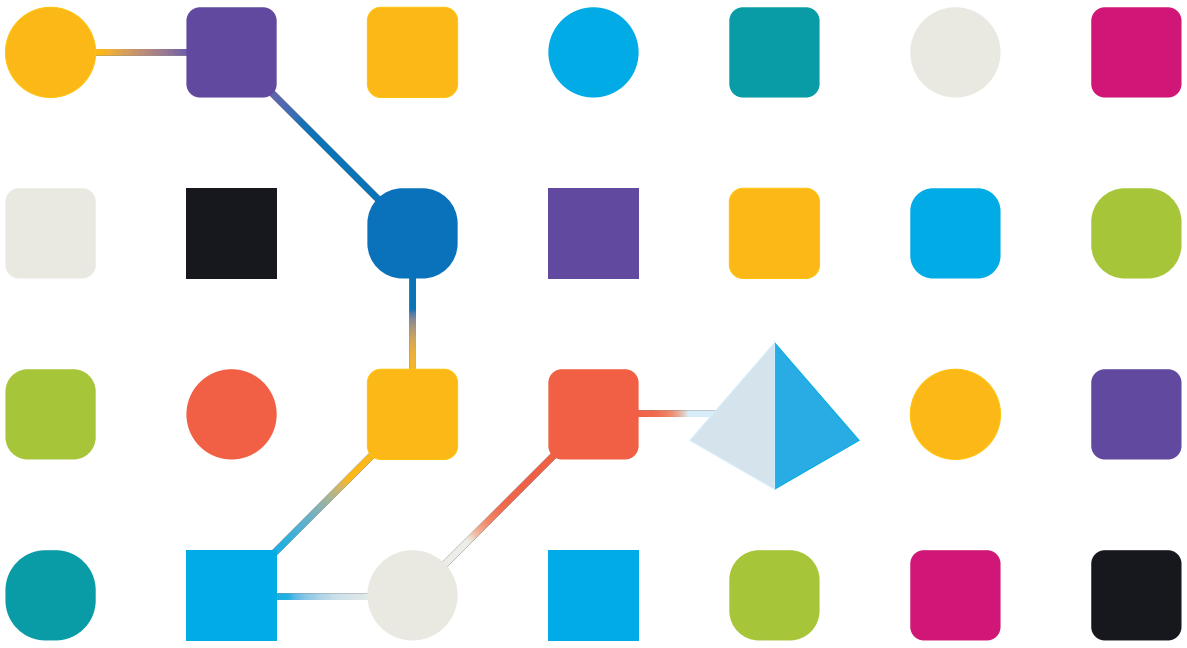
blueprism®

Blue Prism Hub 4.6

Guide de l'administrateur

Révision des documents : 3.0



Marques déposées et droits d'auteur

Blue Prism Limited, 2 Cinnamon Park, Crab Lane, Warrington, WA2 0XP, United Kingdom.
Enregistré en Angleterre : numéro d'enregistrement 4260035. Tél. : +44 370 879 3000. Web : www.blueprism.com

Contenu

Hub

Blue Prism rassemble les principes du cloud, de l'automatisation robotisée des processus (RPA) et de l'intelligence artificielle (IA) conçus pour automatiser et numériser l'exécution des travaux basés sur les connaissances. Les Digital Workers sont déployés dans les opérations et le travail de l'entreprise en imitant la façon dont les gens utilisent ses systèmes, les décisions qu'ils prennent et les processus qu'ils suivent, pour augmenter, remplacer ou numériser les processus de travail manuels.

Au fur et à mesure que le paysage de la Digital Workforce mûrit dans une organisation, les opérateurs et les sponsors doivent adapter leurs approches et leurs méthodologies pour gérer leurs investissements dans l'automatisation. Les informations relatives à la gestion de la Digital Workforce doivent être transparentes pour l'ensemble de l'entreprise et faciles à interpréter. En outre, les meilleures pratiques doivent être surveillées pour garantir le respect des normes du secteur. Blue Prism® Hub fournit aux utilisateurs Blue Prism nouveaux et existants une plateforme de productivité pour la gestion du cycle de vie de l'automatisation. Hub prend en charge les rôles individuels au sein du Robotic Operating Model (ROM) avec un ensemble de capacités pour assurer la livraison réussie et évolutive d'une stratégie d'automatisation.

Hub a été créé comme une application « vide » légère qui est ensuite renseignée par une série de plug-ins ou de fonctionnalités. Cela forme ce que l'on appelle l'architecture de plug-ins qui permet à l'équipe Blue Prism d'itérer les fonctionnalités et de les mettre à la disposition des administrateurs de Hub.

Chaque instance Hub contient une page Référentiel de plug-ins qui permet aux administrateurs d'afficher et de déployer de nouveaux plug-ins ainsi que de mettre à jour les plug-ins existants.

Public visé

Ce guide s'adresse aux utilisateurs Hub disposant de privilèges d'administrateur, appelés administrateurs Hub. Les administrateurs Hub sont responsables de la gestion de la plateforme Blue Prism Hub, y compris, mais sans s'y limiter, de ce qui suit :

- Gestion de l'intégration entre la plateforme Blue Prism Hub, Blue Prism et les API Blue Prism API.
- Gestion des rôles et des utilisateurs, y compris l'intégration à Active Directory.
- Installation des plug-ins.
- Surveillance des logs d'audit.

De ce fait, les administrateurs Hub doivent être des utilisateurs familiarisés avec la gestion des systèmes informatiques et qui comprennent l'architecture logicielle d'entreprise et Active Directory.

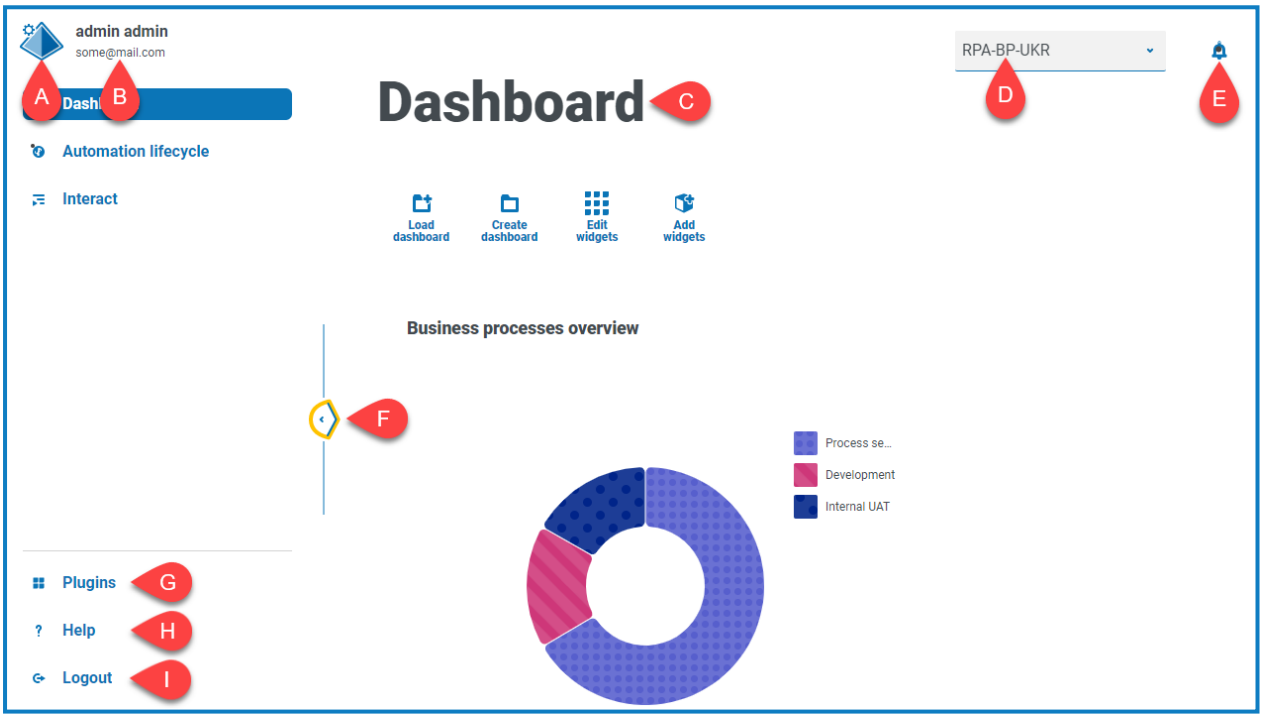
Administration et configuration

Lorsque Hub est installé pour une organisation, il est doté d'un rôle d'administrateur principal. Ce rôle permet de configurer l'environnement avec des informations pour des éléments tels que les e-mails et la connexion à votre base de données RPA.

Hub utilise le contrôle d'accès sur la base des rôles (RBAC) pour s'assurer que les utilisateurs peuvent uniquement accéder aux fonctionnalités requises pour remplir leur rôle au sein de leur organisation.

La barre de navigation supérieure dans Hub permet d'accéder aux réglages du système. Les réglages disponibles dépendent du rôle d'utilisateur. Plusieurs réglages ne sont pas disponibles pour les utilisateurs sans les permissions d'administrateur activées sur leur compte, comme détaillé ci-dessous.

Les fonctionnalités de la barre de navigation supérieure comprennent :



Lorsque le menu de navigation sur la gauche est développé (comme illustré ci-dessus), ces fonctionnalités sont affichées :

A. **Icône de profil** : définie par l'utilisateur dans son profil. Si vous êtes :
   - Un utilisateur, elle fournit un lien vers votre page de profil.
   - Un administrateur, elle fournit un lien vers les réglages système à partir desquels les éléments suivants peuvent être contrôlés :
     - Profil personnel et audit.
     - Gestion des plateformes.
     - Gestion des utilisateurs.

B. **Informations utilisateur** : cette option est masquée lorsque le menu de navigation est réduit.

C. **Titre de la page** : la zone de l'interface utilisateur Hub que vous utilisez actuellement.

D. **Environnement** : l'environnement actuellement sélectionné. Les environnements sont configurés dans le gestionnaire d'environnements et peuvent être sélectionnés ici.

E. **Alertes de notification** : les notifications sont créées par le plug-in Automation Lifecycle Management. Seules les notifications que vous êtes autorisé à voir, ou qui vous sont applicables, s'afficheront lorsque vous cliquez sur l'alerte.

F. **Basculer le menu** : ouvre et ferme le menu. Lorsque le menu est ouvert, les noms des éléments de menu s'affichent. Lorsque le menu est fermé, des icônes s'affichent pour chaque élément du menu.

G. **Plug-ins** : ouvre la page Plug-ins où vous pouvez afficher et télécharger les plug-ins disponibles.

H. **Aide** : ouvre l'aide en ligne. Cliquez avec le bouton droit de la souris et sélectionnez **Ouvrir le lien dans un nouvel onglet** pour ouvrir un onglet de navigateur distinct.

I. **Déconnexion** : vous déconnecte d'Authentication Server.

> Si vous utilisez Interact, vous serez également déconnecté de l'application Web Interact.

Restrictions de Hub

Le tableau suivant répertorie les restrictions appliquées lors de l'utilisation de Hub.

Élément	Restriction	Sections connexes
Noms d'utilisateur	Les noms d'utilisateur des utilisateurs natifs ne peuvent pas dépasser 25 caractères. Ils ne peuvent contenir que des caractères latins (à l'exception des caractères spéciaux), des chiffres, des points, des traits d'union et des traits de soulignement. Ils ne peuvent pas commencer par des points, des traits d'union et des traits de soulignement. Les noms d'utilisateur des utilisateurs Active Directory (leur UPN) ne peuvent pas dépasser 255 caractères.	Utilisateurs sur la page 25
Restrictions de mot de passe	Les mots de passe doivent : • Comporter au moins 1 majuscule • Comporter au moins 1 chiffre • Comporter au moins 1 caractère spécial • Comporter au moins 8 caractères • Être différents des cinq derniers mots de passe • Comporter un maximum de 32 caractères	Profil sur la page 9 et Utilisateurs sur la page 25
Image de profil	Inférieure à 1 Mo et inférieure ou égale à 1920 x 1080 pixels	Profil sur la page 9
Widgets du tableau de bord	Limite de 20 widgets par tableau de bord	Tableaux de bord : consultez le guide de l'utilisateur Hub.
Logo de la marque	PNG, JPEG ou JPG n'excédant pas 30 Ko	Personnalisation sur la page 20

Réglages

La page Réglages vous permet de gérer Hub. Vous n'avez accès à la page Réglages que si vous êtes un administrateur. Si vous êtes un utilisateur, vous n'aurez accès qu'à la page Profil qui s'ouvre lorsque vous cliquez sur l'icône de votre profil.

Pour ouvrir la page Réglages, cliquez sur l'icône de votre profil. La page Réglages s'affiche si vous êtes un administrateur. La page Profil s'affiche si vous êtes un utilisateur.

Présentation

Profil	La page Profil vous permet de modifier vos informations, vos préférences d'affichage et votre mot de passe. Pour plus d'informations, voir Profil sur la page 9.
Audit	Les administrateurs peuvent afficher un historique des activités du système auditées. Pour plus d'informations, voir Audit sur la page 11.

Gestion des plateformes

Les réglages des e-mails et de la base de données sont définis dans le cadre du processus d'installation et de configuration de Hub. Consultez le guide d'installation de Hub. Ils sont essentiels pour un fonctionnement normal.

Gestion des environnements	Les administrateurs peuvent ajouter des connexions aux bases de données Blue Prism RPA, gérer les connexions existantes et supprimer les bases de données RPA redondantes. Pour plus d'informations, voir Gestion des environnements sur la page 14.
Configuration de l'adresse e-mail	Les administrateurs peuvent modifier les détails de l'hôte SMTP. Des modifications doivent être apportées en collaboration avec votre propre équipe d'assistance informatique pour s'assurer que la configuration et les identifiants correspondent au serveur de messagerie de votre organisation. Pour plus d'informations, voir Configuration de l'adresse e-mail sur la page 17.
Personnalisation	Les administrateurs peuvent personnaliser le thème utilisé par l'interface utilisateur Interact. Le thème permet à l'administrateur de définir le nom du thème, la couleur de la marque et le logo de la marque. Pour plus d'informations, voir Personnalisation sur la page 20.
Gestion des plug-ins	Les administrateurs peuvent afficher la description et le numéro de version des plug-ins actuellement installés. Les mises à jour ou les plug-ins supplémentaires disponibles sont également affichés. Pour plus d'informations, voir Gestion des plug-ins sur la page 22.

Gestion des utilisateurs

Utilisateurs	Les administrateurs peuvent ajouter, modifier ou classer des utilisateurs et attribuer leurs permissions d'accès et leurs rôles. Pour plus d'informations, voir Utilisateurs sur la page 25.
Rôles et permissions	Les administrateurs peuvent ajouter, modifier et supprimer des rôles. Pour plus d'informations, voir Rôles et permissions sur la page 33.
Inscriptions	Les administrateurs peuvent gérer les demandes d'inscription que les nouveaux utilisateurs ont formulées pour accéder à Interact. Pour plus d'informations, voir Inscriptions sur la page 41.
d'authentificationRéglages	Les administrateurs peuvent ajouter, modifier, classer ou supprimer des réglages d'authentification. Pour plus d'informations, voir Réglages d'authentification sur la page 43.
Comptes de service	Les administrateurs peuvent ajouter, modifier ou supprimer des comptes de service. Pour plus d'informations, voir Comptes de service sur la page 55.

