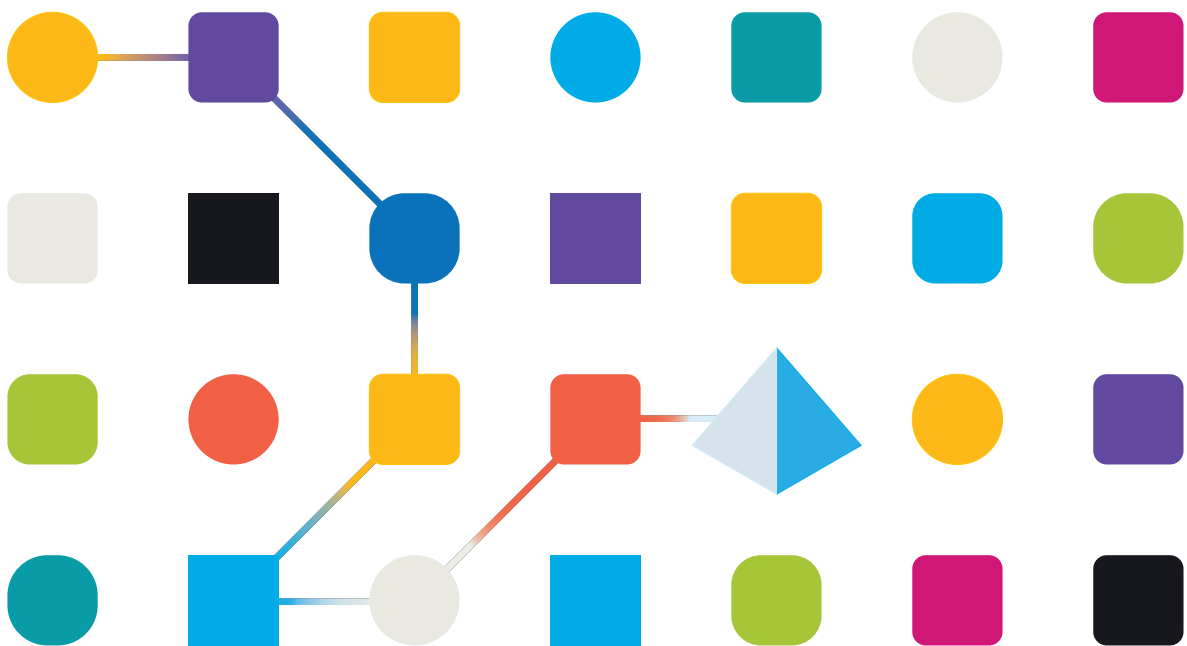


# blueprism<sup>®</sup>

## Blue Prism Hub 4.6

### 管理员指南

文档修订版:2.0



## 商标和版权

本指南中包含的信息是 Blue Prism Limited 和/或附属公司的专有和机密信息，未经获授权的 Blue Prism 代表的书面同意，不得披露给第三方。未经 Blue Prism Limited 或其附属公司的书面同意，不得以任何形式或通过任何手段(电子或实物形式，包括复制)翻印或传输本文档中的任何部分。

### © Blue Prism Limited 2001—2023

“Blue Prism”、“Blue Prism”徽标和 Prism 设备是 Blue Prism Limited 及其附属公司的商标或注册商标。保留所有权利。

其他所有商标在本指南中的使用均得到认可，并用于各自所属方的利益。

Blue Prism Limited 及其附属公司对本指南中引用的外部网站的内容概不负责。

Blue Prism Limited, 2 Cinnamon Park, Crab Lane, Warrington, WA2 0XP, 英国。

在英国境内注册:注册编号:4260035。电话:+44 370 879 3000。网站:[www.blueprism.com](http://www.blueprism.com)

# 目录

<b>Hub</b> .....	<b>4</b>
目标读者 .....	4
<b>管理和配置</b> .....	<b>5</b>
Hub 限制 .....	6
<b>设置</b> .....	<b>7</b>
概述 .....	7
平台管理 .....	7
用户管理 .....	7
个人资料 .....	9
<b>Audit</b> .....	<b>10</b>
环境管理 .....	13
电子邮件配置 .....	16
自定义 .....	19
插件管理 .....	21
用户 .....	24
角色和权限 .....	32
注册 .....	38
身份验证设置 .....	39
服务帐户 .....	50

## Hub

Blue Prism 整合了云、机器人流程自动化 (RPA) 和人工智能 (AI) 的原则,旨在以自动化和数字化的方式执行基于知识的工作。Digital Worker 会部署到业务运营,通过模拟人们使用业务系统的方式、他们所做的决定以及遵循的流程来工作,从而协助、替换人工工作流程或者实现数字化。

随着组织中 Digital Workforce 格局的成熟,运营商和赞助商需要扩展管理自动化投资的方式和方法。有关 Digital Workforce 的管理信息需要在整个业务中保持透明得到直观解释。此外,还需要监控最佳实践,以确保符合行业标准。Blue Prism® Hub 为新的和现有的 Blue Prism 用户提供生产力平台,用于管理自动化生命周期。Hub 适合 Robotic Operating Model (ROM) 内的个人角色,提供一系列功能,旨在确保以成功、可扩展的方式交付自动化策略。

Hub 作为轻量级的“空”应用程序创建,然后填充一系列插件或功能。这样会形成所谓的插件架构,允许 Blue Prism 团队迭代功能,使其可供 Hub 管理员使用。

每个 Hub 实例都包含插件管理库页面,允许管理员查看和部署新插件以及更新现有插件。

## 目标读者

本指南面向具有管理员特权的 Hub 用户,称为 Hub 管理员。Hub 管理员负责管理 Blue Prism Hub 平台,包括但不限于:

- 管理 Blue Prism Hub 平台、Blue Prism 和 Blue Prism API 之间的集成。
- 管理角色和用户,包括与 Active Directory 的集成。
- 安装插件。
- 监控审计日志。

因此,Hub 管理员应该是熟悉 IT 系统管理并了解企业软件架构和 Active Directory 的用户。

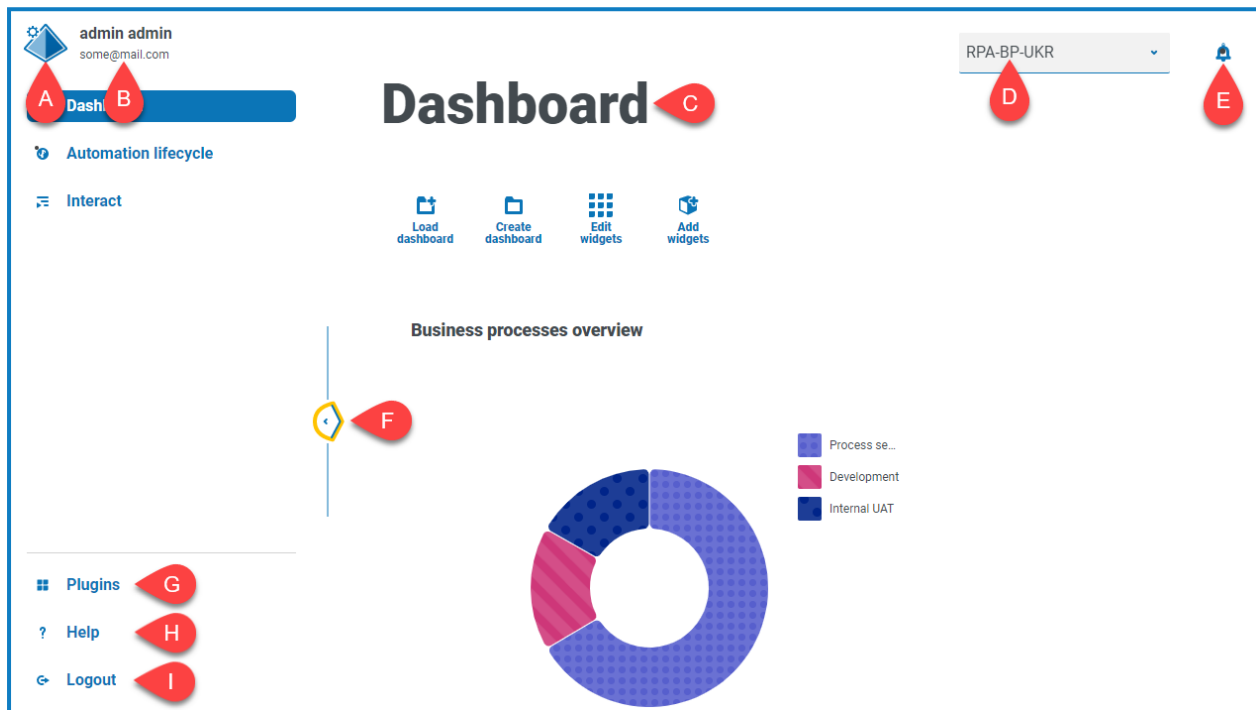
## 管理和配置

为组织安装 Hub 时，它会在安装好之后提供一个主要管理员角色。此角色用于使用项信息(例如电子邮件以及与 RPA 数据库的连接) 配置环境。

Hub 利用基于角色的访问控制 (RBAC)，确保用户只能访问在组织内执行其角色所需的功能。

通过 Hub 的顶部导航栏可访问系统设置。可用设置取决于用户角色。如果用户未在帐户上启用管理员功能，则无法使用一些设置，详见下文。


顶部导航栏的功能包括：



当左侧导航菜单展开(如上所示)时，系统将显示这些功能：

- A. **基本信息图标**—由用户在其**基本信息**中定义。如果您是：
  - 用户，该图标提供指向您的**基本信息**页面的链接。
  - 管理员，该图标提供指向系统**设置**的链接，从中可以控制以下事项：
    - 个人基本信息和审计。
    - 平台管理。
    - 用户管理。
- B. **用户信息**—当导航菜单已折叠时，此信息会隐藏。
- C. **页面标题**—您当前使用的 Hub 用户界面区域。
- D. **环境**—当前选定的环境。环境在**环境管理器**中设置，并可在此处选择。
- E. **通知警报**—通知由 **Automation Lifecycle Management** 插件创建。当您点击警报时，系统仅显示您有权查看或适合您的通知。
- F. **切换菜单**—打开和关闭菜单。当菜单打开时，将显示菜单项的名称。当菜单关闭时，将显示每个菜单项的图标。
- G. **插件**—打开“插件”页面，您可以在其中查看和下载可用的插件。

- H. **帮助**—打开在线帮助。右键点击并选择**在新选项卡中打开链接**以在单独的浏览器选项卡中打开。
- I. **注销**—将您从 Authentication Server 中注销。

 如果您使用 Interact, 您也将从 Interact Web 应用程序中注销。


## Hub 限制

下表列出了使用 Hub 时应遵守的限制。

项	限制	相关部分
用户名	本机用户的用户名长度不能超过 25 个字符。用户名中只能包含拉丁字符(特殊字符除外)、数字、句点、连字符和下划线, 不能以句点、连字符和下划线开头。 Active Directory 用户(其 UPN)的用户名长度不能超过 255 个字符。	<a href="#">用户在本页 24</a>
密码限制	密码必须: <ul style="list-style-type: none"> <li>至少包含 1 个大写字母</li> <li>至少包含 1 个数字</li> <li>至少包含 1 个特殊字符</li> <li>长度至少为 8 个字符</li> <li>不同于最近使用的五个密码</li> <li>不超过 32 个字符</li> </ul>	<a href="#">个人资料在本页 9</a> 和 <a href="#">用户在本页 24</a>
个人资料图像	小于 1MB 且不大于 1920 x 1080 像素	<a href="#">个人资料在本页 9</a>
仪表盘小组件	每个仪表盘仅限 20 个小组件	仪表盘—请参 阅 <a href="#">Hub 用户指南</a> 。
品牌徽标	PNG、JPEG 或 JPG 不大于 30KB	<a href="#">自定义在本页 19</a>

## 设置


通过“设置”页面，您可以管理 Hub。仅在您是管理员时才能访问“设置”页面。如果您是用户，您将只能访问“个人资料”页面，当您点击个人资料图标时可打开该页面。

 要打开“设置”页面，请点击个人资料图标。如果您是管理员，则会显示“设置”页面。如果您是用户，则会显示“个人资料”页面。

## 概述

个人资料	通过“个人资料”页面，您可以更改您的信息、显示首选项和密码。 有关详情，请参阅 <a href="#">个人资料 在本页 9</a> 。
Audit	管理员可以查看已审核的系统活动的历史记录。 有关详情，请参阅 <a href="#">Audit 在本页 10</a> 。

## 平台管理

 在 Hub 安装和配置过程中可定义电子邮件和数据库设置，详情请参阅 [Hub 安装指南](#)。这些对于正常操作是必不可少的。

环境管理	管理员可以向 Blue Prism RPA 数据库添加连接、管理现有连接和删除冗余的 RPA 数据库。 有关详情，请参阅 <a href="#">环境管理 在本页 13</a> 。
电子邮件配置	管理员可以更改 SMTP 主机详细信息。您应该与您自己的 IT 支持团队一起进行更改，确保配置和凭据与组织的电子邮件服务器相匹配。 有关详情，请参阅 <a href="#">电子邮件配置 在本页 16</a> 。
自定义	管理员可以自定义 Interact 用户界面使用的主题。通过主题，管理员可以设置主题名称、品牌颜色和品牌徽标。 有关详情，请参阅 <a href="#">自定义 在本页 19</a> 。
插件管理	管理员可以查看当前安装的插件说明和版本号。任何更新或其他可用插件也会显示。 有关详情，请参阅 <a href="#">插件管理 在本页 21</a> 。

## 用户管理

用户	管理员可以添加、修改或停用用户，并分配他们的访问权限和角色。 有关详情，请参阅 <a href="#">用户 在本页 24</a> 。
角色和权限	管理员可以添加、编辑和删除角色。 有关详情，请参阅 <a href="#">角色和权限 在本页 32</a> 。
注册	管理员可以管理新用户为访问 Interact 而提出的注册请求。 有关详情，请参阅 <a href="#">注册 在本页 38</a> 。
身份验证设置	管理员可以添加、编辑、停用或删除身份验证设置。 有关详情，请参阅 <a href="#">身份验证设置 在本页 39</a> 。

