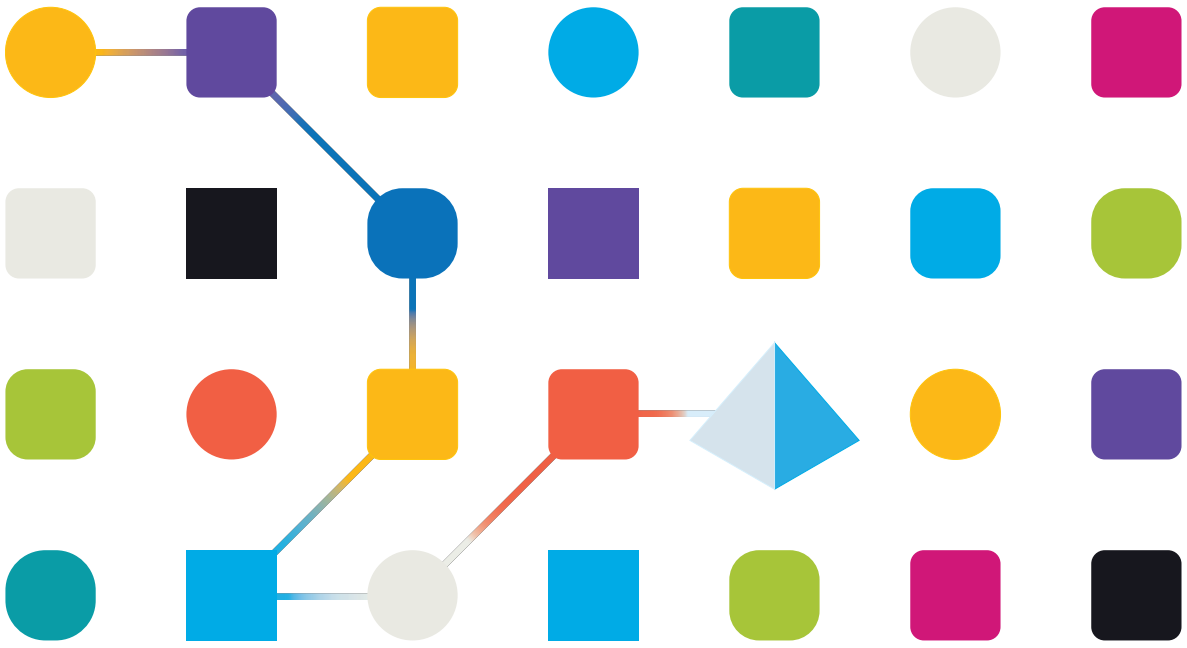
blueprism®

Blue Prism Hub 4.6

Administratorenhandbuch

Dokumentrevision: 3.0



Marken- und Urheberrechtshinweise

Blue Prism Limited, 2 Cinnamon Park, Crab Lane, Warrington, WA2 0XP, United Kingdom.
Registriert in England: Reg.- Nr. 4260035. Tel.: +44 370 879 3000. Web: www.blueprism.com

Inhalt

Hub

Blue Prism vereint die Prinzipien der Cloud, Robotic Process Automation (RPA) und künstlichen Intelligenz (KI), die zur Automatisierung und Digitalisierung wissensbasierter Arbeiten entwickelt wurden. Digital Workers werden in Geschäftsabläufen eingesetzt und ahmen nach, wie Menschen Geschäftssysteme verwenden, Entscheidungen treffen und Prozesse ausführen. Auf diese Weise können manuelle Arbeitsprozesse erweitert, ersetzt oder digitalisiert werden.

Wenn sich die Digital Workforce in einer Organisation weiterentwickelt, müssen Betreiber und Sponsoren ihre Ansätze und Methoden skalieren, um ihre Automatisierungsinvestitionen optimal zu nutzen. Managementinformationen über die Digital Workforce müssen im gesamten Unternehmen transparent und intuitiv verständlich sein. Darüber hinaus müssen Best Practices überwacht werden, um die Ausrichtung an den Branchenstandards sicherzustellen. Blue Prism® Hub bietet neuen und bestehenden Blue Prism Benutzern eine Produktivitätsplattform für das Management des Automatisierungslebenszyklus. Hub ist für einzelne Rollen innerhalb des Robotic Operating Model (ROM) geeignet und bietet eine Reihe von Funktionen für die erfolgreiche und skalierbare Bereitstellung einer Automatisierungsstrategie.

Hub ist eine schlanke „leere“ Anwendung, die durch eine Reihe unterschiedlicher Plug-ins und Funktionen ergänzt wird. Dadurch ergibt sich eine sogenannte Plug-in-Architektur, die es dem Blue Prism Team erlaubt, Funktionen zu iterieren und sie Hub Administratoren zur Verfügung zu stellen.

Jede Hub Instanz umfasst die Seite „Plug-in-Repository“ über die Administratoren neue Plug-ins anzeigen und bereitstellen sowie bestehende Plug-ins aktualisieren können.

Zielgruppe

Dieses Handbuch richtet sich an Hub Benutzer mit Administratorberechtigungen, die als Hub Administratoren bekannt sind. Hub Administratoren sind für die Verwaltung der Blue Prism Hub Plattform verantwortlich, einschließlich, aber nicht beschränkt auf:

- Verwaltung der Integration zwischen der Blue Prism Hub Plattform, Blue Prism und den Blue Prism APIs.
- Verwalten von Rollen und Benutzern, einschließlich Integration mit Active Directory.
- Installieren der Plug-ins.
- Überwachen von Audit-Logs.

Daher sollten Hub Administratoren Benutzer sein, die mit der Verwaltung von IT-Systemen vertraut sind und über ein Verständnis der Unternehmenssoftwarearchitektur und des Active Directory verfügen.

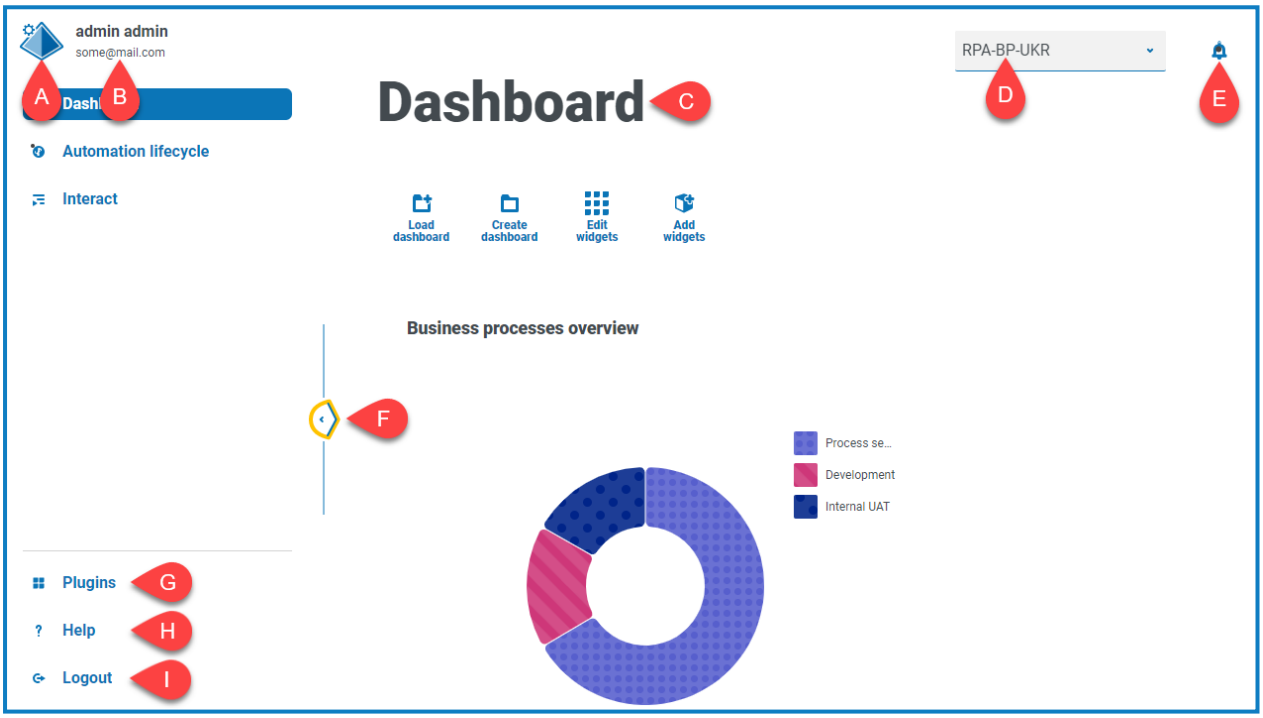
Administration und Konfiguration

Wenn Hub für ein Unternehmen installiert ist, wird es mit einer Hauptadministratorrolle bereitgestellt. Diese Rolle wird verwendet, um die Umgebung mit Informationen für Elemente wie E-Mails und die Verbindung zu Ihrer RPA-Datenbank zu konfigurieren.

Hub nutzt die rollenbasierte Zugriffssteuerung, um dafür zu sorgen, dass Benutzer nur auf die Funktionen zugreifen können, die für die Ausführung ihrer Aufgaben im Unternehmen erforderlich sind.

Die obere Navigationsleiste in Hub bietet Zugriff auf die Systemeinstellungen. Die verfügbaren Einstellungen hängen von der Benutzerrolle ab. Es gibt einige Einstellungen, die für Benutzer nicht verfügbar sind, ohne dass Administratorrechte für ihr Konto aktiviert wurden, wie unten beschrieben.

Zu den Funktionen auf der oberen Navigationsleiste zählen:



Wenn das Navigationsmenü links erweitert wird (wie oben gezeigt), werden diese Funktionen angezeigt:

A. **Profil-Symbol** – Vom Benutzer in seinem Profil definiert. Wenn Sie Folgendes sind:
   - Ein Benutzer: Dann wird ein Link zu Ihrer Profilseite zur Verfügung gestellt.
   - Ein Administrator: Dann wird ein Link zu den Systemeinstellungen bereitgestellt, von denen aus die Folgenden angepasst werden können:
     - Persönliches Profil und Audit.
     - Plattformmanagement.
     - Benutzermanagement.

B. **Benutzerinformationen** – Diese werden beim Einklappen des Navigationsmenüs ausgeblendet.

C. **Seitentitel** – Der Bereich der Hub Benutzeroberfläche, den Sie derzeit verwenden.

D. **Umgebung** – Die aktuell ausgewählte Umgebung. Umgebungen werden im Umgebungsmanager eingerichtet und können hier ausgewählt werden.

E. **Benachrichtigungswarnungen** – Benachrichtigungen werden durch das Plug-in für das Automation Lifecycle Management erstellt. Nur Benachrichtigungen, die Sie sehen dürfen oder die für Sie gelten, werden angezeigt, wenn Sie auf den Alarm klicken.

F. **Menü umschalten** – Öffnet und schließt das Menü. Wenn das Menü geöffnet ist, werden die Namen der Menüelemente angezeigt. Wenn das Menü geschlossen ist, werden Symbole für jeden Menüpunkt angezeigt.

G. **Plug-ins** – Öffnet die Seite „Plug-ins“, auf der Sie verfügbare Plug-ins anzeigen und herunterladen können.

H. **Hilfe** – Öffnet die Onlinehilfe. Klicken Sie mit der rechten Maustaste und wählen Sie **Verknüpfung in neuer Registerkarte öffnen** aus, um sie in einer separaten Browser-Registerkarte zu öffnen.

I. **Abmelden** – Meldet Sie vom Authentication Server ab.

> Wenn Sie Interact verwenden, werden Sie auch von der Interact Webanwendung abgemeldet.

Hub Einschränkungen

In der folgenden Tabelle sind die bei der Verwendung von Hub durchgesetzten Einschränkungen aufgeführt.

Element	Einschränkung	Verwandte Abschnitte
Benutzernamen	Benutzernamen für native Benutzer dürfen nicht länger als 25 Zeichen. Sie dürfen nur lateinische Buchstaben (außer Sonderzeichen), Ziffern, Punkte, Bindestriche und Unterstriche enthalten. Sie können nicht mit Punkten, Bindestrichen und Unterstrichen beginnen. Benutzernamen für Active Directory-Benutzer (ihre UPN) dürfen nicht länger als 255 Zeichen sein.	Benutzer auf Seite 25
Passworteinschränkungen	Passwörter müssen: • Mindestens 1 Großbuchstaben enthalten • Mindestens 1 Zahl enthalten • Mindestens 1 Sonderzeichen enthalten • Mindestens 8 Zeichen lang sein • Sich von den letzten fünf Passwörtern unterscheiden • Kürzer als 32 Zeichen sein	Profil auf Seite 9 und Benutzer auf Seite 25
Profilbild	Kleiner als 1 MB, maximal 1920 x 1080 Pixel	Profil auf Seite 9
Dashboard-Widgets	Begrenzt auf 20 Widgets pro Dashboard	Dashboards – siehe Hub Benutzerhandbuch.
Markenlogo	PNG, JPEG oder JPG, maximal 30 KB	Personalisierung auf Seite 20

Einstellungen

Auf der Einstellungsseite können Sie Hub verwalten. Sie haben nur dann Zugriff auf die Einstellungsseite, wenn Sie ein Administrator sind. Wenn Sie ein Benutzer sind, haben Sie nur Zugriff auf die Profilseite, die sich öffnet, wenn Sie auf Ihr Profilsymbol klicken.

Um die Einstellungsseite zu öffnen, klicken Sie auf Ihr Profilsymbol. Die Einstellungsseite wird angezeigt, wenn Sie ein Administrator sind. Die Profilseite wird angezeigt, wenn Sie ein Benutzer sind.

Übersicht

Profil	Auf der Profilseite können Sie Ihre Informationen, Anzeigeeinstellungen und Ihr Passwort ändern. Mehr erfahren Sie unter Profil auf Seite 9.
Audit	Administratoren können den Verlauf der geprüften Systemaktivitäten anzeigen. Mehr erfahren Sie unter Audit auf Seite 11.

Plattformmanagement

Die E-Mail- und Datenbankeinstellungen werden im Rahmen des Installations- und Konfigurations-Prozesses von Hub festgelegt, mehr hierzu erfahren Sie im Hub Installationshandbuch. Sie sind für einen normalen Betrieb unerlässlich.

Umgebungsmanagement	Administratoren können Verbindungen zu Blue Prism RPA Datenbanken hinzufügen, vorhandene Verbindungen verwalten und redundante RPA Datenbanken entfernen. Mehr erfahren Sie unter Umgebungsmanagement auf Seite 14.
E-Mail-Konfiguration	Administratoren können die SMTP-Host-Details ändern. Änderungen sollten in Abstimmung mit Ihrem eigenen IT-Support-Team vorgenommen werden, um sicherzustellen, dass die Konfiguration und die Anmeldedaten mit dem E-Mail-Server Ihres Unternehmens übereinstimmen. Mehr erfahren Sie unter E-Mail-Konfiguration auf Seite 17.
Personalisierung	Administratoren können das Design anpassen, das von der Interact Benutzeroberfläche verwendet wird. So können Administratoren den Namen des Designs, die Markenfarbe und das Markenlogo anpassen. Mehr erfahren Sie unter Personalisierung auf Seite 20.
Plug-in-Management	Administratoren können die Beschreibung und Versionsnummer der derzeit installierten Plug-ins anzeigen. Alle Updates oder zusätzlichen verfügbaren Plug-ins werden ebenfalls angezeigt. Mehr erfahren Sie unter Plug-in-Management auf Seite 22.

Benutzermanagement

Benutzer	Administratoren können Benutzer hinzufügen, ändern oder zurückziehen sowie Zugriffsberechtigungen und Rollen zuweisen. Mehr erfahren Sie unter Benutzer auf Seite 25.
Rollen und Berechtigungen	Administrationen können Rollen hinzufügen, bearbeiten und löschen. Mehr erfahren Sie unter Rollen und Berechtigungen auf Seite 35.
Registrierungen	Administratoren können Registrierungsanfragen verwalten, die neue Benutzer für den Zugriff auf Interact erstellt haben. Mehr erfahren Sie unter Registrierungen auf Seite 43.
Authentifizierungs-einstellungen	Administratoren können Authentifizierungseinstellungen hinzufügen, bearbeiten, zurückziehen oder löschen. Mehr erfahren Sie unter Authentifizierungseinstellungen auf Seite 45.
Dienstkonten	Administratoren können Dienstkonten hinzufügen, bearbeiten oder löschen. Mehr erfahren Sie unter Dienstkonten auf Seite 59.

Profil

Über die Profileinstellungen können Sie Ihre Informationen und Hub Anzeigeeinstellungen ändern. Die Profileinstellungen, die Sie ändern können, hängen vom Authentifizierungstyp ab, der für Ihr Konto konfiguriert ist. Wenn Sie ein nativer Administrator sind, können Sie Folgendes ändern:

- Ihr Passwort.
- Vor- und Nachname Ihres Profils.
- Ihre E-Mail-Adresse.
- Ihr Profilbild – dieses wird im Profilsymbol angezeigt. Dieses Bild wird nur in Hub verwendet.
- Ihr Hub Anzeigedesign – dunkel oder hell.

Wenn Ihr Hub Konto für die Verwendung der Active Directory-Authentifizierung konfiguriert ist, können Sie nur Ihr Profilbild und Ihr Hub Anzeigedesign ändern. Alle anderen Einstellungen werden in Active Directory verwaltet und aktualisiert, wenn Sie sich bei Hub anmelden oder manuell synchronisiert werden.

Sie können Ihren Benutzernamen nicht ändern, unabhängig von Ihrem Authentifizierungstyp.

Weitere Informationen zu Authentifizierungstypen finden Sie unter Authentifizierungseinstellungen.

Um die Seite „Profil“ zu öffnen, klicken Sie auf Ihr Profilsymbol, um die Seite „Einstellungen“ zu öffnen, und dann auf **Profil**.

Ihr Profil ändern

1. Klicken Sie auf der Seite „Profil“ auf **Bearbeiten**.

   Die Profilseite kann daraufhin bearbeitet werden. Das ist dadurch ersichtlich, dass die Schaltfläche **Bearbeiten** zur Schaltfläche **Abbrechen** wechselt und die Felder bearbeitbar werden.
2. Aktualisieren Sie bei Bedarf Folgendes:
   - Aktualisieren Sie Ihren Vornamen, Nachnamen oder Ihre E-Mail-Adresse.
   - Schalten Sie das **Dunkle Design** ein oder aus. Standardmäßig wird Hub mit dem hellen Design angezeigt.
   - Klicken Sie auf **Hochladen**, um Ihr Profilbild auszuwählen. Das Bild wird innerhalb des Prismasymbols angezeigt. Bilder dürfen nicht größer als 1 MB sein.
3. Klicken Sie auf **Speichern**, um die Änderungen zu speichern. Wenn Sie Ihre Änderungen nicht speichern möchten, klicken Sie auf **Abbrechen**.

   Die Schaltfläche **Speichern** wird erst aktiv, wenn Sie eine Änderung an der Einstellung des Designs vorgenommen haben.

