessed: <ul style="list-style-type: none"> • Interact plugin
Customization	<p>The following changes have been made to Hub's customization functionality:</p> <ul style="list-style-type: none"> • New default Blue Prism inline image • New default Blue Prism logo image on IMS • Company and Strapline values have been removed from Customization
Installer	Base installer
Security	<p>The following enhancements have been added to improve security in Hub:</p> <ul style="list-style-type: none"> • Code Obfuscation for IMS • Code Obfuscation for Hub

Plugin updates

A number of plugins are provided in a release – new and/or updated plugins are listed below.

Updated plugins

Plugin	Description
Interact	Priority and SLA no longer required fields when creating an Interact form.

Known issues

A list of any prominent issues with this release is maintained in the knowledge base, click [here](#) for more information.