Profil

Les réglages de profil vous permettent de modifier vos informations et votre préférence d'affichage Hub. Les réglages de profil que vous pouvez modifier dépendent du type d'authentification configuré pour votre compte. Si vous êtes un administrateur natif, vous pouvez modifier :

- Votre mot de passe.
- Le prénom et le nom de votre profil.
- Votre adresse e-mail.
- Votre photo de profil ; elle s'affiche dans l'icône de profil. Cette image ne sera utilisée que dans Hub.
- Votre thème d'affichage Hub ; sombre ou clair.

Si votre compte Hub est configuré pour utiliser l'authentification Active Directory, vous ne pouvez modifier que votre photo de profil et votre thème d'affichage Hub. Tous les autres réglages sont gérés dans Active Directory et mis à jour lorsque vous vous connectez à Hub ou lors d'une synchronisation manuelle .

Vous ne pouvez pas modifier votre nom d'utilisateur, quel que soit votre type d'authentification.

Pour plus d'informations sur les types d'authentification, voir Réglages d'authentification.

Pour ouvrir la page Profil, cliquez sur l'icône de votre profil pour ouvrir la page Réglages, puis sur **Profil**.

Changer votre profil

1. Sur la page Profil, cliquez sur **Modifier**.

   La page Profil devient modifiable, indiquée par le bouton **Modifier** qui devient **Annuler** et les champs deviennent modifiables.
2. Mettez à jour les éléments suivants si nécessaire :
   - Mettez à jour votre prénom, votre nom ou votre adresse e-mail.
   - Activez ou désactivez le **thème sombre**. Par défaut, Hub est affiché dans le thème clair.
   - Cliquez sur **Charger** pour sélectionner votre image de profil. L'image sera affichée dans l'icône en forme de prisme. La taille des images ne peut pas être supérieure à 1 Mo.
3. Cliquez sur **Enregistrer** pour enregistrer vos modifications. Si vous ne souhaitez pas enregistrer vos modifications, cliquez sur **Annuler**.

   Le bouton **Enregistrer** ne devient actif qu'après avoir apporté une modification au réglage de thème.

Changer votre mot de passe

1. Sur la page Profil, cliquez sur **Mettre à jour le mot de passe**.

   La boîte de dialogue Mettre à jour votre mot de passe s'affiche.
2. Saisissez votre mot de passe actuel.
3. Saisissez et répétez votre nouveau mot de passe.

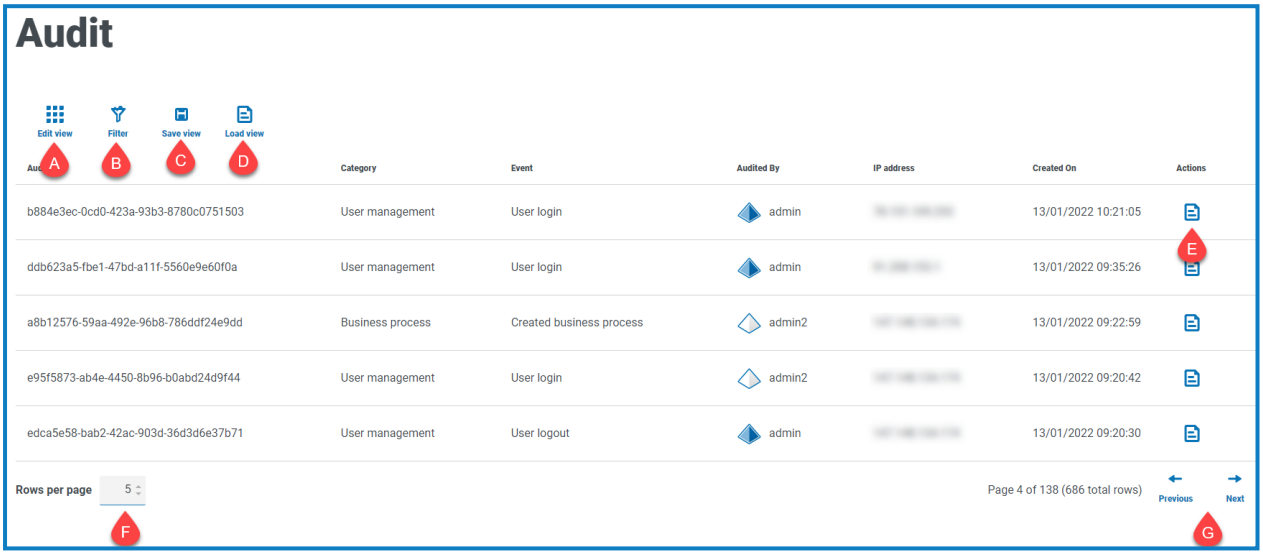
4. Cliquez sur **Mettre à jour**.

   Votre mot de passe est modifié.

Audit

Audit vous permet d'afficher les activités du système auditées. Cette zone n'est disponible que si vous êtes un administrateur.

Pour ouvrir la page Audit, cliquez sur l'icône de votre profil pour ouvrir la page Réglages, puis sur **Audit**.



La page Audit vous fournit les informations et fonctions suivantes :

A. **Modifier l'affichage** : définissez les colonnes qui sont affichées. Vous pouvez ensuite afficher ou masquer les colonnes à l'aide des boutons à bascule.

B. **Filtrer** : filtrez les informations qui sont affichées. Vous pouvez ensuite activer les filtres requis et saisir ou sélectionner les informations appropriées pour l'affichage. Vous pouvez, par exemple, activer lefiltre **Catégorie** et sélectionner **Gestion des utilisateurs**.

C. **Enregistrer l'affichage** : enregistrez les réglages de vos colonnes actuelles. Vous pouvez entrer un nom pour votre affichage afin de le rendre facilement identifiable lors du chargement des affichages.

D. **Charger l'affichage** : chargez un affichage enregistré. Vous pouvez sélectionner l'affichage requis et cliquer sur **Appliquer**.

E. **Afficher le log** : pour afficher les détails d'un élément d'audit.

F. **Lignes par page** : saisissez un nombre, ou utilisez les flèches haut et bas, pour modifier le nombre de lignes affichées sur une page.

G. **Précédent et Suivant** : cliquez sur **Précédent** ou **Suivant** pour vous déplacer dans les pages. d'éléments d'audit.

Afficher un élément

1. Sur la page Audit, cochez la case correspondant à l'élément que vous souhaitez afficher.
2. Cliquez sur **Afficher le log**.

   Les détails de l'événement s'affichent.

Utiliser les filtres sur la page Audit

Les filtres vous permettent de trouver facilement des événements d'audit en fonction des critères sélectionnés.

1. Sur la page Audit, cliquez sur **Filtrer** pour ouvrir le panneau Filtrer.
2. Utilisez le bouton bascule pour activer le filtre requis et renseignez les informations pour trouver l'événement d'audit. Vous pouvez appliquer plusieurs filtres en même temps.

   Les filtres disponibles sont les suivants :

Filtrer	Description
ID d'audit	Saisissez l'identifiant d'audit, ou une partie de l'identifiant.

Catégorie	Sélectionnez une catégorie dans la liste déroulante. Les catégories disponibles sont les suivantes :
	• **Gestion des utilisateurs** : comprend les événements liés aux utilisateurs, tels que la gestion des utilisateurs par les administrateurs et les informations d'accès des utilisateurs.
	• **Gestion SMTP** : comprend les modifications apportées aux réglages SMTP.
	• **Gestion des rôles** : comprend les événements liés aux rôles.
	• **Gestion de l'authentification** : inclut les événements liés aux réglages d'authentification, tels que la gestion des connexions et la synchronisation.
	• **Comptes de service** : comprend les événements liés aux comptes de service, tels que la gestion des comptes et la regénération de clés.
	• **Processus métier** : comprend les événements liés aux processus métier, tels que la création, le classement et l'activation des processus métier.
	Si vous sélectionnez une catégorie, les options du filtre **Événement** seront limitées à celles qui se trouvent dans la catégorie sélectionnée.
	Si les plug-ins suivants sont installés, ces catégories supplémentaires sont également disponibles :
	• **Automation Lifecycle Management (ALM) :**
	  • **Définitions de processus** : inclut les événements liés aux définitions de processus, tels que la gestion des définitions et le flux de travail de validation.
	• **Interact :**
	  • **Interact - Formulaires** : comprend les événements liés au plug-in Formulaires Interact, tels que la gestion des formulaires et l'augmentation du numéro de version majeure.
	  • **Soumissions Interact** : inclut les événements liés à Interact, tels que la soumission par l'utilisateur final de formulaires et le flux de travail d'approbation.

Filtrer	Description
Événement	Sélectionnez un événement dans la liste déroulante. Ceci affiche tous les résultats pour cet événement d'audit spécifique. Si vous utilisez le filtre **Catégorie**, les événements affichés dans la liste déroulante sont limités à ceux de cette catégorie. Si vous souhaitez afficher tous les événements pour une catégorie sélectionnée, désactivez le filtre **Événement** et utilisez simplement le filtre **Catégorie**.
Audité par	Saisissez le nom d'utilisateur ou le nom de compte d'un utilisateur, ou une partie du nom.
Adresse IP	Saisissez l'adresse IP publique, ou une partie de l'adresse.
Créé le	Saisissez une plage de dates : • Dans le premier champ, sélectionnez la date la plus proche. • Dans le second champ, sélectionnez la date la plus lointaine. • Si nécessaire, ajustez les champs d'heure. Par défaut, l'heure de la date antérieure est 00:00:00 et celle de la date ultérieure est 23:59:59, incluant ainsi la journée complète. Cela affiche tous les événements d'audit pendant cette période.

Les informations sur la page Audit sont immédiatement filtrées.

Si vous avez défini les filtres, mais que vous souhaitez afficher à nouveau les informations non filtrées, désactivez les filtres requis ou supprimez tous les réglages du filtre afin qu'il soit vide.

3. Cliquez sur **Fermer le tiroir** pour fermer le panneau Filtrer.

Gestion des environnements

Le gestionnaire d'environnements affiche vos bases de données connectées. Cette zone n'est disponible que si vous êtes un administrateur.

La page Environnement vous fournit les informations et fonctions suivantes :

A. La base de données Hub.

B. La base de données Blue Prism qui a été configurée dans le cadre du processus d'installation initial.

C. Actualise les détails de la main d'œuvre numérique et les files d'attente dans Hub. Actualisez la base de données chaque fois que des connexions sont ajoutées ou modifiées. Si la base de données n'est pas actualisée, vous ne pourrez pas voir les travailleurs numériques ou les files d'attente dans cet environnement Blue Prism particulier.

D. Ouvre la page Modifier la connexion qui vous permet de modifier les détails de la base de données.

E. Supprime la connexion à la base de données. Voir Supprimer une connexion de base de données pour plus d'informations.

F. Ouvre la boîte de dialogue Ajouter une connexion qui vous permet de configurer et d'ajouter une nouvelle connexion à la base de données Blue Prism.

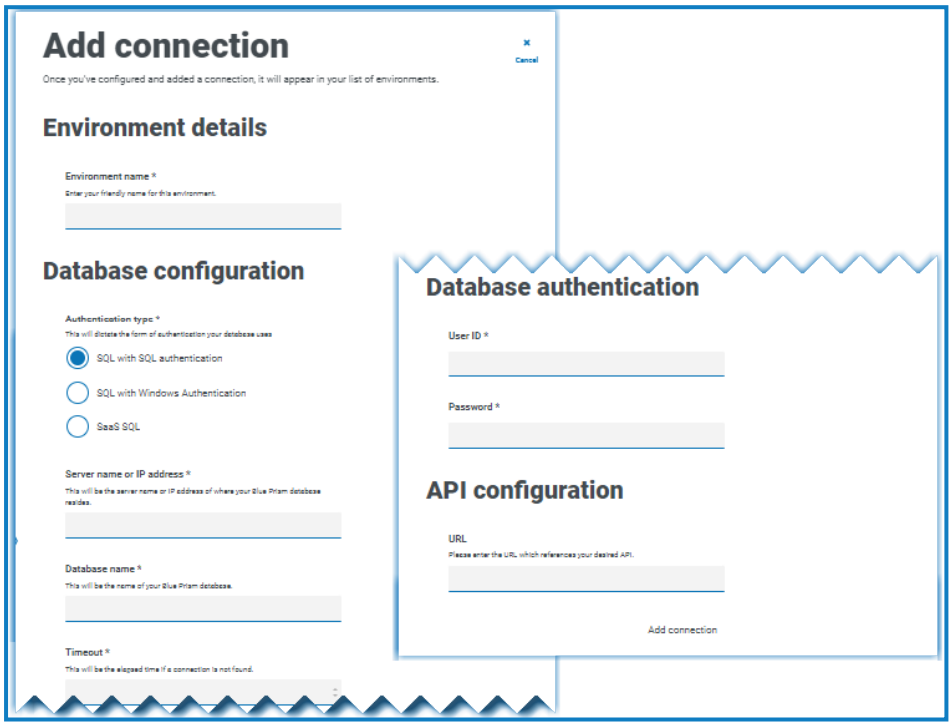
Pour ouvrir le gestionnaire d'environnement, cliquez sur l'icône de votre profil pour ouvrir la page Réglages, puis sur **Gestion des environnements**.

Ajouter une connexion à la base de données Blue Prism

1. Sur la page Gestionnaire d'environnements, cliquez sur **Ajouter une connexion** pour ajouter une connexion de base de données RPA supplémentaire.

   La page Ajouter une connexion s'affiche.

2. Entrez les paramètres de configuration de la connexion de base de données.



   Lorsque tous les champs sont remplis, le lien **Ajouter une connexion** est disponible.

   > ⚠ Vous devez vous assurer que votre mot de passe de base de données ne contient pas de signe égal (=) ou de point-virgule (;). Ces caractères ne sont pas pris en charge et entraîneront des problèmes lors de la tentative de connexion à la base de données.

3. Si nécessaire, saisissez l'URL de l'API Blue Prism API dans le champ URL sous Configuration de l'API. Cette URL est requise si vous souhaitez utiliser le plug-in Control Room. Le plug-in Control Room est compatible avec Blue Prism 7.0 ou une version ultérieure.
4. Cliquez sur **Ajouter une connexion** pour enregistrer les détails.

   La connexion est créée et affichée dans le gestionnaire d'environnements.

5. Dans le gestionnaire d'environnements, cliquez sur l'icône Actualiser sur votre nouvelle connexion. Cela met à jour les informations dans Hub avec la main-d'œuvre numérique et les files d'attente conservées dans la base de données.

Modifier les détails de la base de données

Vous ne pouvez modifier que le champ URL sous Configuration de l'API. Tous les autres champs sont désactivés.

1. Sur la page Gestionnaire d'environnement, cliquez sur l'icône **Modifier** de la connexion de la base de données que vous souhaitez mettre à jour.

   La page Modifier la connexion s'affiche.