Ihr Passwort ändern

1. Klicken Sie auf der Seite „Profil“ auf **Passwort aktualisieren**.

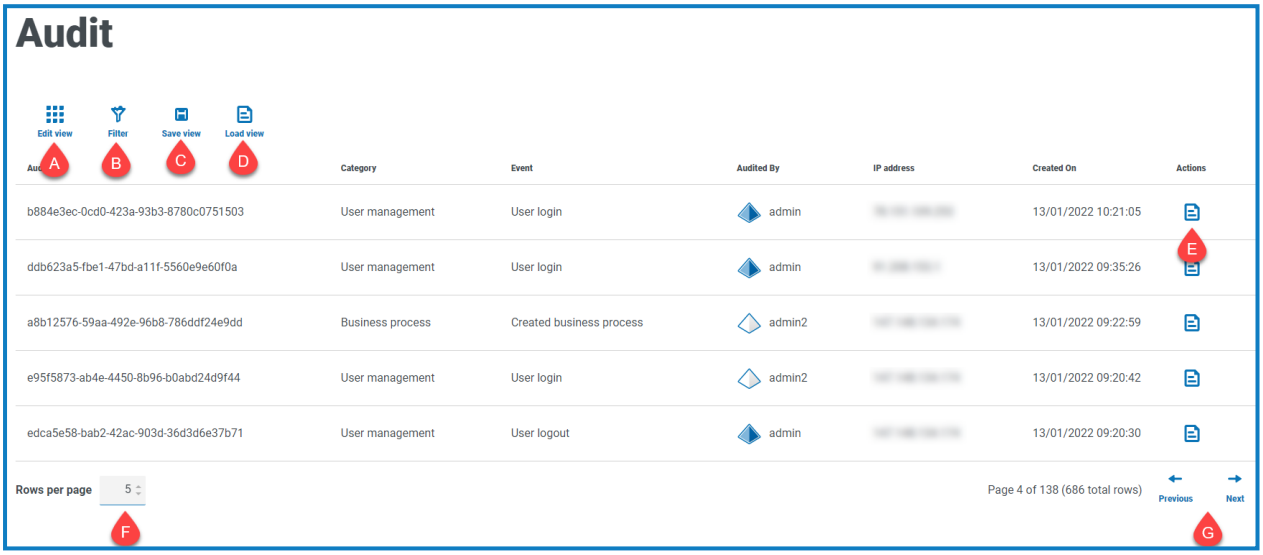
   Das Dialogfeld „Passwort aktualisieren“ wird angezeigt.
2. Geben Sie das aktuelle Passwort ein.
3. Geben Sie Ihr neues Passwort ein und wiederholen Sie es.

4. Klicken Sie auf **Aktualisieren**.
   Ihr Passwort wird geändert.

Audit

Mit Audit können Sie geprüfte Systemaktivitäten aufrufen. Dieser Bereich ist nur für Administratoren verfügbar.

Zum Öffnen der Seite „Audit“ klicken Sie auf Ihr Profilsymbol. Die Seite „Einstellungen“ wird geöffnet. Klicken Sie dann auf **Audit**.



Die Seite „Audit“ umfasst die folgenden Informationen und Funktionen:

A. **Ansicht bearbeiten** – Legen Sie fest, welche Spalten angezeigt werden sollen. Sie können die Spalten dann per Umschalten anzeigen oder ausblenden.

B. **Filtern** – Filtern Sie die angezeigten Informationen. Sie können dann die erforderlichen Filter aktivieren und die entsprechenden Informationen für die Anzeige eingeben oder auswählen. Aktivieren Sie zum Beispiel**Kategorie** filtern und wählen Sie **Benutzermanagement** aus.

C. **Ansicht speichern** – Speichern Sie Ihre aktuellen Spalteneinstellungen. Sie können Ihrer Ansicht einen Namen geben, um sie beim Laden von Ansichten einfacher zu erkennen.

D. **Ansicht laden** – Laden Sie eine gespeicherte Ansicht. Sie können die gewünschte Ansicht auswählen und auf **Anwenden** klicken.

E. **Log anzeigen** – Anzeigen der Details eines Audit-Elements.

F. **Zeilen pro Seite** – Geben Sie eine Zahl ein oder verwenden Sie die Pfeile nach oben und unten, um die Anzahl der auf einer Seite angezeigten Zeilen zu ändern.

G. **Zurück und Weiter** – Klicken Sie auf **Zurück** oder **Weiter**, um durch die Seiten zu navigieren der Audit-Elemente.

Ein Element anzeigen

1. Aktivieren Sie auf der Seite „Audit“ das Kontrollkästchen für das Element, das Sie aufrufen möchten.
2. Klicken Sie auf **Log anzeigen**.

   Die Details des Ereignisses werden angezeigt.

Filter auf der Seite „Audit“ verwenden

Mit Filtern können Sie auf schnelle Weise Audit-Ereignisse anhand ausgewählter Kriterien finden.

1. Klicken Sie auf der Audit-Seite auf **Filter**, um den Filter-Bereich zu öffnen.
2. Verwenden Sie den Umschalter, um den erforderlichen Filter zu aktivieren, und geben Sie die Informationen ein, um das Audit-Ereignis zu finden. Sie können mehrere Filter gleichzeitig anwenden.

   Die verfügbaren Filter sind:

Filter	Beschreibung
Audit-ID	Geben Sie den Audit-Identifikator oder einen Teil des Identifikators ein.
Kategorie	Wählen Sie eine Kategorie aus der Dropdown-Liste aus. Die verfügbaren Kategorien sind: • **Benutzermanagement** – Beinhaltet Ereignisse im Zusammenhang mit Benutzern, wie die Verwaltung von Benutzern durch Administratoren und Benutzerzugriffsinformationen. • **SMTP-Management** – Beinhaltet Änderungen an den SMTP-Einstellungen. • **Rollenmanagement** – Beinhaltet Ereignisse im Zusammenhang mit Rollen. • **Authentifizierungsmanagement** – Beinhaltet Ereignisse im Zusammenhang mit den Authentifizierungseinstellungen, wie z. B. Verwaltung der Verbindungen und Synchronisierung. • **Dienstkonten** – Beinhaltet Ereignisse im Zusammenhang mit Dienstkonten, wie z. B. das Management der Konten und die erneute Schlüsselgenerierung. • **Geschäftsprozess** – Beinhaltet Ereignisse im Zusammenhang mit Geschäftsprozessen, wie z. B. das Erstellen, Zurückziehen und Aktivieren von Geschäftsprozessen. Wenn Sie eine Kategorie auswählen, sind die Optionen im Filter **Ereignis** auf die Optionen beschränkt, die sich in der ausgewählten Kategorie befinden. Wenn Sie die folgenden Plug-ins installiert haben, sind auch diese zusätzlichen Kategorien verfügbar: • **Automation Lifecycle Management (ALM):** • **Prozessdefinitionen** – Beinhaltet Ereignisse im Zusammenhang mit Prozessdefinitionen, wie z. B. das Management der Definitionen und den Unterzeichnungs-Workflow.

Filter	Beschreibung

	• **Interact:**
	  • **Interact - Formulare** – Beinhaltet Ereignisse im Zusammenhang mit dem Interact Formular-Plug-in, wie z. B. die Verwaltung der Formulare und die Erhöhung der Hauptversionsnummer.
	  • **Interact Einsendungen** – Beinhaltet Ereignisse im Zusammenhang mit Interact, wie z. B. die Einsendung von Formularen durch den Endbenutzer und den Genehmigungsworkflow.

Ereignis	Wählen Sie ein Ereignis aus der Dropdown-Liste aus. Dadurch werden alle Ergebnisse für dieses spezifische Audit-Ereignis angezeigt. Wenn Sie den Filter **Kategorie** verwenden, sind die in der Dropdown-Liste angezeigten Ereignisse auf die Ereignisse für diese Kategorie beschränkt. Wenn Sie alle Ereignisse für eine ausgewählte Kategorie anzeigen möchten, schalten Sie den Filter **Ereignis** aus und verwenden Sie einfach den Filter **Kategorie**.
Geprüft von	Geben Sie den Benutzernamen oder Kontonamen eines Benutzers oder einen Teil davon ein.
IP-Adresse	Geben Sie die öffentliche IP-Adresse oder einen Teil davon ein.
Erstellt am	Geben Sie einen Datumsbereich ein: • Wählen Sie im ersten Feld das früheste Datum aus. • Wählen Sie im zweiten Feld das letzte Datum aus. • Falls erforderlich, passen Sie die Zeitfelder an. Standardmäßig hat das erste Datum den Zeitwert „00:00:00“ und das letzte Datum den Zeitwert „23:59:59“, was einen vollständigen Tag ergibt. Dies zeigt alle Audit-Ereignisse während dieses Zeitrahmens an.

Die Informationen auf der Audit-Seite werden sofort gefiltert.

Wenn Sie die Filter eingestellt haben, aber die ungefilterten Informationen noch einmal anzeigen möchten, schalten Sie entweder die erforderlichen Filter aus oder entfernen Sie alle Einstellungen innerhalb des Filters, damit er leer ist.

3. Klicken Sie auf **Bereich schließen**, um den Filter-Bereich zu schließen.

Umgebungsmanagement

Im Umgebungsmanager werden Ihre verbundenen Datenbanken angezeigt. Dieser Bereich ist nur für Administratoren verfügbar.

Die Seite „Umgebung“ bietet die folgenden Informationen und Funktionen:

A. Die Hub Datenbank.

B. Die Blue Prism Datenbank, die im Rahmen des anfänglichen Installationsvorgangs konfiguriert wurde.

C. Aktualisiert die Details der Digital Workforce und der Warteschlangen in Hub. Aktualisieren Sie die Datenbank, wenn Verbindungen hinzugefügt oder geändert werden. Wenn die Datenbank nicht aktualisiert wird, können Sie die Digital Workers oder Warteschlangen in dieser speziellen Blue Prism Umgebung nicht sehen.

D. Öffnet die Seite „Verbindung bearbeiten“, auf der Sie Datenbankdetails bearbeiten können.

E. Löscht die Datenbankverbindung. Weitere Informationen finden Sie unter Eine Datenbankverbindung löschen.

F. Öffnet das Dialogfeld „Verbindung hinzufügen,“ in dem Sie eine neue Blue Prism Datenbankverbindung konfigurieren und hinzufügen können.

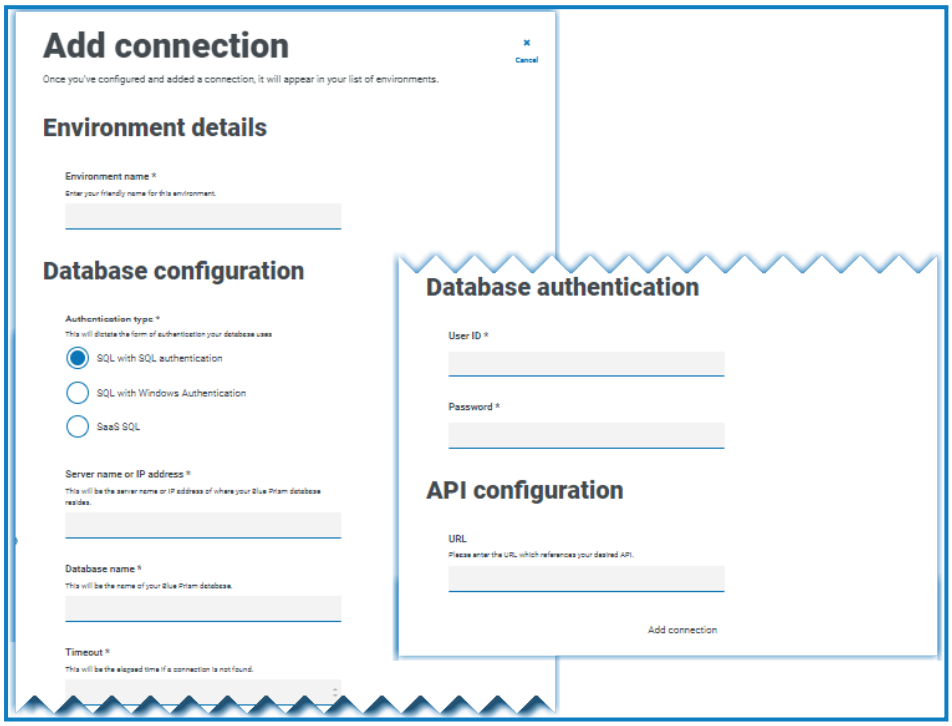
Zum Öffnen des Umgebungsmanagers klicken Sie auf Ihr Profilsymbol. Daraufhin wird die Seite „Einstellungen“ geöffnet. Klicken Sie dann auf **Umgebungsmanagement**.

Blue Prism Datenbankverbindung hinzufügen

1. Klicken Sie auf der Seite „Umgebungsmanager“ auf **Verbindung hinzufügen**, um eine zusätzliche RPA-Datenbankverbindung hinzuzufügen.

   Die Seite „Verbindung hinzufügen“ wird angezeigt.

2. Geben Sie die Konfigurationsparameter der Datenbankverbindung ein.



   Wenn alle Felder ausgefüllt sind, ist der Link **Verbindung hinzufügen** verfügbar.

   > ⚠ Sie müssen sicherstellen, dass Ihr Datenbankpasswort kein Gleichheitszeichen (=) und keinen Strichpunkt (;) enthält. Diese Zeichen werden nicht unterstützt und führen zu Problemen, wenn versucht wird, eine Verbindung zur Datenbank herzustellen.

3. Geben Sie bei Bedarf die URL für die Blue Prism API in das Feld „URL“ unter „API-Konfiguration“ ein. Diese URL ist erforderlich, wenn Sie das Control Room Plug-in verwenden möchten. Das Control Room Plug-in ist mit Blue Prism 7.0 oder höher kompatibel.
4. Klicken Sie auf **Verbindung hinzufügen**, um die Details zu speichern.

   Die Verbindung wird im Umgebungsmanager erstellt und angezeigt.

5. Klicken Sie im Umgebungsmanager für Ihre neue Verbindung auf das Symbol „Aktualisieren“. Dadurch werden die Informationen in Hub mit der Digital Workforce und den Warteschlangen in der Datenbank aktualisiert.

Datenbankdetails bearbeiten

Sie können das URL-Feld nur unter „API-Konfiguration“ bearbeiten. Alle anderen Felder sind deaktiviert.

1. Klicken Sie auf der Seite „Umgebungsmanagement“ auf das Symbol **Bearbeiten** für die Datenbankverbindung, die Sie aktualisieren möchten.

   Die Seite „Verbindung bearbeiten“ wird angezeigt.

2. Geben Sie die **URL** im Abschnitt **API-Konfiguration** ein.

   Sie müssen die vollständige URL einschließlich des Protokolls eingeben, z. B. http:// oder https://. Zum Beispiel: *https://bpapi.yourdomain.com*

3. Klicken Sie auf **Speichern**.
4. Klicken Sie auf der Seite „Umgebungsmanagement“ für Ihre aktualisierte Verbindung auf das Symbol „Aktualisieren“. Dadurch werden die Informationen in Hub mit den digitalen Mitarbeitern und Warteschlangen in der Datenbank aktualisiert.

Datenbankverbindung löschen

Sie können eine Verbindung zu einer Datenbank nur dann löschen, wenn für diese Datenbank keine Abhängigkeiten bestehen. Sie können eine Datenbank in folgenden Fällen nicht löschen:

- Interact Formulare hängen von einer Warteschlange innerhalb dieser RPA-Datenbank ab, zum Beispiel dem Senden eines Formulars an eine Warteschlange.
- Die ALM Prozessdefinitionen verwenden Objekte, die in dieser RPA-Datenbank definiert sind.

Sie müssen die Formulare oder Prozessdefinitionen ändern, um auf eine alternative Datenbank zu verweisen, um die Abhängigkeit zu entfernen.

Mit der Löschfunktion können Sie Datenbanken entfernen, die versehentlich hinzugefügt wurden und nicht in Gebrauch sind, wenn zum Beispiel während der Konfiguration die falschen Datenbankinformationen hinzugefügt wurden.

So löschen Sie eine RPA-Datenbank:

1. Klicken Sie auf der Seite „Umgebungsmanager“ auf der Datenbankkachel auf das Symbol „Löschen“.

   Wenn es keine Abhängigkeiten gibt, wird eine Meldung angezeigt, die Sie zur Bestätigung des Löschvorgangs auffordert. Wenn es Abhängigkeiten gibt, wird oben rechts in der Hub Benutzeroberfläche eine Fehlermeldung angezeigt.

2. Klicken Sie auf **Ja**, um das Löschen zu bestätigen.

E-Mail-Konfiguration

Mit den E-Mail-Einstellungen können Sie die Konfiguration von SMTP ändern und E-Mails für Benachrichtigungen konfigurieren, z. B. Anfragen zum Zurücksetzen des Passworts von Benutzern. Dieser Bereich ist nur für Administratoren verfügbar. Änderungen sollten in Abstimmung mit Ihrem eigenen IT-Support-Team vorgenommen werden, um sicherzustellen, dass die Konfiguration und die Anmeldedaten mit dem E-Mail-Server Ihres Unternehmens übereinstimmen.

Sie können Ihre E-Mail-Einstellungen so konfigurieren, dass eine der folgenden Authentifizierungsmethoden verwendet wird:

- Benutzername und Passwort
- Microsoft OAuth 2.0

Wenn Sie die SMTP-Einstellungen speichern, wird an Sie eine Test-E-Mail gesendet. Das dient zur Überprüfung, dass die Einrichtung korrekt ist. Falls Sie nach dem Speichern der Änderungen keine Test-E-Mail erhalten, überprüfen Sie die Details und aktualisieren Sie sie entsprechend.

Zum Öffnen der E-Mail-Konfigurationsseite klicken Sie auf Ihr Profilsymbol. Die Seite „Einstellungen“ wird geöffnet. Klicken Sie dann auf **E-Mail-Konfiguration**.

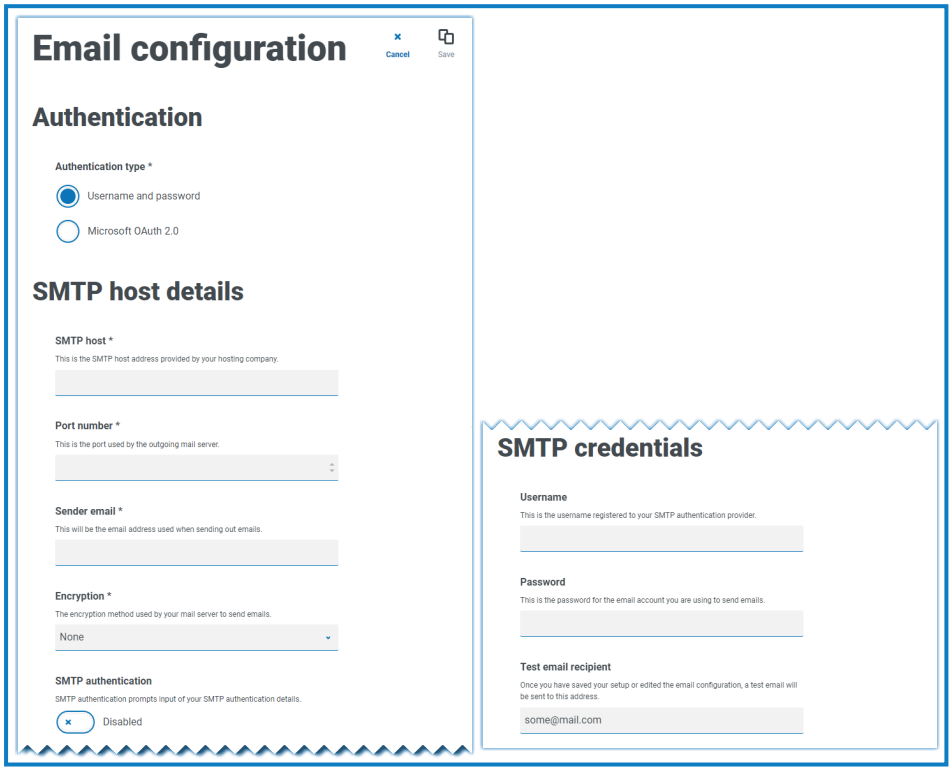
E-Mail-Einstellungen aktualisieren

Die E-Mail-Einstellungen werden als Teil der ersten Konfiguration von Hub eingegeben. Sie müssen diese Einstellungen nur im Falle einer Änderung der IT-Infrastruktur ändern, z. B. bei einem anderen SMTP-Host, oder bei einer Änderung am vorhandenen Host, die sich auf diese Einstellungen auswirkt.

Authentifizierung mit Benutzername und Passwort

1. Klicken Sie auf der Seite „E-Mail-Konfiguration“ auf **Bearbeiten**.
2. Wählen Sie im Abschnitt „Authentifizierung“ unter **Authentifizierungstyp** die Option **Benutzername und Passwort** aus.