**服务帐户**

管理员可以添加、编辑或删除服务帐户。  
有关详情, 请参阅 [服务帐户](#) 在本页 50。



## 个人资料

通过基本信息设置，您可以更改您的信息和 Hub 视图首选项。您可以更改的基本信息设置取决于为您的帐户配置的身份验证类型。如果您是本地管理员，您可以更改：

- 您的密码。
- 您的个人资料名字和姓氏。
- 您的电子邮件地址。
- 您的个人资料图片—显示在个人资料图标中。此图像将仅用于 Hub。
- 您的 Hub 显示主题—深色或浅色。

如果您的 Hub 帐户配置为使用 Active Directory 身份验证，则您只能更改您的基本信息图片和 Hub 显示主题。所有其他设置均在 Active Directory 中管理，并在您登录 Hub 时更新或您的帐户由手动同步时更新。


 无论您的身份验证类型如何，您都无法更改用户名。

有关身份验证类型的更多信息，请参阅[身份验证设置](#)。

 要打开“基本信息”页面；请点击您的基本信息图标以打开“设置”页面，然后点击**基本信息**。

## 更改您的个人资料

1. 在“个人资料”页面上，点击**编辑**。  
**编辑**按钮变为**取消**按钮，并且这些字段变为可编辑状态，即表示“个人资料”页面变为可编辑状态。
2. 根据需要更新以下内容：
  - 更新您的名字、姓氏或电子邮件地址。
  - 打开或关闭**深色主题**。默认情况下，Hub 以浅色主题显示。
  - 点击**上传**以选择您的个人资料图像。图像将在 Prism 图标中显示。图像大小不得超过 1 MB。
3. 点击**保存**以保存更改。如果您不想保存更改，请点击**取消**。

 **保存**按钮只有在更改主题设置后才会变为活动状态。

## 更改密码

1. 在“个人资料”页面上，点击**更新密码**。  
此时会显示“更新您的密码”对话框。
2. 输入当前密码。
3. 输入并重复新密码。
4. 点击**更新**。  
您的密码已更改。

## Audit

Audit 能让您查看已审核的系统活动。此区域仅在您是管理员时才可用。

要打开 Audit 页面，请点击您的基本信息图标以打开“设置”页面，然后点击 **Audit**。

ID	Category	Event	Audited By	IP address	Created On	Actions
b884e3ec-0cd0-423a-93b3-8780c0751503	User management	User login	admin		13/01/2022 10:21:05	
ddb623a5-fbe1-47bd-a11f-5560e9e60f0a	User management	User login	admin		13/01/2022 09:35:26	
a8b12576-59aa-492e-96b8-786ddf24e9dd	Business process	Created business process	admin2		13/01/2022 09:22:59	
e95f5873-ab4e-4450-8b96-b0abd24d9f44	User management	User login	admin2		13/01/2022 09:20:42	
edca5e58-bab2-42ac-903d-36d3d6e37b71	User management	User logout	admin		13/01/2022 09:20:30	

Audit 页面为您提供以下信息和功能：

- 编辑视图**—定义显示的列。然后，您可以使用切换开关显示或隐藏列。
- 筛选器**—筛选显示的信息。然后，您可以打开所需的筛选器并输入或选择相应的显示信息，例如，您可以打开**类别**筛选器并选择**用户管理**。
- 保存视图**—保存当前列设置。您可以输入视图的名称，以便在加载视图时轻松识别。
- 加载视图**—加载已保存的视图。您可以选择所需的视图，然后点击**应用**。
- 查看日志**—查看审核项目的**详细信息**。
- 每页行数**—输入数字，或使用向上箭头和向下箭头更改页面上的行数。
- 审计项目的**上一页和下一页**—点击**上一页**或**下一页**可浏览页面。

## 查看项目

- 在 Audit 页面上，选中要查看的项目对应的复选框。
- 点击**查看日志**。  
系统会显示事件的详细信息。

## 在 Audit 页面上使用筛选器

通过筛选器，您可以根据所选条件轻松查找审计事件。

- 在 Audit 页面上，点击**筛选器**，打开“筛选器”面板。
- 使用切换开关打开所需的筛选器，填写信息以查找审计事件。您可以同时应用多个筛选器。  
可用的筛选器如下：

筛选器	描述
审计 ID	输入审计标识符或部分标识符。
类别	<p>从下拉列表中选择一个类别。可用类别如下：</p> <ul style="list-style-type: none"> <li>• <b>用户管理</b>—包括与用户相关的事件，例如管理管理员用户和用户访问信息。</li> <li>• <b>SMTP 管理</b>—包括 SMTP 设置更改。</li> <li>• <b>角色管理</b>—包括与角色相关的事件。</li> <li>• <b>身份验证管理</b>—包括与身份验证设置相关的事件，例如管理连接和同步。</li> <li>• <b>服务帐户</b>—包括与服务帐户相关的事件，例如管理帐户和密钥重新生成。</li> <li>• <b>业务流程</b>—包括与业务流程相关的事件，例如创建、停用和激活业务流程。</li> </ul> <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p> 如果您选择一个类别，<b>事件</b>筛选器中的选项仅限于选定类别的选项。</p> </div> <p>如果您安装了以下插件，这些附加类别也可用：</p> <ul style="list-style-type: none"> <li>• <b>Automated Lifecycle Management (ALM):</b> <ul style="list-style-type: none"> <li>• <b>流程定义</b>—包括与流程定义相关的事件，例如管理定义和签核工作流程。</li> </ul> </li> <li>• <b>Interact:</b> <ul style="list-style-type: none"> <li>• <b>Interact—表单</b>—包括与 Interact 表单插件相关的事件，例如管理表单以及增加主要版本号。</li> <li>• <b>Interact 提交</b>—包括与 Interact 相关的事件，例如最终用户提交表单和审批工作流程。</li> </ul> </li> </ul>
事件	<p>从下拉列表中选择一个事件。这将显示此特定审计事件的所有结果。</p> <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p> 如果您使用<b>类别</b>筛选器，下拉列表中所显示的事件仅限于该类别的事件。</p> </div> <div style="border: 1px solid #FFD700; padding: 5px; margin-top: 10px;"> <p> 如果您要查看选定类别的所有事件，请关闭<b>事件</b>筛选器，仅使用<b>类别</b>筛选器即可。</p> </div>
审核人	输入用户的用户名或帐户名称，或者部分名称。
IP 地址	输入公共 IP 地址或部分地址。
创建时间	<p>输入日期范围：</p> <ul style="list-style-type: none"> <li>• 在第一个字段中，选择最早日期。</li> <li>• 在第二个字段中，选择最新日期。</li> <li>• 如果需要，调整时间字段。默认情况下，较早日期包含时间 00:00:00，而较晚日期包含时间 23:59:59，因此包括全天。</li> </ul> <p>这将显示此时间范围内的所有审计事件。</p>

Audit 页面上的信息会立即得到筛选。



如果已经设置了筛选器,但想要再次查看未筛选的信息,请关闭所需的筛选器,或移除筛选器中的任何设置以将其留空。

3. 点击**关闭抽屉**以关闭“筛选器”面板。

## 环境管理

环境管理器会显示您已连接的数据库。此区域仅在您是管理员时才可用。

**Environment management**

Here you can see your configured database connections, and also add new ones.

**Connected environments**

**Hub** **A**

Database name: Hub  
Server name or IP address: 10.30.0.4

**RPA-BP-UKR** **B**


Database name: RPA-BP-UKR  
Server name or IP address: sqlserver.database.windows.net

**C** **D** **E**

**Add connection** **F**

“环境”页面为您提供以下信息和功能：

- A. Hub 数据库。
- B. 在初始安装过程中配置的 Blue Prism 数据库。
- C. 跨 Hub 刷新数字化员工和队列的详细信息。在添加或更改任何连接时，请刷新数据库。如果不刷新数据库，您将无法查看特定 Blue Prism 环境中的数字化员工或队列。
- D. 打开“编辑连接”页面，您可以在该页面中 [编辑数据库详细信息](#)。
- E. 删除数据库连接。有关详细信息，请参阅 [删除数据库连接](#)。
- F. 打开“添加连接”对话框，您可以在其中配置和 [添加新的 Blue Prism 数据库连接](#)。

 要打开环境管理器，请点击您的基本信息图标以打开“设置”页面，然后点击 **环境管理**。

## 添加 Blue Prism 数据库连接

1. 在“环境管理器”页面上，点击**添加连接**以添加其他 RPA 数据库连接。系统将显示“添加连接”页面。
2. 输入数据库连接配置参数。

完成所有字段之后，**添加连接**链接将可用。

**⚠ 您必须确保您的数据库密码不包含等号 (=) 或分号 (;)。这些字符不受支持，并且在尝试连接到数据库时将导致出现问题。**

3. 如果需要，在“API 配置”下的 URL 字段中输入 Blue Prism API 的 URL。如果要使用 Control Room 插件，必须提供此 URL。Control Room 插件与 Blue Prism 7.0 或更高版本兼容。
4. 点击**添加连接**以保存详细信息。环境管理器中创建并显示连接。
5. 在环境管理器中，点击新连接上的刷新图标。这样会使用数据库中存储的 Digital Workforce 和队列更新 Hub 中的信息。

## 编辑数据库详细信息

您只能编辑“API 配置”下的 URL 字段。所有其他字段均被禁用。

1. 在“环境管理”页面上，点击要更新的数据库连接上的**编辑**图标。系统将显示“编辑连接”页面。

2. 在 **API 配置** 部分下输入 **URL**。

 您必须输入包含协议的完整 URL, 例如 `http://` 或 `https://`。例如: `https://bpapi.yourdomain.com`

3. 点击“保存”。
4. 在“环境管理”页面上, 点击已更新的连接上的刷新图标。这样会使用数据库中存储的数字化员工和队列更新 Hub 中的信息。

## 删除数据库连接

仅当数据库没有依赖项时, 您才能删除该数据库上的连接。如果出现以下情况, 您将无法删除数据库:

- **Interact** 表单依赖 RPA 数据库中的队列, 例如, 将表单提交到队列。
- **ALM** 流程定义使用该 RPA 数据库中定义的对象。

您必须将表单或流程定义修改为指向替代数据库, 才能删除依赖项。

删除功能允许您删除任何意外添加且未使用的数据库, 例如, 在配置期间添加的错误的数据库信息。

删除 RPA 数据库:

1. 在“环境管理器”页面上, 点击数据库磁贴上的删除图标。  
如果没有依赖项, 系统会显示一条消息, 要求您确认删除。如果存在依赖项, 则 Hub 用户界面的右上角会显示一条错误消息。
2. 点击**是**以确认删除。


## 电子邮件配置

借助电子邮件设置，您可以更改 SMTP 的配置，并且配置电子邮件以接收相关通知，例如来自用户的密码重置请求。此区域仅在您是管理员时才可用。您应该与您自己的 IT 支持团队一起进行更改，确保配置和凭据与组织的电子邮件服务器相匹配。

您可以配置电子邮件设置，以使用以下任一身份验证方法：

- 用户名和密码
- Microsoft OAuth 2.0

每当您保存 SMTP 设置时，您都会收到一封测试电子邮件，旨在确保设置正确。如果您在保存更改后没有收到测试电子邮件，请检查详细信息并相应进行更新。

 要打开“电子邮件配置”页面，请点击您的基本信息图标以打开“设置”页面，然后点击**电子邮件配置**。

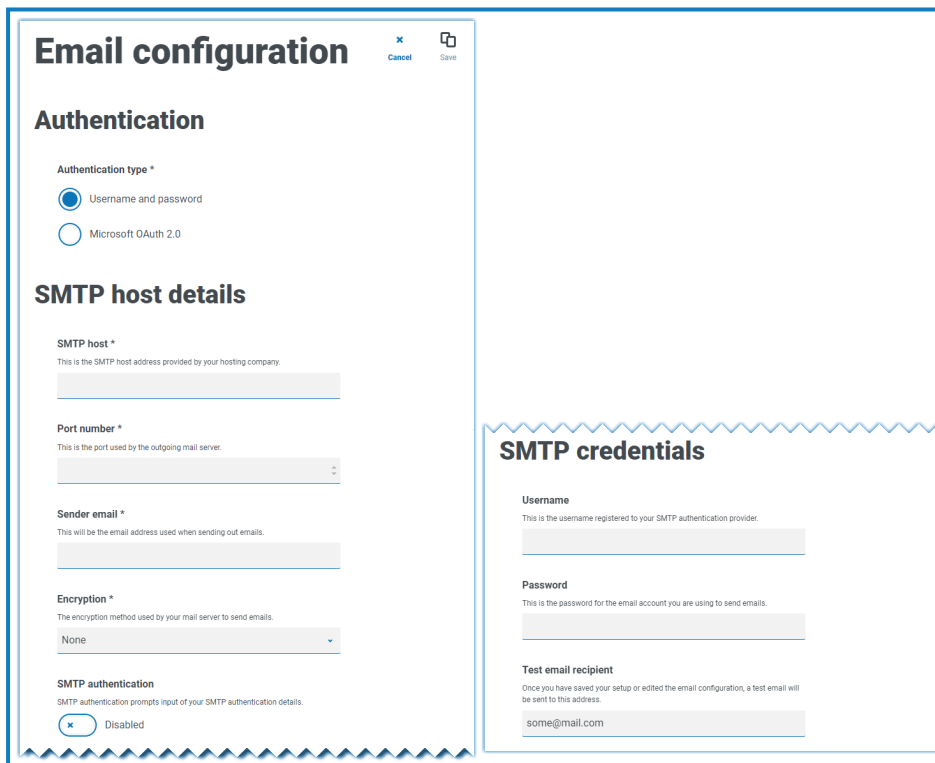
## 更新电子邮件设置

电子邮件设置作为 Hub 初始配置的一部分输入。仅当发生 IT 基础设施变更(如不同的 SMTP 主机)或者会影响这些设置的现有主机变更时，您才需要更改这些设置。

### 用户名和密码身份验证

1. 在“电子邮件配置”页面上，点击**编辑**。
2. 在“身份验证”部分的**身份验证类型**下面，选择**用户名和密码**。

“电子邮件配置”页面将刷新，显示相应的字段：



**Email configuration** Cancel Save

**Authentication**

Authentication type \*

Username and password

Microsoft OAuth 2.0

**SMTP host details**

SMTP host \*

This is the SMTP host address provided by your hosting company.