2. Saisissez **l'URL** sous la section **Configuration de l'API**.

   > Vous devez saisir l'URL complète, y compris le protocole, tel que http:// ou https://. Par exemple : *https://bpapi.votredomaine.com*.

3. Cliquez sur **Enregistrer**.
4. Dans le Gestionnaire d'environnements, cliquez sur l'icône d'actualisation de votre connexion mise à jour. Cela met à jour les informations dans Hub avec les travailleurs numériques et les files d'attente conservées dans la base de données.

Supprimer une connexion de base de données

Vous pouvez supprimer une connexion à une base de données uniquement s'il n'y a aucune dépendance sur cette base de données. Vous ne pourrez pas supprimer une base de données si :

- Les formulaires Interact dépendent d'une file d'attente au sein de cette base de données RPA, par exemple, la soumission d'un formulaire à une file d'attente.
- Les définitions de processus ALM utilisent des objets définis dans cette base de données RPA.

Vous devez modifier les formulaires ou les définitions de processus pour pointer vers une autre base de données afin de supprimer la dépendance.

La fonction de suppression vous permet de supprimer toutes les bases de données qui ont été ajoutées accidentellement et qui ne sont pas utilisées. Par exemple, si des informations de base de données erronées ont été ajoutées pendant la configuration.

Pour supprimer une base de données RPA :

1. Sur la page Gestionnaire d'environnements, cliquez sur l'icône Supprimer sur la dalle de la base de données.

   S'il n'y a pas de dépendance, un message s'affiche vous demandant de confirmer la suppression. S'il existe des dépendances, un message d'erreur s'affiche dans le coin supérieur droit de l'interface utilisateur Hub.

2. Cliquez sur **Oui** pour confirmer la suppression.

Configuration de l'adresse e-mail

Les réglages de messagerie permettent de modifier la configuration de SMTP et de configurer l'adresse e-mail pour les notifications, telles que les demandes de réinitialisation de mot de passe des utilisateurs. Cette zone n'est disponible que si vous êtes un administrateur. Des modifications doivent être apportées en collaboration avec votre propre équipe d'assistance informatique pour s'assurer que la configuration et les identifiants correspondent au serveur de messagerie de votre entreprise.

Vous pouvez configurer les réglages de vos e-mails pour utiliser l'une des méthodes d'authentification suivantes :

- Nom d'utilisateur et mot de passe
- Microsoft OAuth 2.0

Chaque fois que vous enregistrez les réglages SMTP, un e-mail de test vous est envoyé pour vous assurer que la configuration est correcte. Si vous ne recevez pas d'e-mail de test après avoir enregistré les modifications, vérifiez les détails et mettez-les à jour en conséquence.

Pour ouvrir la page Configuration de l'adresse e-mail, cliquez sur l'icône de votre profil pour ouvrir la page Réglages, puis sur **Configuration de l'adresse e-mail**.

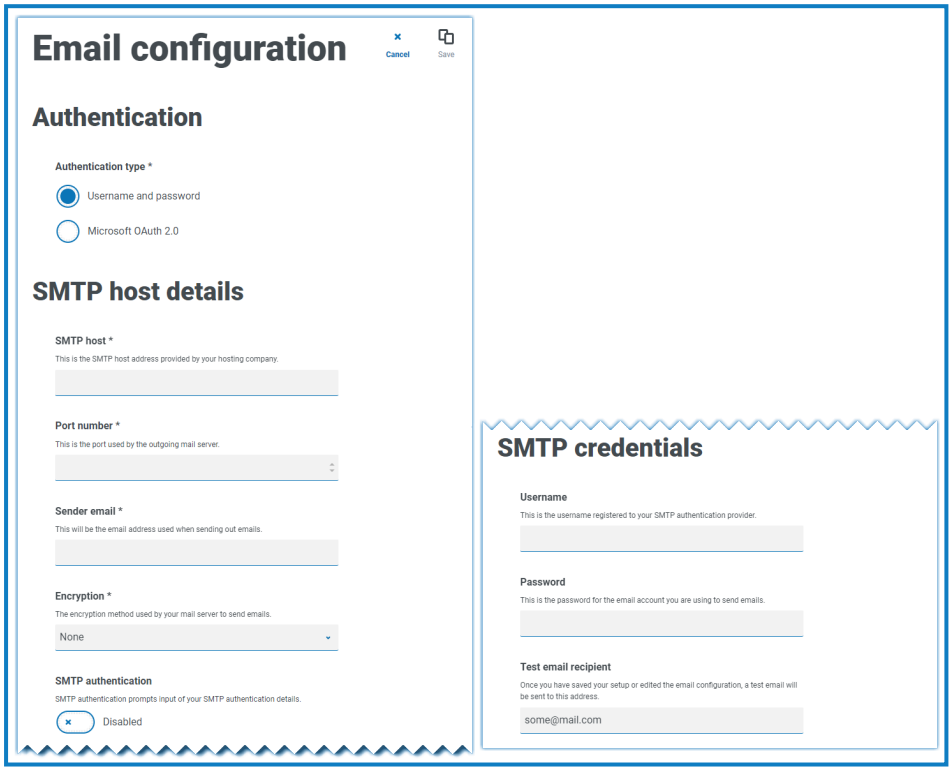
Mettre à jour les réglages des e-mails

Les réglages des e-mails sont entrés dans le cadre de la configuration initiale de Hub. Vous n'avez besoin de modifier ces réglages qu'en cas de modification d'une infrastructure informatique, telle qu'un hôte SMTP différent, ou d'une modification de l'hôte existant qui affecte ces réglages.

Authentification par nom d'utilisateur et mot de passe

1. Sur la page Configuration de l'adresse e-mail, cliquez sur **Modifier**.
2. Dans la section Authentification, sous **Type d'authentification**, sélectionnez **Nom d'utilisateur et mot de passe**.

   La page Configuration de l'adresse e-mail est actualisée pour afficher les champs appropriés :



3. Saisissez les informations suivantes :
   - **Hôte SMTP** : l'adresse de votre hôte SMTP.
   - **Numéro de port** : le numéro de port utilisé par le serveur de messagerie sortant.
   - **Adresse e-mail de l'expéditeur** : l'adresse e-mail utilisée lors de l'envoi d'e-mails. Les destinataires des e-mails verront cela comme l'adresse De.
   - **Chiffrement** : la méthode de chiffrement utilisée par le serveur de messagerie pour envoyer les e-mails.
   - **Authentification SMTP** : sélectionnez cette option si l'authentification SMTP demande la saisie des informations d'authentification. Si vous définissez ce paramètre sur **Activé**, les champs **Nom d'utilisateur** et **Mot de passe** deviennent obligatoires.
   - **Nom d'utilisateur** : le nom d'utilisateur pour l'authentification SMTP.
   - **Mot de passe** : le mot de passe du compte.
   - **Destinataire de l'e-mail de test** : l'e-mail de test sera envoyé à cette adresse e-mail. Par défaut, l'adresse e-mail de l'utilisateur qui apporte les modifications est utilisée et ne peut pas être modifiée.
4. Cliquez sur **Enregistrer** pour enregistrer vos modifications.

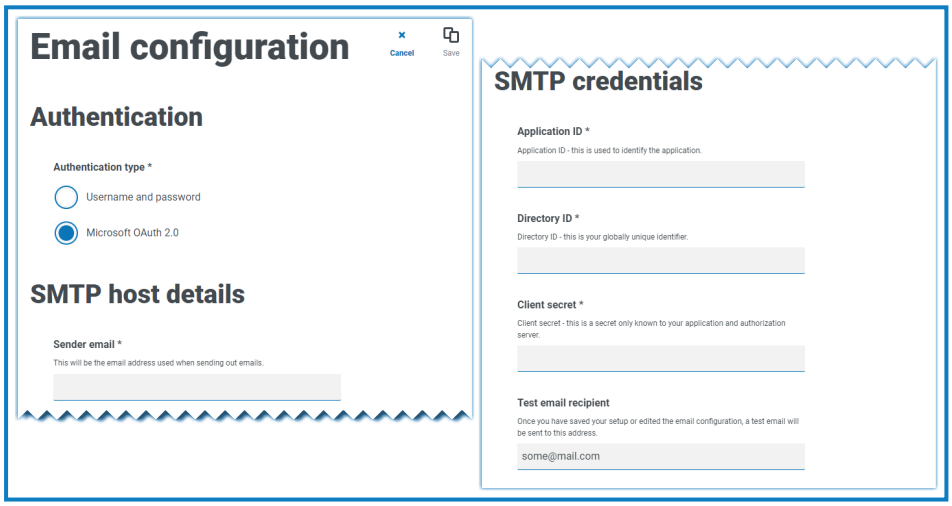
Authentification Microsoft OAuth 2.0

Vous pouvez utiliser le service d'authentification Microsoft OAuth 2.0 fourni par Azure Active Directory pour vous connecter à l'hôte SMTP. Votre équipe d'assistance informatique devra enregistrer une application dans Azure AD et vous fournir l'ID d'application (client), l'ID de répertoire (locataire) et le secret client pour compléter les informations de l'étape 3. Pour plus d'informations sur la recherche de ces détails dans Azure AD, consultez la documentation Microsoft.

Si vous utilisez Microsoft OAuth 2.0, la permission Mail.Send doit être activée dans Azure Active Directory. Cela doit être configuré par votre équipe d'assistance informatique dans Azure Active Directory. Pour plus d'informations, voir Dépanner une installation Hub dans le guide d'installation de Blue Prism Hub.

1. Sur la page Configuration de l'adresse e-mail, cliquez sur **Modifier**.
2. Dans la section Authentification, sous **Type d'authentification**, sélectionnez **Microsoft OAuth 2.0**.

   La page Configuration de l'adresse e-mail est actualisée pour afficher les champs appropriés :



3. Saisissez les informations suivantes :
   - **Adresse e-mail de l'expéditeur** : l'adresse e-mail utilisée lors de l'envoi d'e-mails. Les destinataires des e-mails verront cela comme l'adresse De.
   - **ID d'application** : ces informations sont l'ID d'application (client) défini dans Azure AD et vous seront fournies par votre équipe d'assistance informatique.
   - **ID de répertoire** : ces informations sont l'ID de répertoire (locataire) défini dans Azure AD et vous seront fournies par votre équipe d'assistance informatique.
   - **Secret client** : il s'agit du secret client généré par Azure AD et qui vous sera fourni par votre équipe d'assistance informatique et qui contrôle le processus d'authentification.
   - **Destinataire de l'e-mail de test** : l'e-mail de test sera envoyé à cette adresse e-mail. Par défaut, l'adresse e-mail de l'utilisateur qui apporte les modifications est utilisée et ne peut pas être modifiée.
4. Cliquez sur **Enregistrer** pour enregistrer vos modifications.

Personnalisation

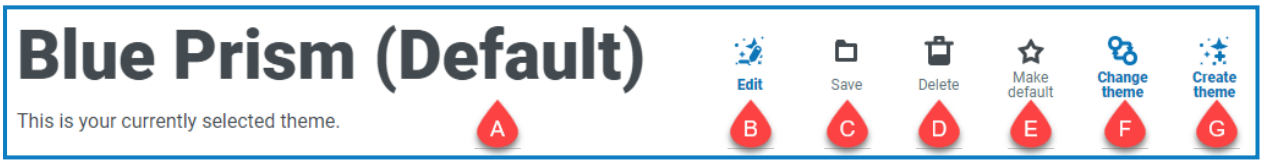
Les réglages de personnalisation vous permettent de modifier l'apparence de l'interface utilisateur Interact. Cette zone n'est disponible que si vous êtes un administrateur. Vous pouvez créer des thèmes qui contrôlent les éléments suivants :

- **Nom du thème** : il s'agit également du nom de marque qui apparaîtra sur l'interface utilisateur.
- **Couleur de la marque** : il s'agit de la couleur qui sera utilisée par les boutons et les étiquettes dans l'interface utilisateur.
- **Logo de la marque** : il s'agit d'une image qui sera utilisée comme logo sur l'interface utilisateur.

Vous pouvez créer plusieurs thèmes pouvant être appliqués en fonction de l'utilisateur, en fournissant une apparence et une convivialité différentes selon la personne qui se connecte. Le thème par défaut est automatiquement sélectionné lors de la création d'un utilisateur. Cependant, il peut être modifié.

Pour ouvrir la page Personnalisation, cliquez sur l'icône de votre profil pour ouvrir la page Réglages, puis sur **Personnalisation**.

Lorsque vous ouvrez la page Personnalisation, le thème par défaut s'affiche :



Cela vous fournit les informations et fonctions suivantes :

A. Nom du thème actuellement affiché.
B. Modifier : pour modifier le thème actuellement affiché.
C. Enregistrer : pour enregistrer toutes les modifications que vous avez apportées. Cette icône n'est active que lorsque vous modifiez un thème.
D. Supprimer : pour supprimer le thème actuellement affiché. Cette icône n'est active que si vous disposez de plusieurs thèmes.
E. Définir par défaut : pour définir le thème actuellement affiché comme thème par défaut pour le système. Cette icône n'est active que si le thème actuel n'est pas celui par défaut.
F. Changer le thème : pour sélectionner le thème que vous souhaitez afficher sur la page.
G. Créer un thème : pour créer un thème.

Modifier et enregistrer un thème

1. Sur la page Personnalisation, cliquez sur **Modifier le thème**.

   La page Thème devient modifiable, indiqué par le bouton **Modifier le thème** qui devient **Annuler** et le bouton **Réinitialiser** qui devient actif.

2. Si nécessaire, modifiez le **nom** du thème.

   À mesure que vous tapez, le titre *Créer un thème* change également.

3. Si nécessaire, modifiez la **couleur principale** en cliquant sur la barre de couleur. Vous pouvez :
   - Sélectionner une couleur à l'aide de la barre coulissante.
   - Saisir une valeur à l'aide des zones de texte. Vous pouvez cliquer sur l'icône ⇕ pour basculer entre les différents types : RVB, HSL ou Hex.

4. Si nécessaire, cliquez sur **Charger** pour modifier le logo par un fichier de votre choix.
5. Cliquez sur **Enregistrer** pour enregistrer vos modifications. Si vous ne souhaitez pas enregistrer vos modifications, cliquez sur **Annuler**.

> Le bouton **Enregistrer** ne devient actif qu'après avoir apporté une modification au réglage de thème.

Supprimer un thème

1. Avec le thème que vous souhaitez supprimer affiché à l'écran (voir Changer le thème en dessous), cliquez sur **Supprimer**.

   Un message s'affiche vous demandant de confirmer la suppression.
2. Cliquez sur **Oui** pour supprimer le thème.

Définir un nouveau thème par défaut

1. Cliquez sur **Définir par défaut** avec le thème que vous souhaitez utiliser affiché à l'écran (voir Changer le thème en dessous).

   (par défaut) apparaît à côté du nom du thème et une notification apparaît pour confirmer la modification. Le changement de thème se verra dans Interact.

Changer le thème

> L'icône **Changer le thème** modifie le thème que vous êtes en train d'afficher. Si vous souhaitez apporter des modifications au thème lui-même, vous devez modifier le thème.