   Die E-Mail-Konfigurationsseite wird mit den entsprechenden Feldern aktualisiert:



3. Geben Sie die folgenden Informationen ein:
   - **SMTP-Host** – Die Adresse Ihres SMTP-Hosts.
   - **Portnummer** – Die Portnummer, die vom Server für ausgehende E-Mails verwendet wird.
   - **E-Mail-Adresse des Absenders** – Die E-Mail-Adresse, die beim Senden von E-Mails verwendet wird. Die E-Mail-Empfänger werden diese Adresse im Feld „Von“ sehen.
   - **Verschlüsselung** – Die Verschlüsselungsmethode, die vom E-Mail-Server zum Senden der E-Mails verwendet wird.
   - **SMTP-Authentifizierung** – Wählen Sie diese Option aus, wenn die SMTP-Authentifizierung zur Eingabe von Authentifizierungsdetails auffordert. Durch die Auswahl von **Aktiviert** werden **Benutzername** und **Passwort** zu Pflichtfeldern.
   - **Benutzername** – Der Benutzername für die SMTP-Authentifizierung.
   - **Passwort** – Das Passwort für das Konto.
   - **Empfänger der Test-E-Mail** – Die Test-E-Mail wird an diese E-Mail-Adresse gesendet. Das ist standardmäßig die E-Mail-Adresse des Benutzers, der die Änderungen vornimmt. Sie kann nicht geändert werden.
4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

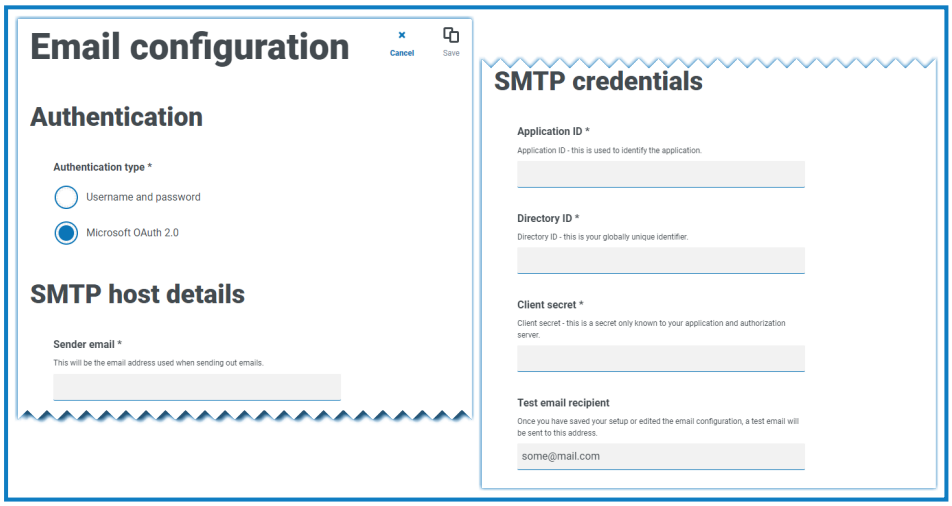
Microsoft OAuth 2.0 Authentifizierung

Sie können mithilfe des von Azure Active Directory bereitgestellten Authentifizierungsdienstes Microsoft OAuth 2.0 eine Verbindung zum SMTP-Host herstellen. Ihr IT-Support-Team muss eine Anwendung in Azure AD registrieren und Ihnen die Anwendungs-ID (Client-ID), die Verzeichnis-ID (Mandanten-ID) und das Client-Geheimnis zur Verfügung stellen, damit Sie die Informationen in Schritt 3 eingeben können. Informationen zum Auffinden dieser Details in Azure AD finden Sie in der Microsoft-Dokumentation.

Wenn Sie Microsoft OAuth 2.0 verwenden, muss die Berechtigung „Mail.Send“ in Azure Active Directory aktiviert sein. Dies muss von Ihrem IT-Support-Team in Azure Active Directory konfiguriert werden. Weitere Informationen finden Sie unter Fehlerbehebung einer Hub Installation in der Blue Prism Hub Installationsanleitung.

1. Klicken Sie auf der Seite „E-Mail-Konfiguration“ auf **Bearbeiten**.
2. Wählen Sie im Abschnitt „Authentifizierung“ unter **Authentifizierungstyp** die Option **Microsoft OAuth 2.0** aus.

   Die E-Mail-Konfigurationsseite wird mit den entsprechenden Feldern aktualisiert:



3. Geben Sie die folgenden Informationen ein:
   - **E-Mail-Adresse des Absenders** – Die E-Mail-Adresse, die beim Senden von E-Mails verwendet wird. Die E-Mail-Empfänger werden diese Adresse im Feld „Von“ sehen.
   - **Anwendungs-ID** – Dies ist die Anwendungs-ID (Client-ID), die in Azure AD definiert ist und Ihnen von Ihrem IT-Support-Team zur Verfügung gestellt wird.
   - **Verzeichnis-ID** – Dies ist die Verzeichnis-ID (Mandanten-ID), die in Azure AD definiert ist und Ihnen von Ihrem IT-Support-Team zur Verfügung gestellt wird.
   - **Client-Geheimnis** – Hierbei handelt es sich um das von Azure AD generierte Client-Geheimnis, das Ihnen von Ihrem IT-Support-Team zur Verfügung gestellt wird und den Authentifizierungsprozess steuert.
   - **Empfänger der Test-E-Mail** – Die Test-E-Mail wird an diese E-Mail-Adresse gesendet. Das ist standardmäßig die E-Mail-Adresse des Benutzers, der die Änderungen vornimmt. Sie kann nicht geändert werden.
4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Personalisierung

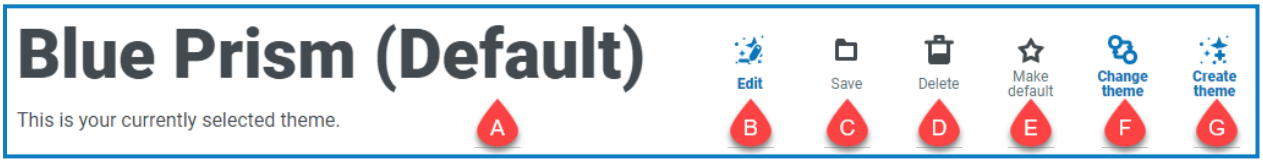
Mit den Personalisierungseinstellungen können Sie das Erscheinungsbild der Interact Benutzeroberfläche ändern. Dieser Bereich ist nur für Administratoren verfügbar. Sie können Designs mit folgenden Merkmalen erstellen:

- **Designname** – Das ist auch der Markenname, der auf der Benutzeroberfläche angezeigt wird.
- **Markenfarbe** – Das ist die Farbe der Schaltflächen und Beschriftungen auf der Benutzeroberfläche.
- **Markenlogo** – Dieses Bild wird als Logo auf der Benutzeroberfläche verwendet.

Sie können mehrere Designs erstellen, die sich abhängig vom Benutzer anwenden lassen. Dadurch verändert sich das Erscheinungsbild je nach angemeldetem Benutzer. Das Standarddesign wird beim Erstellen eines Benutzers automatisch ausgewählt, es kann jedoch geändert werden.

Zum Öffnen der Seite „Personalisierung“ klicken Sie auf Ihr Profilsymbol. Die Seite „Einstellungen“ wird geöffnet. Klicken Sie dann auf **Personalisierung**.

Wenn Sie die Seite „Personalisierung“ öffnen, wird das Standarddesign angezeigt:



Das umfasst die folgenden Informationen und Funktionen:

A. Name des aktuell angezeigten Designs.
B. Bearbeiten – Bearbeiten Sie das aktuell angezeigte Design.
C. Speichern – Speichern Sie alle vorgenommenen Änderungen. Dieses Symbol ist nur bei der Bearbeitung eines Designs aktiv.
D. Löschen – Das aktuell angezeigte Design löschen. Dieses Symbol ist nur bei mehreren vorhandenen Designs aktiv.
E. Als Standardeinstellung festlegen – Legen Sie das aktuell angezeigte Design als Standardeinstellung für das System fest. Dieses Symbol ist nur dann aktiv, wenn das aktuelle Design nicht der Standardwert ist.
F. Design ändern – Wählen Sie das Design aus, das auf der Seite dargestellt werden soll.
G. Design erstellen – Ein neues Design erstellen.

Ein Design bearbeiten und speichern

1. Klicken Sie auf der Seite „Personalisierung“ auf **Design bearbeiten**.

   Die Seite „Design“ kann daraufhin bearbeitet werden. Dabei wechselt die Schaltfläche **Design bearbeiten** zur Schaltfläche **Abbrechen** und die Schaltflächen zum **Zurücksetzen** werden aktiv.

2. Falls erforderlich, ändern Sie den **Designnamen**.

   Beim Tippen ändert sich auch der Titel *Design erstellen*.

3. Falls erforderlich, ändern Sie die **Primärfarbe** per Klick auf die Farbleiste. Sie können:
   - eine Farbe mithilfe des Schiebers auswählen.
   - mithilfe der Textfelder einen Wert eingeben. Sie können auf das Symbol ⇕ klicken, um zwischen den verschiedenen Typen umzuschalten: RGB, HSL oder Hex.

4. Klicken Sie bei Bedarf auf **Hochladen**, um das Logo in eine Datei Ihrer Wahl zu ändern.
5. Klicken Sie auf **Speichern**, um die Änderungen zu speichern. Wenn Sie Ihre Änderungen nicht speichern möchten, klicken Sie auf **Abbrechen**.

> Die Schaltfläche **Speichern** wird erst aktiv, wenn Sie eine Änderung an der Einstellung des Designs vorgenommen haben.

Ein Design löschen

1. Wenn das Design, das Sie löschen möchten, auf dem Bildschirm angezeigt wird (siehe Das Design ändern unten), klicken Sie auf **Löschen**.

   Eine Meldung wird angezeigt, in der Sie zur Bestätigung des Löschvorgangs aufgefordert werden.
2. Klicken Sie auf **Ja**, um das Design zu löschen.

Ein neues Standarddesign festlegen

1. Wenn das Design, das Sie verwenden möchten, auf dem Bildschirm angezeigt wird (siehe Das Design ändern unten), klicken Sie auf **Als Standardeinstellung festlegen**.

   (Standard) wird neben dem Namen des Designs angezeigt. Eine Benachrichtigung bestätigt die Änderung. Das geänderte Design wird in Interact dargestellt.

Das Design ändern

> Das Symbol **Design ändern** ändert das derzeit dargestellte Design. Wenn Sie Änderungen am Design selbst vornehmen möchten, müssen Sie das Design bearbeiten.

1. Klicken Sie auf der Seite „Personalisierung“ auf **Design ändern**.

   Eine Liste der verfügbaren Designs wird angezeigt.
2. Klicken Sie auf das gewünschte Design.

   Das ausgewählte Design wird angezeigt.
3. Schließen Sie die Liste, um zu den Haupt-Tools zurückzukehren.

Ein neues Design erstellen

1. Klicken Sie auf der Seite „Personalisierung“ auf **Design erstellen**.

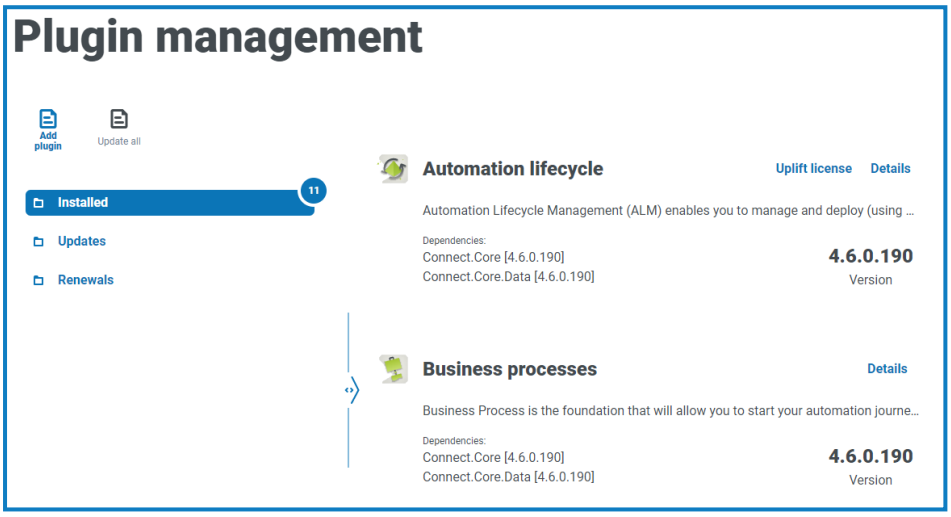
   Die Seite „Design erstellen“ wird angezeigt.
2. Geben Sie den **Namen** des Designs ein.

   Beim Tippen ändert sich auch der Titel *Design erstellen*.
3. Klicken Sie auf die Leiste **Primärfarbe**, um die Farbe zu ändern. Sie können:
   - eine Farbe mithilfe des Schiebers auswählen.
   - mithilfe der Textfelder einen Wert eingeben. Sie können auf das Symbol ⇕ klicken, um zwischen den verschiedenen Typen umzuschalten: RGB, HSL oder Hex.
4. Klicken Sie auf **Hochladen**, um das Logo in eine Datei Ihrer Wahl zu ändern.
5. Klicken Sie auf **Design erstellen**, um Ihr neues Design zu speichern.

Plug-in-Management

Im Plug-in-Management werden die Details der installierten Plug-ins angezeigt. Einige davon sind standardmäßig während des Installationsprozesses verfügbar. Sie können vorhandene Plug-ins verwalten, aktualisieren und neue Plug-ins hinzufügen. Dieser Bereich ist nur für Administratoren verfügbar.

Plug-ins sind das Herzstück von Hub und eigenständige Funktionen, die individuell installiert und angepasst werden können und Informationen über Ihre automatisierten Prozesse bereitstellen. Einige Plug-ins bieten auch Entwicklungstools für das Erstellen von Automatisierungen.



Um die Seite „Plug-in-Management“ zu öffnen, klicken Sie auf Ihr Profilsymbol, um die Seite „Einstellungen“ zu öffnen und dann auf **Plug-in-Verwaltung**.

Installierte Plug-ins anzeigen

Wenn Sie das Plug-in-Management öffnen, werden die aktuell installierten Plug-ins angezeigt. Der Name des Plug-ins, ein Auszug aus der Beschreibung und die Versionsnummern werden angezeigt. So rufen Sie:

- Weitere Informationen über ein Plug-in auf: Klicken Sie auf **Details**.
- Informationen über Aktualisierungen auf: Klicken Sie auf **Aktualisierungen**. Beachten Sie, dass diese Funktion derzeit nicht für Hub On-Premises verfügbar ist.
- Informationen über kommende oder ausstehende Verlängerungen der Lizenz auf: Klicken Sie auf **Erneuerungen**. Wenn Plug-ins eine Erneuerung der Lizenz erfordern, wird neben dem Link **Erneuerungen** die Anzahl der Aktualisierungen angezeigt. Wird keine Anzahl angezeigt, gibt es keine Erneuerungen.

Ein Plug-in hinzufügen

Wenn ein Plug-in installiert ist, wird die Website automatisch neu gestartet. Es ist daher wichtig, dass die Installation von Plug-ins außerhalb der Geschäftszeiten oder während eines Wartungszeitfensters durchgeführt wird.

1. Klicken Sie auf der Seite „Plug-in-Management“ auf **Plug-in hinzufügen**.

   Das Dialogfeld „Öffnen“ wird angezeigt, damit Sie eine lokale Datei auswählen können.

2. Navigieren Sie zur Plug-in-Datei, wählen Sie diese aus und klicken Sie auf **Öffnen**.

   Die Plug-in-Datei wird hochgeladen und installiert. Die Website wird automatisch neu gestartet, um die Installation abzuschließen.

Plug-ins aktualisieren

Wenn eine Aktualisierung verfügbar ist, wird neben dem Link **Updates** eine Zahl angezeigt.

> Diese Funktion ist für Hub On-Premises Installationen nur unmittelbar nach einem Upgrade verfügbar. Die On-Premises-Version kann zwischen Upgrades nicht online nach Aktualisierungen suchen.

1. Klicken Sie auf der Seite „Plug-in-Management“ auf **Updates**.

   Die potenziellen Aktualisierungen werden mit Details der neuen Version angezeigt.

2. Klicken Sie auf **Alle aktualisieren**, um alle Plug-ins zu aktualisieren.

   Es wird eine Meldung mit der Bestätigung angezeigt, dass die Plug-ins aktualisiert wurden.

3. Klicken Sie auf **OK**.

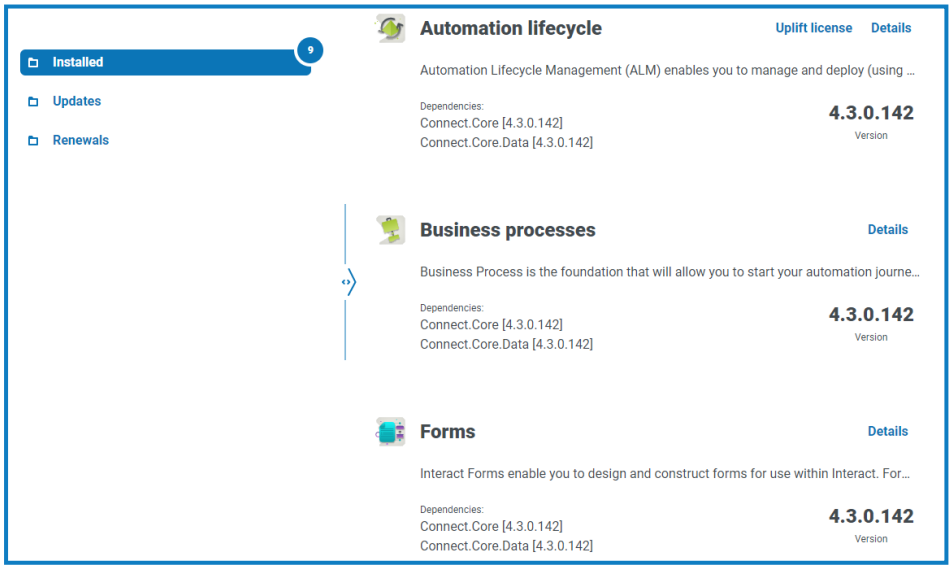
   Die Site wird neu gestartet.

Lizenz upgraden

Die Option **Lizenz upgraden** ist nur verfügbar, wenn sich das von einem Plug-in verwendete Lizenzmodell zwischen den veröffentlichten Versionen geändert hat. Damit können Sie eine neue Lizenz für Ihr Plug-in außerhalb des normalen Erneuerungszeitraums laden.

1. Klicken Sie auf der Seite „Plug-in-Management“ auf **Installiert**.

   Die installierten Plug-ins werden angezeigt.



2. Klicken Sie für das erforderliche Plug-in auf **Lizenz upgraden**. Oben im Beispiel wird die Option für den automatisierten Lebenszyklus angezeigt.

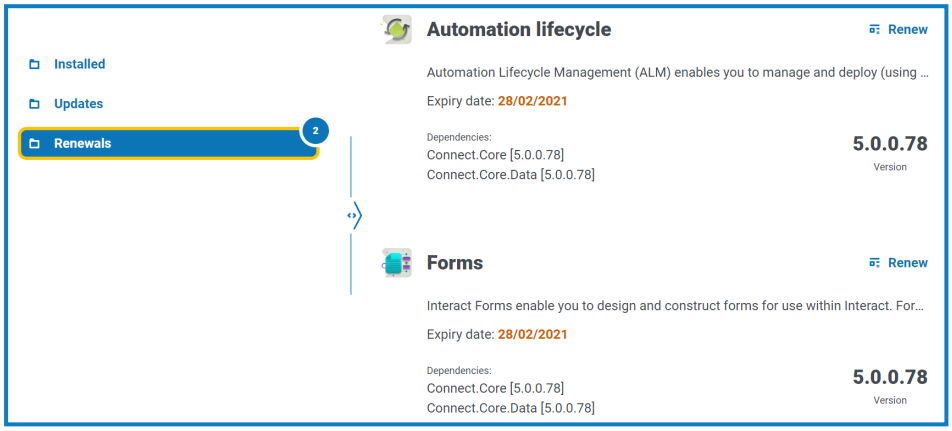
   Der Bereich „Lizenzschlüssel erneuern“ wird angezeigt.