Port number \*

This is the port used by the outgoing mail server.

Sender email \*

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

Encryption \*

The encryption method used by your mail server to send emails.

None

SMTP authentication

SMTP authentication prompts input of your SMTP authentication details.

Disabled

**SMTP credentials**

Username

This is the username registered to your SMTP authentication provider.

Password

This is the password for the email account you are using to send emails.

Test email recipient

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

some@mail.com



### 3. 输入以下信息：

- **SMTP 主机**—SMTP 主机的地址。
- **端口号**—传出邮件服务器使用的端口号。
- **发件人电子邮件地址**—发送电子邮件时使用的电子邮件地址。电子邮件收件人会将其视为发件人地址。
- **加密**—电子邮件服务器用于发送电子邮件的加密方法。
- **SMTP 身份验证**—如果 SMTP 身份验证提示输入身份验证详细信息，请选择此选项。如果将其设置为已启用，则**用户名**和**密码**为必填字段。
- **用户名**—用于进行 SMTP 身份验证的用户名。
- **密码**—帐户的密码。
- **测试电子邮件收件人**—测试电子邮件将发送至此电子邮件地址。此地址默认为进行更改的用户的电子邮件地址，而且此默认设置无法更改。

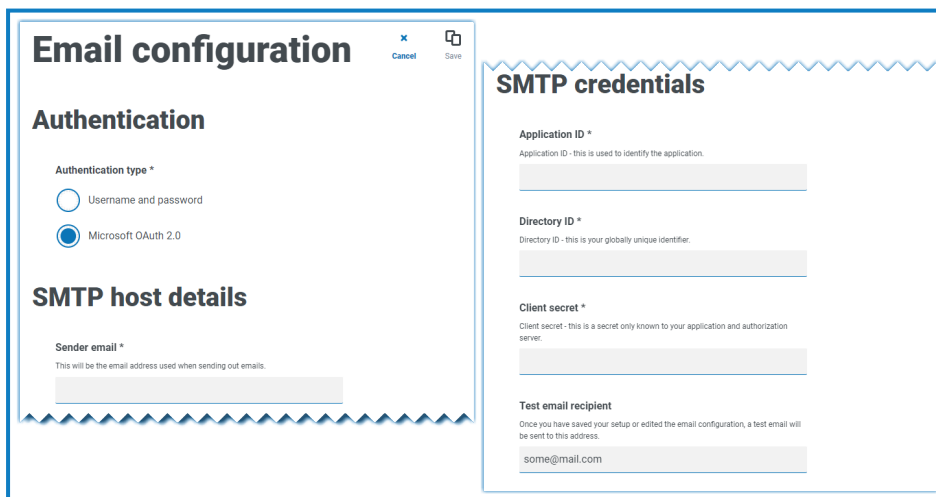
### 4. 点击**保存**以保存更改。

## Microsoft OAuth 2.0 身份验证

您可以使用 Azure Active Directory 提供的 Microsoft OAuth 2.0 身份验证服务连接到 SMTP 主机。您的 IT 支持团队需要在 Azure AD 中注册应用程序，并为您提供应用程序(客户端) ID、目录(租户) ID 和客户端密钥，以填写第 3 步中的信息。有关在 Azure AD 中查找这些详细信息的信息，请参阅 [Microsoft 文档](#)。

 如果您使用的是 Microsoft OAuth 2.0，则必须启用 Azure Active Directory 中的 Mail.Send 权限。这必须由您的 IT 支持团队在 Azure Active Directory 中配置。有关更多信息，请参阅 [Blue Prism Hub 安装指南中的 Hub 安装故障排除](#)。

1. 在“电子邮件配置”页面上，点击**编辑**。
2. 在“身份验证”部分的**身份验证类型**下面，选择 **Microsoft OAuth 2.0**。  
“电子邮件配置”页面将刷新，显示相应的字段：



The screenshot shows the 'Email configuration' dialog box with two main sections: 'Authentication' and 'SMTP host details'. The 'Authentication' section has two radio buttons: 'Username and password' (unselected) and 'Microsoft OAuth 2.0' (selected). The 'SMTP host details' section has a text input field for 'Sender email \*'. The 'SMTP credentials' section is expanded and contains four text input fields: 'Application ID \*', 'Directory ID \*', 'Client secret \*', and 'Test email recipient'. The 'Test email recipient' field contains the text 'some@mail.com'.

### 3. 输入以下信息：

- **发件人电子邮件地址**—发送电子邮件时使用的电子邮件地址。电子邮件收件人会将其视为发件人地址。
- **应用程序 ID**—此信息是 Azure AD 中定义的应用程序(客户端) ID, 由您的 IT 支持团队提供。
- **用户 ID**—此信息是 Azure AD 中定义的目录(租户) ID, 由您的 IT 支持团队提供。
- **客户端密钥**—这是 Azure AD 生成的客户端密钥, 由您的 IT 支持团队提供, 用于控制身份验证流程
- **测试电子邮件收件人**—测试电子邮件将发送至此电子邮件地址。此地址默认为进行更改的用户的电子邮件地址, 而且此默认设置无法更改。


### 4. 点击**保存**以保存更改。

## 自定义

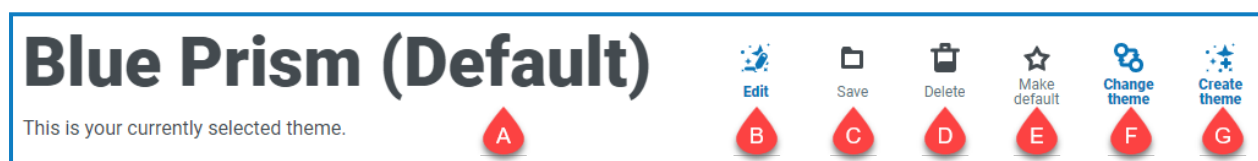
通过自定义设置，您可以更改 Interact 用户界面的外观。此区域仅在您是管理员时才可用。您可以创建控制以下内容的主题：

- **主题名称**—这也是将在用户界面上显示的品牌名称。
- **品牌颜色**—这是用户界面中的按钮和标签将使用的颜色。
- **品牌徽标**—这是将用作用户界面上的徽标的图像。

您可以根据用户情况创建可应用的多个主题，根据登录者提供不同的外观和风格。创建用户时会自动选择默认主题，但可以更改。

 要打开“自定义”页面，请点击您的基本信息图标打开“设置”页面，然后点击**自定义**。


打开“自定义”页面时，默认主题会显示：




此页面为您提供以下信息和功能：

- A. 当前显示的主题名称。
- B. **编辑**—编辑当前显示的主题。
- C. **保存**—保存您所做的任何更改。此图标仅在您编辑主题时才处于活动状态。
- D. **删除**—删除当前显示的主题。此图标仅在您有多个主题时才处于活动状态。
- E. **设为默认**—将当前显示的主题设为系统默认主题。此图标仅在当前主题不是默认主题时才处于活动状态。
- F. **更改主题**—选择要在页面上显示的主题。
- G. **创建主题**—创建新主题。

## 编辑并保存主题

1. 在“自定义”页面上，点击**编辑主题**。  
**编辑主题**按钮变为**取消**按钮，并且**重置**按钮变为活动状态，即表示“主题”页面变为可编辑状态。
2. 如果需要，请更改**主题名称**。  
输入时，**创建主题**标题也会发生变化。
3. 如果需要，通过点击颜色条可以更改**基本颜色**。您可以：
  - 使用滑动条选择颜色。
  - 使用文本框输入值。您可以点击  图标，在不同类型 (RGB、HSL 或 Hex) 之间进行切换。
4. 如果需要，点击**上传**，将徽标更改为您选择的文件。
5. 点击**保存**以保存更改。如果您不想保存更改，请点击**取消**。

 **保存**按钮只有在更改主题设置后才会变为活动状态。


## 删除主题

1. 通过屏幕上显示的要删除的主题(请参阅 [更改主题](#) 向下), 点击**删除**。  
系统会显示一则消息, 要求您确认删除。
2. 点击**是**以删除主题。

## 设置新的默认主题


1. 通过屏幕上显示的要使用的主题(请参阅 [更改主题](#) 向下), 点击**设为默认**。  
(默认) 出现在主题名称旁边, 并出现确认更改的通知。主题更改将在 Interact 中显示。

## 更改主题

 通过**更改主题**图标, 可以更改您当前查看的主题。如果要更改主题本身, 则需要**编辑**主题。

1. 在“自定义”页面上, 点击**更改主题**。  
系统会显示可用主题列表。
2. 点击要查看的主题。  
系统会显示选定的主题。
3. 关闭列表以返回主要工具。

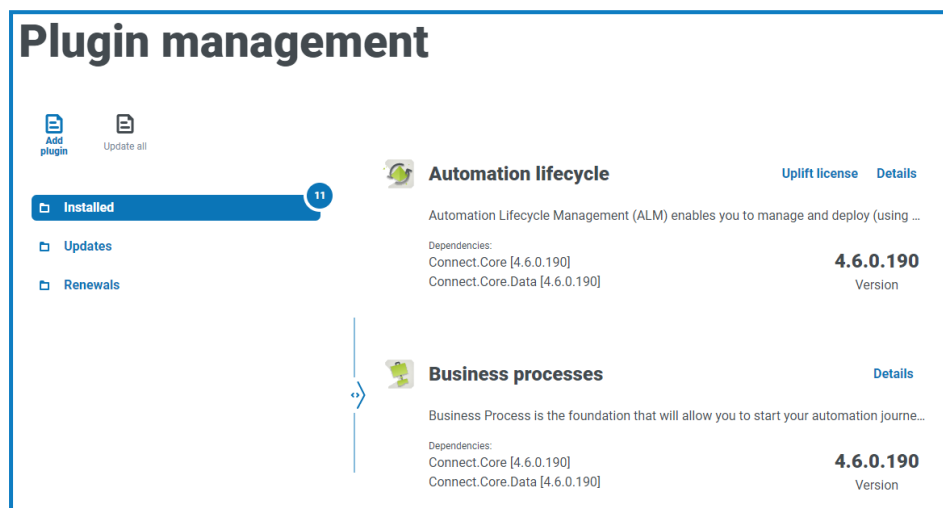
## 创建新主题

1. 在“自定义”页面上, 点击**创建主题**。  
系统会显示“创建主题”页面。
2. 输入**主题名称**。  
输入时, *创建主题*标题也会发生变化。
3. 点击**基本颜色**条以更改颜色。您可以:
  - 使用滑动条选择颜色。
  - 使用文本框输入值。您可以点击  图标, 在不同类型(RGB、HSL 或 Hex) 之间进行切换。
4. 点击**上传**, 将徽标更改为您选择的文件。
5. 点击**创建主题**以保存您的新主题。

## 插件管理

插件管理显示已安装插件的详细信息，其中一些插件默认在安装流程期间可用。您可以管理和更新现有插件，也可以添加新插件。此区域仅在您是管理员时才可用。

插件是 Hub 的核心，属于独立功能，可以单独安装和自定义，提供有关您的自动化流程的信息。有些插件还提供开发工具，帮助构建自动化。



要打开“插件管理”页面，请点击您的基本信息图标以打开“设置”页面，然后点击**插件管理**。

## 查看已安装的插件

打开“插件管理”后，当前已安装的插件将显示。插件名称、说明摘要和版本号将显示。查看：

- 有关插件的更多信息，请点击**详细信息**。
- 有关任何更新的信息，请点击**更新**。请注意，此功能目前不适用于 Hub 本地安装。
- 有关任何即将到来或挂起的许可证续订的信息，请点击**续订**。如果任何插件需要许可证续订，**续订**链接旁会显示一个数字，指明更新数量。如果未显示数字，则表示没有续订。

## 添加插件

安装插件后，网站将自动重新启动。因此，务必在工作时间之外或维护窗口期间安装插件。

- 在“插件管理”页面上，点击**添加插件**。  
系统会显示“打开”对话框，以便您查找本地文件。
- 导航到插件文件并将其选中，然后点击**打开**。  
插件文件会上传并安装。网站会自动重新启动以完成安装。

## 更新插件

有可用的更新时，**更新**链接旁会显示一个数字。

此功能仅适用于升级后立即进行 Hub 本地安装。本地版本无法在升级期间在线检查更新。

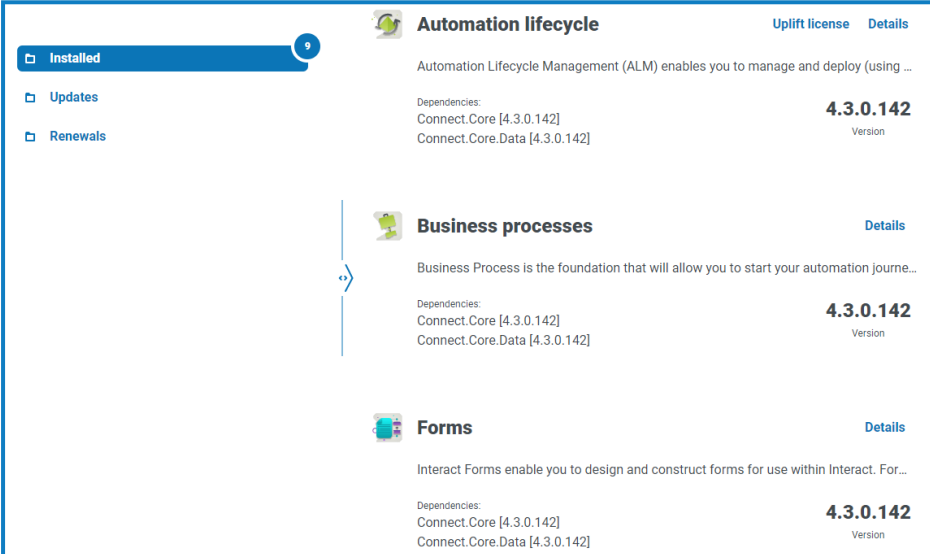
- 在“插件管理”页面上，点击**更新**。  
潜在更新将显示，展示新版本的详细信息。

2. 点击**全部更新**以更新所有插件。  
系统将显示一条消息，确认插件已更新。
3. 点击**确定**。  
站点重新启动。

## 提升许可证

仅当插件在已发布版本之间使用的许可模型存在更新时，**提升许可证**选项才可用。借助此选项，您可以在正常续订期外为插件加载新许可证。


1. 在“插件管理”页面上，点击**已安装**。  
系统将显示已安装的插件。



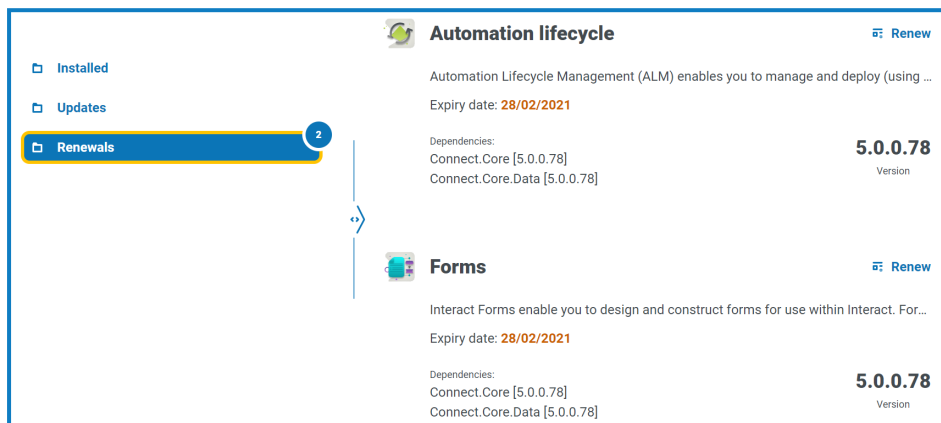
The screenshot displays the 'Automation lifecycle' section of the Blue Prism plugin management interface. It features a sidebar with 'Installed' (9), 'Updates', and 'Renewals'. The main content area lists three plugins: 'Automation lifecycle', 'Business processes', and 'Forms'. Each plugin entry includes a description, dependencies (Connect.Core [4.3.0.142] and Connect.Core.Data [4.3.0.142]), and a version number (4.3.0.142) with a 'Details' link. An 'Uplift license' link is visible at the top right of the 'Automation lifecycle' section.