1. Sur la page Personnalisation, cliquez sur **Changer le thème**.

   Une liste des thèmes disponibles s'affiche.
2. Cliquez sur le thème que vous souhaitez afficher.

   Le thème sélectionné s'affiche.
3. Fermez la liste pour revenir aux principaux outils.

Créer un thème

1. Sur la page Personnalisation, cliquez sur **Créer un thème**.

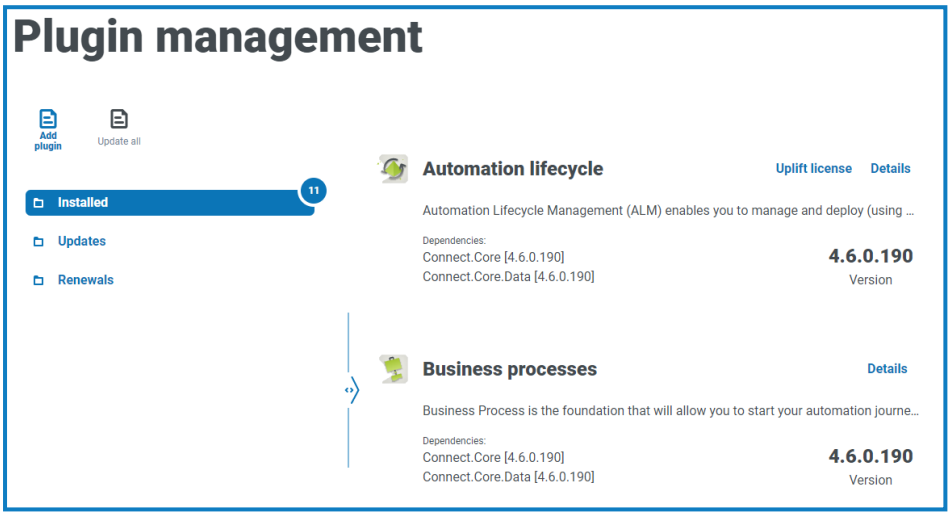
   La page Créer un thème s'affiche.
2. Saisissez le **nom** du thème.

   À mesure que vous tapez, le titre *Créer un thème* change également.
3. Cliquez sur la barre **Couleur principale** pour modifier la couleur. Vous pouvez :
   - Sélectionner une couleur à l'aide de la barre coulissante.
   - Saisir une valeur à l'aide des zones de texte. Vous pouvez cliquer sur l'icône ⇕ pour basculer entre les différents types : RVB, HSL ou Hex.
4. Cliquez sur **Charger** pour modifier le logo par un fichier de votre choix.
5. Cliquez sur **Créer un thème** pour enregistrer votre nouveau thème.

Gestion des plug-ins

La gestion des plug-ins affiche les détails des plug-ins installés, certains étant disponibles par défaut pendant le processus d'installation. Vous pouvez gérer vos plug-ins existants, les mettre à jour et ajouter de nouveaux plug-ins. Cette zone n'est disponible que si vous êtes un administrateur.

Les plug-ins sont au cœur de Hub et sont des fonctionnalités autonomes qui peuvent être installées individuellement et personnalisées pour fournir des informations sur vos processus automatisés. Certains plug-ins fournissent également des outils de développement pour faciliter la création d'automatisations.



Pour ouvrir la page Gestion des plug-ins, cliquez sur l'icône de votre profil pour ouvrir la page Réglages, puis sur **Gestion des plug-ins**.

Afficher les plug-ins installés

Lorsque vous ouvrez la page Gestion des plug-ins, les plug-ins actuellement installés sont affichés. Le nom du plug-in, un extrait de la description et les numéros de version sont affichés. Pour afficher :

- plus d'informations sur un plug-in, cliquez sur **Détails**.
- des informations sur les mises à jour, cliquez sur **Mises à jour**. Notez que cette fonctionnalité n'est actuellement pas disponible pour Hub sur site.
- des informations sur les renouvellements de licence à venir ou en attente, cliquez sur **Renouvellements**. Si des plug-ins nécessitent un renouvellement de licence, un nombre s'affiche à côté du lien **Renouvellements** indiquant le nombre de mises à jour. Si aucun numéro n'est affiché, il n'y a aucun renouvellement.

Ajouter un plug-in

Lorsqu'un plug-in est installé, le site Web redémarre automatiquement. Il est donc essentiel que l'installation des plug-ins soit effectuée en dehors des heures d'ouverture ou pendant les périodes de maintenance.

1. Sur la page Gestion des plug-ins, cliquez sur **Ajouter un plug-in**.

   La boîte de dialogue Ouvrir s'affiche pour vous permettre de trouver un fichier local.
2. Naviguez jusqu'au fichier du plug-in, sélectionnez-le et cliquez sur **Ouvrir**.

   Le fichier du plug-in charge et s'installe. Le site Web redémarre automatiquement pour terminer l'installation.

Mettre à jour les plug-ins

Lorsqu'une mise à jour est disponible, un numéro apparaît à côté du lien **Mises à jour**.

Cette fonctionnalité est uniquement disponible pour les installations sur site de Hub immédiatement après une mise à niveau. La version sur site ne peut pas vérifier les mises à jour en ligne entre les mises à niveau.

1. Sur la page Gestion des plug-ins, cliquez sur **Mises à jour**.

   Les mises à jour potentielles s'affichent avec les détails de la nouvelle version.
2. Cliquez sur **Mettre à jour tout** pour mettre à jour tous les plug-ins.

   Un message s'affiche confirmant que les plug-ins ont été mis à jour.
3. Cliquez sur **OK**.

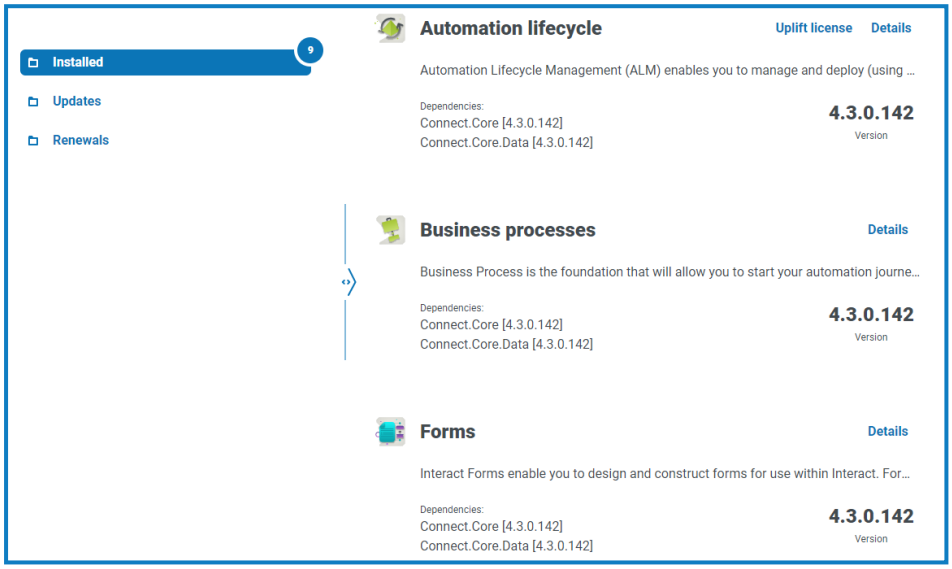
   Le site redémarre.

Mettre à niveau la licence

L'option **Mettre à niveau la licence** n'est disponible que lorsqu'il y a eu une mise à jour du modèle de licence utilisé par un plug-in entre les versions publiées. Elle vous permet de charger une nouvelle licence pour votre plug-in en dehors de la période de renouvellement normale.

1. Sur la page Gestion des plug-ins, cliquez sur **Installés**.

   Les plug-ins installés s'affichent.



2. Cliquez sur **Mettre à niveau la licence** pour le plug-in requis. Dans l'exemple ci-dessus, l'option apparaît pour le cycle de vie automatisé.

   Le panneau Renouveler la clé de licence s'affiche.

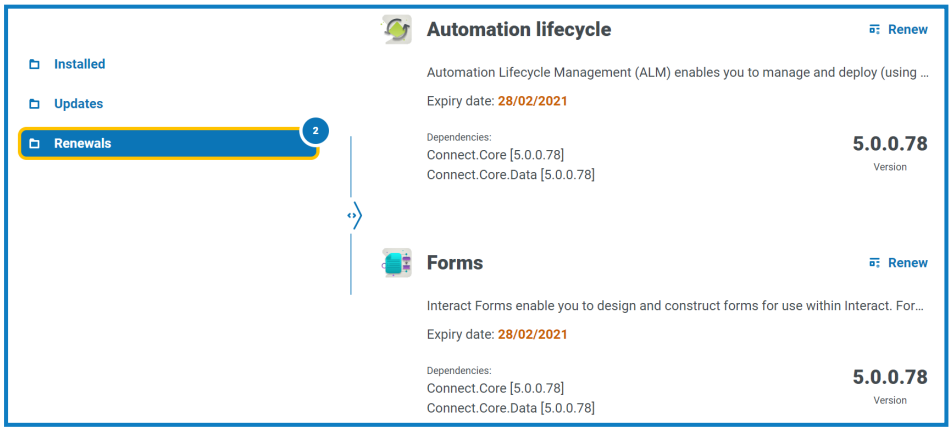
3. Chargez une licence valide et cliquez sur **Terminer** pour l'appliquer.

Renouveler les plug-ins

Vous recevez un préavis de 14 jours avant l'expiration de la licence.

1. Sur la page Gestion des plug-ins, cliquez sur **Renouvellements**.

   Les plug-ins arrivant à expiration s'affichent.

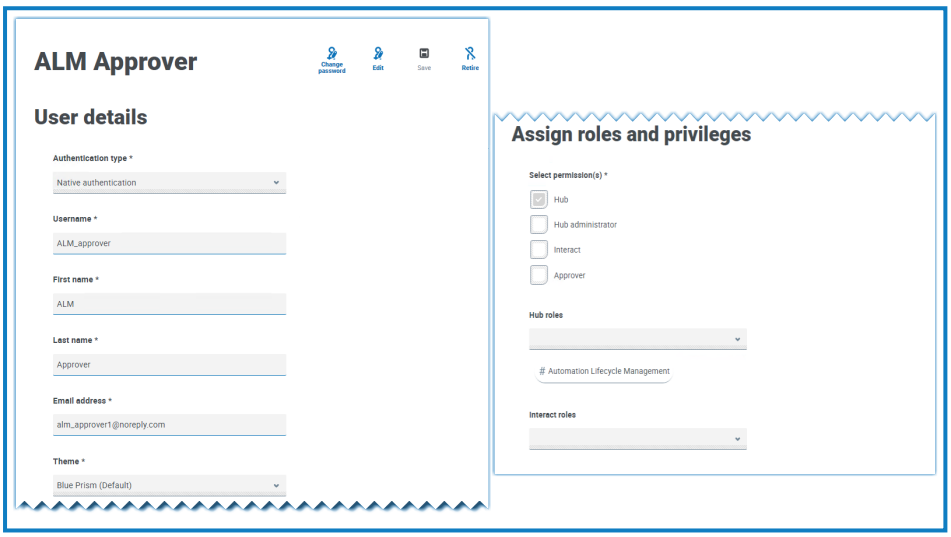


2. Cliquez sur **Renouveler** à côté du plug-in requis.
3. Chargez une licence valide et cliquez sur **Terminer** pour l'appliquer.

Utilisateurs

Les réglages utilisateur vous permettent de gérer les comptes utilisateur dans Hub en fonction de leur type d'authentification. Il peut s'agir de l'authentification native pour les utilisateurs natifs ou de l'authentification Windows pour les utilisateurs Active Directory. Vous pouvez également définir l'accès de l'utilisateur à Hub et à Interact et à ses rôles dans ces derniers. Avant de configurer les utilisateurs, il est recommandé de configurer les rôles d'utilisateur.

La page Utilisateurs affiche une liste des utilisateurs existants. Vous pouvez cliquer sur un utilisateur pour afficher ses informations. Si seule l'authentification native a été configurée dans votre environnement, le champ Type d'authentification est masqué.



Pour ouvrir la page Utilisateurs, cliquez sur l'icône de votre profil pour ouvrir la page Réglages, puis sur **Utilisateurs**.

Trouver des utilisateurs

La page Utilisateurs comprend deux méthodes pour trouver des utilisateurs :

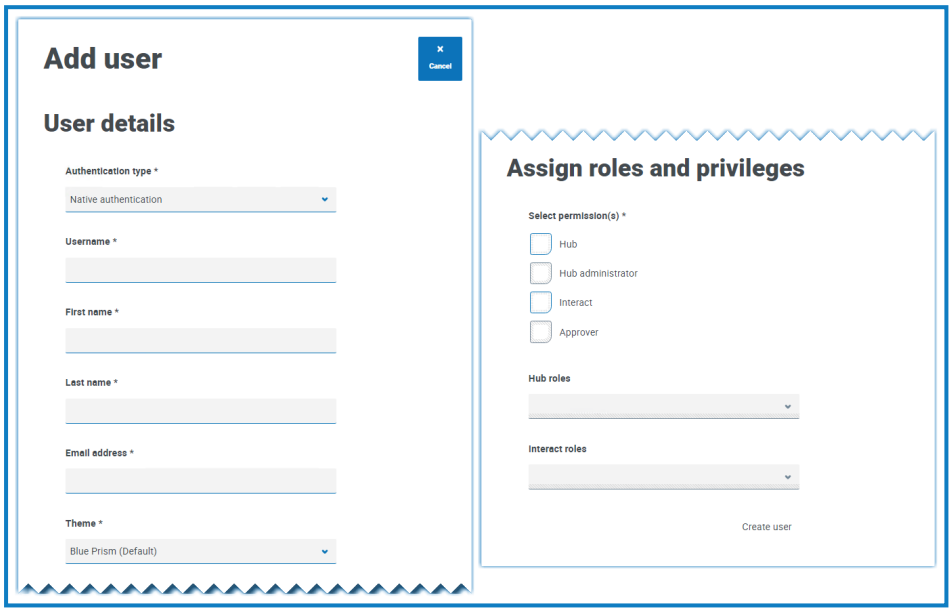
- **Champ de** par nom d'utilisateur : il se trouve au-dessus de la liste des utilisateurs. Commencez à taper le nom d'un utilisateur pour filtrer les résultats de la recherche. La liste filtre de façon dynamique à mesure que vous saisissez plus de caractères.
- **Filtres** : les filtres vous permettent de trouver facilement un utilisateur spécifique ou des types d'utilisateurs en fonction des critères sélectionnés. Cliquez sur **Filtrer** pour afficher et utiliser les filtres. Par défaut, les filtres sont définis pour vous montrer uniquement les utilisateurs actifs et non les utilisateurs classés. Si vous souhaitez voir tous les utilisateurs, désactivez le filtre **Actif**. Pour en savoir plus, voir Utiliser les filtres sur la page Utilisateurs sur la page 31.

Ajouter des utilisateurs

Ajouter un utilisateur natif

1. Sur la page Utilisateurs, cliquez sur **Ajouter un utilisateur**.

   La section Ajouter un utilisateur s'affiche.