3. Laden Sie eine gültige Lizenz hoch und klicken Sie auf **Fertig stellen**, um sie anzuwenden.

Plug-ins erneuern

Sie werden 14 Tage im Voraus benachrichtigt, bevor die Lizenz abläuft.

1. Klicken Sie auf der Seite „Plug-in-Management“ auf **Erneuerungen**.
   Die ablaufenden Plug-ins werden angezeigt.

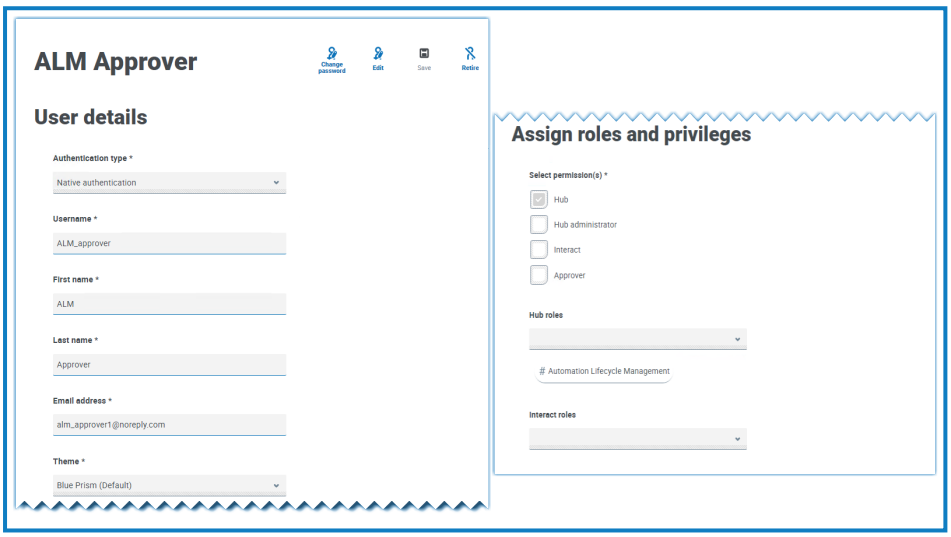


2. Klicken Sie neben dem erforderlichen Plug-in auf **Erneuern**.
3. Laden Sie eine gültige Lizenz hoch und klicken Sie auf **Fertig stellen**, um sie anzuwenden.

Benutzer

Über die Benutzereinstellungen können Sie Benutzerkonten in Hub basierend auf ihrem Authentifizierungstyp verwalten. Dies kann eine native Authentifizierung für native Benutzer oder eine Windows-Authentifizierung für Active Directory-Benutzer sein. Sie können auch den Zugriff des Benutzers auf Hub und Interact sowie seine Rollen darin festlegen. Bevor Sie Benutzer konfigurieren, sollten Sie die Benutzerrollen konfigurieren.

Die Seite „Benutzer“ zeigt eine Liste der vorhandenen Benutzer an. Sie können auf einen Benutzer klicken, um seine Informationen anzuzeigen. Wenn in Ihrer Umgebung nur die native Authentifizierung konfiguriert wurde, ist das Feld „Authentifizierungstyp“ ausgeblendet.



Zum Öffnen der Seite „Benutzer“ klicken Sie auf Ihr Profilsymbol, um die Seite „Einstellungen“ zu öffnen. Klicken Sie dann auf **Benutzer**.

Benutzer suchen

Die Seite „Benutzer“ bietet zwei Methoden zur Benutzersuche:

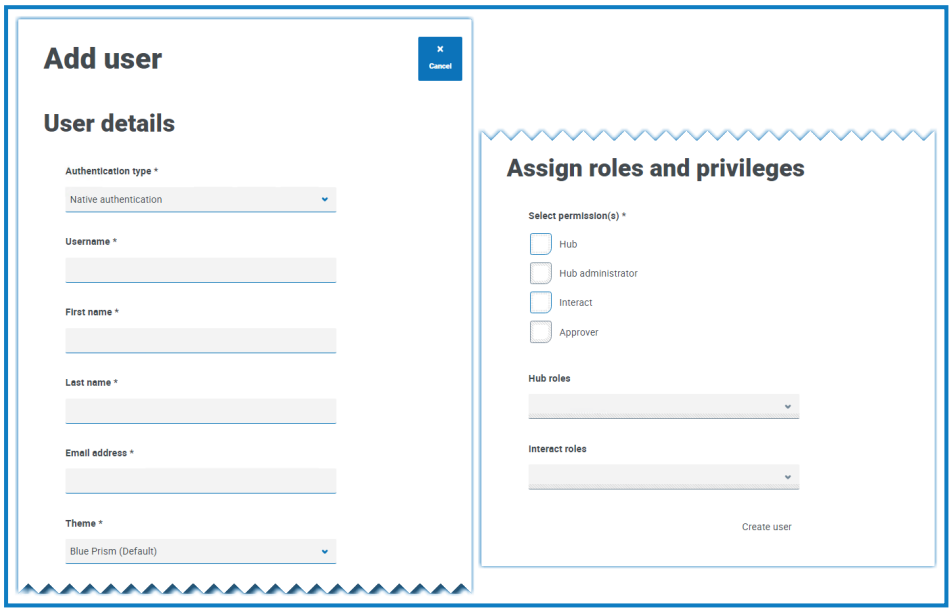
- **Feld**Benutzername durchsuchen – Befindet sich über der Benutzerliste. Geben Sie einen Benutzernamen ein, um die Sucherergebnisse zu filtern. Die Liste wird dynamisch gefiltert, wenn Sie weitere Zeichen eingeben.
- **Filter** – Mit Filtern können Sie auf schnelle Weise bestimmte Benutzer oder Benutzertypen anhand ausgewählter Kriterien finden. Klicken Sie auf **Filter**, um die Filter anzuzeigen und zu verwenden. Standardmäßig sind die Filter so eingestellt, dass sie Ihnen nur die „Live“-Benutzer und nicht die zurückgezogenen Benutzer anzeigen. Wenn Sie alle Benutzer sehen möchten, schalten Sie den Filter **Live** aus. Weitere Informationen finden Sie unter Filter auf der Seite „Benutzer“ verwenden auf Seite 32.

Benutzer hinzufügen

Nativen Benutzer hinzufügen

1. Klicken Sie auf der Seite „Benutzer“ auf **Benutzer hinzufügen**.

   Der Bereich „Benutzer hinzufügen“ wird angezeigt.



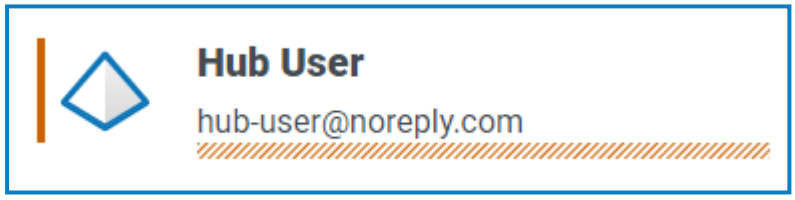
2. Geben Sie die Details des Benutzers ein:
   - **Authentifizierungstyp** (falls angezeigt) – Wählen Sie **Native Authentifizierung** aus.

     Dieses Feld wird nur angezeigt, wenn sowohl die native als auch die Windows-Authentifizierung in Ihrer Umgebung konfiguriert wurden. Wenn nur die native Authentifizierung konfiguriert wurde, ist der hinzugefügte Benutzer standardmäßig ein nativer Benutzer.

   - **Benutzername** – Geben Sie einen Benutzernamen für den Benutzer ein.
   - **Vorname** – Geben Sie den Vornamen des Benutzers ein.
   - **Nachname** – Geben Sie den Nachnamen des Benutzers ein.
   - **E-Mail-Adresse** – Geben Sie die E-Mail-Adresse des Benutzers ein.
   - **Design** – das Standarddesign wird automatisch ausgewählt. Sie können ein anderes Design für den Benutzer auswählen. Siehe Personalisierung auf Seite 20 für weitere Informationen zu Designs.

3. Wählen Sie die Berechtigungen für den Benutzer aus:
   - **Hub** – Aktivieren Sie dieses Kontrollkästchen für standardmäßige Hub Benutzer und Administratoren.
   - **Hub Administrator** – Aktivieren Sie dieses Kontrollkästchen, um der Benutzerrolle Administratorberechtigungen zu erteilen. Sie müssen **Hub** auswählen, damit diese Option verfügbar wird.
   - **Interact** – Aktivieren Sie dieses Kontrollkästchen, damit dem Benutzer Interact Formulare zugewiesen werden können. Weitere Informationen finden Sie unter Interact Benutzerhandbuch.
   - **Genehmiger** – Aktivieren Sie dieses Kontrollkästchen, um der Benutzerrolle die Genehmigungsrechte für Interact zu erteilen. Sie müssen **Interact** auswählen, damit diese Option verfügbar wird.
4. Wählen Sie die Rollen für den Benutzer aus:
   - **Hub Rollen** – Wählen Sie die Hub Rollen aus, die für den Benutzer erforderlich sind. Wenn die erforderliche Rolle noch nicht erstellt wurde, können Sie den Benutzer zu einem späteren Zeitpunkt bearbeiten, um neue Rollen zuzuweisen.

     Wenn ein Benutzer ohne Hub Rolle erstellt wird, wird er in der Benutzerliste unterstrichen, um anzuzeigen, dass die Benutzereinrichtung nicht abgeschlossen wurde, zum Beispiel:

     Der Benutzer kann sich bei Hub anmelden, kann jedoch keine Aufgaben durchführen, da er keinen Zugriff auf Plug-ins hat.
   - **Interact Rollen** – Wählen Sie die für den Benutzer erforderlichen Interact Rollen aus. Wenn die erforderliche Rolle noch nicht erstellt wurde, können Sie den Benutzer zu einem späteren Zeitpunkt bearbeiten, um neue Rollen zuzuweisen. Sie können mehr als eine Rolle auswählen.

> Benutzer können auch auf der Seite Rollen und Berechtigungen zu Rollen hinzugefügt werden.

5. Klicken Sie auf **Benutzer erstellen**.

   Das Dialogfeld „Passwort erstellen“ wird angezeigt.
6. Wählen Sie eine der Passwortoptionen aus:
   - **E-Mail zur Passwortaktualisierung an Benutzer senden** – Sendet dem Benutzer eine E-Mail mit einem Link und fordert ihn auf, ein Passwort für die Anmeldung einzugeben.
   - **Benutzerpasswort manuell aktualisieren** – Legen Sie selbst ein Passwort für den Benutzer fest.

> Passwörter müssen den Einschränkungen von Hub entsprechen. Weitere Informationen finden Sie unter Hub Einschränkungen auf Seite 6.

7. Klicken Sie auf **Weiter**
   - Wenn Sie ausgewählt haben, dem Benutzer eine E-Mail zur Aktualisierung des Passworts zu senden, klicken Sie im Bestätigungsdialog auf **Fertigstellen**.
   - Wenn Sie die Festlegung eines Passworts für den Benutzer ausgewählt haben, legen Sie ein Passwort fest und klicken Sie auf **Erstellen**.

Der neue Benutzer wird in der Liste der Benutzer angezeigt.

Active Directory-Benutzer hinzufügen

Um einen Active Directory-Benutzer hinzuzufügen, muss die Windows-Authentifizierung für Ihre Umgebung konfiguriert und die Active Directory-Authentifizierung auf der Seite „Authentifizierungseinstellungen“ aktiviert sein. Weitere Informationen finden Sie unter Authentifizierungseinstellungen auf Seite 45.

Sie können einen Active Directory-Benutzer hinzufügen, indem Sie die folgenden Schritte befolgen oder eine Active Directory-Sicherheitsgruppe zu einer Rolle hinzufügen, in der Benutzer, die Mitglieder der Sicherheitsrolle sind, automatisch zu Hub hinzugefügt werden, wenn sie sich zum ersten Mal anmelden. Weitere Informationen erhalten Sie unter Active Directory-Sicherheitsgruppen zu einer Rolle hinzufügen auf Seite 38.

1. Klicken Sie auf der Seite „Benutzer“ auf **Benutzer hinzufügen**.

   Der Bereich „Benutzer hinzufügen“ wird angezeigt.
2. Wählen Sie im Feld **Authentifizierungstyp** die Option **Windows-Authentifizierung** aus.
3. Klicken Sie auf **Active Directory durchsuchen**.

   Der Bereich „Active Directory durchsuchen“ wird geöffnet.

   > Bevor Sie nach Benutzern in Active Directory suchen, stellen Sie sicher, dass ein Benutzername (UPN) und eine E-Mail-Adresse für sie in Active Directory ausgefüllt sind.
4. Geben Sie den Suchpfad für den Active Directory-Benutzer ein, den Sie hinzufügen möchten. Dies ist der Distinguished Name des Stamm-Speicherorts, z. B. dc=bvdevops,dc=co,dc=uk.

   Sie können auch die Platzhaltersuche verwenden und Suchfilter anwenden, basierend auf:

   - **CN** – Das Attribut für den allgemeinen Namen enthält Namen eines Objekts. Wenn das Objekt einer Person entspricht, ist es typischerweise der vollständige Name der Person.
   - **UPN** – Ein Benutzerprinzipalname ist der Name eines Systembenutzers in einem E-Mail-Adressformat. Ein UPN besteht aus dem Benutzernamen (Anmeldename), einem Trennzeichen (das @-Symbol) und einem Domäne-Namen (UPN-Suffix), zum Beispiel john.doe@domain.com.
   - **SID** – Eine Sicherheitsidentifikation ist ein eindeutiger unveränderlicher Kennzeichner eines Benutzers, einer Benutzergruppe oder eines Sicherheitsprinzipals. Ein Sicherheitsprinzipal verfügt (in einer bestimmten Domain) über einen einzigen SID für seine Lebensdauer und alle Eigenschaften des Prinzipals, darunter auch sein Name, sind dem SID zugeordnet.

5. Nachdem Sie die Suchkriterien eingegeben haben, klicken Sie auf **Suchen**.

> Beim Durchsuchen von Active Directory nach Benutzern oder Sicherheitsgruppen in Hub werden die für die Domain in der Authentication Server Datenbank gespeicherten Anmeldedaten verwendet. Wenn keine gespeicherten Anmeldedaten gefunden werden, werden Abfragen, die eine zusätzliche Authentifizierung erfordern, im Kontext des Windows-Kontos ausgeführt, auf dem der Authentication Server Anwendungspool in IIS ausgeführt wird.

Die verfügbaren Benutzer werden angezeigt. Sie können nach unten scrollen, um alle abgerufenen Benutzer anzuzeigen.

6. Wählen Sie den Benutzer aus, den Sie hinzufügen möchten, und klicken Sie auf **Anwenden**. Sie können jeweils nur einen Benutzer auswählen. Zuvor hinzugefügte Benutzer werden ausgegraut angezeigt und können nicht ausgewählt werden.
7. Wählen Sie auf der Seite „Einen Benutzer hinzufügen“ die Berechtigungen und Rollen für den neuen Benutzer aus (siehe Schritte 3 und 4 im Abschnitt „Einen nativen Benutzer hinzufügen“) und klicken Sie auf **Benutzer erstellen**.

Der neue Benutzer wird in der Liste der Benutzer angezeigt.

> Die Anmeldeinformationen der Active Directory-Benutzer werden in Active Directory verwaltet, sodass Sie kein Passwort für den Benutzer erstellen müssen. Diese Benutzer können sich mit Single Sign-on bei Hub anmelden, indem sie auf der Anmeldeseite die Option **Mit Active Directory anmelden** auswählen.

Benutzer bearbeiten

1. Wählen Sie auf der Seite „Benutzer“ den gewünschten Benutzer aus und klicken Sie auf **Bearbeiten**.
2. Ändern Sie die Informationen nach Bedarf.

   Wenn der Benutzer:

   - ein nativer Benutzer ist, können Sie die Informationen nach Bedarf ändern.
   - ein Active Directory-Benutzer ist, können Sie nur seine Rollen und Berechtigungen ändern. Alle anderen Details werden in Active Directory verwaltet.

   > Der Benutzername kann nicht geändert werden.

3. Klicken Sie auf **Speichern**, um Ihre Änderungen zu übernehmen.

Active Directory-Benutzer synchronisieren

1. Wählen Sie auf der Seite „Benutzer“ den gewünschten Active Directory-Benutzer aus.
2. Klicken Sie auf **Benutzer synchronisieren**.

Die folgenden Details eines Active Directory-Benutzers werden aktualisiert: UPN, Benutzername, vollständiger Name, E-Mail-Adresse und Status (aktiv, gelöscht oder deaktiviert).

Native Benutzer zurückziehen

1. Wählen Sie auf der Seite „Benutzer“ den gewünschten Benutzer aus und klicken Sie auf **Zurückziehen**.

   Eine Nachricht wird angezeigt, in der Sie zur Bestätigung aufgefordert werden.

   > Sie können den Filter **Live** verwenden, um die Benutzerliste nach zurückgezogenen Benutzern zu filtern. Siehe Benutzer suchen auf Seite 25.

2. Klicken Sie auf **Ja**.

   Der Benutzer wird zurückgezogen und das Symbol **Zurückziehen** wird durch das Symbol **Live schalten** ersetzt. Sie können es verwenden, um den Benutzer bei Bedarf wiederherzustellen. Außerdem wird der Benutzer in der Benutzerliste unterstrichen angezeigt, um darauf hinzuweisen, dass er zurückgezogen wurde.

Native Benutzer entsperren

Wenn ein Benutzer sein Passwort fünfmal falsch eingibt, kann er für drei Stunden nicht auf das System zugreifen. Sie können das Konto allerdings für den Benutzer entsperren.

1. Wählen Sie auf der Seite „Benutzer“ den gewünschten Benutzer aus und klicken Sie auf **Entsperren**.

   Es wird eine Benachrichtigung angezeigt, die bestätigt, dass der Benutzer erfolgreich entsperrt wurde.

   > Sie können den Filter **Gesperrt** verwenden, um die Benutzerliste nach gesperrten Benutzern zu filtern. Siehe Benutzer suchen auf Seite 25.

Passwort für native Benutzer ändern

Native Benutzer können ihr Passwort auf der Seite „Profil“ selbst ändern (weitere Informationen finden Sie unter Profil auf Seite 9). Sollte ein Benutzer sein Passwort vergessen haben, kann er den Link **Passwort vergessen** auf der Anmeldeseite verwenden. Bei Bedarf können jedoch auch Sie das Passwort der Benutzer ändern. Dies ist zum Beispiel möglich, wenn ein Benutzer, der das Unternehmen verlassen hat, ein Interact Genehmiger war und es noch ausstehende Formulare in Interact gibt, die von diesem Benutzer genehmigt werden müssen. Abhängig von den Richtlinien Ihrer Organisation können Sie auf ihr Konto zugreifen und diese bearbeiten.

1. Wählen Sie auf der Seite „Benutzer“ den gewünschten Benutzer aus und klicken Sie auf **Passwort ändern**.

   Der Bildschirm „Passwort ändern“ wird angezeigt.
2. Geben Sie in beiden Feldern ein neues Passwort für den Benutzer ein. Das Passwort muss den Zeichenbeschränkungen entsprechen. Die Einschränkungen hinsichtlich der Wiederverwendung von Passwörtern gelten jedoch nicht. Weitere Informationen finden Sie unter Hub Einschränkungen auf Seite 6.
3. Klicken Sie auf **Absenden**.

   Es wird eine Benachrichtigung angezeigt, die bestätigt, dass das Passwort des Benutzers geändert wurde.

Filter auf der Seite „Benutzer“ verwenden

Mit Filtern können Sie auf schnelle Weise bestimmte Benutzer oder Benutzertypen anhand ausgewählter Kriterien finden.