2. 点击所需插件对应的**提升许可证**。在上述示例中，将显示“自动化生命周期”对应的该选项。  
“续订许可证密钥”面板显示。
3. 上传有效的许可证并点击**完成**以应用。

## 续订插件

 我们将在许可证到期前 **14** 天通知您。

1. 在“插件管理”页面上, 点击**续订**。  
系统将显示即将到期的插件。

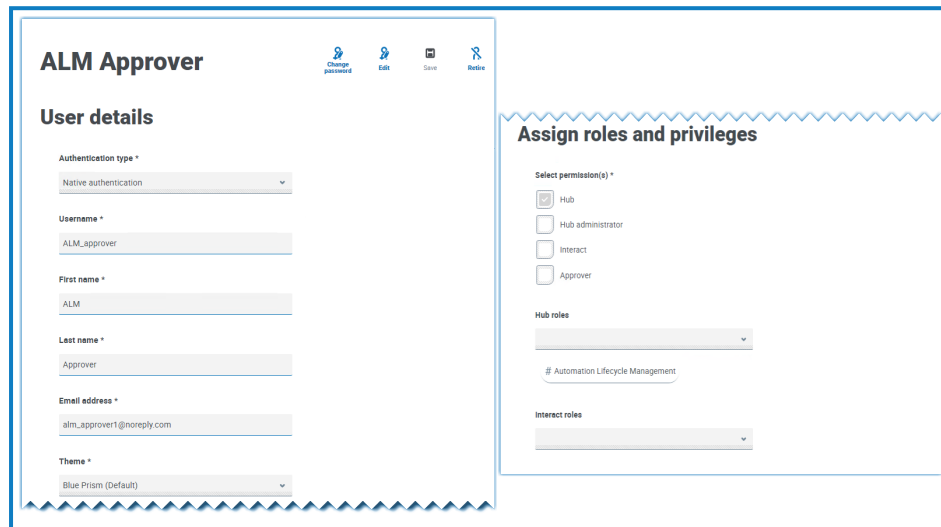


2. 点击所需插件旁边的**续订**。
3. 上传有效的许可证并点击**完成**以应用。

## 用户

通过用户设置，您可以根据身份验证类型在 Hub 中管理用户帐户。这可以是适用于本机用户的本机身份验证，也可以是适用于 Active Directory 用户的 Windows 身份验证。您还可以设置用户对 Hub 和 Interact 的访问权限及其在其中的角色。在配置用户之前，建议先配置好[用户角色](#)。

“用户”页面显示现有用户列表。您可以点击相应用户以查看其信息。如果您的环境中仅配置了本机身份验证，则“身份验证类型”字段会被隐藏。



要打开“用户”页面，请点击您的个人资料图标打开“设置”页面，然后点击用户。

## 查找用户

“用户”页面包含两种查找用户的方法：

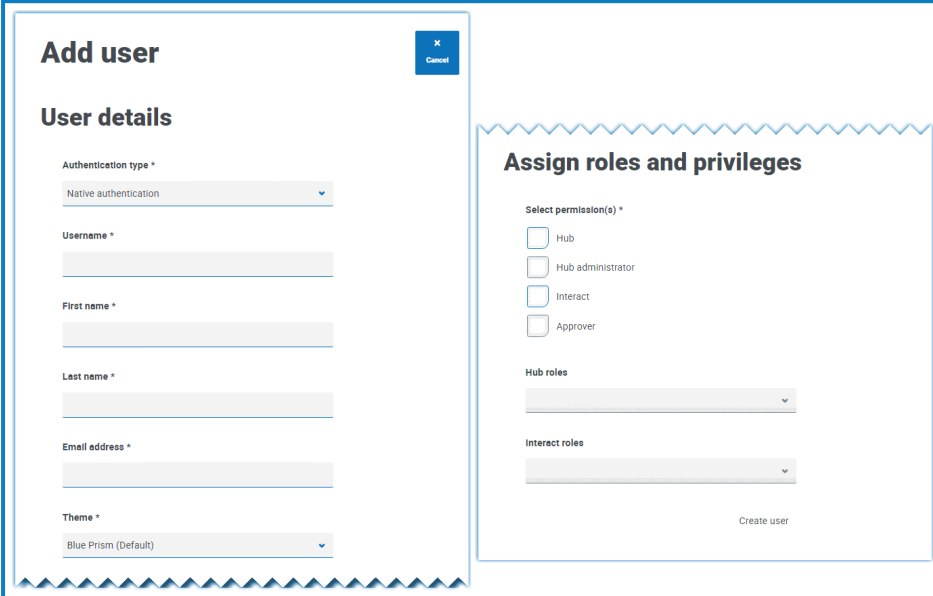
- **按用户名搜索**—这位于用户列表上方。开始输入用户名以筛选搜索结果，随着您输入更多字符，列表将进行动态筛选。
- **筛选器**—通过筛选器，您可以根据所选条件轻松查找特定用户或用户类型。点击**筛选器**可查看和使用筛选器。默认情况下，筛选器设置为仅显示“实时”用户，而不是已停用的用户。如果要查看所有用户，请关闭**实时**筛选器。有关更多信息，请参阅在[“用户”页面上使用筛选器](#)在[本页30](#)。



## 添加用户


### 添加本机用户

1. 在“用户”页面上，点击**添加用户**。  
此时会显示“添加用户”部分。



2. 输入用户的详细信息：

- **身份验证类型** (如果显示) —选择本机身份验证。

 仅当您的环境中同时配置了本机身份验证和 Windows 身份验证时，才会显示此字段。如果仅配置了本机身份验证，则添加的用户默认为本机用户。

- **用户名** —输入用户的用户名。
- **名字**—输入用户的名字。
- **姓氏**—输入用户的姓氏。
- **电子邮件地址**—输入用户的电子邮件地址。
- **主题**—自动选择默认主题。您可以为用户选择其他主题。有关主题的更多信息，请参阅[自定义 在本页 19](#)。

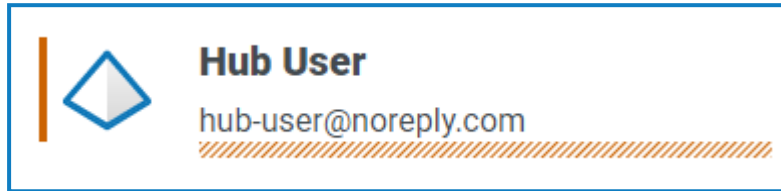
3. 为用户选择权限：

- **Hub**—为标准 Hub 用户和管理员选中此复选框。
- **Hub 管理员**—选中此复选框，向用户角色授予管理员权限。您必须选择 **Hub** 才能使用在此选项。
- **Interact**—选中此复选框，为用户分配 Interact 表单。有关详情，请参阅[Interact 用户指南](#)。
- **审批者**—选中此复选框，向用户角色授予 Interact 审批权限。您必须选择 **Interact**，才能使用此选项。

#### 4. 为用户选择角色：

- **Hub 角色**—选择用户所需的 Hub 角色。如果尚未创建所需角色，您可以在以后编辑用户以分配新角色。

如果用户是在没有 Hub 角色的情况下创建的，则用户列表中会用下划线标记此用户，显示用户设置尚未完成，例如：



用户将能够登录 Hub，但无法执行任何任务，因为他们无权访问任何插件。

- **Interact 角色**—选择用户所需的 Interact 角色。如果尚未创建所需角色，您可以在以后编辑用户以分配新角色。您可以选择多个角色。


 您也可以从[角色和权限](#)页面为角色添加用户。

#### 5. 点击**创建用户**。

此时会显示“创建密码”对话框。

#### 6. 选择其中一个密码选项：

- **向用户发送密码更新电子邮件**—这会向用户发送一封电子邮件，提示他们在使用链接登录时输入密码。
- **手动更新用户密码**—这使您能够为用户设置密码。

 密码必须遵守 Hub 内的限制。有关更多信息，请参阅[Hub 限制](#)在本页6。

#### 7. 点击**继续**

- 如果您选择向用户发送密码更新电子邮件，请在“确认”对话框中点击**完成**。
- 如果您选择为用户设置密码，请设置密码并点击**创建**。

新用户将显示在用户列表中。

## 添加 Active Directory 用户

要添加 Active Directory 用户，必须为您的环境配置 Windows 身份验证，并且必须在“身份验证设置”页面上启用 Active Directory 身份验证。有关更多信息，请参阅[身份验证设置](#)在本页 39。

您可以按照以下步骤添加 Active Directory 用户，或者将 Active Directory 安全组添加到角色中，在该角色中，属于安全角色成员的用户在首次登录时会自动添加到 Hub。有关更多信息，请参阅[将 Active Directory 安全组添加到角色](#)在本页 34。

1. 在“用户”页面上，点击**添加用户**。  
此时会显示“添加用户”部分。
2. 在**身份验证类型**字段中，选择 **Windows 身份验证**。
3. 点击**搜索 Active Directory**。

系统会打开“搜索 Active Directory”抽屉。




在 Active Directory 中搜索用户之前，请确保在 Active Directory 中为其填充用户名 (UPN) 和电子邮件地址。

4. 输入要添加的 Active Directory 用户的搜索根目录。这是根位置的可分辨名称，例如，`dc=bvdevops`、`dc=co`、`dc=uk`。

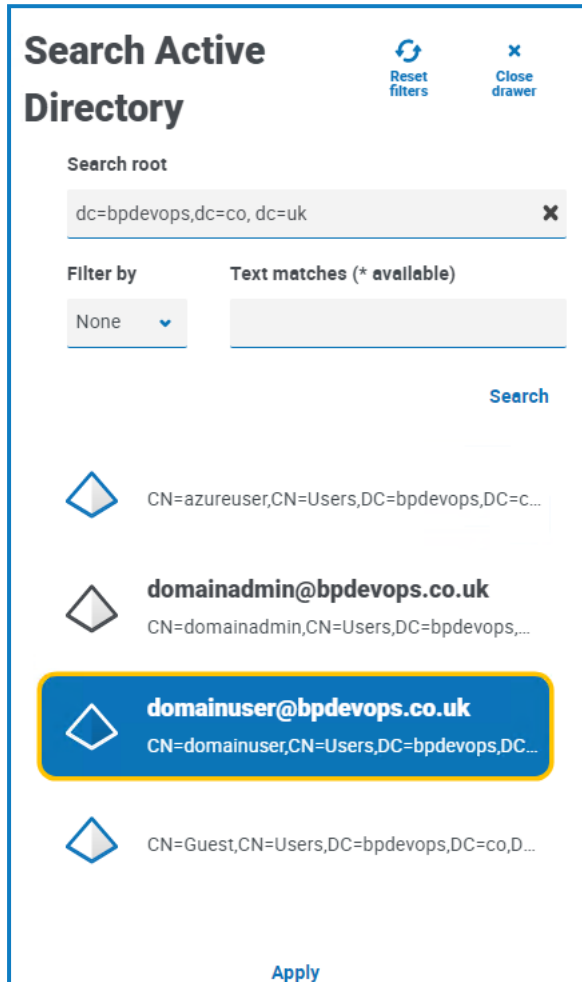
您还可以使用通配符搜索，并应用基于以下各项的搜索筛选器：

- **CN**—“通用名”属性包含对象名称。如果对象对应某个人，则此属性通常是该人的全名。
- **UPN**—用户主体名称是系统用户名称，使用电子邮件地址格式。UPN 由用户名(登录名)、分隔符(@符号)和域名(UPN 后缀)组成，例如 `john.doe@domain.com`。
- **SID**—安全标识符是用户、用户组或其他安全主体的不可变唯一标识符。安全主体在寿命期内(在给定域内)都具有一个 SID，而且主体的所有属性(包括其名称)均与 SID 关联。

5. 输入搜索条件后，点击**搜索**。

 在 Hub 中搜索 Active Directory 以查找用户或安全组时，将使用针对 Authentication Server 数据库中的域存储的凭据。如果未找到存储的凭据，则需要额外身份验证的查询将在 IIS 中运行 Authentication Server 应用程序池的 Windows 帐户上下文中执行。

将显示可用用户。您可以向下滚动查看所有检索到的用户。



**Search Active Directory**

Reset filters Close drawer

Search root

dc=bpdevops,dc=co, dc=uk

Filter by Text matches (\* available)