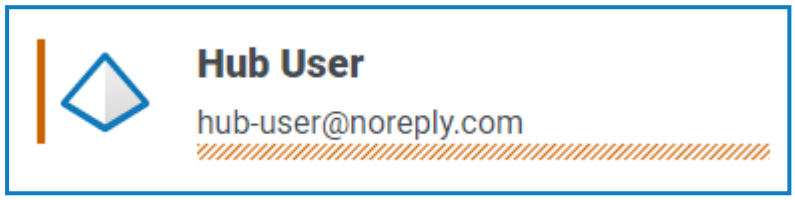
2. Saisissez les détails de l'utilisateur :
   - **Type d'authentification** (si affiché) : sélectionnez **Authentification native**.

     Ce champ s'affiche uniquement si l'authentification native et l'authentification Windows ont été configurées dans votre environnement. Si seule l'authentification native a été configurée, l'utilisateur ajouté est un utilisateur natif par défaut.

   - **Nom d'utilisateur** : saisissez un nom d'utilisateur pour l'utilisateur.
   - **Prénom** : saisissez le prénom de l'utilisateur.
   - **Nom** : saisissez le nom de l'utilisateur.
   - **Adresse e-mail** : saisissez l'adresse e-mail de l'utilisateur.
   - **Thème** : le thème par défaut est automatiquement sélectionné. Vous pouvez sélectionner un thème différent pour l'utilisateur. Voir Personnalisation sur la page 20 pour plus d'informations sur les thèmes.
3. Sélectionnez les permissions pour l'utilisateur :
   - **Hub** : cochez cette case pour les utilisateurs et administrateurs Hub standard.
   - **Administrateur Hub** : cochez cette case pour accorder les permissions d'administrateur au rôle d'utilisateur. Vous devez sélectionner **Hub** avant que cette option ne soit disponible.
   - **Interact** : cochez cette case pour permettre à l'utilisateur de se voir attribuer des formulaires Interact. Voir le guide de l'utilisateur Interact pour plus d'informations.
   - **Approbateur** : cochez cette case pour accorder les droits d'approbation pour Interact au rôle d'utilisateur. Vous devez sélectionner **Interact** avant que cette option ne soit disponible.

4. Sélectionnez les rôles pour l'utilisateur :
   - **Rôles Hub** : sélectionnez les rôles Hub requis pour l'utilisateur. Si le rôle requis n'a pas encore été créé, vous pouvez modifier l'utilisateur à une date ultérieure pour attribuer de nouveaux rôles.

     Si l'utilisateur est créé sans rôle Hub, il est souligné dans la liste des utilisateurs pour indiquer que la configuration de l'utilisateur n'a pas été effectuée, par exemple :

     L'utilisateur pourra se connecter à Hub, mais il ne pourra pas effectuer de tâches, car il n'aura pas accès aux plug-ins.
   - **Rôles Interact** : sélectionnez les rôles Interact requis pour l'utilisateur. Si le rôle requis n'a pas encore été créé, vous pouvez modifier l'utilisateur à une date ultérieure pour attribuer de nouveaux rôles. Vous pouvez sélectionner plusieurs rôles.

   Les utilisateurs peuvent également être ajoutés aux rôles à partir de la page Rôles et permissions.
5. Cliquez sur **Créer un utilisateur**.

   La boîte de dialogue Créer un mot de passe s'affiche.
6. Sélectionnez l'une des options de mot de passe :
   - **Envoyer à l'utilisateur un e-mail de mise à jour du mot de passe** : cela envoie à l'utilisateur un e-mail l'invitant à entrer un mot de passe lors de la connexion à l'aide d'un lien.
   - **Mettre à jour manuellement le mot de passe de l'utilisateur** : cela vous permet de définir un mot de passe pour l'utilisateur.

   Les mots de passe doivent respecter les restrictions au sein de Hub. Pour en savoir plus, voir Restrictions de Hub sur la page 6.
7. Cliquez sur **Continuer**.
   - Si vous avez choisi d'envoyer à l'utilisateur un e-mail de mise à jour du mot de passe, cliquez sur **Terminer** dans la boîte de dialogue de confirmation.
   - Si vous avez choisi de définir un mot de passe pour l'utilisateur, définissez un mot de passe et cliquez sur **Créer**.

Le nouvel utilisateur apparaît dans la liste des utilisateurs.

Ajouter un utilisateur Active Directory

Pour ajouter un utilisateur Active Directory, l'authentification Windows doit être configurée pour votre environnement et l'authentification Active Directory doit être activée sur la page Réglages d'authentification. Voir Réglages d'authentification sur la page 43 pour en savoir plus.

Vous pouvez ajouter un utilisateur Active Directory en suivant les étapes ci-dessous ou en ajoutant un groupe de sécurité Active Directory à un rôle où les utilisateurs membres du rôle de sécurité sont automatiquement ajoutés à Hub lorsqu'ils se connectent pour la première fois. Voir Ajouter des groupes de sécurité Active Directory à un rôle sur la page 36 pour en savoir plus.

1. Sur la page Utilisateurs, cliquez sur **Ajouter un utilisateur**.

   La section Ajouter un utilisateur s'affiche.

2. Dans le champ **Type d'authentification**, sélectionnez **Authentification Windows**.
3. Cliquez sur **Rechercher dans Active Directory**.

   Le tiroir Rechercher dans Active Directory s'ouvre.

   > Avant de rechercher des utilisateurs dans Active Directory, assurez-vous qu'un nom d'utilisateur (UPN) et qu'une adresse e-mail sont renseignés pour eux dans Active Directory.

4. Saisissez la racine de recherche pour l'utilisateur Active Directory que vous souhaitez ajouter. Il s'agit du nom distinctif de l'emplacement racine, par exemple, dc=bvdevops,dc=co,dc=uk.

   Vous pouvez également utiliser la recherche par caractères génériques et appliquer des filtres de recherche basés sur :

   - **CN** : l'attribut Nom commun contient les noms d'un objet. Si l'objet correspond à une personne, il s'agit généralement du nom complet de la personne.
   - **UPN** : un nom d'utilisateur principal correspond au nom d'un utilisateur du système dans un format d'adresse e-mail. Un UPN se compose du nom d'utilisateur (nom de connexion), du séparateur (le symbole @) et du nom de domaine (suffixe UPN). Par exemple : john.doe@domaine.com.
   - **SID** : un identificateur de sécurité est un identifiant unique et immuable d'un utilisateur, d'un groupe d'utilisateurs ou d'un autre principal de sécurité. Un principal de sécurité dispose d'un SID unique à vie (dans un domaine donné) et toutes les propriétés du principal, y compris son nom, sont associées au SID.

5. Une fois que vous avez saisi les critères de recherche, cliquez sur **Rechercher**.

> Les identifiants stockés dans le domaine de la base de données Authentication Server sont utilisés pour rechercher des utilisateurs ou des groupes de sécurité dans Active Directory. Si aucun identifiant stocké n'est trouvé, les requêtes nécessitant une authentification supplémentaire seront exécutées dans le contexte du compte Windows exécutant le pool d'applications Authentication Server dans IIS.

Les utilisateurs disponibles s'affichent. Vous pouvez faire défiler vers le bas pour afficher tous les utilisateurs récupérés.

6. Sélectionnez l'utilisateur que vous souhaitez ajouter et cliquez sur **Appliquer**. Vous ne pouvez sélectionner qu'un seul utilisateur à la fois. Les utilisateurs précédemment ajoutés sont grisés et ne peuvent pas être sélectionnés.
7. Sur la page Ajouter un utilisateur, sélectionnez les permissions et les rôles du nouvel utilisateur (voir les étapes 3 et 4 dans la section Ajouter un utilisateur natif) et cliquez sur **Créer un utilisateur**.

Le nouvel utilisateur apparaît dans la liste des utilisateurs.

> Les identifiants des utilisateurs Active Directory sont gérés dans Active Directory, vous n'avez donc pas besoin de créer un mot de passe pour l'utilisateur. Ces utilisateurs peuvent se connecter à Hub à l'aide de l'authentification unique en sélectionnant l'option **Connexion à l'aide d'Active Directory** sur la page de connexion.

Modifier des utilisateurs

1. Sur la page Utilisateurs, sélectionnez l'utilisateur requis et cliquez sur **Modifier**.
2. Modifiez les informations comme requis.

   Si l'utilisateur est :

   - un utilisateur natif, vous pouvez modifier les informations si nécessaire.
   - un utilisateur Active Directory, vous ne pouvez modifier que ses rôles et permissions. Tous les autres détails sont gérés dans Active Directory.

   Vous ne pouvez pas changer leur nom d'utilisateur.
3. Cliquez sur **Enregistrer** pour appliquer vos modifications.

Synchroniser un utilisateur Active Directory

1. Sur la page Utilisateurs, sélectionnez l'utilisateur Active Directory requis.
2. Cliquez sur **Synchroniser l'utilisateur**.

Les détails suivants d'un utilisateur Active Directory sont actualisés : UPN, nom d'utilisateur, nom complet, adresse e-mail et statut (actif, supprimé ou désactivé).

Classer des utilisateurs natifs

1. Sur la page Utilisateurs, sélectionnez l'utilisateur requis et cliquez sur **Classer**.

   Un message s'affiche vous demandant de confirmer.

   Vous pouvez utiliser le filtre **Actif** pour filtrer la liste des utilisateurs pour afficher les utilisateurs classés. Voir Trouver des utilisateurs sur la page 25.
2. Cliquez sur **Oui**.

   L'utilisateur est classé et l'icône **Classer** est remplacée par l'icône **Activer**. Vous pouvez l'utiliser pour rétablir l'utilisateur si nécessaire. L'utilisateur est également souligné dans la liste des utilisateurs pour indiquer qu'ils sont classés.

Déverrouiller des utilisateurs natifs

Si un utilisateur saisit son mot de passe incorrectement cinq fois, il sera bloqué dans le système pendant trois heures. Sinon, vous pouvez déverrouiller son compte.

1. Sur la page Utilisateurs, sélectionnez l'utilisateur requis et cliquez sur **Déverrouiller**.

   Un message de notification s'affiche confirmant que l'utilisateur a été déverrouillé avec succès.

   Vous pouvez utiliser le filtre **Verrouillé** pour filtrer la liste des utilisateurs et afficher les utilisateurs verrouillés. Voir Trouver des utilisateurs sur la page 25.

Modifier le mot de passe pour les utilisateurs natifs

Les utilisateurs natifs peuvent modifier leur propre mot de passe à l'aide de la page Profil (pour plus d'informations, voir Profil sur la page 9). Si un utilisateur a oublié son mot de passe, il peut utiliser le lien **Mot de passe oublié** sur la page de connexion. Toutefois, vous pouvez modifier son mot de passe si

nécessaire. Par exemple, vous pouvez le faire si un utilisateur était un approbateur Interact, qu'il a quitté votre organisation et qu'il y a des formulaires en attente d'approbation par des approbateurs dans Interact. En fonction de la politique de votre organisation, vous pouvez accéder à son compte et les traiter.

1. Sur la page Utilisateurs, sélectionnez l'utilisateur requis et cliquez sur **Modifier le mot de passe**.

   L'écran Modifier le mot de passe s'affiche.
2. Saisissez un nouveau mot de passe pour l'utilisateur dans les deux champs. Le mot de passe doit répondre aux restrictions de caractères, cependant, la restriction concernant la réutilisation du mot de passe n'est pas appliquée. Pour en savoir plus, voir Restrictions de Hub sur la page 6.
3. Cliquez sur **Soumettre**.

   Un message de notification s'affiche confirmant que le mot de passe de l'utilisateur a été modifié.

Utiliser les filtres sur la page Utilisateurs

Les filtres vous permettent de trouver facilement un utilisateur spécifique ou des types d'utilisateurs en fonction des critères sélectionnés.

1. Sur la page Utilisateurs, cliquez sur **Filtrer** pour ouvrir le panneau Filtrer.
2. Utilisez le bouton bascule pour activer le filtre requis et renseignez les informations pour trouver l'utilisateur. Vous pouvez appliquer plusieurs filtres en même temps.

   Les filtres disponibles sont les suivants :

Filtrer	Description
Nom complet	Saisissez le nom complet de l'utilisateur, ou une partie de son nom complet.
Adresse e-mail	Saisissez l'adresse e-mail de l'utilisateur, ou une partie de son adresse e-mail.
Verrouillé	Sélectionnez le statut verrouillé de l'utilisateur dans la liste déroulante, parmi les options suivantes : • **Verrouillé** : affiche tous les utilisateurs dont les comptes ont été verrouillés. • **Déverrouillé** : affiche tous les utilisateurs dont les comptes sont déverrouillés.
Actif	Sélectionnez le statut actif de l'utilisateur dans la liste déroulante, parmi les options suivantes : • **Actif** : affiche tous les utilisateurs qui ont des identifiants de connexion actifs. • **Classé** : affiche tous les utilisateurs qui ont été classés par l'administrateur et qui ne peuvent plus se connecter. Par défaut, le filtre **Actif** est déjà activé. Vous pouvez désactiver cette option si vous souhaitez afficher tous les utilisateurs.

Filtrer	Description
Statut de la configuration	Sélectionnez le statut de configuration de l'utilisateur dans la liste déroulante, parmi les options suivantes : • **Configuration correcte** : affiche tous les utilisateurs qui sont correctement configurés dans Hub, c'est-à-dire pour lesquels les identifiants utilisateur ont été complétés et les rôles attribués. • **Nécessite une action** : affiche tous les utilisateurs dont les comptes utilisateur ne sont pas correctement configurés, par exemple, s'il leur manque leurs rôles.
Domaine	Saisissez le nom d'un domaine, ou une partie du nom. Cela correspond aux noms de domaine spécifiés dans la page Réglages d'authentification, et affiche tous les utilisateurs qui ont été importés dans Hub à partir du domaine correspondant. Si vous avez saisi une partie du nom d'un domaine, les résultats s'affichent pour toutes les correspondances partielles. Il peut y avoir des utilisateurs d'autres domaines ainsi que de celui que vous vouliez.
Nom de la connexion	Saisissez le nom d'une connexion, ou une partie du nom. Cela correspond aux noms de connexion spécifiés dans la page Réglages d'authentification, et affiche tous les utilisateurs qui ont été importés dans Hub à l'aide de la connexion correspondante. Si vous avez saisi une partie du nom d'une connexion, les résultats s'affichent pour toutes les correspondances partielles. Il peut y avoir des utilisateurs d'autres connexions ainsi que de celle que vous vouliez.
Accès	Sélectionnez le niveau d'accès de l'utilisateur dans la liste déroulante. Ils sont basés sur le niveau de permission accordé à l'utilisateur, parmi les options suivantes : • **Hub** : accès à Hub. • **Interact** : accès à Interact. • **Approbateur** : accès à Interact avec les permissions approbateur.
Rôle(s) Hub	Saisissez le nom du rôle, ou une partie du nom du rôle. Cela recherche tous les rôles pour lesquels Hub est défini comme type de rôle.
Rôle(s) Interact	Saisissez le nom d'un rôle, ou une partie du nom du rôle. Cela recherche par rapport à tous les rôles pour lesquels Interact est défini comme type de rôle.
Thèmes	Sélectionnez le thème dans la liste déroulante. Les utilisateurs qui ont le thème sélectionné sont affichés.