1. Klicken Sie auf der Seite „Benutzer“ auf **Filter**, um den Filter-Bereich zu öffnen.
2. Verwenden Sie den Umschalter, um den erforderlichen Filter zu aktivieren, und geben Sie die Informationen ein, um den Benutzer zu finden. Sie können mehrere Filter gleichzeitig anwenden.

   Die verfügbaren Filter sind:

Filter	Beschreibung
Vollständiger Name	Geben Sie den vollständigen Namen des Benutzers oder einen Teil seines vollständigen Namens ein.
E-Mail-Adresse	Geben Sie die E-Mail-Adresse des Benutzers oder einen Teil seiner E-Mail-Adresse ein.
Gesperrt	Wählen Sie den gesperrten Status des Benutzers aus der Dropdown-Liste aus. Die Optionen lauten: • **Gesperrt** – Zeigt alle Benutzer an, deren Konten gesperrt wurden. • **Entsperrt** – Zeigt alle Benutzer mit entsperrten Konten an.

Filter	Beschreibung
Live	Wählen Sie den Live-Status des Benutzers aus der Dropdown-Liste aus. Die Optionen lauten: • **Live** – Zeigt alle Benutzer an, die über aktive Anmeldedaten verfügen. • **Zurückgezogen** – Zeigt alle Benutzer an, die vom Administrator zurückgezogen wurden und sich nicht mehr anmelden können. Standardmäßig ist der Filter **Live** bereits aktiviert. Sie können ihn deaktivieren, wenn Sie alle Benutzer anzeigen möchten.
Einrichtungsstatus	Wählen Sie den Setup-Status des Benutzers aus der Dropdown-Liste aus. Die Optionen lauten: • **Richtig eingerichtet** – Zeigt alle Benutzer an, die innerhalb von Hub korrekt eingerichtet sind, d. h. sie verfügen über vollständige Anmeldedaten und ihnen sind Rollen zugewiesen. • **Erfordert Maßnahmen** – Zeigt alle Benutzer an, deren Benutzerkonten nicht korrekt konfiguriert sind, zum Beispiel fehlen möglicherweise ihre Rollen.
Domain	Geben Sie den Namen einer Domain oder einen Teil eines Namens ein. Dieser wird mit Domain-Namen abgeglichen, die auf der Seite Authentifizierungseinstellungen angegeben sind, und zeigt alle Benutzer an, die von der übereinstimmenden Domain in Hub importiert wurden. Wenn Sie einen Teil eines Domäne-Namens eingegeben haben, werden die Ergebnisse für alle teilweisen Übereinstimmungen angezeigt. Neben den beabsichtigten Benutzern können auch Benutzer aus anderen Domains angezeigt werden.
Verbindungsname	Geben Sie den Namen einer Verbindung oder einen Teil davon ein. Dieser wird mit Verbindungsnamen abgeglichen, die auf der Seite Authentifizierungseinstellungen angegeben sind, und zeigt alle Benutzer an, die über die übereinstimmende Verbindung in Hub importiert wurden. Wenn Sie einen Teil eines Verbindungsnamens eingegeben haben, werden die Ergebnisse für alle teilweisen Übereinstimmungen angezeigt. Neben den beabsichtigten Benutzern können auch Benutzer aus anderen Verbindungen angezeigt werden.

Filter	Beschreibung
Zugriff	Wählen Sie die Zugriffsstufe des Benutzers in der Dropdown-Liste aus. Diese basieren auf der Berechtigungsstufe des Benutzers. Die Optionen lauten: • **Hub** – Zugriff auf Hub. • **Interact** – Zugriff auf Interact. • **Genehmiger** – Zugriff auf Interact mit Genehmiger-Berechtigungen.
Hub Rolle(n)	Geben Sie den Namen einer Rolle oder einen Teil davon ein. Dadurch wird nach allen Rollen gesucht, für die Hub als Rollentyp festgelegt ist.
Interact Rolle(n)	Geben Sie den Namen einer Rolle oder einen Teil des Rollennamens ein. Dadurch wird nach allen Rollen gesucht, für die Interact als Rollentyp festgelegt ist.
Themen	Wählen Sie das Thema aus der Dropdown-Liste aus. Die Benutzer, die das ausgewählte Thema haben, werden angezeigt.

Die Informationen auf der Seite „Benutzer“ werden sofort gefiltert.

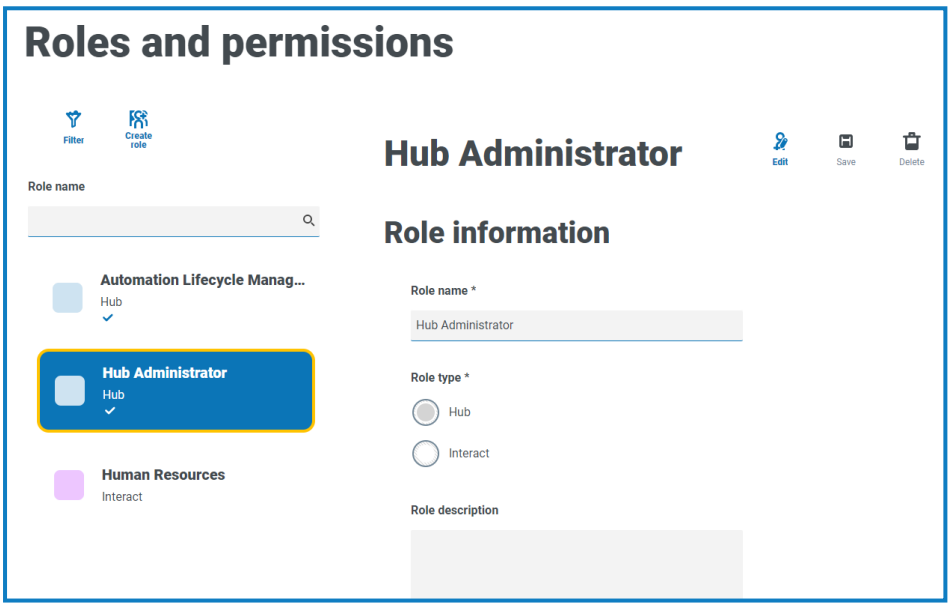
Wenn Sie die Filter eingestellt haben, aber die ungefilterten Informationen noch einmal anzeigen möchten, schalten Sie entweder die erforderlichen Filter aus oder entfernen Sie alle Einstellungen innerhalb des Filters, damit er leer ist.

3. Klicken Sie auf **Bereich schließen**, um den Filter-Bereich zu schließen.

Rollen und Berechtigungen

Mit Rollen und Berechtigungen können Sie Rollen erstellen und Berechtigungen bestimmten Bereichen von Hub oder Interact für diese Rollen zuweisen. Dieser Bereich ist nur für Administratoren verfügbar. Bevor Sie Benutzer konfigurieren, sollten Sie die Benutzerrollen konfigurieren. Wenn Rollen nicht konfiguriert sind, können sich die Benutzer anmelden, aber ohne eine zugewiesene Rolle werden ihnen nur begrenzt Informationen angezeigt und sie erhalten keinen Zugriff auf Funktionen.

Die Seite „Rollen und Berechtigungen“ zeigt eine Liste der vorhandenen Rollen an. Es gibt vordefinierte Rollen, die automatisch im Rahmen der Hub Installation erstellt werden. Diese werden durch ein blaues Häkchen angezeigt, zum Beispiel die Rolle „Hub Administrator“. Diese automatisch erstellten vordefinierten Rollen sind gesperrt und können nicht geändert oder gelöscht werden, auch wenn Sie ihnen Benutzer hinzufügen können. Durch das Anklicken einer Rolle werden die Berechtigungen angezeigt.



Zum Öffnen der Seite „Rollen und Berechtigungen“ klicken Sie auf Ihr Profilsymbol. Daraufhin wird die Seite „Einstellungen“ geöffnet. Klicken Sie dann auf **Rollen und Berechtigungen**.

Rollen finden

Die Seite „Rollen und Berechtigungen“ enthält zwei Methoden zum Auffinden von Rollen:

- **Feld Rollenname durchsuchen** – Befindet sich über der Rollenliste. Beginnen Sie mit der Eingabe des Namens einer Rolle, um die Suchergebnisse zu filtern. Die Liste wird dynamisch gefiltert, wenn Sie weitere Zeichen eingeben.
- **Filter** – Mit den Filtern können Sie eine bestimmte Rolle oder Rollen mit bestimmten Berechtigungen basierend auf den ausgewählten Kriterien einfach auffinden. Klicken Sie auf **Filter**, um die Filter anzuzeigen und zu verwenden. Weitere Informationen finden Sie unter Filter auf der Seite „Rollen und Berechtigungen“ verwenden auf Seite 41.

Rollen hinzufügen

Basierend auf dem Authentifizierungstyp und den Einstellungen, die für Ihre Umgebung auf der Seite Authentifizierungseinstellungen konfiguriert sind, gibt es mehrere Möglichkeiten, Benutzer zu der Rolle hinzuzufügen, die Sie erstellen:

- Wenn die native Authentifizierung aktiviert ist, können Sie native Benutzer direkt zu einer Rolle hinzufügen.
- Wenn die Active Directory-Authentifizierung aktiviert ist, können Sie:
  - Active Directory-Benutzer direkt zu einer Rolle hinzufügen – **Zulassen, dass Active Directory-Benutzer direkt zu Rollen hinzugefügt werden** muss auf der Seite „Authentifizierungseinstellungen“ aktiviert sein.
  - Active Directory-Sicherheitsgruppen zu einer Rolle hinzufügen – **Autorisierung über Mitgliedschaft in Active Directory-Sicherheitsgruppen zulassen** muss auf der Seite „Authentifizierungseinstellungen“ aktiviert sein.

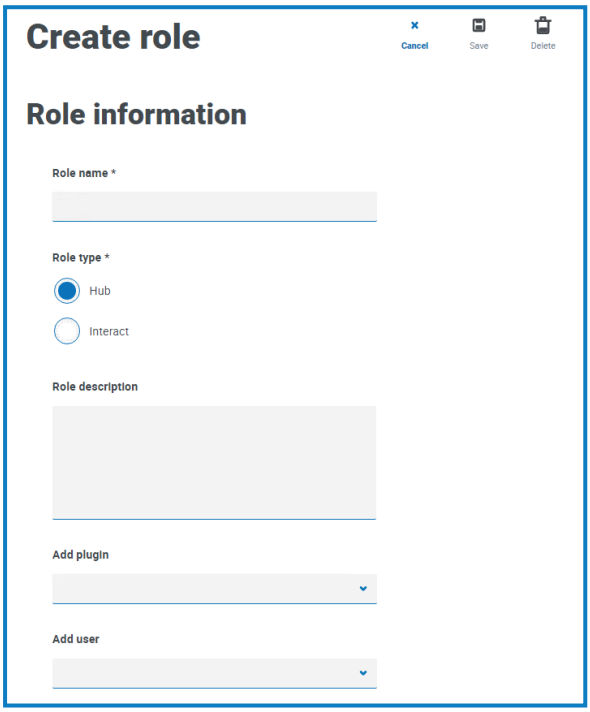
    ⚠ Wenn Sie Interact mit Active Directory verwenden, beachten Sie, dass einige Aktionen im Interact Web-API-Dienst die Verwendung von Sicherheitsgruppen nicht unterstützen. Alle Aktionen unterstützen Active Directory-Benutzer, die Interact Rollen direkt zugewiesen werden. Weitere Informationen finden Sie unter Interact Web-API-Dienst Benutzerhandbuch.

Benutzer direkt zu einer Rolle hinzufügen

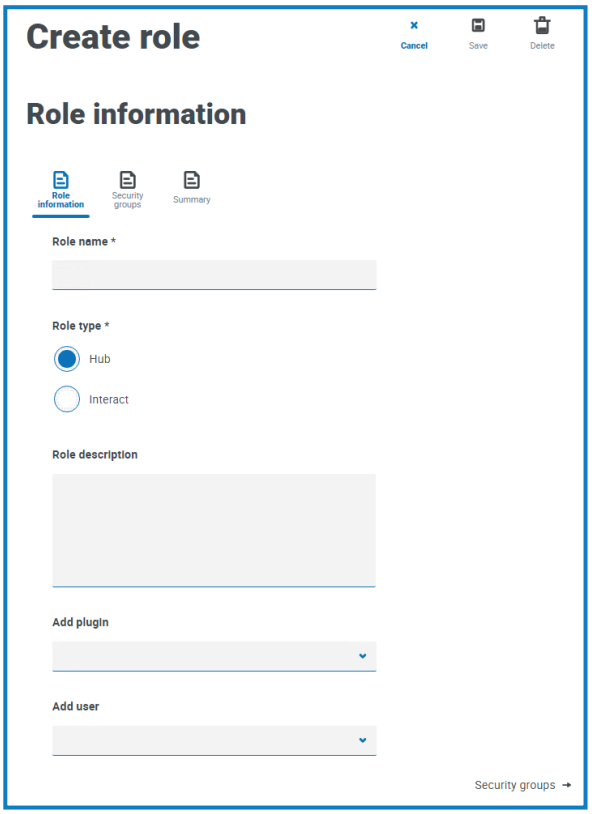
1. Klicken Sie auf der Seite „Rollen und Berechtigungen“ auf **Rolle erstellen**.

   Der Abschnitt „Rolle erstellen“ wird angezeigt. Wenn die Umgebung so konfiguriert ist, dass Active Directory-Sicherheitsgruppen zu Rollen hinzugefügt werden können, zeigt diese Seite drei Registerkarten an: Rolleninformationen, Sicherheitsgruppen und Zusammenfassung.

   Beispielseite, wenn AD-Sicherheitsgruppen nicht zu Rollen hinzugefügt werden können:

   Beispielseite, wenn AD-Sicherheitsgruppen zu Rollen hinzugefügt werden können:

2. Geben Sie einen Rollennamen ein und wählen Sie aus, ob er für **Hub** oder **Interact** gültig ist.
3. Falls erforderlich, geben Sie eine Beschreibung ein.
4. Wählen Sie die Elemente aus, auf welche die Rolle Zugriff haben soll. Wenn Sie folgende Auswahl getroffen haben:
   - **Hub**, dann wählen Sie die erforderlichen Plug-ins aus der Dropdown-Liste **Plug-in hinzufügen** aus.
   - **Interact**, dann wählen Sie die erforderlichen Formulare aus der Dropdown-Liste **Formulare hinzufügen** aus.

   Sie können mehr als ein Element aus der Liste auswählen.
5. Wählen Sie aus der Dropdown-Liste **Benutzer hinzufügen** die Benutzer aus, denen diese Rolle zugewiesen wird. In der Liste werden nur Benutzer angezeigt, die über entsprechende Berechtigungen verfügen, zum Beispiel, wenn die Rolle für Interact gilt, werden nur Interact Benutzer und keine Hub Benutzer angezeigt. Siehe Benutzer auf Seite 25 für weitere Informationen zu Benutzerberechtigungen.

   > Benutzer können auch auf der Seite Benutzer zu Rollen hinzugefügt werden.

6. Klicken Sie auf **Speichern**, um die Rolle zu erstellen.

Active Directory-Sicherheitsgruppen zu einer Rolle hinzufügen

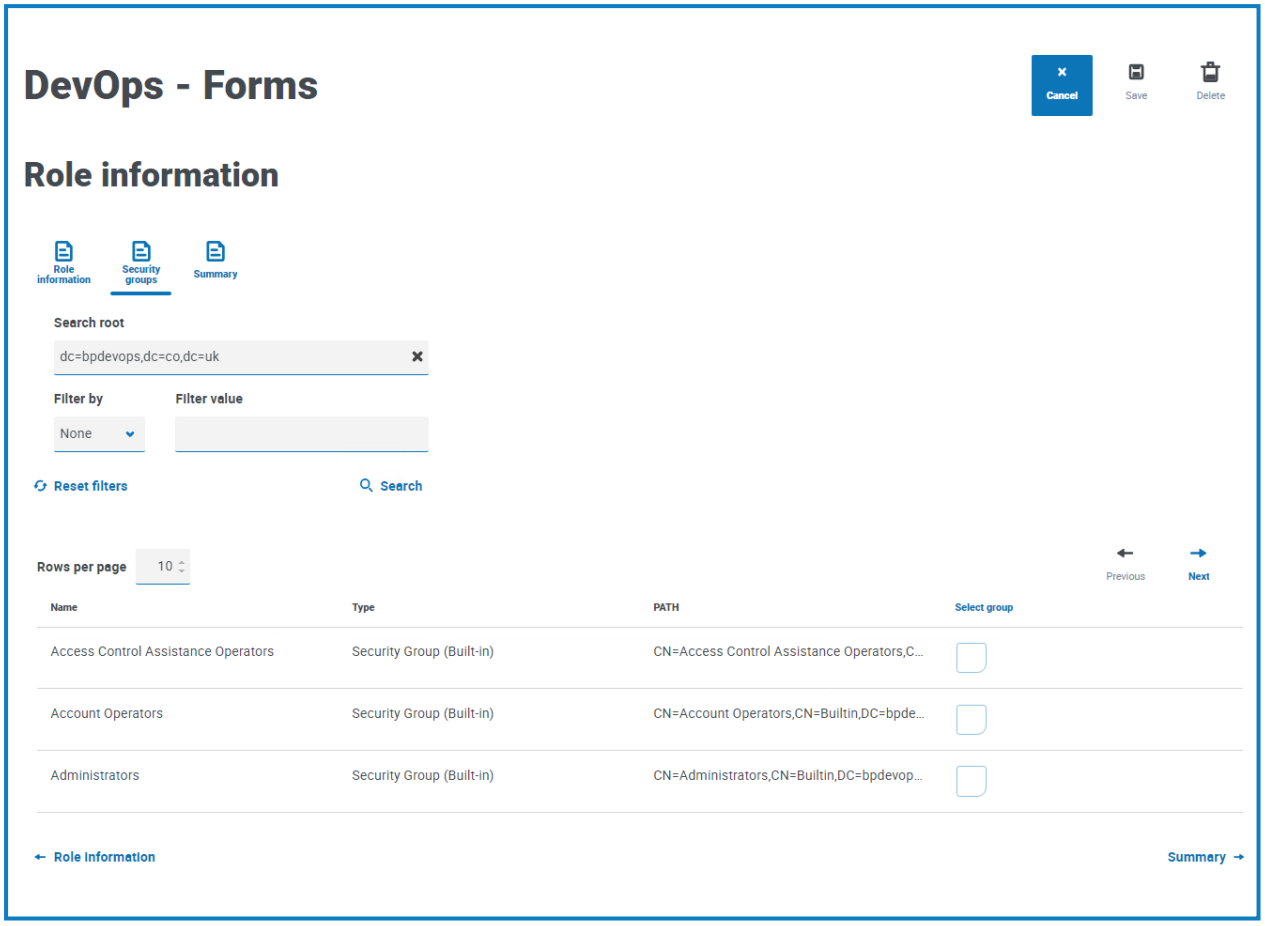
⚠ Wenn Sie Interact mit Active Directory verwenden, beachten Sie, dass einige Aktionen im Interact Web-API-Dienst die Verwendung von Sicherheitsgruppen nicht unterstützen. Alle Aktionen unterstützen Active Directory-Benutzer, die Interact Rollen direkt zugewiesen werden. Weitere Informationen finden Sie unter Interact Web-API-Dienst Benutzerhandbuch.

1. Klicken Sie auf der Seite „Rollen und Berechtigungen“ auf **Rolle erstellen**.

   Der Abschnitt „Rolle erstellen“ wird angezeigt.
2. Geben Sie auf der Registerkarte „Rolleninformationen“ einen Rollennamen ein und wählen Sie aus, ob er für **Hub** oder **Interact** gültig ist.
3. Falls erforderlich, geben Sie eine Beschreibung ein.
4. Wählen Sie die Elemente aus, auf welche die Rolle Zugriff haben soll. Wenn Sie folgende Auswahl getroffen haben:
   - **Hub**, dann wählen Sie die erforderlichen Plug-ins aus der Dropdown-Liste **Plug-in hinzufügen** aus.
   - **Interact**, dann wählen Sie die erforderlichen Formulare aus der Dropdown-Liste **Formulare hinzufügen** aus.