None


Search

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

Apply

6. 选择要添加的用户，然后点击**应用**。您一次只能选择一个用户。之前已添加的用户显示为灰色，无法选择。
7. 在“添加用户”页面上，选择新用户的权限和角色(请参阅“添加本机用户”部分中的**步骤 3 和 4**)，然后点击**创建用户**。

新用户将显示在用户列表中。


 Active Directory 用户的凭据在 Active Directory 中管理，因此您无需为用户创建密码。这些用户可以选择登录页面上的**使用 Active Directory 登录**选项，通过单点登录来登录 Hub。

## 编辑用户

1. 在“用户”页面上，选择所需用户并点击**编辑**。
2. 根据需要更改信息。

如果用户是：

- 本机用户，您可以根据需要更改信息。
- Active Directory 用户，您只能更改其角色和权限。所有其他详细信息均在 Active Directory 中管理。

 您无法更改他们的用户名。

3. 点击**保存**以应用更改。


## 同步 Active Directory 用户

1. 在“用户”页面上，选择所需的 Active Directory 用户。
2. 点击**同步用户**。

系统会刷新 Active Directory 用户的以下详细信息：UPN、用户名、完整名称、电子邮件地址和状态（活动、已删除或已禁用）。

## 停用本机用户

1. 在“用户”页面上，选择所需用户并点击**停用**。  
系统会显示一则消息，要求您确认。

 您可以使用**实时**筛选器来筛选用户列表中已停用的用户。请参阅[查找用户 在本页 24](#)。


2. 点击**是**。

用户会停用，**停用**图标会替换为**设为实时**图标。如果需要，您可以用它来恢复用户。用户列表中的此用户也带有下划线，表示用户已停用。

## 解锁本机用户

如果用户错误地输入了 5 次密码，他们将会被锁定在系统外 3 小时。或者，您可以为他们解锁帐户。

1. 在“用户”页面上，选择所需用户并点击**解锁**。  
系统会显示一条通知消息，确认用户已成功解锁。

 您可以使用**已锁定**筛选器来筛选用户列表中已锁定的用户。请参阅[查找用户 在本页 24](#)。

## 更改本机用户的密码

本机用户可以使用“基本信息”页面(更多信息请参阅[个人资料 在本页 9](#))更改自己的密码。如果用户忘记了密码，则可以使用登录页面上的**忘记密码**链接。但是，如果需要，您可以更改其密码。例如，如果用户是 Interact 审批者且他们已离开您的组织，而且 Interact 中有待他们批准的未完成表单，则您可能需要更改密码。根据您的组织的政策，您可以访问他们的帐户并处理这些表单。

1. 在“用户”页面上，选择所需用户并点击**更改密码**。  
系统会显示“更改密码”屏幕。
2. 在这两个字段中输入该用户的新密码。密码必须符合字符限制，但是，有关密码重复使用的限制不适用。有关更多信息，请参阅 [Hub 限制 在本页 6](#)。
3. 点击**提交**。  
系统会显示一条通知消息，确认用户密码已更改。

## 在“用户”页面上使用筛选器

通过筛选器，您可以根据所选条件轻松查找特定用户或用户类型。

1. 在“用户”页面上，点击**筛选器**，打开“筛选器”面板。
2. 使用切换开关打开所需的筛选器，填写信息以查找用户。您可以同时应用多个筛选器。  
可用的筛选器如下：

筛选器	描述
完整名称	输入用户的全名或其全名的一部分。
电子邮件地址	输入用户的电子邮件地址或其电子邮件地址的一部分。
已锁定	<p>从下拉列表中选择用户的锁定状态；选项如下：</p> <ul style="list-style-type: none"> <li>• <b>已锁定</b>—显示已锁定帐户的所有用户。</li> <li>• <b>已解锁</b>—显示已解锁帐户的所有用户。</li> </ul>
投入使用	<p>从下拉列表中选择用户的实时状态；选项如下：</p> <ul style="list-style-type: none"> <li>• <b>实时</b>—显示具有活动登录凭据的所有用户。</li> <li>• <b>已停用</b>—显示已由管理员停用且无法再登录的所有用户。</li> </ul> <p> 默认情况下，<b>实时</b>筛选器已打开。如果您要查看所有用户，可以关闭此筛选器。</p>
设置状态	<p>从下拉列表中选择用户的设置状态；选项如下：</p> <ul style="list-style-type: none"> <li>• <b>设置正确</b>—显示 Hub 内所有设置正确的用户，即他们已完成用户凭据和分配的角色。</li> <li>• <b>需要执行操作</b>—显示未正确配置用户帐户的所有用户，例如，他们可能缺少角色。</li> </ul>
域	<p>输入域的全名或部分名称。此处与“<a href="#">身份验证设置</a>”页面中指定的域名匹配，并显示从匹配域导入 Hub 的所有用户。</p> <p> 如果您输入了部分域名，则显示所有部分匹配的结果。可能有来自其他域的用户以及您预期的用户。</p>
连接名称	<p>输入连接的全名或部分名称。此处与“<a href="#">身份验证设置</a>”页面中指定的连接名称匹配，并显示使用匹配连接导入 Hub 的所有用户。</p> <p> 如果您输入了部分连接名称，则显示所有部分匹配的结果。可能有来自其他连接的用户以及您预期的用户。</p>

筛选器	描述
访问	从下拉列表中选择用户的访问权限级别。这些选项基于为用户提供的权限级别;选项如下: <ul style="list-style-type: none"><li>• <b>Hub</b>—Hub 的访问权限。</li><li>• <b>Interact</b>—Interact 的访问权限。</li><li>• <b>审批者</b>—具有审批者权限的 Interact 的访问权限。</li></ul>
Hub 角色	输入角色的全名或部分角色名称。这会搜索将 Hub 设置为角色类型的所有角色。
Interact 角色	输入角色名称或角色名称的一部分。这会搜索将 Interact 设置为角色类型的任何角色。
主题	从下拉列表中选择主题。这样会显示具有所选主题的用户。

“用户”页面上的信息会立即得到筛选。



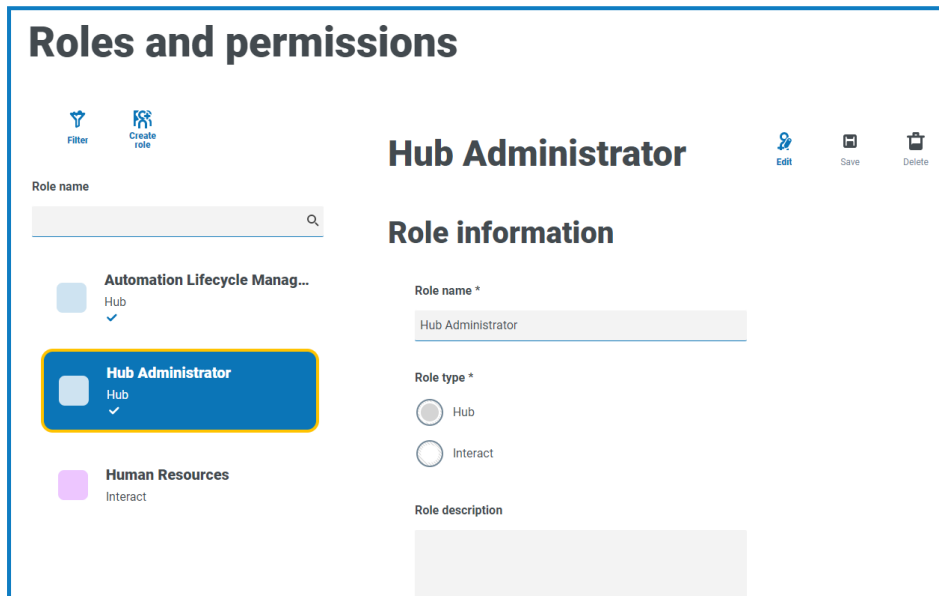
如果已经设置了筛选器,但想要再次查看未筛选的信息,请关闭所需的筛选器,或移除筛选器中的任何设置以将其留空。


3. 点击**关闭抽屉**以关闭“筛选器”面板。

## 角色和权限

通过角色和权限，您可以创建角色，并为这些角色分配 Hub 或 Interact 特定区域的权限。此区域仅在您是管理员时才可用。在配置用户之前，建议先配置好[用户角色](#)。如果未配置角色，用户将能够登录，但如果没有分配角色，显示给用户的内容会受限，并且用户无法访问特性或功能。

“角色和权限”页面会显示现有角色列表。在 Hub 安装过程中会自动创建预定义角色。这些角色以蓝色勾号表示，例如，Hub 管理员角色。这些自动创建的预定义角色已锁定，无法更改或删除，但您可以为这些角色添加用户。您可以点击相应角色以查看权限。



 要打开“角色和权限”页面，请点击您的基本信息图标以打开“设置”页面，然后点击[角色和权限](#)。

## 查找角色

“角色和权限”页面包含两种查找角色的方法：

- **按角色名称搜索**—这位于角色列表上方。开始输入角色名称以筛选搜索结果，随着您输入更多字符，列表将进行动态筛选。
- **筛选器**—通过筛选器，您可以根据所选条件轻松查找具有特定权限的一个或多个角色。点击**筛选器**可查看和使用筛选器。有关更多信息，请参阅在[“角色和权限”页面上使用筛选器](#)在本页 37。



## 添加角色

根据在身份验证设置页面上为您的环境配置的身份验证类型和设置，有几种方法可以将用户添加到您正在创建的角色：

- 如果启用了本机身份验证，您可以直接将本机用户添加到角色。
- 如果启用了 Active Directory 身份验证，您可以：
  - 将 Active Directory 用户直接添加到角色—必须在“身份验证设置”页面上启用允许将 Active Directory 用户直接添加到角色。
  - 将 Active Directory 安全组添加到角色—必须在“身份验证设置”页面上启用允许通过 Active Directory 安全组成员资格进行授权。

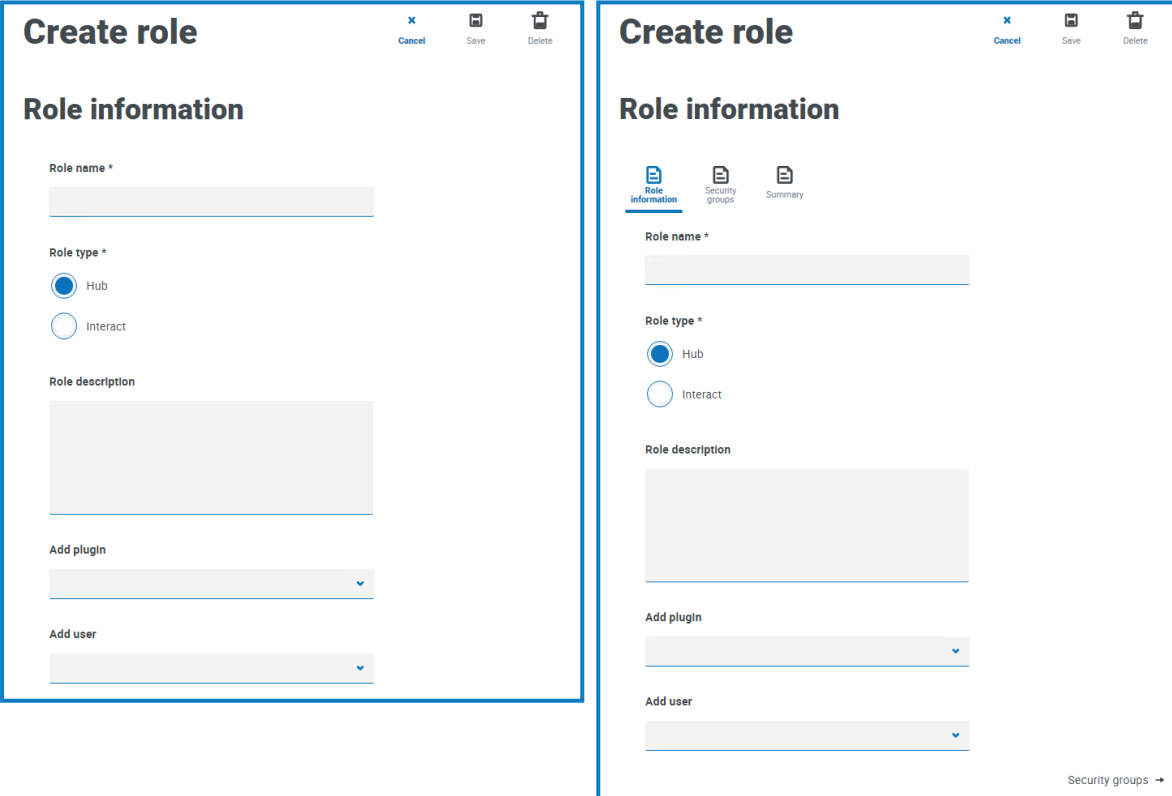
 如果您结合使用 Interact 与 Active Directory，请注意 Interact Web API 服务中的某些操作不支持使用安全组。所有操作都支持直接分配给 Interact 角色的 Active Directory 用户。有关更多信息，请参阅 [Interact Web API 服务用户指南](#)。

## 将用户直接添加到角色

1. 在“角色和权限”页面上，点击**创建角色**。

此时会显示“创建角色”部分。如果环境配置为允许将 Active Directory 安全组添加到角色，则此页面将显示三个选项卡：“角色信息”、“安全组”和“摘要”。

不能将 AD 安全组添加到角色的示例页面：允许将 AD 安全组添加到角色的示例页面：



The image shows two side-by-side screenshots of the 'Create role' form. Both screenshots show the 'Role information' tab selected. The left screenshot shows the form with the following fields: 'Role name \*' (text input), 'Role type \*' (radio buttons for 'Hub' and 'Interact'), 'Role description' (text area), 'Add plugin' (dropdown menu), and 'Add user' (dropdown menu). The right screenshot shows the same form but with three tabs at the top: 'Role information' (selected), 'Security groups', and 'Summary'. Additionally, there is a 'Security groups →' link at the bottom right of the right screenshot.