Les informations sur la page Utilisateurs sont immédiatement filtrées.

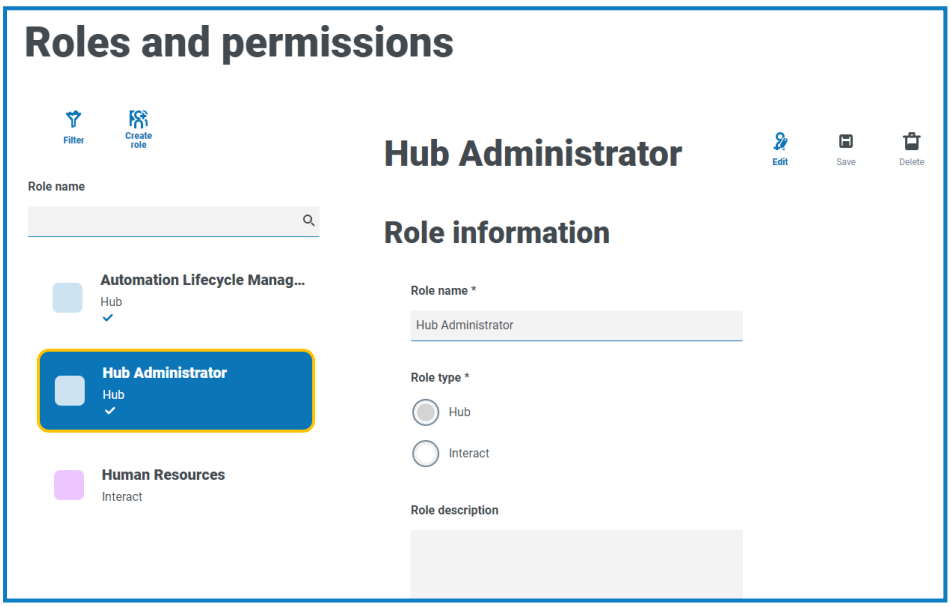
Si vous avez défini les filtres, mais que vous souhaitez afficher à nouveau les informations non filtrées, désactivez les filtres requis ou supprimez tous les réglages du filtre afin qu'il soit vide.

3. Cliquez sur **Fermer le tiroir** pour fermer le panneau Filtrer.

Rôles et permissions

Les rôles et permissions vous permettent de créer des rôles et d'attribuer des permissions à des zones spécifiques de Hub ou de Interact à ces rôles. Cette zone n'est disponible que si vous êtes un administrateur. Avant de configurer les utilisateurs, il est recommandé de configurer les rôles d'utilisateur. Si les rôles ne sont pas configurés, les utilisateurs pourront se connecter mais, sans rôle, ils obtiendront un affichage limité et n'auront aucun accès aux fonctionnalités.

La page Rôles et permissions affiche une liste des rôles existants. Des rôles prédéfinis sont automatiquement créés dans le cadre du processus d'installation de Hub. Ceux-ci sont indiqués par une coche bleue, par exemple, le rôle d'administrateur Hub. Ces rôles prédéfinis créés automatiquement sont verrouillés et ne peuvent pas être modifiés ou supprimés, bien que vous puissiez leur ajouter des utilisateurs. Vous pouvez cliquer sur un rôle pour afficher les permissions.



Pour ouvrir la page Rôles et permissions, cliquez sur l'icône de votre profil pour ouvrir la page Réglages, puis sur **Rôles et permissions**.

Rechercher des rôles

La page Rôles et permissions comprend deux méthodes pour trouver des rôles :

- **Champ de par nom de rôle** : il se trouve au-dessus de la liste des rôles. Commencez à taper le nom d'un rôle pour filtrer les résultats de la recherche. La liste filtre de façon dynamique à mesure que vous saisissez plus de caractères.
- **Filtres** : les filtres vous permettent de trouver facilement un ou plusieurs rôles spécifiques avec des permissions spécifiques en fonction des critères sélectionnés. Cliquez sur **Filtrer** pour afficher et utiliser les filtres. Pour en savoir plus, voir Utiliser les filtres sur la page Rôles et permissions sur la page 39.

Ajouter des rôles

En fonction du type d'authentification et des réglages configurés pour votre environnement sur la page Réglages d'authentification, il existe plusieurs façons d'ajouter des utilisateurs au rôle que vous créez :

- Si l'authentification native est activée, vous pouvez ajouter des utilisateurs natifs directement à un rôle.
- Si l'authentification Active Directory est activée, vous pouvez :
  - Ajouter des utilisateurs Active Directory directement à un rôle : l'option **Permettre aux utilisateurs Active Directory d'être ajoutés directement aux rôles** doit être activée sur la page Réglages d'authentification.
  - Ajouter des groupes de sécurité Active Directory à un rôle : l'option **Accorder l'autorisation via l'appartenance au groupe de sécurité Active Directory** doit être activée sur la page Réglages d'authentification.

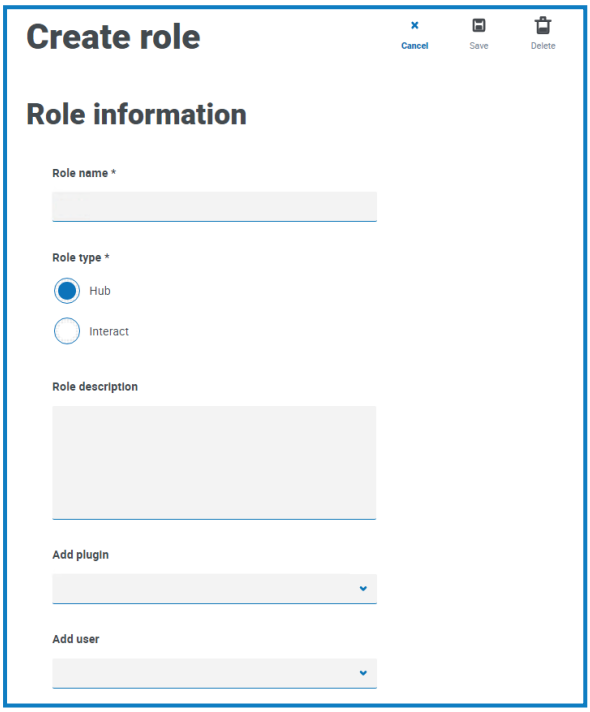
> ⚠ Si vous utilisez Interact avec Active Directory, sachez que certaines actions du service API Web Interact ne prennent pas en charge l'utilisation de groupes de sécurité. Toutes les actions prennent en charge les utilisateurs Active Directory directement assignés aux rôles Interact. Pour plus d'informations, veuillez consulter le guide de l'utilisateur Service API Web Interact.

Ajouter des utilisateurs directement à un rôle

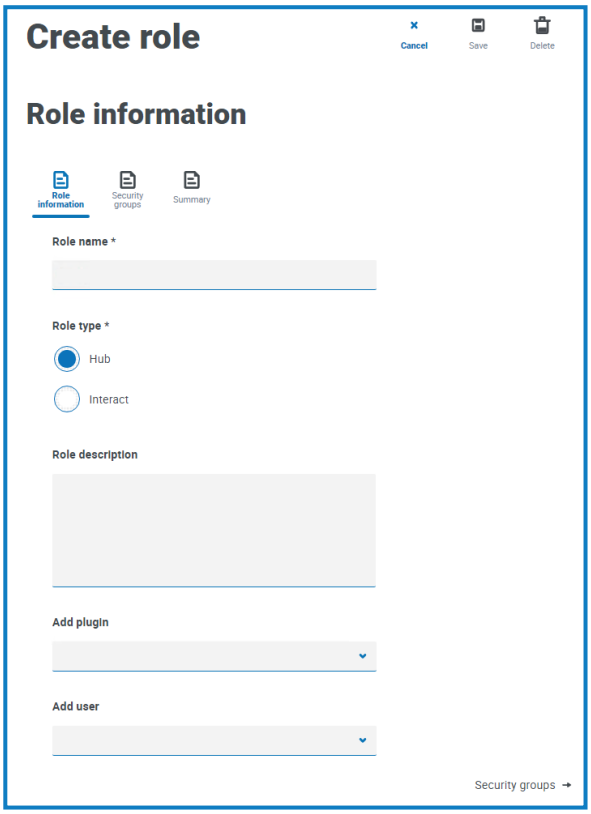
1. Sur la page Rôles et permissions, cliquez sur **Créer un rôle**.

   La section Créer un rôle s'affiche. Si l'environnement est configuré pour permettre l'ajout de groupes de sécurité Active Directory aux rôles, cette page affiche trois onglets : Informations sur les rôles, Groupes de sécurité et Résumé.

   Exemple de page lorsque les groupes de sécurité AD ne peuvent pas être ajoutés aux rôles :

   Exemple de page lorsque vous autorisez l'ajout de groupes de sécurité AD aux rôles :

2. Saisissez un nom de rôle et sélectionnez s'il s'applique à **Hub** ou à **Interact**.
3. Si nécessaire, saisissez une description.
4. Sélectionnez les éléments auxquels vous souhaitez que le rôle ait accès. Si vous avez sélectionné :
   - **Hub**, sélectionnez les plug-ins requis dans la liste déroulante **Ajouter un plug-in**.
   - **Interact**, sélectionnez les formulaires requis dans la liste déroulante **Ajouter des formulaires**.

   Vous pouvez sélectionner plusieurs éléments dans la liste.
5. Sélectionnez les utilisateurs auxquels ce rôle sera attribué dans la liste déroulante **Ajouter un utilisateur**. La liste affiche uniquement les utilisateurs qui disposent des privilèges appropriés. Par exemple, si le rôle est pour Interact, elle affichera uniquement les utilisateurs Interact et non les utilisateurs Hub. Voir Utilisateurs sur la page 25 pour plus d'informations sur les permissions utilisateur.

   > Des utilisateurs peuvent également être ajoutés aux rôles à partir de la page Utilisateurs.

6. Cliquez sur **Enregistrer** pour créer le rôle.

Ajouter des groupes de sécurité Active Directory à un rôle

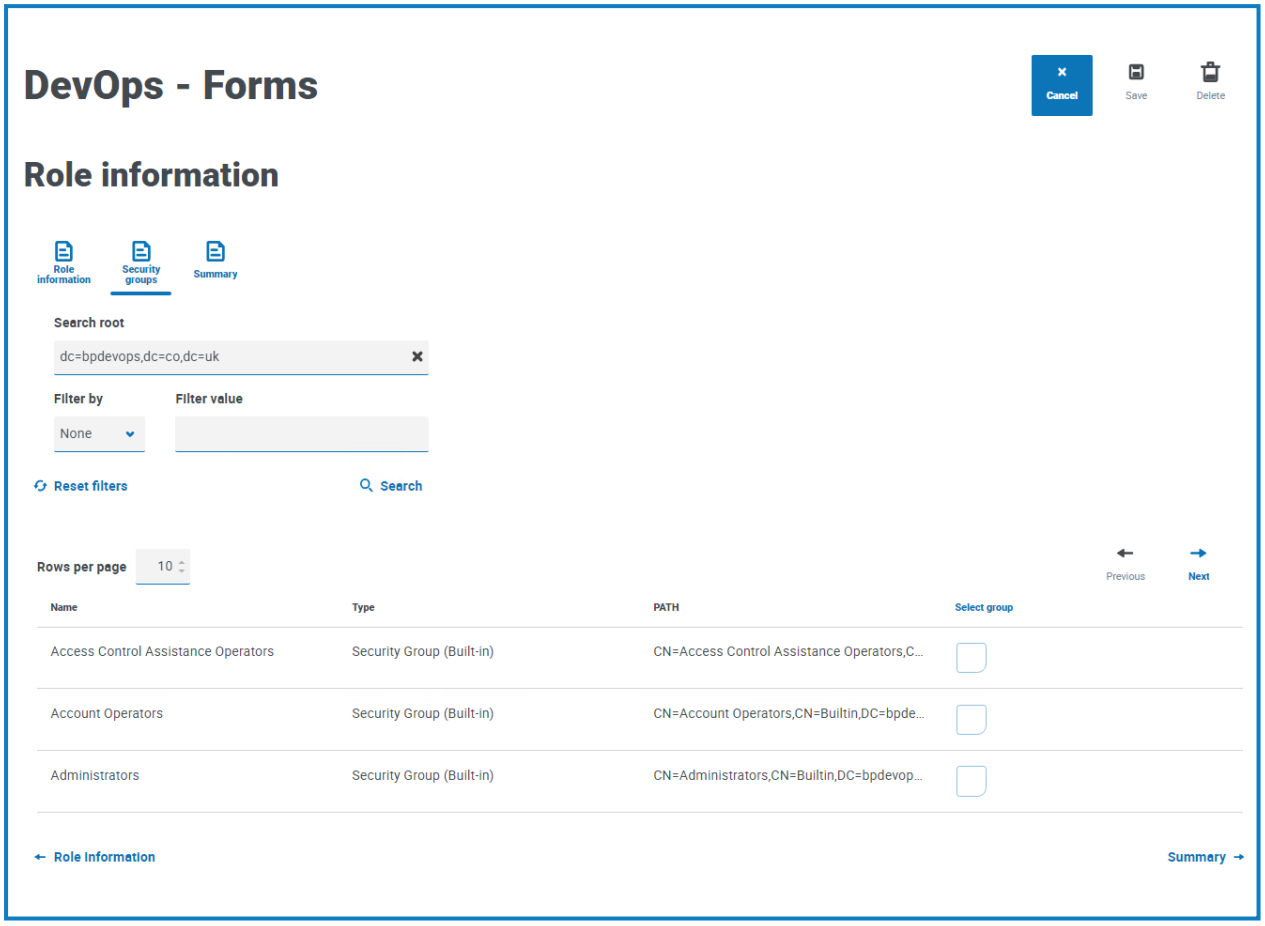
⚠ Si vous utilisez Interact avec Active Directory, sachez que certaines actions du service API Web Interact ne prennent pas en charge l'utilisation de groupes de sécurité. Toutes les actions prennent en charge les utilisateurs Active Directory directement assignés aux rôles Interact. Pour plus d'informations, veuillez consulter le guide de l'utilisateur Service API Web Interact.

1. Sur la page Rôles et permissions, cliquez sur **Créer un rôle**.

   La section Créer un rôle s'affiche.
2. Dans l'onglet Informations sur les rôles, saisissez un nom de rôle et sélectionnez s'il s'applique à **Hub** ou à **Interact**.
3. Si nécessaire, saisissez une description.
4. Sélectionnez les éléments auxquels vous souhaitez que le rôle ait accès. Si vous avez sélectionné :
   - **Hub**, sélectionnez les plug-ins requis dans la liste déroulante **Ajouter un plug-in**.
   - **Interact**, sélectionnez les formulaires requis dans la liste déroulante **Ajouter des formulaires**.

   Vous pouvez sélectionner plusieurs éléments dans la liste.
5. Cliquez sur **Groupes de sécurité**.

6. Recherchez des groupes de sécurité en saisissant le nom distinctif de l'emplacement racine, par exemple, dc=bpdevops, dc=co, dc=uk.