   Sie können mehr als ein Element aus der Liste auswählen.
5. Klicken Sie auf **Sicherheitsgruppen**.

6. Suchen Sie nach Sicherheitsgruppen, indem Sie den Distinguished Name des Stamm-Speicherorts eingeben, z. B. dc=bpdevops, dc=co, dc=uk.

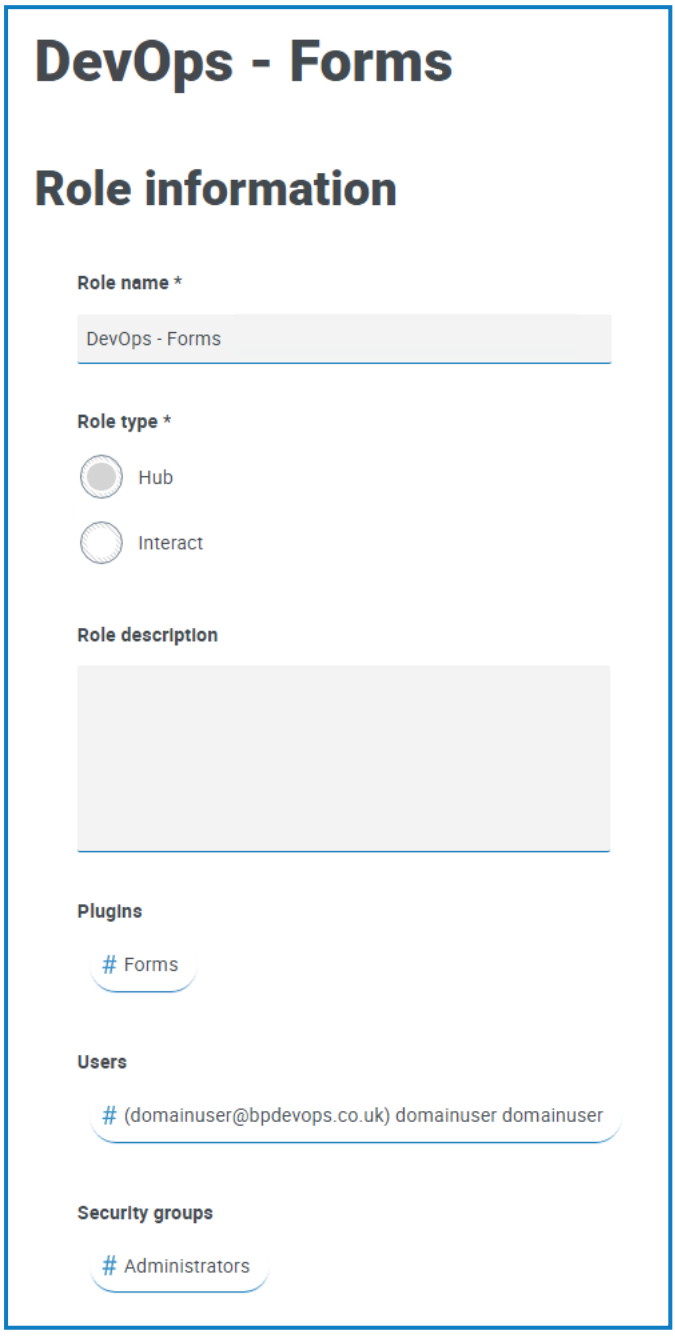


Sie können Suchfilter auf Grundlage von CN (allgemeiner Name), UPN (Benutzerprinzipalname) oder SID (Sicherheits-ID) anwenden oder mit Platzhaltern suchen. Für weitere Informationen siehe Active Directory-Benutzer hinzufügen auf Seite 29.

Sie können auch auf der Seite nach unten scrollen, auf **Weiter** oder **Zurück** klicken, um zwischen mehreren Seiten von Sicherheitsgruppen zu navigieren oder zwischen den Registerkarten „Rolleninformationen“ und „Zusammenfassung“ zu wechseln.

7. Wählen Sie die Gruppe(n) aus, die Sie der Rolle hinzufügen möchten, und klicken Sie auf **Speichern**.

   Die hinzugefügten Sicherheitsgruppen werden als Teil der Rolleninformationen angezeigt. Alle Benutzer, die Mitglieder der hinzugefügten Sicherheitsgruppen sind, werden automatisch zu der Rolle hinzugefügt und haben ein Konto in Hub erstellt, wenn sie sich zum ersten Mal anmelden.



Rollen bearbeiten

1. Wählen Sie auf der Seite „Rollen und Berechtigungen“ die gewünschte Rolle aus und klicken Sie auf **Bearbeiten**.
2. Ändern Sie die Informationen nach Bedarf, einschließlich Hinzufügen oder Entfernen von Benutzern und/oder Sicherheitsgruppen.

   Sie können den Rollentyp nicht ändern. Wenn Sie eine Rolle bearbeiten, für die ein blaues Häkchen angezeigt wird, können Sie nur die der Rolle zugewiesenen Benutzer ändern.
3. Klicken Sie auf **Speichern**, um Ihre Änderungen zu übernehmen.

Rollen löschen

Sie können eine Rolle, für die ein blaues Häkchen angezeigt wird, nicht löschen. Hierbei handelt es sich um eine Rolle, die bei der Installation von Hub oder einem Plug-in automatisch erstellt wurde.

1. Wählen Sie auf der Seite „Rollen und Berechtigungen“ die gewünschte Rolle aus und klicken Sie auf **Löschen**.

   Eine Nachricht wird angezeigt, in der Sie zur Bestätigung aufgefordert werden.
2. Klicken Sie auf **Ja**.

   Die Rolle wird gelöscht und eine Bestätigungsbenachrichtigung angezeigt.

Filter auf der Seite „Rollen und Berechtigungen“ verwenden

Mit Filtern können Sie auf schnelle Weise bestimmte Rollen anhand ausgewählter Kriterien finden.

1. Klicken Sie auf der Seite „Rollen und Berechtigungen“ auf **Filter**, um den Filter-Bereich zu öffnen.
2. Verwenden Sie den Umschalter, um den erforderlichen Filter zu aktivieren, und geben Sie die Informationen ein, um die gewünschte Rolle zu finden. Sie können mehrere Filter gleichzeitig anwenden.

   Die verfügbaren Filter sind:

Filter	Beschreibung
Typ	Wählen Sie den Rollentyp aus der Dropdown-Liste aus. Die Optionen sind: • **Hub** – Zeigt die Rollen an, für die Hub als Rollentyp festgelegt ist. • **Interact** – Zeigt die Rollen an, für die Interact als Rollentyp festgelegt ist.
Beschreibung	Geben Sie einen Begriff oder ein Wort ein, um in der Rollenbeschreibung nach dem Text zu suchen.

Filter	Beschreibung
Hub Plug-ins	Geben Sie den Namen des Plug-ins, nach dem Sie suchen möchten, oder einen Teil davon ein. Zum Beispiel: • **Automatisierungslebenszyklus** – Zeigt alle Rollen an, die Zugriff auf ALM haben. • **Formulare** – Zeigt alle Rollen an, die Zugriff auf Interact Formulare haben. • **Geschäftsprozess** – Zeigt alle Rollen an, die Zugriff auf das Geschäftsprozess-Plug-in haben. • **Control Room** – Zeigt alle Rollen an, die Zugriff auf Control Room haben.
Interact Formulare	Geben Sie den Namen des Interact Formulars, nach dem Sie suchen möchten, oder einen Teil davon ein.
Benutzer	Geben Sie einen Benutzernamen oder einen Teil davon ein, um die Rollen zu finden, die diesem Benutzer zugeordnet sind. Wenn Sie einen Teil eines Benutzernamens eingegeben haben, werden die Rollen für alle teilweisen Übereinstimmungen angezeigt. Dabei kann es sich auch um andere Benutzer als den beabsichtigten handeln.

Die Informationen auf der Seite „Rollen und Berechtigungen“ werden sofort gefiltert.

Wenn Sie die Filter eingestellt haben, aber die ungefilterten Informationen noch einmal anzeigen möchten, schalten Sie entweder die erforderlichen Filter aus oder entfernen Sie alle Einstellungen innerhalb des Filters, damit er leer ist.

3. Klicken Sie auf **Bereich schließen**, um den Filter-Bereich zu schließen.

Registrierungen

Auf der Seite „Registrierungen“ können Sie Registrierungsanfragen verwalten, die neue Benutzer für den Zugriff auf Interact erstellt haben. Dieser Bereich ist nur für Administratoren verfügbar.

Benutzer können ein Interact Benutzerkonto von der Registrierungsseite anfordern: https://{hostname}/#/user-registration

Auf der Seite „Registrierungen“ werden die eingereichten Registrierungsanfragen angezeigt, die Sie genehmigen oder ablehnen können.

Zum Öffnen der Seite „Registrierungen“ klicken Sie auf Ihr Profilsymbol. Die Seite „Einstellungen“ wird aufgerufen. Klicken Sie dann auf **Registrierungen**. Ein numerischer Wert wird gegenüber der Option „Registrierungen“ auf der Seite „Einstellungen“ angezeigt, wenn noch ausstehende Anfragen vorliegen.

Einen Antrag genehmigen

Dem Benutzer muss eine Rolle zugewiesen werden, bevor der Zugriff auf Formulare in Interact möglich ist. Sie können dies entweder als Teil des Genehmigungsprozesses tun, wie unten gezeigt, oder Sie können den Antrag genehmigen und dann den Benutzer bearbeiten.

1. Wählen Sie auf der Seite „Registrierungen“ den Benutzer aus und klicken Sie auf **Bearbeiten**.
2. Wählen Sie die gewünschte Rolle aus der Dropdown-Liste aus. Das ist das einzige Feld, das Sie bearbeiten können.
3. Klicken Sie auf **Speichern**.
4. Klicken Sie auf **Genehmigen**.

   Der Benutzer wird aus der Registrierungsliste entfernt und auf der Seite Benutzer dargestellt. Der Benutzer erhält eine E-Mail mit einem Link zur einmaligen Verwendung, um die Registrierung durch Eingabe eines Passworts abzuschließen. Daraufhin kann er auf Interact zugreifen.

Eine Anfrage ablehnen

1. Wählen Sie auf der Seite „Registrierungen“ den Benutzer aus und klicken Sie auf **Verweigern**.

   Die Zugriffsanforderung wird abgelehnt und die Benutzerdetails werden aus der Liste entfernt.

Filter auf der Seite „Registrierungen“ verwenden

Mit Filtern können Sie auf schnelle Weise bestimmte Benutzer anhand ausgewählter Kriterien finden.

1. Klicken Sie auf der Seite „Registrierungen“ auf **Filter**, um den Filter-Bereich zu öffnen.
2. Verwenden Sie den Umschalter, um den erforderlichen Filter zu aktivieren, und geben Sie die Informationen ein, um den Benutzer zu finden. Sie können mehrere Filter gleichzeitig anwenden.

   Die verfügbaren Filter sind:

Filter	Beschreibung
Vollständiger Name	Geben Sie den vollständigen Namen des Benutzers oder einen Teil seines vollständigen Namens ein.

Filter	Beschreibung
E-Mail-Adresse	Geben Sie die E-Mail-Adresse des Benutzers oder einen Teil seiner E-Mail-Adresse ein.
Interact Rolle(n)	Geben Sie den Namen einer Rolle oder einen Teil des Rollennamens ein. Dadurch wird nach allen Rollen gesucht, für die Interact als Rollentyp festgelegt ist.

Die Informationen auf der Seite „Registrierungen“ werden sofort gefiltert.

Wenn Sie die Filter eingestellt haben, aber die ungefilterten Informationen noch einmal anzeigen möchten, schalten Sie entweder die erforderlichen Filter aus oder entfernen Sie alle Einstellungen innerhalb des Filters, damit er leer ist.

3. Klicken Sie auf **Bereich schließen**, um den Filter-Bereich zu schließen.

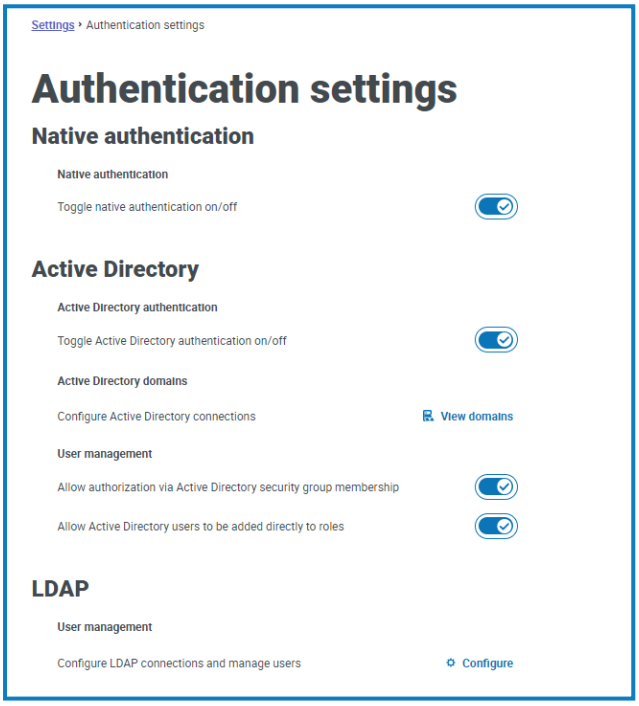
Authentifizierungseinstellungen

Sie können die Authentifizierungseinstellungen Ihres Unternehmens mithilfe der folgenden Optionen konfigurieren:

- Native Authentifizierung
- Active Directory-Authentifizierung
- LDAP

Dieser Bereich ist nur für Administratoren verfügbar.

Um die Seite mit den Authentifizierungseinstellungen zu öffnen, klicken Sie auf Ihr Profilsymbol, um die Seite „Einstellungen“ zu öffnen, und klicken Sie dann auf **Authentifizierungseinstellungen**.



Native Authentifizierung

Die native Authentifizierung ist standardmäßig auf der Seite „Authentifizierungseinstellungen“ in neuen Umgebungen oder beim Upgrade des Hubs aktiviert.

So können Sie die native Authentifizierung aktivieren/deaktivieren:

1. Verwenden Sie den Schieberegler, um zur gewünschten Position zu wechseln:
   - Kreuz = deaktiviert
   - Häkchen = aktiviert
2. Klicken Sie in der Bestätigungsmeldung zum Akzeptieren auf **OK**.

Sie können die native Authentifizierung nur deaktivieren, wenn mindestens ein Hub Administrator im System vorhanden ist, der sich mit einer der anderen Authentifizierungsmethoden anmelden kann.

Sie können native Benutzer auf der Seite Benutzer hinzufügen hinzufügen. Diese können sich bei Hub anmelden, indem sie ihren Benutzernamen und ihr Passwort eingeben.

Active Directory-Authentifizierung

Die Active Directory-Authentifizierung kann nur auf der Seite „Authentifizierungseinstellungen“ aktiviert werden, wenn der Server, der Authentication Server hostet, Mitglied einer Active Directory-Domain ist.

So können Sie die Active Directory-Authentifizierung aktivieren/deaktivieren:

1. Verwenden Sie den Schieberegler, um zur gewünschten Position zu wechseln:
   - Kreuz = deaktiviert
   - Häkchen = aktiviert
2. Klicken Sie in der Bestätigungsmeldung zum Akzeptieren auf **OK**.

Nach der Aktivierung können Sie Active Directory-Benutzer auf der Seite Benutzer hinzufügen hinzufügen. Diese können sich direkt mit der Option **Mit Active Directory anmelden** bei Hub anmelden.

Dies gilt nicht für LDAP-Benutzer, die weiterhin ihre Anmeldedaten eingeben müssen.

Active Directory-Benutzermanagement

Wenn die Active Directory-Authentifizierung auf der Seite „Authentifizierungseinstellungen“ aktiviert wurde, müssen Sie auswählen, wie der Zugriff für Active Directory-Benutzer in Hub verwaltet werden soll, indem Sie mindestens eine der folgenden Optionen auf der Seite „Authentifizierungseinstellungen“ aktivieren:

- **Autorisierung über Mitgliedschaft in Active Directory-Sicherheitsgruppen zulassen** – Ermöglicht das Hinzufügen von Active Directory-Sicherheitsgruppen zu Hub Rollen. Benutzer können mehreren Hub Rollen zugewiesen werden, indem sie Mitglied von Active Directory-Sicherheitsgruppen sind, die diesen Rollen zugeordnet sind.
- **Zulassen, dass Active Directory-Benutzer direkt zu Rollen hinzugefügt werden** – Ermöglicht das direkte Zuweisen von Active Directory-Benutzern zu Hub Rollen. Benutzer können mehreren Hub Rollen zugewiesen werden.

Weitere Informationen zum Zuweisen von Active Directory-Benutzern und -Sicherheitsgruppen zu Rollen finden Sie unter Rollen und Berechtigungen auf Seite 35.

In diesem Video erhalten Sie einen Überblick über die Active Directory-Integration in Authentication Server.

Active Directory-Domains

Auf der Seite „Active Directory-Domains“ können Sie Active Directory-Domains und zugehörige Anmeldedaten, die in der Authentication Server Datenbank gespeichert sind, anzeigen, hinzufügen, bearbeiten und löschen. Dieser Bereich ist nur für Administratoren verfügbar.

Um die Seite „Active Directory-Domains“ zu öffnen, klicken Sie auf Ihr Profilsymbol, um die Seite „Einstellungen“ zu öffnen, klicken Sie auf **Authentifizierungseinstellungen** und dann auf **Domains anzeigen**.

Sie müssen nur neue Active Directory-Domains für Umgebungen mit mehreren Gesamtstrukturen mit einseitigen Vertrauensbeziehungen hinzufügen. Weitere Informationen finden Sie unter Active Directory-Domains oben.

Die Seite „Active Directory-Domains“ umfasst die folgenden Informationen und Funktionen:

A. **Hinzufügen** – Eine neues Active Directory-Domain hinzufügen.
B. **Bearbeiten** – Die Details einer vorhandenen Active Directory-Domain anzeigen. Sie können jeweils nur eine Domäne bearbeiten.
C. **Löschen** – Eine oder mehrere Active Directory-Domains löschen.

Eine Domain hinzufügen

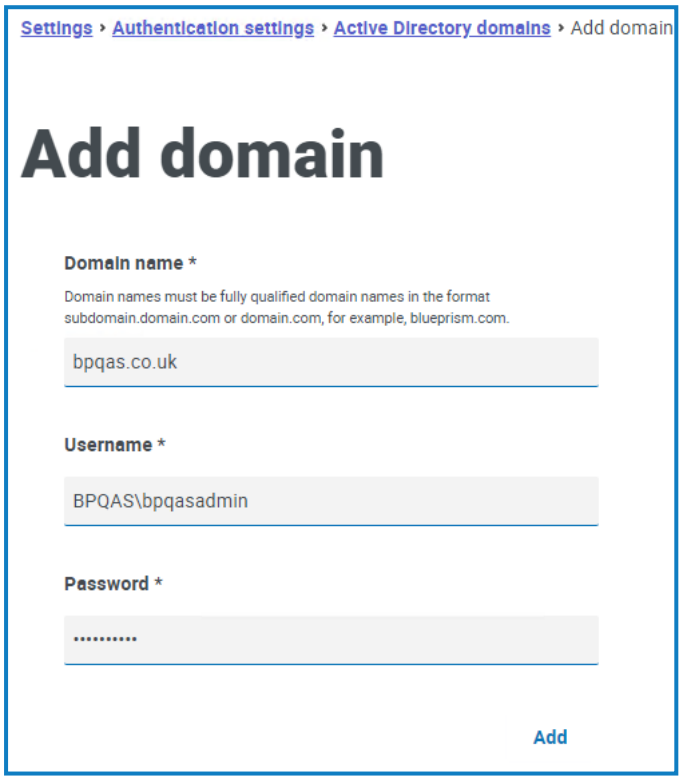
1. Klicken Sie auf der Seite „Active Directory-Domains“ auf **Hinzufügen**.

   Die Seite „Domain hinzufügen“ wird angezeigt.
2. Geben Sie einen Domain-Namen ein.