2. 输入角色名称，并选择它是应用于 **Hub** 还是 **Interact**。
3. 如果需要，请输入说明。

4. 选择您希望角色有权访问的项目。如果您已选择：
  - **Hub**, 请从**添加插件**下拉列表中选择所需插件。
  - **Interact**, 请从**添加表单**下拉列表中选择所需表单。


您可以从列表中选择多个项目。

5. 从**添加用户**下拉列表中选择将分配给此角色的用户。该列表仅显示具有相应权限的用户, 例如, 如果角色用于 **Interact**, 该列表将仅显示 **Interact** 用户, 而不是 **Hub** 用户。有关用户权限的更多信息, 请参阅[用户](#) 在本页 24。

 您还可以通过[用户](#)页面为角色添加用户。

6. 点击**保存**以创建角色。

## 将 Active Directory 安全组添加到角色

 如果您结合使用 **Interact** 与 **Active Directory**, 请注意 **Interact** Web API 服务中的某些操作不支持使用安全组。所有操作都支持直接分配给 **Interact** 角色的 **Active Directory** 用户。有关更多信息, 请参阅 [Interact Web API 服务用户指南](#)。

1. 在“角色和权限”页面上, 点击**创建角色**。  
此时会显示“创建角色”部分。
2. 在“角色信息”选项卡中, 输入角色名称, 并选择它是应用于 **Hub** 还是 **Interact**。
3. 如果需要, 请输入说明。
4. 选择您希望角色有权访问的项目。如果您已选择：
  - **Hub**, 请从**添加插件**下拉列表中选择所需插件。
  - **Interact**, 请从**添加表单**下拉列表中选择所需表单。您可以从列表中选择多个项目。
5. 点击**安全组**。

6. 通过输入根位置的可分辨名称来搜索安全组，例如 dc=bpdevops、dc=co、dc=uk。

The screenshot shows the 'DevOps - Forms' interface. At the top right, there are buttons for 'Cancel', 'Save', and 'Delete'. Below the title, there are three tabs: 'Role information', 'Security groups', and 'Summary'. The 'Security groups' tab is active. Underneath, there is a 'Search root' field containing 'dc=bpdevops,dc=co,dc=uk'. Below that is a 'Filter by' dropdown menu set to 'None' and a 'Filter value' input field. There are 'Reset filters' and 'Search' buttons. A 'Rows per page' dropdown is set to '10'. On the right side of the table, there are 'Previous' and 'Next' navigation arrows. The table has four columns: 'Name', 'Type', 'PATH', and 'Select group'. It lists three security groups: 'Access Control Assistance Operators', 'Account Operators', and 'Administrators'. At the bottom, there are navigation links for 'Role information' and 'Summary'.

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

您可以应用基于 CN(通用名)、UPN(用户主体名称)或 SID(安全标识符)的搜索筛选器，也可使用通配符搜索。有关更多信息，请参阅[添加 Active Directory 用户](#) 在本页 27。

您还可以向下滚动页面，点击下一个或上一个在多个安全组页面之间导航，或在“角色信息”和“摘要”选项卡之间移动。

7. 选择要添加到角色的组，然后点击**保存**。

添加的安全组显示为角色信息的一部分。作为已添加的安全组成员的所有用户都将自动添加到角色中，并在首次登录时在 Hub 中创建帐户。

## DevOps - Forms

### Role information

**Role name \***

**Role type \***

Hub

Interact

**Role description**

**Plugins**

# Forms

**Users**


# (domainuser@bpdevops.co.uk) domainuser domainuser

**Security groups**

# Administrators

## 编辑角色

1. 在“角色和权限”页面上，选择所需角色并点击**编辑**。
2. 根据需要更改信息，包括添加或删除用户和/或安全组。

 您无法更改角色类型。如果您要编辑显示蓝色勾号的角色，则只能修改分配给该角色的用户。

3. 点击**保存**以应用更改

## 删除角色


 您无法删除显示蓝色勾号的角色。这是在安装 Hub 或插件时自动创建的角色。

1. 在“角色和权限”页面上，选择所需角色并点击**删除**。  
系统会显示一则消息，要求您确认。
2. 点击**是**。  
该角色将被删除，并显示确认通知。


## 在“角色和权限”页面上使用筛选器

通过筛选器，您可以根据所选条件轻松查找特定角色。

1. 在“角色和权限”页面上，点击**筛选器**，打开“筛选器”面板。
2. 使用切换开关打开所需的筛选器，填写信息以查找所需角色。您可以同时应用多个筛选器。  
可用的筛选器如下：

筛选器	描述
类型	从下拉列表中选择所需角色类型。选项包括： <ul style="list-style-type: none"> <li>• <b>Hub</b>—显示将 Hub 设置为角色类型的角色。</li> <li>• <b>Interact</b>—显示将 Interact 设置为角色类型的角色。</li> </ul>
描述	输入根据“角色”描述中的文本要搜索的术语或单词。
Hub 插件	输入您要据此搜索的插件的名称或部分名称。例如： <ul style="list-style-type: none"> <li>• <b>自动化生命周期</b>—显示有权访问 ALM 的所有角色。</li> <li>• <b>表单</b>—显示有权访问 Interact 表单的所有角色。</li> <li>• <b>业务流程</b>—显示有权访问业务流程插件的所有角色。</li> <li>• <b>Control Room</b>—显示有权访问 Control Room 的所有角色。</li> </ul>
Interact 表单	输入您要据此搜索的 Interact 表单的名称或部分名称。
用户	输入用户的用户名或其部分用户名，查找与该用户关联的角色。 <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;">  如果您输入了部分用户名，则显示所有部分匹配的角色。这些角色可能适用于其他用户以及您预期的用户。           </div>

“角色和权限”页面上的信息会立即得到筛选。

 如果已经设置了筛选器，但想要再次查看未筛选的信息，请关闭所需的筛选器，或移除筛选器中的任何设置以将其留空。

3. 点击**关闭抽屉**以关闭“筛选器”面板。


## 注册

您可以在“注册”页面管理新用户为访问 **Interact** 而提出的注册请求。此区域仅在您是管理员时才可用。

用户可以通过以下“注册”页面请求 **Interact** 用户帐户：

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

“注册”页面会显示已提交的注册请求，您可以批准或拒绝这些注册请求。

 要打开“注册”页面，请点击您的个人资料图标以打开“设置”页面，然后点击**注册**。如果有未处理的请求，则会在“设置”页面上的“注册”选项旁边显示数值。

## 批准请求

在用户能够访问 **Interact** 中的任何表单之前，需要为其分配一个角色。您可以在审批过程中执行此操作(如下所示)，或者您可以批准请求，然后**编辑用户**。

1. 在“注册”页面上，选择相应用户并点击**编辑**。
2. 从下拉列表中选择所需角色。这是您可以编辑的唯一字段。
3. 点击**保存**。
4. 点击**批准**。

用户会从注册列表中删除，并会在**用户**页面上显示。用户会收到一封电子邮件，其中提供了通过输入密码完成注册的一次性使用链接，之后用户便可访问 **Interact**。

## 拒绝请求

1. 在“注册”页面上，选择相应用户并点击**拒绝**。  
访问请求将被拒绝，用户详细信息将从列表中删除。


## 使用“注册”页面上的筛选器。

通过筛选器，您可以根据所选条件轻松查找特定用户。

1. 在“注册”页面上，点击**筛选器**，打开“筛选器”面板。
2. 使用切换开关打开所需的筛选器，填写信息以查找用户。您可以同时应用多个筛选器。  
可用的筛选器如下：

筛选器	描述
完整名称	输入用户的全名或其全名的一部分。
电子邮件地址	输入用户的电子邮件地址或其电子邮件地址的一部分。
<b>Interact</b> 角色	输入角色名称或角色名称的一部分。这会搜索将 <b>Interact</b> 设置为角色类型的任何角色。

“注册”页面上的信息会立即得到筛选。

 如果已经设置了筛选器，但想要再次查看未筛选的信息，请关闭所需的筛选器，或移除筛选器中的任何设置以将其留空。


3. 点击**关闭抽屉**以关闭“筛选器”面板。

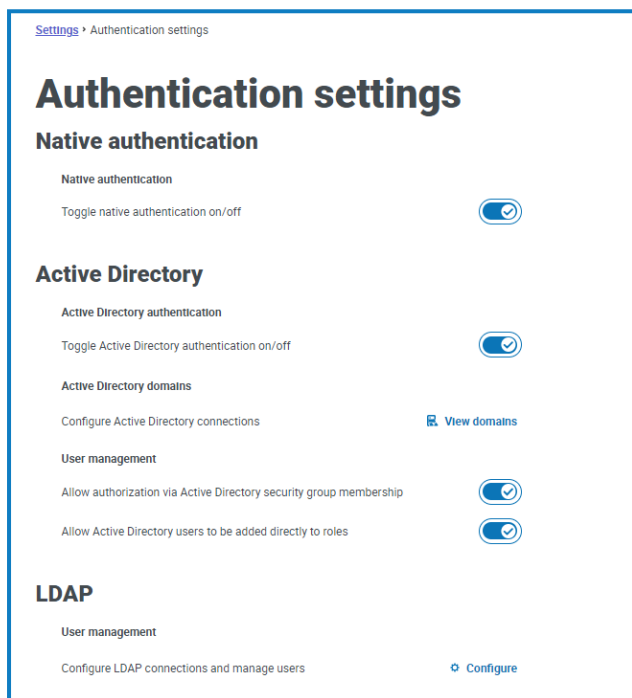
## 身份验证设置

您可以使用以下选项配置组织的身份验证设置：

- 本机身份验证
- Active Directory 身份验证
- LDAP

此区域仅在您是管理员时才可用。

 要打开“身份验证设置”页面，请点击您的基本信息图标以打开“设置”页面，然后点击**身份验证设置**。




### 本机身份验证

在新环境中或在升级 Hub 时，默认情况下会在“身份验证设置”页面上启用本机身份验证。

要启用或禁用本机身份验证：

1. 使用滑块切换至所需位置：
  - 叉号表示关闭
  - 勾号表示开启
2. 点击**确定**以接受确认消息。

 只有在系统中至少有一个 Hub 管理员可以使用其他身份验证方法之一登录时，才能禁用本机身份验证。

您可以在**添加用户**页面上添加本机用户，他们可以通过输入用户名和密码登录 Hub。


## Active Directory 身份验证

只有在托管 Authentication Server 的服务器是 Active Directory 域的成员时，才能在“身份验证设置”页面上启用 Active Directory 身份验证。

要启用或禁用 Active Directory 身份验证：

1. 使用滑块切换至所需位置：
  - 叉号表示关闭
  - 勾号表示开启
2. 点击**确定**以接受确认消息。

启用后，您可以在[添加用户](#)页面上添加 Active Directory 用户，他们可以使用**使用 Active Directory 登录**选项直接登录 Hub。


 这不适用于仍需要输入其凭据的 LDAP 用户。

## Active Directory 用户管理

如果在“身份验证设置”页面上启用了 Active Directory 身份验证，则必须通过在“身份验证设置”页面上启用以下至少一个选项来选择如何在 Hub 中管理 Active Directory 用户的访问权限：


- **允许通过 Active Directory 安全组成员进行授权**—允许将 Active Directory 安全组添加到 Hub 角色。用户可以通过成为与这些角色关联的任意 Active Directory 安全组的成员而被分配到多个 Hub 角色。
- **允许将 Active Directory 用户直接添加到角色**—允许将 Active Directory 用户直接分配到 Hub 角色。可以将用户分配到多个 Hub 角色。




有关如何为角色分配 Active Directory 用户和安全组的详细信息，请参阅[角色和权限](#)在本页 32。


 观看[此视频](#)，了解 Active Directory 与 Authentication Server 集成的概述。

## Active Directory 域

Active Directory 域页面允许您查看、添加、编辑和删除存储在 Authentication Server 数据库中的 Active Directory 域和相关凭据。此区域仅在您是管理员时才可用。

 要打开 Active Directory 域页面，请点击您的基本信息图标以打开“设置”页面，点击[身份验证设置](#)，然后点击[查看域](#)。

Active Directory domains		 <b>A</b>	 <b>B</b>	 <b>C</b>
Domain name	Domain DN	Add	Edit	Delete
bpdevs.co.uk	DC=bpdevs,DC=co,DC=uk	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
bpqas.co.uk	DC=bpqas,DC=co,DC=uk	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

 您只需为具有单向信任关系的多林环境添加新的 Active Directory 域。有关更多详细信息，请参阅[Active Directory 域](#)向上。



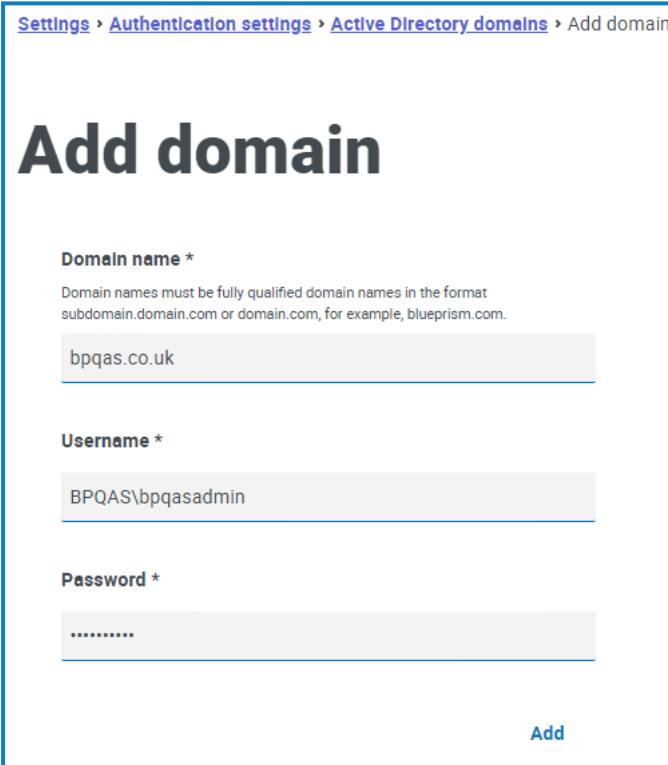
Active Directory 域页面为您提供以下信息和功能：

- A. **添加**—添加新的 Active Directory 域。
- B. **编辑**—编辑现有 Active Directory 域的详细信息。您一次只能编辑一个域。
- C. **删除**—删除一个或多个 Active Directory 域。

## 添加域

1. 在 Active Directory 域页面上，点击**添加**。  
随即显示“添加域”页面。
2. 输入域名。  
这必须是使用 subdomain.domain.com 或 domain.com 格式的完全限定域名 (FQDN)。
3. 输入域的用户名和密码。用户名的格式必须为 username@domain.co.uk 或 DOMAIN\username。必须事先向系统管理员请求凭据。

Active Directory 域凭据存储在数据库中，且在存储之前已加密。为每个域存储的凭据必须是 Active Directory 服务帐户的凭据。服务帐户密码不得过期，服务帐户不得是用户帐户，并且应遵循 [Active Directory 服务帐户最佳实践](#)。



Settings > Authentication settings > Active Directory domains > Add domain

## Add domain

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

bpqas.co.uk

**Username \***

BPQAS\bpqasadmin

**Password \***

.....