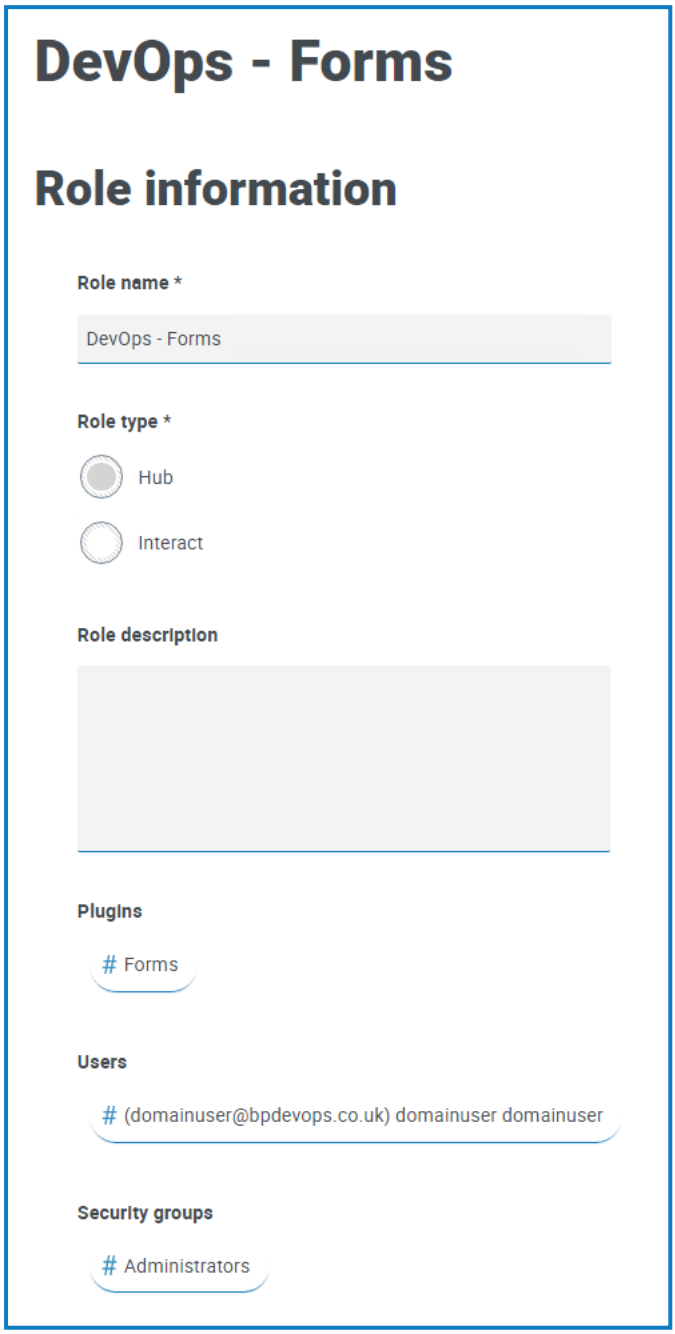


Vous pouvez appliquer des filtres de recherche sur la base du nom commun (CN), du nom d'utilisateur principal (UPN) ou de l'identificateur de sécurité (SID), ou utiliser une recherche par caractères génériques. Pour plus d'informations, voir Ajouter un utilisateur Active Directory sur la page 28.

Vous pouvez également faire défiler la page vers le bas, cliquer sur **Suivant** ou **Précédent** pour naviguer entre plusieurs pages de groupes de sécurité, ou vous déplacer entre les onglets Informations sur les rôles et Résumé.

7. Sélectionnez le(s) groupe(s) que vous souhaitez ajouter au rôle et cliquez sur **Enregistrer**.

   Les groupes de sécurité ajoutés s'affichent dans le cadre des informations sur les rôles. Tous les utilisateurs qui sont membres des groupes de sécurité ajoutés seront automatiquement ajoutés au rôle et auront un compte créé dans Hub lorsqu'ils se connecteront pour la première fois.



Modifier des rôles

1. Sur la page Rôles et permissions, sélectionnez le rôle requis et cliquez sur **Modifier**.
2. Modifiez les informations selon les besoins, y compris en ajoutant ou en supprimant des utilisateurs et/ou des groupes de sécurité.

   > Vous ne pouvez pas changer le type de rôle. Si vous modifiez un rôle qui affiche une coche bleue, vous ne pouvez modifier que les utilisateurs affectés au rôle.

3. Cliquez sur **Enregistrer** pour appliquer vos modifications.

Supprimer des rôles

> Vous ne pouvez pas supprimer un rôle qui affiche une coche bleue. Il s'agit d'un rôle qui a été automatiquement créé lors de l'installation de Hub ou d'un plug-in.

1. Sur la page Rôles et permissions, sélectionnez le rôle requis et cliquez sur **Supprimer**.

   Un message s'affiche vous demandant de confirmer.

2. Cliquez sur **Oui**.

   Le rôle est supprimé et une notification de confirmation s'affiche.

Utiliser les filtres sur la page Rôles et permissions

Les filtres vous permettent de trouver facilement un rôle spécifique en fonction des critères sélectionnés.

1. Sur la page Rôles et permissions, cliquez sur **Filtrer** pour ouvrir le panneau Filtrer.
2. Utilisez le bouton bascule pour activer le filtre requis et renseignez les informations pour trouver le rôle requis. Vous pouvez appliquer plusieurs filtres en même temps.

   Les filtres disponibles sont les suivants :

Filtrer	Description
Type	Sélectionnez le type de rôle dans la liste déroulante. Les options sont les suivantes : • **Hub** : affiche les rôles pour lesquels Hub est défini comme type de rôle. • **Interact** : affiche les rôles pour lesquels Interact est défini comme type de rôle.
Description	Saisissez un terme ou un mot à rechercher dans le texte dans la description du rôle.

Filtrer	Description
Plug-ins de Hub	Saisissez le nom, ou une partie du nom, du plug-in que vous souhaitez rechercher. Par exemple : • **Cycle de vie de l'automatisation** : affiche tous les rôles qui ont accès à ALM. • **Formulaires** : affiche tous les rôles qui ont accès aux formulaires d'Interact. • **Processus métier** : affiche tous les rôles qui ont accès au plug-in Processus métier. • **Control Room** : affiche tous les rôles qui ont accès à Control Room.
Formulaires Interact	Saisissez le nom, ou une partie du nom, du formulaire Interact que vous souhaitez rechercher.
Utilisateurs	Saisissez le nom d'utilisateur d'un utilisateur, ou une partie de son nom d'utilisateur, pour trouver les rôles qui lui sont associés. Si vous avez saisi une partie d'un nom d'utilisateur, les rôles s'affichent pour toutes les correspondances partielles. Elles peuvent être destinées à d'autres utilisateurs ainsi qu'à celui que vous vouliez.

Les informations sur la page Rôles et permissions sont immédiatement filtrées.

Si vous avez défini les filtres, mais que vous souhaitez afficher à nouveau les informations non filtrées, désactivez les filtres requis ou supprimez tous les réglages du filtre afin qu'il soit vide.

3. Cliquez sur **Fermer le tiroir** pour fermer le panneau Filtrer.

Inscriptions

La page Inscriptions vous permet de gérer les requêtes d'inscription que les nouveaux utilisateurs ont formulées pour accéder à Interact. Cette zone n'est disponible que si vous êtes un administrateur.

Les utilisateurs peuvent demander un compte utilisateur Interact à partir de la page d'inscription : https://{nom d'hôte}/#/user-registration

La page Inscriptions affiche les requêtes d'inscription soumises, que vous pouvez approuver ou refuser.

Pour ouvrir la page Inscriptions, cliquez sur l'icône de votre profil pour ouvrir la page Réglages, puis sur **Inscriptions**. Une valeur numérique est affichée à côté de l'option Inscriptions sur la page Réglages s'il y a des requêtes en attente.

Approuver une requête

L'utilisateur devra se voir attribuer un rôle avant de pouvoir accéder à tout formulaire dans Interact. Vous pouvez faire cela dans le cadre du processus d'approbation, comme illustré ci-dessous, ou vous pouvez approuver la requête, puis modifier l'utilisateur.

1. Sur la page Inscriptions, sélectionnez l'utilisateur et cliquez sur **Modifier**.
2. Sélectionnez le rôle requis dans la liste déroulante. C'est le seul champ que vous pouvez modifier.
3. Cliquez sur **Enregistrer**.
4. Cliquez sur **Approuver**.

   L'utilisateur est supprimé de la liste des inscriptions et s'affiche sur la page Utilisateur. L'utilisateur reçoit un e-mail fournissant un lien à usage unique pour terminer l'inscription en saisissant un mot de passe. Il peut ensuite accéder à Interact.

Rejeter une requête

1. Sur la page Inscriptions, sélectionnez l'utilisateur et cliquez sur **Refuser**.

   La requête d'accès est rejetée et les détails de l'utilisateur sont supprimés de la liste.

Utiliser les filtres sur la page Inscriptions

Les filtres vous permettent de trouver facilement un utilisateur spécifique en fonction des critères sélectionnés.

1. Sur la page Inscriptions, cliquez sur **Filtrer** pour ouvrir le panneau Filtrer.
2. Utilisez le bouton bascule pour activer le filtre requis et renseignez les informations pour trouver l'utilisateur. Vous pouvez appliquer plusieurs filtres en même temps.

   Les filtres disponibles sont les suivants :

Filtrer	Description
Nom complet	Saisissez le nom complet de l'utilisateur, ou une partie de son nom complet.
Adresse e-mail	Saisissez l'adresse e-mail de l'utilisateur, ou une partie de son adresse e-mail.
Rôle(s) Interact	Saisissez le nom d'un rôle, ou une partie du nom du rôle. Cela recherche par rapport à tous les rôles pour lesquels Interact est défini comme type de rôle.

Les informations de la page Inscriptions sont immédiatement filtrées.

> Si vous avez défini les filtres, mais que vous souhaitez afficher à nouveau les informations non filtrées, désactivez les filtres requis ou supprimez tous les réglages du filtre afin qu'il soit vide.

3. Cliquez sur **Fermer le tiroir** pour fermer le panneau Filtrer.

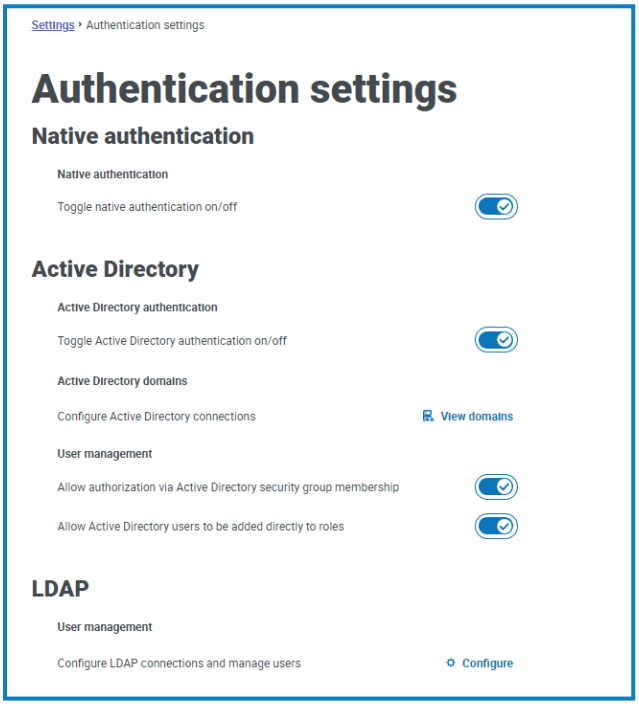
Réglages d'authentification

Vous pouvez configurer les réglages d'authentification de votre organisation à l'aide des options suivantes :

- Authentification native
- Authentification Active Directory
- LDAP

Cette zone n'est disponible que si vous êtes un administrateur.

Pour ouvrir la page Réglages d'authentification, cliquez sur l'icône de votre profil afin d'ouvrir la page Réglages, puis sur **Réglages d'authentification**.



Authentification native

L'authentification native est activée par défaut sur la page Réglages d'authentification dans les nouveaux environnements ou lors de la mise à niveau de Hub.

Pour activer ou désactiver l'authentification native :

1. Utilisez le curseur pour basculer vers la position requise :
   - La croix sert à désactiver l'option
   - La coche sert à activer l'option
2. Cliquez sur **OK** pour accepter le message de confirmation.

Vous pouvez désactiver l'authentification native uniquement si au moins l'un des administrateurs Hub du système peut se connecter via une autre méthode d'authentification.

Vous pouvez ajouter des utilisateurs natifs sur la page Ajouter un utilisateur. Ils peuvent se connecter à Hub en saisissant leur nom d'utilisateur et leur mot de passe.

Authentification Active Directory

L'authentification Active Directory ne peut être activée sur la page Réglages d'authentification que si le serveur hébergeant Authentication Server est membre d'un domaine Active Directory.

Pour activer ou désactiver l'authentification Active Directory :

1. Utilisez le curseur pour basculer vers la position requise :
   - La croix sert à désactiver l'option
   - La coche sert à activer l'option
2. Cliquez sur **OK** pour accepter le message de confirmation.

Une fois activé, vous pouvez ajouter des utilisateurs Active Directory sur la page Ajouter un utilisateur. Ils peuvent se connecter directement à Hub à l'aide de l'option **Connexion à l'aide d'Active Directory**.

Cela ne s'applique pas aux utilisateurs LDAP qui devront toujours saisir leurs identifiants.

Gestion des utilisateurs Active Directory

Si l'authentification Active Directory a été activée sur la page Réglages d'authentification, vous devez sélectionner comment gérer l'accès des utilisateurs Active Directory dans Hub en activant au moins l'une des options suivantes sur la page Réglages d'authentification :

- **Accorder l'autorisation via l'appartenance au groupe de sécurité Active Directory** : permet d'ajouter des groupes de sécurité Active Directory aux rôles Hub. Les utilisateurs peuvent être affectés à plusieurs rôles Hub en étant membre de tout groupe de sécurité Active Directory associé à ces rôles.
- **Permettre aux utilisateurs Active Directory d'être ajoutés directement aux rôles** : permet d'affecter directement des utilisateurs Active Directory aux rôles Hub. Les utilisateurs peuvent être affectés à plusieurs rôles Hub.

Pour plus d'informations sur l'affectation des utilisateurs Active Directory et des groupes de sécurité aux rôles, voir Rôles et permissions sur la page 33.

Regardez cette vidéo pour obtenir un aperçu de l'intégration d'Active Directory à Authentication Server.

Domaines Active Directory

La page Domaines Active Directory vous permet d'afficher, d'ajouter, de modifier et de supprimer les domaines Active Directory et les identifiants associés stockés dans la base de données Authentication Server. Cette zone n'est disponible que si vous êtes un administrateur.

Pour ouvrir la page Domaines Active Directory, cliquez sur l'icône de votre profil pour ouvrir la page Réglages, sur **Réglages d'authentification**, puis sur **Afficher les domaines**.