   Dies muss der Fully Qualified Domain Name (FQDN) im Format subdomain.domain.com oder domain.com sein

3. Geben Sie den Benutzernamen und das Passwort für die Domain ein. Benutzernamen müssen im Format username@domain.co.uk oder DOMAIN\\username vorliegen. Die Anmeldeinformationen müssen vorher von einem Systemadministrator angefordert werden.

   Die Anmeldedaten der Active Directory-Domain werden in der Datenbank gespeichert und vor der Speicherung verschlüsselt. Die für jede Domain gespeicherten Anmeldedaten müssen die eines Active Directory-Dienstkontos sein. Das Passwort für das Dienstkonto darf nicht ablaufen, das Dienstkonto darf kein Benutzerkonto sein und sollte die Best Practices für das Active Directory-Dienstkonto befolgen.



4. Klicken Sie auf **Hinzufügen**.

   Der Domain-Name und die Anmeldedaten werden mit dem Active Directory-Domain-Controller verglichen und die hinzugefügte Domain wird in der Domain-Liste angezeigt.

Eine Domain bearbeiten

1. Wählen Sie auf der Seite „Active Directory-Domains“ eine Domain aus und klicken Sie auf **Bearbeiten**.

   Sie können jeweils nur eine Domain auswählen.

2. Ändern Sie die Informationen nach Bedarf. Wenn Sie den Domain-Namen bearbeiten möchten, müssen Sie diese Domain löschen und eine neue Domain erstellen.
3. Klicken Sie auf **Speichern**, um Ihre Änderungen zu übernehmen.

Domains löschen

1. Wählen Sie in der Active Directory-Domain die gewünschte(n) Domain(s) aus und klicken Sie auf **Löschen**.

   Eine Meldung wird angezeigt, in der Sie zur Bestätigung des Löschvorgangs aufgefordert werden.

2. Klicken Sie auf **Ja**, um die ausgewählte(n) Domain(s) zu löschen, oder auf **Nein**, um abzubrechen.

Vertrauensbeziehung zwischen Domains

Für Umgebungen mit mehreren Gesamtstrukturen müssen Vertrauensbeziehungen zwischen Domains konfiguriert werden. Diese können bilateral oder unilateral zur Domain verlaufen, der vertraut werden soll.

Zum Beispiel:

- Bei einer unilateralen Vertrauensbeziehung zwischen Domain A und Domain B können Benutzer in Domain A auf Ressourcen in Domain B zugreifen. Benutzer in Domain B können jedoch nicht auf Ressourcen in Domain A zugreifen.
- In einer bilateralen Vertrauensbeziehung vertraut Domain A Domain B und Domain B vertraut Domain A. Das bedeutet, dass Authentifizierungsanforderungen zwischen den beiden Domains in beide Richtungen weitergeleitet werden können.

Bilaterale Vertrauensbeziehungen erfordern nicht, dass der Benutzer Domain-Anmeldeinformationen bereitstellt, wenn der Benutzer des Authentication Server Anwendungspools relevanten Lesezugriff auf die Domain hat, zu der der Benutzer gehört. In diesen Beispielen würde sich der Webserver, der den Authentication Server hostet, in Domain B befinden. Bilaterale Vertrauensbeziehungen erfordern die Bereitstellung von Anmeldeinformationen, wenn der Benutzer eine vertrauenswürdige Domain unter Verwendung eines Kontos abfragen muss, das sich von dem Benutzer des Authentication Server Anwendungspools unterscheidet. Unilaterale Vertrauensbeziehungen erfordern, dass eine Domain mit Anmeldedaten erstellt wird.

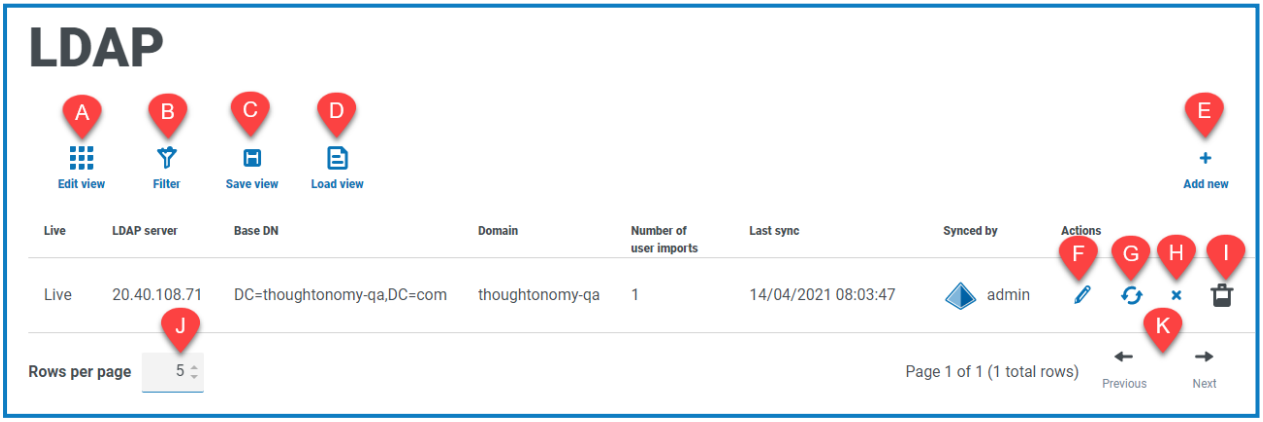
Die folgenden Vertrauensarten werden unterstützt:

- Extern
- Übergeordnet-untergeordnet
- Struktur-Stamm
- Gesamtstruktur

LDAP

Auf der LDAP-Seite können Sie eine LDAP-Verbindung (Lightweight Directory Access Protocol) zur Active Directory-Umgebung eines Unternehmens konfigurieren. Dieser Bereich ist nur für Administratoren verfügbar.

Um die LDAP-Seite zu öffnen, klicken Sie auf Ihr Profilsymbol, um die Seite „Einstellungen“ zu öffnen, klicken Sie auf **Authentifizierungseinstellungen** und klicken Sie dann auf **Konfigurieren** im LDAP-Abschnitt.



Die LDAP -Seite umfasst die folgenden Informationen und Funktionen:

A. **Ansicht bearbeiten** – Legen Sie fest, welche Spalten angezeigt werden sollen. Sie können die Spalten dann per Umschalten anzeigen oder ausblenden.

B. **Filtern** – Filtern Sie die angezeigten Informationen. Sie können dann die erforderlichen Filter aktivieren und die entsprechenden Informationen für die Anzeige eingeben oder auswählen. Aktivieren Sie zum Beispiel den Filter **Domain** und geben Sie den Domain-Namen ein.

C. **Ansicht speichern** – Speichern Sie Ihre aktuellen Spalteneinstellungen. Sie können Ihrer Ansicht einen Namen geben, um sie beim Laden von Ansichten einfacher zu erkennen.

D. **Ansicht laden** – Laden Sie eine gespeicherte Ansicht. Sie können die gewünschte Ansicht auswählen und auf **Anwenden** klicken.

E. **Neu hinzufügen** – Eine neue Verbindung hinzufügen.

F. **Bearbeiten** – Bearbeiten Sie die ausgewählten Verbindungsdetails.

G. **Re-Sync** – Synchronisieren Sie die Benutzer erneut mit Hub. Das ist erforderlich, wenn neue Benutzer zu Active Directory hinzugefügt werden.

H. **Zurückziehen/Wiederherstellen** – Mit einem Häkchen können Sie eine zurückgezogene Verbindung aktivieren und mit einem Kreuz können Sie eine Verbindung zurückziehen. Weitere Informationen finden Sie unter Zurückziehen und Wiederherstellen einer Anwendung.

I. **Löschen** – Die ausgewählte Verbindung löschen. Sie können nur eine zurückgezogene Verbindung löschen.

J. **Zeilen pro Seite** – Geben Sie eine Zahl ein oder verwenden Sie die Pfeile nach oben und unten, um die Anzahl der auf einer Seite angezeigten Zeilen zu ändern.

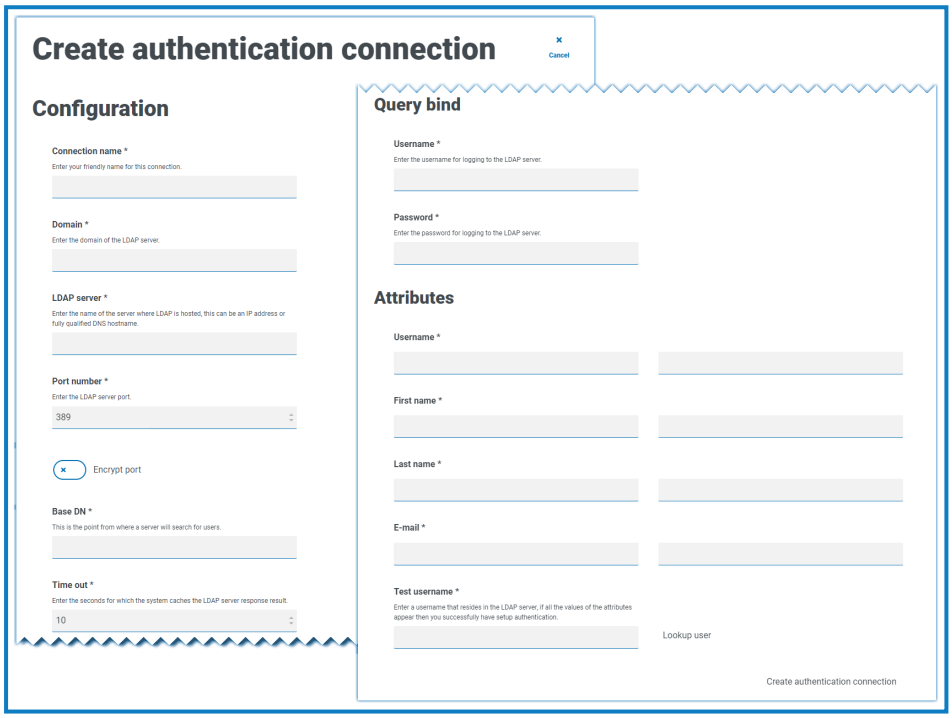
K. **Zurück und Weiter** – Klicken Sie auf **Zurück** oder **Weiter**, um durch die Seiten zu navigieren.

Eine neue Verbindung hinzufügen

Wenn Sie mehrere LDAP-Verbindungen im Hub hinzufügen, welche die gleichen Benutzer enthalten (wie Name, E-Mail-Adresse und Domain), werden doppelte Benutzer erstellt, wodurch Anmeldeprobleme entstehen können. Wenn Sie die Benutzer mit der nachfolgenden Methode synchronisieren, wählen Sie nur die Benutzer aus, die Sie benötigen, um zu verhindern, dass doppelte Benutzer importiert werden.

1. Klicken Sie auf der LDAP -Seite auf **Neu hinzufügen**.

   Die Seite „Authentifizierungsverbindung erstellen“ wird angezeigt.



2. Füllen Sie die Konfigurationsfelder aus:
   - **Verbindungsname** – Der Name, den die Verbindung erhalten soll.
   - **Domain** – Der Name der Domain, mit der Sie sich verbinden, zum Beispiel „bp“.

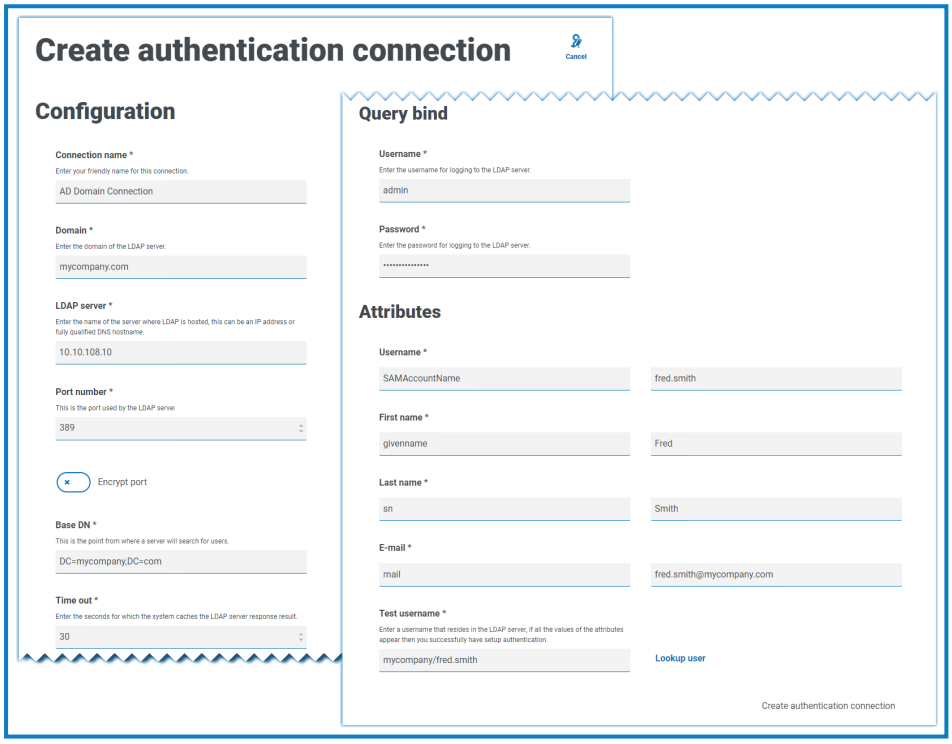
     Verwenden Sie nicht den Fully Qualified Domain Name (FQDN) Ihrer Domain. Sie müssen das Kurznamenformat verwenden.

   - **LDAP-Server** – Der Hostname des LDAP-Servers, zum Beispiel blueprism-srv1.local.
   - **Portnummer** – Die verwendete Portnummer, standardmäßig ist das Port 389.
   - **Port verschlüsseln** – Wählen Sie diese Option aus, wenn Sie den Port verschlüsseln möchten. Wenn Sie Port 636 (den LDAPS-Port) verwenden, sollten Sie diese Option aktivieren.
   - **Base DN** – Der Startpunkt im Active Directory, an dem das System mit der Suche nach Benutzern beginnt, zum Beispiel dc=blueprism, dc=local.

3. Füllen Sie die Felder der „Abfragebindung“ aus:
    - **Timeout** – Der Timeout-Zeitraum in Sekunden, für den das System auf eine Antwort vom Active Directory-Server wartet.
    - **Benutzername für Abfragebindung** – Ein Active Directory-Benutzer, der Zugriff auf das LDAP-System des Unternehmens hat.
    - **Passwort für Abfragebindung** – Das Passwort für den Active Directory-Benutzer.
4. Füllen Sie die „Attribute“-Felder aus. Der Zweck dieses Abschnitts ist es, die Active Directory-Attribute den Hub Feldern zuzuordnen. Der in diese Felder eingegebene Text muss mit den benannten Attributen im Benutzerprofil in Active Directory übereinstimmen. Sie können das Tool Active Directory-Benutzer und -Computer (ADUC) verwenden, um die Benutzerattribute zu finden. Wählen Sie dazu einen Benutzer aus und klicken Sie dann auf die Registerkarte **Attribut-Editor**, um die Zuordnung von Attributen zu Werten aufzurufen.
    - **Benutzername** – Der Name des Active Directory-Attributs für den Benutzernamen, zum Beispiel „SAMAccountName“.
    - **Vorname** – Der Name des Active Directory-Attributs für den Vornamen des Benutzers, zum Beispiel „givenname“.
    - **Nachname** – Der Name des Active Directory-Attributs für den Nachnamen des Benutzers, zum Beispiel „sn“.
    - **E-Mail** – Der Name des Active Directory-Attributs für die E-Mail-Adresse des Benutzers, zum Beispiel „mail“.

5. Um zu testen, ob alles korrekt eingerichtet ist, geben Sie den Benutzernamen in das Feld **Benutzernamen testen** ein und klicken Sie auf **Benutzer nachschlagen**. Der im Feld **Benutzername testen** eingegebene Text muss mit dem Textformat des Active Directory-Attributs übereinstimmen. Wenn beispielsweise der Benutzername auf:
   - „SAMKontoName“ eingestellt ist, dann werden die Testdaten wahrscheinlich im Format *domain\user* vorliegen.
   - „Name“ eingestellt ist, dann werden die Testdaten wahrscheinlich im Format *user* vorliegen.

   Die zugehörigen Informationen werden abgerufen und in die entsprechenden „Attribute“-Felder eingetragen, zum Beispiel:



6. Klicken Sie auf **Authentifizierungsverbindung erstellen**.

   Es wird eine Benachrichtigung angezeigt, in der bestätigt wird, dass die Verbindung erfolgreich ist. Sie werden aufgefordert, Benutzer zu importieren.

7. Klicken Sie auf **Ja**, um jetzt zu synchronisieren. Alternativ können Sie **Nein** auswählen und später mithilfe des Prozesses in Active Directory-Benutzer synchronisieren auf Seite 55 synchronisieren.

   Eine Benachrichtigung wird angezeigt, die die Anzahl der gefundenen Benutzer angibt.

> ⚠ Beim Importieren einer großen Anzahl von Benutzern (z. B. Zehntausende) steigt die Größe der Transaktionslogdateien der Datenbanken AuthenticationServerDB, HubDB und InteractDB. Wenn die Größe der Transaktionslogdatei einer dieser drei Datenbanken entweder durch eine zu kleine maximale Dateigröße eingeschränkt ist oder die Datei nicht größer werden darf, kann der Import fehlschlagen. Es wird daher empfohlen, dass Sie die Einstellung für das automatische Wachstum der Datenbank-Transaktionslogdateien aktivieren und die Wachstumseinstellung auf 1.024 MB festlegen. Stellen Sie dabei sicher, dass eine ausreichende maximale Größe eingestellt ist, um zu verhindern, dass der Import fehlschlägt. Weitere Informationen zum automatischen Wachstum finden Sie in der Microsoft-Dokumentation.

8. Klicken Sie auf **Fortfahren**.

   Eine Liste der Benutzer wird angezeigt. Diese wurden noch nicht in Hub importiert, da Sie die Berechtigungen und Rollen für die erforderlichen Benutzer konfigurieren müssen.

9. Wählen Sie einen Benutzer zum Importieren und Zuweisen der entsprechenden Hub Rollen und/oder aller Interact Verantwortlichkeiten aus.

   > Wenn Sie einen Benutzer so konfigurieren, dass er über eine Hub Administratorrolle verfügt, hat er Zugriff auf alle Plug-ins und Funktionen von Hub. Das beinhaltet auch die Möglichkeit, neue Datenbank- und LDAP-Verbindungen und andere Sicherheitsfunktionen zu erstellen. Daher muss diese Rolle mit Sorgfalt zugewiesen werden.

10. Für alle erforderlichen Benutzer wiederholen.
11. Klicken Sie auf **Zugriff und Rollen speichern**.

    Nur die Benutzer, für die Rollen und Berechtigungen definiert wurden, werden gespeichert und die Seite Benutzer wird mit den neuen Benutzern dargestellt.

Verbindung bearbeiten

1. Wählen Sie auf der LDAP-Seite das **Bleistiftsymbol** für die gewünschte Verbindung aus.
2. Bearbeiten Sie die Informationen nach Bedarf. Sie können die Domain, den LDAP-Server, die Portnummer oder Base DN nicht ändern.
3. Klicken Sie auf **Speichern**.