Add

4. 点击**添加**。  
域名和凭据将根据 Active Directory 域控制器进行验证，添加的域将显示在域列表中。

## 编辑域

1. 在 Active Directory 域页面上，选择一个域，然后点击**编辑**。  
您一次只能选择一个域。
2. 根据需要更改信息。如果要编辑域名，必须删除此域并创建新域。
3. 点击**保存**以应用更改。

## 删除域

1. 在 Active Directory 域上，选择所需的域，然后点击**删除**。  
系统会显示一则消息，要求您确认删除。
2. 点击**是**以删除选定域，或点击**否**以取消。

## 域之间的信任关系

对于多林环境，必须在域之间配置信任关系。对于应受信任的域，它们可以是双向的，也可以是单向的。

例如：

- 在域 A 和域 B 之间的单向信任中，域 A 中的用户可以访问域 B 中的资源。但是，域 B 中的用户无法访问域 A 中的资源。
- 在双向信任中，域 A 信任域 B，域 B 信任域 A。这意味着身份验证请求可以在两个域之间双向传递。


如果 Authentication Server 应用程序池用户具有对用户所属域的相关读取访问权限，则双向信任不需要用户提供域凭据。在这些示例中，托管 Authentication Server 的 Web 服务器将驻留在域 B 中。当用户需要使用与 Authentication Server 应用程序池用户不同的帐户查询受信任域时，双向信任需要提供凭据。单向信任需要创建具有凭据的域。

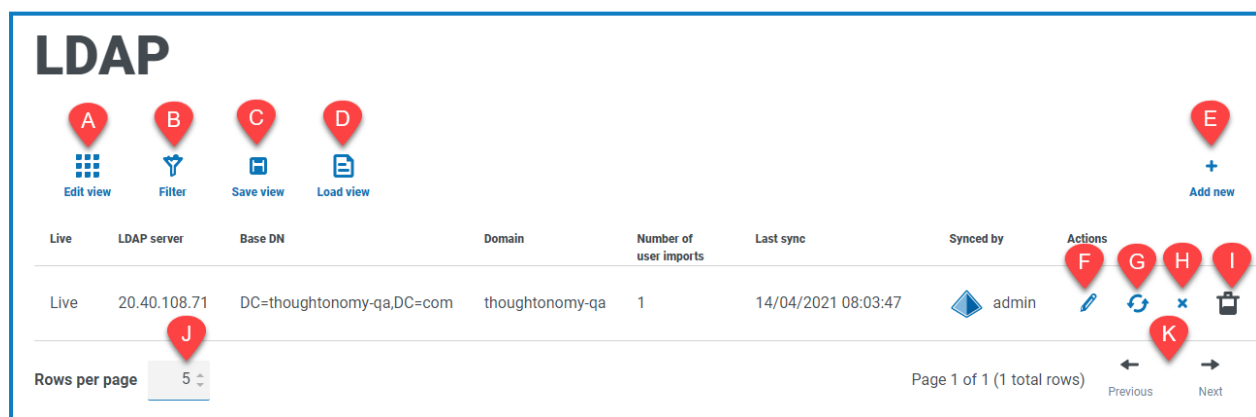
支持以下信任类型：

- 外部
- 父-子
- 树-根
- 林

## LDAP

通过 LDAP 页面，您可以配置轻型目录访问协议 (LDAP) 以连接到组织的 Active Directory 环境。此区域仅在您是管理员时才可用。

 要打开“LDAP”页面，请点击您的基本信息图标以打开“设置”页面，然后点击**身份验证设置**，再点击“LDAP”部分下的**配置**。




Live	LDAP server	Base DN	Domain	Number of user imports	Last sync	Synced by	Actions
Live	20.40.108.71	DC=thoughtonomy-qa,DC=com	thoughtonomy-qa	1	14/04/2021 08:03:47	admin	[Edit] [Refresh] [Delete] [Add new]

“LDAP”页面为您提供以下信息和功能：

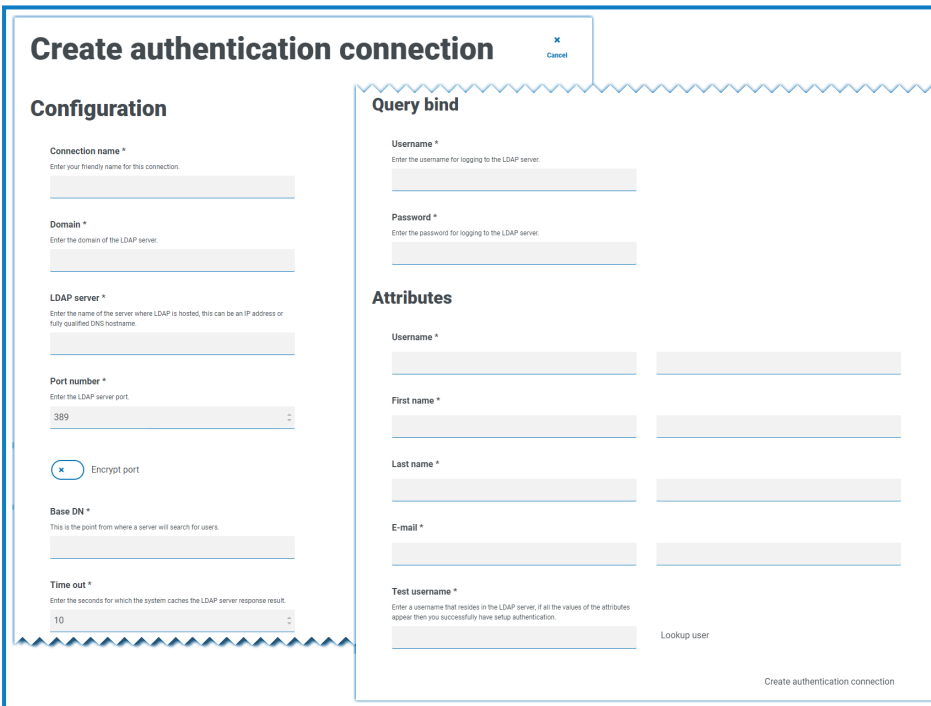
- A. **编辑视图**—定义显示的列。然后，您可以使用切换开关显示或隐藏列。
- B. **筛选器**—筛选显示的信息。然后，您可以打开所需的筛选器并输入或选择相应的显示信息，例如，您可以打开**域**过滤器并输入域名。

- C. **保存视图**—保存当前列设置。您可以输入视图的名称,以便在加载视图时轻松识别。
- D. **加载视图**—加载已保存的视图。您可以选择所需的视图,然后点击**应用**。
- E. **新增**—添加**新连接**。
- F. **编辑**—**编辑选定的连接**详细信息。
- G. **重新同步**—通过 Hub **重新同步用户**。如果将新用户添加到 Active Directory,您需要执行此操作。
- H. **停用/恢复**—使用勾号图标可激活已停用的连接,使用叉号可停用连接。有关详细信息,请参阅**停用和恢复应用程序**。
- I. **删除**—**删除选定的连接**。您只能删除已停用的连接。
- J. **每页行数**—输入数字,或使用向上箭头和向下箭头更改页面上的行数。
- K. **上一页和下一页**—点击**上一页**或**下一页**可浏览页面。

## 添加新连接

 如果将多个 LDAP 连接添加到包含相同用户(例如名称、电子邮件地址和域)的 Hub,这将创建重复用户,从而可能导致出现登录问题。在下述程序中同步用户时,请确保仅选择需要防止导入重复用户的用户。

1. 在“LDAP”页面上,点击**新增**。  
系统会显示“创建身份验证连接”页面。



**Create authentication connection** Cancel

**Configuration**

**Connection name \***  
Enter your friendly name for this connection.

**Domain \***  
Enter the domain of the LDAP server.

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

**Port number \***  
Enter the LDAP server port.  
389

Encrypt port

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

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

**Query bind**

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

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

**Attributes**

**Username \***

**First name \***

**Last name \***


**E-mail \***

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

Create authentication connection

## 2. 填写“配置”字段：

- **连接名称**—您希望使用的连接名称。
- **域**—您要连接的域名称，例如“bp”。

 请勿使用您的域的完全限定域名 (FQDN)。您必须使用短名称格式。

- **LDAP 服务器**—LDAP 服务器的主机名称，例如 blueprism-srv1.local。
- **端口号**—它所操作的端口号，默认为端口 389。
- **加密端口**—如果要加密端口，请选择此选项。如果您使用端口 636(LDAPS 端口)，则应启用此选项。
- **基本 DN**—系统开始在 Active Directory 内查找用户的起始点，例如 dc=blueprism, dc=local。

## 3. 填写“查询绑定”字段：

- **超时**—系统等待从 Active Directory 服务器获得响应的超时时间(以秒为单位)。
- **查询绑定用户名**—可以访问组织的 LDAP 系统的 Active Directory 用户。
- **查询绑定密码**—Active Directory 用户的密码。

## 4. 填写“属性”字段。此部分的目的是将 Active Directory 属性映射到 Hub 字段。这些字段中输入的文本必须与 Active Directory 中用户基本信息内的命名属性匹配。您可以使用 Active Directory 用户和计算机 (ADUC) 工具查找用户属性，方法是选择用户，然后点击**属性编辑器**选项卡以查看属性到值的映射。

- **用户名**—用户名的 Active Directory 属性名称，例如“SAMAccountName”。
- **名字**—用户名字的 Active Directory 属性名称，例如“givenname”。
- **姓氏**—用户姓氏的 Active Directory 属性名称，例如“sn”。
- **电子邮件**—用户电子邮件的 Active Directory 属性名称，例如“mail”。

5. 要测试一切设置是否正确，请在**测试用户名**字段中输入用户名，然后点击**查找用户**。在**测试用户名**字段中输入的文本必须与 Active Directory 属性的文本格式匹配。例如，如果用户名设置为：

- “SAMAccountName”，则测试数据可能采用 *domain\user* 格式。
- “name”，则测试数据可能采用 *user* 格式。

系统将检索关联的信息，然后将其填入相应的“属性”字段，例如：

**Create authentication connection**

**Configuration**

Connection name \*  
Enter your friendly name for this connection.  
AD Domain Connection

Domain \*  
Enter the domain of the LDAP server.  
mycompany.com

LDAP server \*  
Enter the name of the server where LDAP is hosted, this can be an IP address or fully qualified DNS hostname.  
10.10.108.10

Port number \*  
This is the port used by the LDAP server.  
389

Encrypt port

Base DN \*  
This is the point from where a server will search for users.  
DC=mycompany,DC=com

Time out \*  
Enter the seconds for which the system caches the LDAP server response result.  
30

**Query bind**

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

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

**Attributes**

Attribute Name	Value
SAMAccountName	fred.smith
First name *	Fred
Last name *	Smith
E-mail *	fred.smith@mycompany.com

Test username \*  
Enter a username that resides in the LDAP server. If all the values of the attributes above then you successfully have setup authentication.  
mycompany/fred.smith

Lookup user

Create authentication connection

6. 点击**创建身份验证连接**。

系统会显示一条通知消息，确认连接成功，并提示您导入用户。

7. 点击**是**，立即同步。或者，您也可以选择**否**，稍后通过 [同步 Active Directory 用户](#) 在本页 47 中的流程进行同步。

系统会显示一则消息，指示找到的用户数量。

**⚠ 导入大量 (例如, 数万) 用户时, 数据库 AuthenticationServerDB、HubDB 和 InteractDB 的数据库事务日志文件将增大。如果这三个数据库中任何一个的事务日志文件的大小受到限制, 要么文件大小上限太小, 要么文件大小不允许增大, 则导入可能会失败。因此, 建议您为数据库事务日志文件启用自动增长设置, 并将增长设置设为 1024 MB, 同时确保设置足够的大小上限以防止导入失败。有关自动增长的更多信息, 请参阅 [Microsoft 的文档](#)。**

8. 点击**继续**。

系统会显示用户列表。由于您需要为所需用户配置权限和角色，因此这些内容尚未导入 Hub。

9. 选择用户以导入并分配相应的 Hub 角色和/或任何 Interact 职责。

**🔑 如果您将用户配置为具有 Hub 管理员角色, 则他们将有权访问 Hub 的所有插件和功能 (包括创建新数据库与 LDAP 连接以及其他安全功能), 因此请务必谨慎分配此角色。**

10. 为所有必需用户重复此操作。

### 11. 点击保存访问权限和角色。

系统仅保存已定义其角色和权限的用户，并显示“用户”页面，其中会显示新用户。

#### 编辑连接

1. 在“LDAP”页面上，选择所需连接的**铅笔**图标。
2. 根据需要编辑信息。您无法更改域、LDAP 服务器、端口号或基本 DN。
3. 点击“保存”。

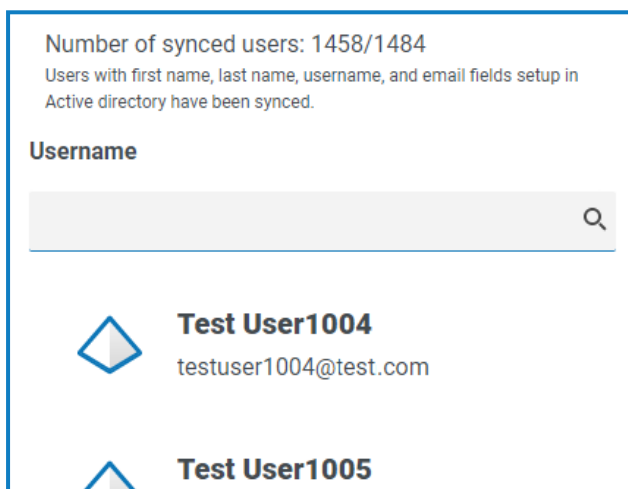
## 同步 Active Directory 用户

**⚠️** 导入大量(例如, 数万)用户时, 数据库 AuthenticationServerDB、HubDB 和 InteractDB 的数据库事务日志文件将增大。如果这三个数据库中任何一个的事务日志文件的大小受到限制, 要么文件大小上限太小, 要么文件大小不允许增大, 则导入可能会失败。因此, 建议您为数据库事务日志文件启用自动增长设置, 并将增长设置设为 1024 MB, 同时确保设置足够的大小上限以防止导入失败。有关自动增长的更多信息, 请参阅 [Microsoft 的文档](#)。