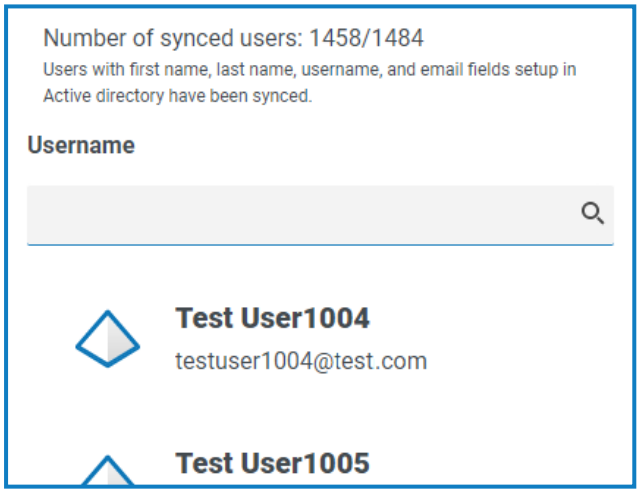
Active Directory-Benutzer synchronisieren

⚠ Beim Importieren einer großen Anzahl von Benutzern (z. B. Zehntausende) steigt die Größe der Transaktionslogdateien der Datenbanken AuthenticationServerDB, HubDB und InteractDB. Wenn die Größe der Transaktionslogdatei einer dieser drei Datenbanken entweder durch eine zu kleine maximale Dateigröße eingeschränkt ist oder die Datei nicht größer werden darf, kann der Import fehlschlagen. Es wird daher empfohlen, dass Sie die Einstellung für das automatische Wachstum der Datenbank-Transaktionslogdateien aktivieren und die Wachstumseinstellung auf 1.024 MB festlegen. Stellen Sie dabei sicher, dass eine ausreichende maximale Größe eingestellt ist, um zu verhindern, dass der Import fehlschlägt. Weitere Informationen zum automatischen Wachstum finden Sie in der Microsoft-Dokumentation.

Wenn zusätzliche Benutzer zum Active Directory hinzugefügt werden, müssen diese Benutzer mit Hub synchronisiert werden.

1. Klicken Sie auf der LDAP-Seite in der Zeile für die gewünschte Verbindung auf das Symbol für die **Neusynchronisierung**.

   Eine Nachricht wird über der Liste der Benutzer angezeigt, die die Anzahl der synchronisierten Benutzer (diejenigen mit gültigen Informationen in Active Directory – Vorname, Nachname, Benutzername und E-Mail-Adresse) im Vergleich zur Gesamtzahl der gefundenen Benutzer darstellt. Nur synchronisierte Benutzer werden in der Liste angezeigt. Sie müssen die Berechtigungen und Rollen für die erforderlichen Benutzer konfigurieren.



   ✎ Weitere Informationen zu den Active Directory-Attributen, die Hub mit den Informationen zu Vorname, Nachname, Benutzername und E-Mail-Adresse versorgen, finden Sie unter Eine neue Verbindung hinzufügen auf Seite 51. Hub synchronisiert nur Benutzer, die Informationen in allen zugeordneten Attributen haben.

2. Wählen Sie den erforderlichen Benutzer aus, der zur Hub Benutzerbasis hinzugefügt werden soll, und weisen Sie die entsprechenden Hub Rollen und/oder Interact Verantwortlichkeiten zu.
3. Für alle erforderlichen Benutzer wiederholen.
4. Klicken Sie auf **Zugriff und Rollen speichern**.

   Nur die Benutzer, für die Rollen und Berechtigungen definiert wurden, werden gespeichert und die Seite Benutzer wird mit den neuen Benutzern dargestellt.

Zurückziehen und Wiederherstellen einer Verbindung

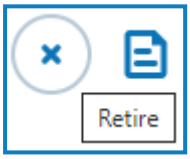
Das Zurückziehen einer Verbindung hat keinen Einfluss auf den Status der zugeordneten Benutzer – die Benutzer können sich weiterhin anmelden und die Anwendungen verwenden. Alle Benutzer, die mit einer LDAP-Verbindung zugeordnet sind, können durch Löschen der Verbindung zurückgezogen werden.

1. Wählen Sie auf der LDAP-Seite das Symbol **Zurückziehen/Wiederherstellen** für die gewünschte Verbindung aus.

   Wenn die Verbindung:

   - Live ist, wird das Symbol **Zurückziehen/Wiederherstellen** als Kreuz angezeigt.
   - zurückgezogen ist, wird das Symbol **Zurückziehen/Wiederherstellen** als Häkchen angezeigt.

2. So ziehen Sie eine Verbindung zurück:
   a. Klicken Sie auf das Kreuz.

   Eine Nachricht wird angezeigt, in der Sie zur Bestätigung aufgefordert werden.

   b. Klicken Sie auf **Ja**.

   Die Verbindung wird zurückgezogen und das Kreuz ändert sich zu einem Häkchen.

3. Um eine zurückgezogene Verbindung live zu schalten, klicken Sie auf das Häkchen.

   Die Verbindung wird sofort wiederhergestellt und das Häkchen ändert sich zu einem Kreuz.

   Sie können den Filter **Live** verwenden, um die Liste nach zurückgezogenen Verbindungen zu filtern.

Verbindung löschen

Sie können nur eine zurückgezogene Verbindung löschen.

1. Wählen Sie auf der LDAP-Seite **Löschen** (den Papierkorb) für die gewünschte Verbindung aus.

   Eine Nachricht wird angezeigt, in der Sie zur Bestätigung aufgefordert werden.

2. Klicken Sie auf **Ja**.

   Die Verbindung wird gelöscht und alle damit verbundenen Benutzer werden zurückgezogen.

Filter auf der LDAP -Seite verwenden

Mit Filtern können Sie auf schnelle Weise eine bestimmte Verbindung oder ähnliche Verbindungen anhand ausgewählter Kriterien finden.

1. Klicken Sie auf der LDAP -Seite auf **Filter**, um den Filter-Bereich zu öffnen.
2. Verwenden Sie den Umschalter, um den erforderlichen Filter zu aktivieren, und geben Sie die Informationen ein, um die gewünschte Verbindung zu finden. Sie können mehrere Filter gleichzeitig anwenden.

   Die verfügbaren Filter sind:

Filter	Beschreibung
Live	Wählen Sie eine der folgenden Optionen für den Verbindungsstatus aus: • **Live** – Zeigt die aktiven, nicht zurückgezogenen Verbindungen an. • **Zurückgezogen** – Zeigt die Verbindungen an, die von einem Administrator zurückgezogen wurden.
Verbindungsname	Geben Sie den vollständigen Namen einer Verbindung oder einen Teil davon ein.
LDAP Server	Geben Sie den Hostnamen des Servers oder einen Teil davon ein.
Base DN	Geben Sie die Base DN oder einen Teil davon für den Abgleich ein.
Domain	Geben Sie den vollständigen Namen einer Domain oder einen Teil davon ein.
Anzahl Benutzerimporte	Geben Sie einen numerischen Bereich ein: • Im ersten Feld geben Sie die geringste Anzahl an Importen ein. • Im zweiten Feld geben Sie die höchste Anzahl von Importen ein. Es werden alle Verbindungen angezeigt, die Benutzer innerhalb dieses Bereichs importiert haben.
Zuletzt synchronisiert	Geben Sie einen Datumsbereich ein: • Wählen Sie im ersten Feld das früheste Datum aus. • Wählen Sie im zweiten Feld das letzte Datum aus. • Falls erforderlich, passen Sie die Zeitfelder an. Standardmäßig hat das erste Datum den Zeitwert „00:00:00“ und das letzte Datum den Zeitwert „23:59:59“, was einen vollständigen Tag ergibt. Dies zeigt alle Verbindungen an, die in diesem Zeitraum synchronisiert wurden.
Synchronisiert von	Geben Sie einen Benutzernamen oder einen Teil davon ein. Wenn Sie einen Teil eines Benutzernamens eingegeben haben, werden die Ergebnisse für alle teilweisen Übereinstimmungen angezeigt. Dabei kann es sich auch um andere Benutzer als den beabsichtigten handeln.

Die Informationen auf der LDAP -Seite werden sofort gefiltert.

> Wenn Sie die Filter eingestellt haben, aber die ungefilterten Informationen noch einmal anzeigen möchten, schalten Sie entweder die erforderlichen Filter aus oder entfernen Sie alle Einstellungen innerhalb des Filters, damit er leer ist.

3. Klicken Sie auf **Bereich schließen**, um den Filter-Bereich zu schließen.

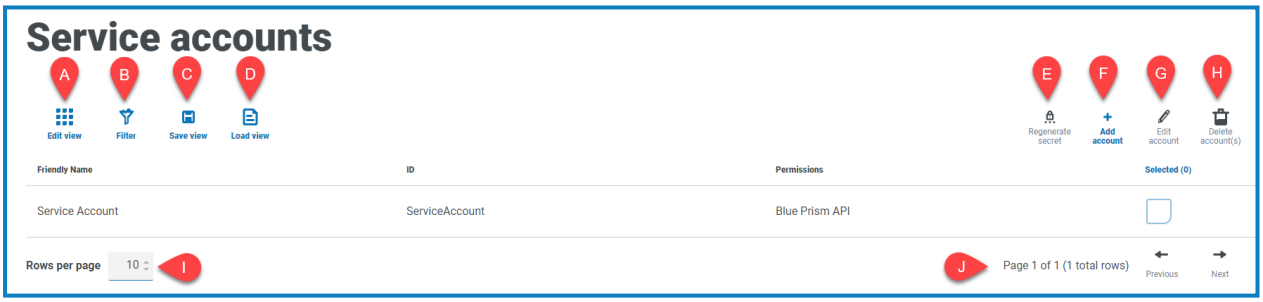
Dienstkonten

Auf der Seite „Dienstkonten“ können Sie die authentifizierten Anwendungskonten verwalten. Dieser Bereich ist nur für Administratoren verfügbar.

Dienstkonten werden von Anwendungen verwendet, die Zugriffstoken für ihren eigenen Gebrauch anstatt im Namen eines Benutzers erhalten müssen. Diese Zugriffstoken dienen dann dazu, authentifizierte Anfragen an APIs zu stellen. Die APIs, für die Dienstkonten Zugriffstoken erhalten können:

- **Authentication Server API** – Für alle Anwendungen, die mit der Authentication Server API integriert sind, muss ein Dienstkonto erstellt werden. Weitere Details finden Sie im Authentication Server Konfigurationshandbuch.
- **Blue Prism API** – Für alle Anwendungen von Drittanbietern, die mit der Blue Prism API integriert sind, muss ein Dienstkonto erstellt werden. Weitere Details finden Sie im Blue Prism API Installationshandbuch.
- **Decision API** – Damit Blue Prism Decision Modelle verwenden kann, die im Decision Plug-in trainiert und kalibriert wurden, muss ein Dienstkonto erstellt werden. Weitere Details finden Sie im Blue Prism Decision Installationshandbuch.
- **Interact Remote API** – Ein Dienstkonto muss für alle Anwendungen erstellt werden, die mit der Interact Remote API integriert sind, wie z. B. der interaktive Blue Prism Client. Weitere Informationen finden Sie im Interact Web-API-Dienst Benutzerhandbuch.

Um die Seite „Dienstkonten“ zu öffnen, klicken Sie auf Ihr Profilsymbol. Daraufhin wird die Seite „Einstellungen“ geöffnet. Klicken Sie dann auf **Dienstkonten**.



Die Seite „Dienstkonten“ umfasst die folgenden Informationen und Funktionen:

A. **Ansicht bearbeiten** – Legen Sie fest, welche Spalten angezeigt werden sollen. Sie können die Spalten dann per Umschalten anzeigen oder ausblenden.

B. **Filtern** – Filtern Sie die angezeigten Informationen. Sie können dann die erforderlichen Filter aktivieren und die entsprechenden Informationen für die Anzeige eingeben oder auswählen. Aktivieren Sie zum Beispiel Aktivieren Sie den Filter für **Berechtigungen** und wählen Sie **Blue Prism API** aus.

C. **Ansicht speichern** – Speichern Sie Ihre aktuellen Spalteneinstellungen. Sie können Ihrer Ansicht einen Namen geben, um sie beim Laden von Ansichten einfacher zu erkennen.

D. **Ansicht laden** – Laden Sie eine gespeicherte Ansicht. Sie können die gewünschte Ansicht auswählen und auf **Anwenden** klicken.

E. **Geheimnis erneut generieren** – Erstellen Sie ein neues Geheimnis für ein vorhandenes Dienstkonto.

F. **Konto hinzufügen** – Ein neues Dienstkonto hinzufügen.

G. **Konto bearbeiten** – Die Details eines bestehenden Dienstkontos bearbeiten.

H. **Konto(s) löschen** – Ein oder mehrere Dienstkonten löschen.

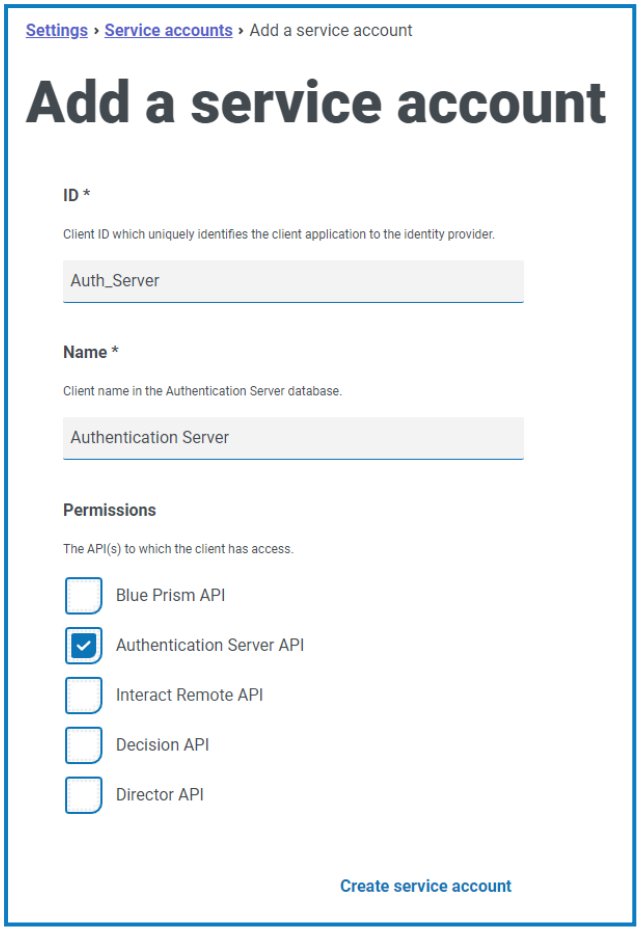
I. **Zeilen pro Seite** – Geben Sie eine Zahl ein oder verwenden Sie die Pfeile nach oben und unten, um die Anzahl der auf einer Seite angezeigten Zeilen zu ändern.

J. **Zurück und Weiter** – Klicken Sie auf **Zurück** oder **Weiter**, um durch die Seiten zu navigieren von Dienstkonten.

Dienstkonto hinzufügen

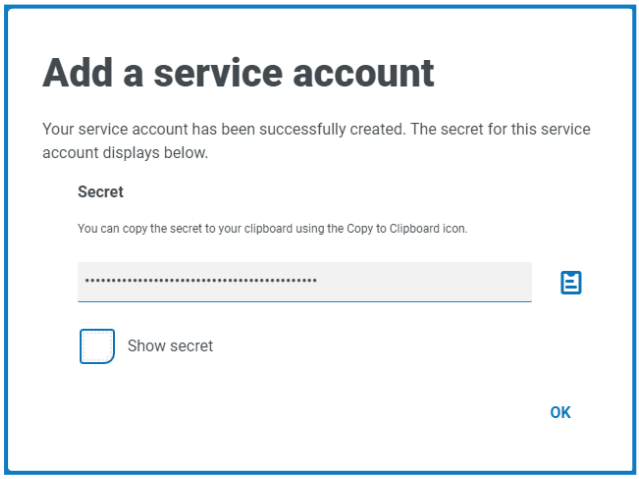
1. Klicken Sie auf der Seite „Dienstkonten“ auf **Konto hinzufügen**.
2. Geben Sie eine eindeutige ID für die Client-Anwendung und einen Anzeigenamen für den Client in der Authentication Server Datenbank ein.
3. Wählen Sie unter **Berechtigungen** die entsprechende Option aus:
   - **Blue Prism API** – Das Geheimnis des Dienstkontos wird verwendet, um ein Zugriffstoken zur Authentifizierung mit der Blue Prism API zu erhalten.
   - **Authentication Server API** – Das Geheimnis des Dienstkontos wird verwendet, um authentifizierte Anfragen an die Authentication Server API zu senden.
   - **Interact Remote API** – Das Geheimnis des Dienstkontos wird verwendet, um ein Zugriffstoken zur Authentifizierung mit der Interact Remote API zu erhalten.
   - **Decision API** – Das Geheimnis des Dienstkontos wird verwendet, um ein Zugriffstoken zur Authentifizierung mit der Decision Web API zu erhalten.
   - **Director API** – Diese Berechtigung hat keine Funktion. Sie ist für zukünftige Funktionen reserviert.

4. Klicken Sie auf **Dienstkonto erstellen**.



Das Dialogfeld „Dienstkonto hinzufügen“ wird mit einem generierten Geheimnis angezeigt, das verwendet wird, um das Zugriffstoken für die ausgewählte(n) API(s) zu erhalten.

5. Klicken Sie auf das Symbol für „In die Zwischenablage kopieren“, um den generierten geheimen Schlüssel in die Zwischenablage zu kopieren.



6. Klicken Sie auf **OK**, um das Dialogfeld zu schließen.

   Die Seite „Dienstkonten“ wird mit dem neu erstellten Konto angezeigt.

Geheimnis erneut generieren

Wenn Sie ein zuvor generiertes Geheimnis für ein vorhandenes Dienstkonto verlegt haben, können Sie ein neues generieren.

1. Wählen Sie auf der Seite „Dienstkonten“ das gewünschte Dienstkonto aus, und klicken Sie auf **Geheimnis erneut generieren**.

   Das neue Geheimnis für dieses Dienstkonto wird angezeigt.
2. Klicken Sie auf das Symbol für „In die Zwischenablage kopieren“, um den generierten geheimen Schlüssel in die Zwischenablage zu kopieren.
3. Klicken Sie auf **OK**, um das Dialogfeld zu schließen.

Dienstkonto bearbeiten

1. Wählen Sie auf der Seite „Dienstkonten“ das gewünschte Dienstkonto aus, und klicken Sie auf **Konto bearbeiten**.
2. Ändern Sie die Informationen nach Bedarf.

   Sie können die Client-ID für ein Dienstkonto nicht ändern.
3. Klicken Sie auf **Speichern**, um Ihre Änderungen zu übernehmen.

Dienstkonten löschen

1. Wählen Sie auf der Seite „Dienstkonten“ das gewünschte Dienstkonto aus, und klicken Sie auf **Konto(s) löschen**.

   Eine Meldung wird angezeigt, in der Sie zur Bestätigung des Löschvorgangs aufgefordert werden.
2. Klicken Sie auf **Ja**, um das/die ausgewählte(n) Konto(s) zu löschen, oder auf **Nein**, um abzubrechen.

Filter auf der Seite „Dienstkonten“ verwenden

Mit Filtern können Sie auf schnelle Weise bestimmte Dienstkonten anhand ausgewählter Kriterien finden.

1. Klicken Sie auf der Seite „Dienstkoten“ auf **Filter**, um den Filter-Bereich zu öffnen.
2. Verwenden Sie den Umschalter, um den erforderlichen Filter zu aktivieren, und geben Sie die Informationen ein, um das Dienstkonto zu finden. Sie können mehrere Filter gleichzeitig anwenden.

   Die verfügbaren Filter sind:

Filter	Beschreibung
Anzeigename	Geben Sie den Namen des Dienstkontos oder einen Teil eines Namens ein.
ID	Geben Sie den Dienstkonto-Identifikator oder einen Teil des Identifikators ein.
Berechtigungen	Wählen Sie die gewünschte Berechtigungsstufe aus. Sie können mehr als eine Option auswählen. Wenn Sie keine Berechtigungsstufen auswählen, sind alle Stufen auf der Seite „Dienstkonten“ enthalten.

   Die Informationen auf der Seite „Dienstkonten“ werden sofort gefiltert.

   Wenn Sie die Filter eingestellt haben, aber die ungefilterten Informationen noch einmal anzeigen möchten, schalten Sie entweder die erforderlichen Filter aus oder entfernen Sie alle Einstellungen innerhalb des Filters, damit er leer ist.

3. Klicken Sie auf **Bereich schließen**, um den Filter-Bereich zu schließen.