将其他用户添加到 Active Directory 时, 这些用户必须与 Hub 同步。

1. 在 LDAP 页面上, 在行中选择所需连接的**重新同步**图标。

用户列表上方会显示一则消息, 其中对比显示了已同步用户的数量(这些用户在 Active Directory 中拥有有效信息—名字、姓氏、用户名和电子邮件)与找到的用户总数。列表中仅显示已同步的用户。您需要为所需用户配置权限和角色。



**🔗** 有关为 Hub 提供名字、姓氏、用户名和电子邮件的 Active Directory 属性的更多信息, 请参阅 [添加新连接](#) 在本页 43。Hub 将仅同步在所有映射属性中具有信息的用户。

2. 选择要添加到 Hub 用户群的所需用户, 分配相应的 Hub 角色和/或任何 Interact 职责。
3. 为所有必需用户重复此操作。
4. 点击**保存访问权限和角色**。

系统仅保存已定义其角色和权限的用户, 并显示“[用户](#)”页面, 其中会显示新用户。

## 停用和恢复连接

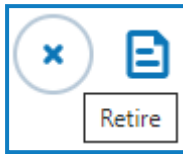
**🔗** 停用连接不会影响相关用户的状态—用户仍可登录并使用此应用程序。可以通过[删除连接](#)来停用与 LDAP 连接相关联的所有用户。

1. 在“LDAP”页面上, 选择所需连接的**停用/恢复**图标。

如果连接:

- 已启用, **停用/恢复**图标显示为叉号。
- 已停用, **停用/恢复**图标显示为勾号。

2. 要停用连接：
  - a. 点击叉号。

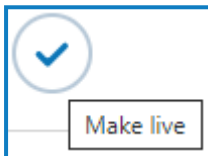


系统会显示一则消息，要求您确认。


- b. 点击**是**。

连接已停用，叉号变为勾号。

3. 要激活已停用的连接，请点击勾号。



连接将立即恢复，并且勾号会变为叉号。

 您可以使用**已启用筛选器**来筛选已停用的连接列表。

## 删除连接

您只能删除**已停用的连接**。

1. 在“LDAP”页面上，选择所需连接的**删除**(垃圾桶)图标。  
系统会显示一则消息，要求您确认。
2. 点击**是**。  
该连接将删除，与其关联的所有用户将停用。


## 在 LDAP 页面上使用筛选器

通过筛选器，您可以根据所选条件轻松查找特定连接或类似连接。


1. 在 LDAP 页面上，点击**筛选器**，打开“筛选器”面板。
2. 使用切换开关打开所需的筛选器，填写信息以查找所需连接。您可以同时应用多个筛选器。  
可用的筛选器如下：

筛选器	描述
投入使用	从以下选项中选择连接的状态： <ul style="list-style-type: none"> <li>• <b>实时</b>—显示活动连接；那些尚未停用的连接。</li> <li>• <b>已停用</b>—显示管理员已停用的连接。</li> </ul>
连接名称	输入连接的全名或部分名称。
LDAP 服务器	输入服务器的主机名称，或部分服务器主机名称。
基本 DN	输入要匹配的基本 DN 或部分基本 DN。
域	输入域的全名或部分名称。



筛选器	描述
用户导入数	输入数值范围： <ul style="list-style-type: none"><li>在第一个字段中，输入最小导入数。</li><li>在第二个字段中，输入最大导入数。</li></ul> 这将显示已导入该范围内用户的连接。
上次同步	输入日期范围： <ul style="list-style-type: none"><li>在第一个字段中，选择最早日期。</li><li>在第二个字段中，选择最新日期。</li><li>如果需要，调整时间字段。默认情况下，较早日期包含时间 00:00:00，而较晚日期包含时间 23:59:59，因此包括全天。</li></ul> 这将显示此时间范围内同步的连接。
同步者	输入用户的用户名或其用户名的一部分。  如果您输入了部分用户名，则显示所有部分匹配的结果。这些角色可能适用于其他用户以及您预期的用户。

LDAP 页面上的信息会立即得到筛选。

 如果已经设置了筛选器，但想要再次查看未筛选的信息，请关闭所需的筛选器，或移除筛选器中的任何设置以将其留空。


3. 点击**关闭抽屉**以关闭“筛选器”面板。

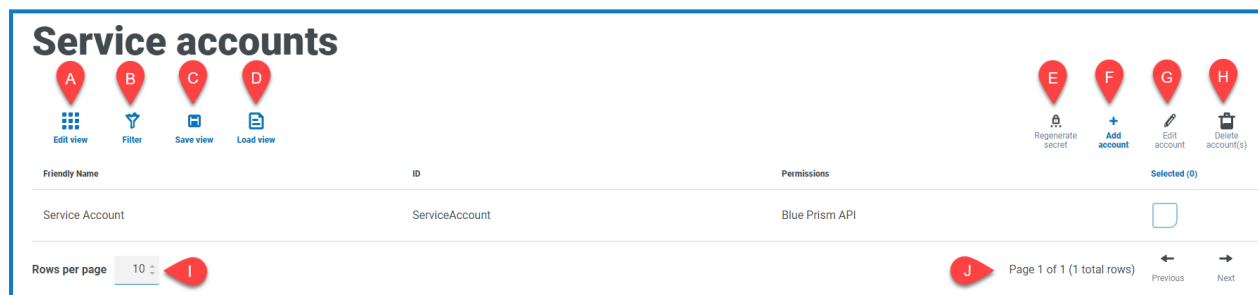
## 服务帐户

通过“服务帐户”页面，您可以管理已经过身份验证的应用程序帐户。此区域仅在您是管理员时才可用。

服务帐户由需要获取访问令牌以供自己使用（而不是代表用户获取访问令牌）的应用程序使用。这些访问令牌之后可用于向 API 发出已经过身份验证的请求。服务帐户可以获取访问令牌的 API 是：

- **Authentication Server API**—必须为与 Authentication Server API 集成的任何应用程序创建服务帐户。有关更多详细信息，请参阅 [Authentication Server 配置指南](#)。
- **Blue Prism API**—必须为与 Blue Prism API 集成的任何第三方应用程序创建服务帐户。有关更多详细信息，请参阅 [Blue Prism API 安装指南](#)。
- **Decision API**—必须创建服务帐户，以便 Blue Prism 使用在 Decision 插件中训练和校准的 Decision 模型。有关更多详细信息，请参阅 [Blue Prism Decision 安装指南](#)。
- **Interact Remote API**—必须为任何与 Interact Remote API 集成的应用程序（如 Blue Prism 交互式客户端）创建服务帐户。有关更多详细信息，请参阅 [Interact Web API 服务用户指南](#)。

 要打开“服务帐户”页面，请点击您的个人资料图标以打开“设置”页面，然后点击 **服务帐户**。



Friendly Name	ID	Permissions
Service Account	ServiceAccount	Blue Prism API

“服务帐户”页面为您提供以下信息和功能：

- 编辑视图**—定义显示的列。然后，您可以使用切换开关显示或隐藏列。
- 筛选器**—筛选显示的信息。然后，您可以打开所需的筛选器并输入或选择相应的显示信息，例如，您可以打开 **权限** 筛选器，并选择 **Blue Prism API**。
- 保存视图**—保存当前列设置。您可以输入视图的名称，以便在加载视图时轻松识别。
- 加载视图**—加载已保存的视图。您可以选择所需的视图，然后点击 **应用**。
- 重新生成密钥**—为现有服务帐户 **创建新密钥**。
- 添加帐户**—**添加** 新的服务帐户。
- 编辑帐户**—**编辑** 现有服务帐户的详细信息。
- 删除帐户**—**删除** 一个或多个服务帐户。
- 每页行数**—输入数字，或使用向上箭头和向下箭头更改页面上的行数。
- 服务帐户的 **上一页** 和 **下一页**—点击 **上一页** 或 **下一页** 可浏览页面。

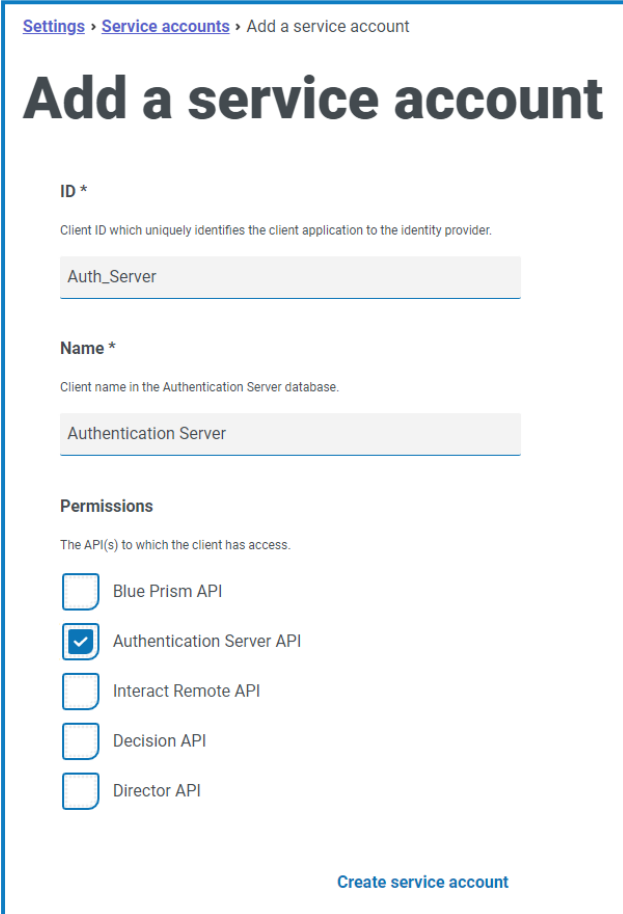
## 添加服务帐户

1. 在“服务帐户”页面上，点击 **添加帐户**。
2. 在 Authentication Server 数据库中，为客户端应用程序输入唯一 ID，并为客户端输入一个好记的名称。

3. 在**权限**下面, 选择相应的选项:

- **Blue Prism API**—服务帐户密钥用于获取访问令牌, 以使用 Blue Prism API 进行身份验证。
- **Authentication Server API**—服务帐户密钥用于向 Authentication Server API 发出已经过身份验证的请求。。
- **Interact Remote API**—服务帐户密钥用于获取访问令牌, 以使用 Interact Remote API 进行身份验证。
- **Decision API**—服务帐户密钥用于获取访问令牌, 以使用 Decision Web API 进行身份验证。
- **Director API**—此权限没有功能。它是为将来的功能而保留的。

4. 点击**创建服务帐户**。



Settings > Service accounts > Add a service account

## Add a service account

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

Auth\_Server

**Name \***  
Client name in the Authentication Server database.

Authentication Server

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

Blue Prism API

Authentication Server API

Interact Remote API

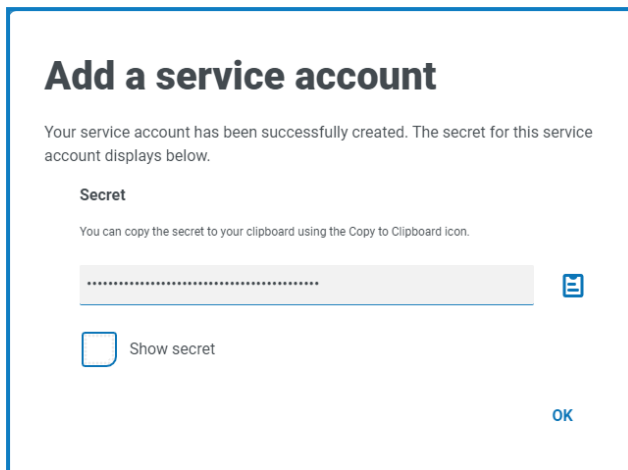
Decision API

Director API

Create service account

“添加服务帐户”对话框会显示生成的密钥, 该密钥将用于获取所选 API 的访问令牌。

5. 点击“复制到剪贴板”图标，将生成的密钥复制到剪贴板。



6. 点击**确定**以关闭对话框。  
“服务帐户”页面会显示新创建的帐户。


## 重新生成密钥

如果您忘了先前为现有服务帐户生成的密钥，您可以重新生成密钥。

1. 在“服务帐户”页面上，选择所需服务帐户并点击**重新生成密钥**。  
此服务帐户的新密钥会显示。
2. 点击“复制到剪贴板”图标，将生成的密钥复制到剪贴板。
3. 点击**确定**以关闭对话框。

## 编辑服务帐户

1. 在“服务帐户”页面上，选择所需服务帐户并点击**编辑帐户**。
2. 根据需要更改信息。

 您无法更改服务帐户的客户端 ID。

3. 点击**保存**以应用更改。

## 删除服务帐户

1. 在“服务帐户”页面上，选择所需服务帐户并点击**删除帐户**。  
系统会显示一则消息，要求您确认删除。
2. 点击**是**以删除选定帐户，或点击**否**以取消。

## 在“服务帐户”页面上使用筛选器

通过筛选器，您可以根据所选条件轻松查找特定服务帐户。

1. 在“服务帐户”页面上，点击**筛选器**，打开“筛选器”面板。
2. 使用切换开关打开所需的筛选器，填写信息以查找服务帐户。您可以同时应用多个筛选器。

可用的筛选器如下：

筛选器	描述
易记名称	输入服务帐户名称或部分名称。
ID	输入服务帐户标识符或部分标识符。
权限	选择相应的权限级别选项。您可以选择多个选项。如果您没有选择任何权限级别，“服务帐户”页面会包含所有级别。

“服务帐户”页面上的信息会立即得到筛选。



如果已经设置了筛选器，但想要再次查看未筛选的信息，请关闭所需的筛选器，或移除筛选器中的任何设置以将其留空。

3. 点击**关闭抽屉**以关闭“筛选器”面板。