Il vous suffit d'ajouter de nouveaux domaines Active Directory pour les environnements multiforêts avec des relations de confiance unidirectionnelles. Pour en savoir plus, voir Domaines Active Directory sur la page précédente.

La page Domaines Active Directory vous fournit les informations et fonctions suivantes :

A. **Ajouter** : pour ajouter un nouveau domaine Active Directory.
B. **Modifier** : pour modifier les détails d'un domaine Active Directory existant. Vous ne pouvez modifier qu'un seul domaine à la fois.
C. **Supprimer** : pour supprimer un ou plusieurs domaines Active Directory.

Ajouter un domaine

1. Sur la page Domaines Active Directory, cliquez sur **Ajouter**.

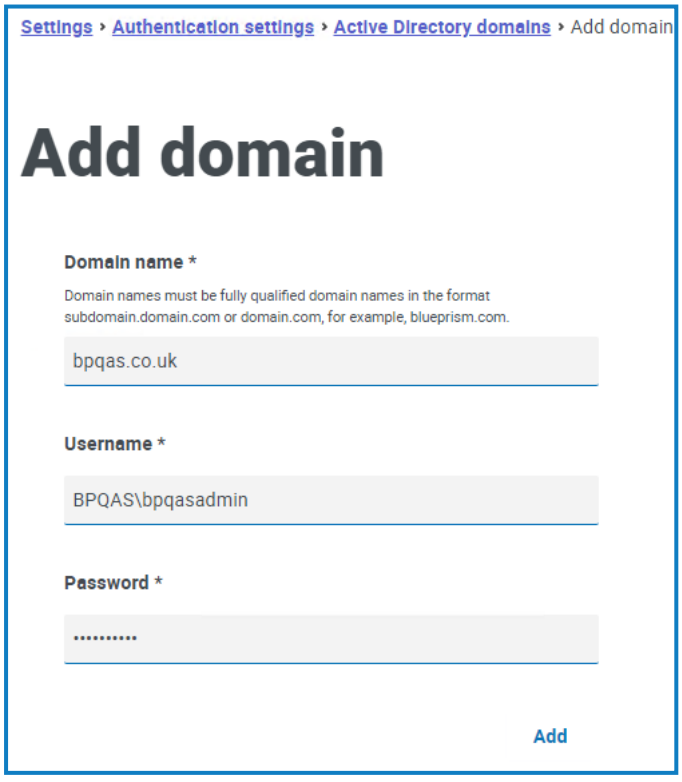
   La page Ajouter un domaine s'affiche.

2. Saisissez un nom de domaine.

   Il doit s'agir du nom de domaine explicite (FQDN) au format sousdomaine.domaine.com ou domaine.com.

3. Saisissez le nom d'utilisateur et le mot de passe du domaine. Les noms d'utilisateur doivent être au format nomutilisateur@domaine.co.uk ou DOMAINE\nomutilisateur. Les identifiants doivent être demandés au préalable à un administrateur système.

   Les identifiants du domaine Active Directory sont stockés dans la base de données et sont chiffrés avant le stockage. Les identifiants stockés pour chaque domaine doivent être ceux d'un compte de service Active Directory. Le mot de passe du compte de service ne doit pas expirer, le compte de service ne doit pas être un compte utilisateur et doit suivre les meilleures pratiques du compte de service Active Directory.



4. Cliquez sur **Ajouter**.

   Le nom de domaine et les identifiants sont validés en fonction du contrôleur de domaine Active Directory et le domaine ajouté s'affiche dans la liste des domaines.

Modifier un domaine

1. Sur la page Domaines Active Directory, sélectionnez un domaine et cliquez sur **Modifier**.

   Vous ne pouvez sélectionner qu'un seul domaine à la fois.
2. Modifiez les informations comme requis. Si vous souhaitez modifier le nom d'un domaine, vous devez supprimer ce domaine et en créer un nouveau.
3. Cliquez sur **Enregistrer** pour appliquer vos modifications.

Supprimer les domaines

1. Dans le domaine Active Directory, sélectionnez le(s) domaine(s) requis et cliquez sur **Supprimer**.

   Un message s'affiche vous demandant de confirmer la suppression.
2. Cliquez sur **Oui** pour supprimer le(s) domaine(s) ou sur **Non** pour annuler.

Relation de confiance entre les domaines

Pour les environnements multiforêts, les relations de confiance doivent être configurées entre les domaines. Elles peuvent être bidirectionnelles ou unidirectionnelles vers le domaine approuvé.

Par exemple :

- Dans une confiance unidirectionnelle entre le domaine A et le domaine B, les utilisateurs du domaine A peuvent accéder aux ressources du domaine B. Cependant, les utilisateurs du domaine B ne peuvent pas accéder aux ressources du domaine A.
- Dans une confiance bidirectionnelle, le domaine A fait confiance au domaine B et le domaine B fait confiance au domaine A. Cela signifie que les requêtes d'authentification peuvent être transmises entre les deux domaines dans les deux directions.

Les confiances bidirectionnelles n'exigent pas que l'utilisateur fournisse des identifiants de domaine si l'utilisateur du pool d'applications Authentication Server dispose d'un accès en lecture pertinent au domaine auquel l'utilisateur appartient. Dans ces exemples, le serveur Web hébergeant Authentication Server résiderait dans le domaine B. Les confiances bidirectionnelles nécessitent des identifiants lorsque l'utilisateur doit interroger un domaine approuvé à l'aide d'un compte différent de l'utilisateur du pool d'applications Authentication Server. Les confiances unidirectionnelles nécessitent la création d'un domaine avec des identifiants.

Les types d'approbation suivants sont pris en charge :

- Externe
- Parent-enfant
- Arbre-racine
- Forêt

LDAP

La page LDAP permet de configurer une connexion LDAP (Lightweight Directory Access Protocol) à l'environnement Active Directory d'une entreprise. Cette zone n'est disponible que si vous êtes un administrateur.

Pour ouvrir la page LDAP, cliquez sur l'icône de votre profil pour ouvrir la page Réglages, sur **Réglages d'authentification**, puis sur **Configurer** sous la section LDAP.

La LDAPpage vous fournit les informations et fonctions suivantes :

A. **Modifier l'affichage** : définissez les colonnes qui sont affichées. Vous pouvez ensuite afficher ou masquer les colonnes à l'aide des boutons à bascule.

B. **Filtrer** : filtrez les informations qui sont affichées. Vous pouvez ensuite activer les filtres requis et saisir ou sélectionner les informations appropriées pour l'affichage. Vous pouvez, par exemple, activer le Filtrer selon le **domaine** et saisir le nom de domaine.

C. **Enregistrer l'affichage** : enregistrez les réglages de vos colonnes actuelles. Vous pouvez entrer un nom pour votre affichage afin de le rendre facilement identifiable lors du chargement des affichages.

D. **Charger l'affichage** : chargez un affichage enregistré. Vous pouvez sélectionner l'affichage requis et cliquer sur **Appliquer**.

E. **Ajouter nouveau** : pour ajouter une nouvelle connexion.

F. **Modifier** : pour modifier les détails de la connexion sélectionnée.

G. **Resynchroniser** : pour resynchroniser les utilisateurs avec Hub. Vous devez le faire si de nouveaux utilisateurs sont ajoutés à Active Directory.

H. **Classer/Rétablir** : une icône de coche permet d'activer une connexion classée et une croix vous permet de classer une connexion. Reportez-vous à la section Classer et rétablir une application pour plus d'informations.

I. **Supprimer** : pour supprimer la connexion sélectionnée. Vous pouvez uniquement supprimer une connexion classée.

J. **Lignes par page** : saisissez un nombre, ou utilisez les flèches haut et bas, pour modifier le nombre de lignes affichées sur une page.

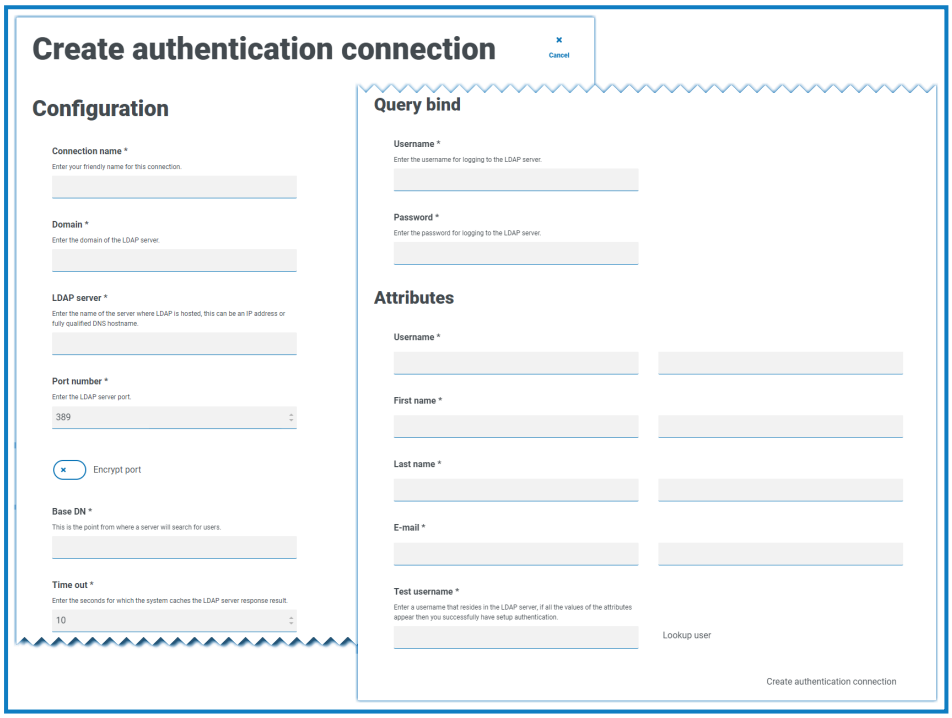
K. **Précédent et Suivant** : cliquez sur **Précédent** ou **Suivant** pour vous déplacer dans les pages..

Ajouter une nouvelle connexion

Si vous ajoutez plus d'une connexion LDAP dans Hub qui contient les mêmes utilisateurs (tels que le nom, l'adresse e-mail et le domaine), des utilisateurs en double seront créés, ce qui pourrait entraîner des problèmes de connexion. Lors de la synchronisation des utilisateurs dans la procédure décrite ci-dessous, assurez-vous de ne sélectionner que les utilisateurs dont vous avez besoin pour empêcher l'importation d'utilisateurs en double.

1. Sur la LDAPpage, cliquez sur **Ajouter nouveau**.

   La page Créer une connexion d'authentification s'affiche.



2. Remplissez les champs de configuration :
   - **Nom de connexion** : un nom sous lequel vous souhaitez que la connexion soit connue.
   - **Domaine** : le nom du domaine auquel vous vous connectez, par exemple « bp ».

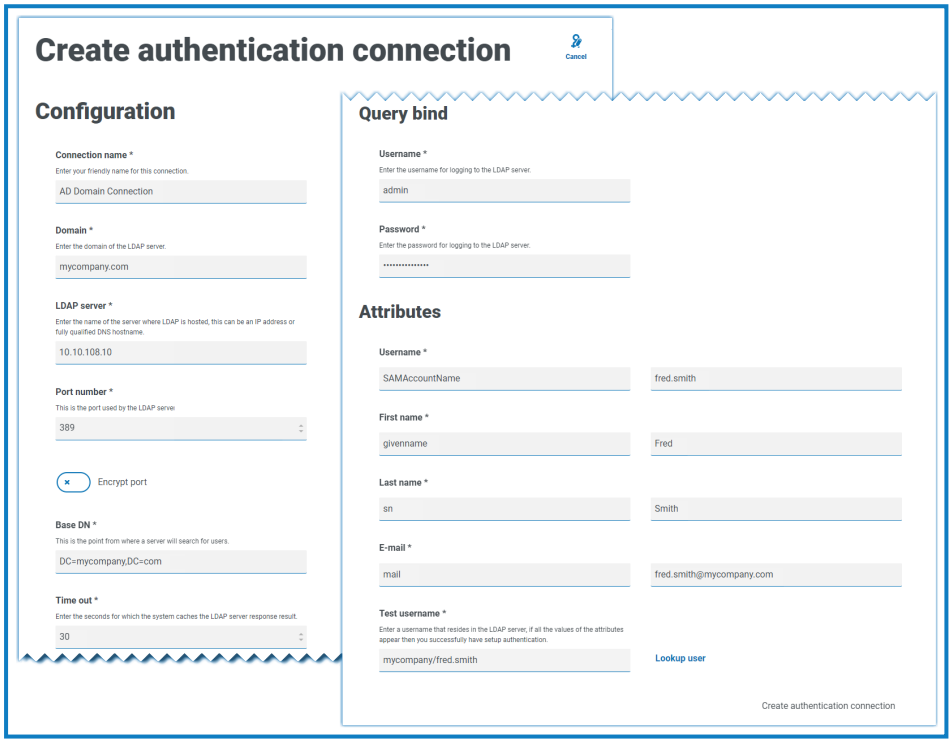
     N'utilisez pas le nom de domaine explicite (FQDN) de votre domaine. Vous devez utiliser le format de nom court.

   - **Serveur LDAP** : le nom d'hôte du serveur LDAP, par exemple blueprism-srv1.local.
   - **Numéro de port** : le numéro de port sur lequel il fonctionne. Il s'agit par défaut du port 389.
   - **Chiffrer le port** : sélectionnez cette option si vous souhaitez chiffrer le port. Si vous utilisez le port 636 (le port LDAPS), vous devez activer cette option.
   - **DN de base** : point de départ dans Active Directory où le système commence à rechercher des utilisateurs, par exemple dc=blueprism, dc=local.

3. Remplissez les champs de liaison de requête :
   - **Délai avant expiration** : le délai avant expiration en secondes pendant lequel le système attendra pour obtenir une réponse du serveur Active Directory.
   - **Nom d'utilisateur de liaison de requête** : un utilisateur Active Directory qui a accès au système LDAP de l'organisation.
   - **Mot de passe de liaison de requête** : le mot de passe de l'utilisateur Active Directory.
4. Remplissez les champs d'attributs. L'objectif de cette section est de mapper les attributs Active Directory aux champs Hub. Le texte saisi dans ces champs doit correspondre aux attributs nommés dans le profil utilisateur dans Active Directory. Vous pouvez utiliser l'outil Utilisateurs et ordinateurs Active Directory (ADUC) pour trouver les attributs utilisateur en sélectionnant un utilisateur, puis en cliquant sur l'onglet **Éditeur d'attributs** pour afficher le mappage des attributs aux valeurs.
   - **Nom d'utilisateur** : le nom d'attribut Active Directory pour le nom d'utilisateur, par exemple, « SAMAccountName ».
   - **Prénom** : le nom d'attribut Active Directory pour le prénom de l'utilisateur, par exemple, « givenname ».
   - **Nom** : le nom d'attribut Active Directory pour le nom de l'utilisateur, par exemple, « sn ».
   - **Adresse e-mail** : le nom d'attribut Active Directory pour l'adresse e-mail de l'utilisateur, par exemple, « mail ».

5. Pour vérifier que tout est correctement configuré, saisissez le nom d'utilisateur dans le champ **Nom d'utilisateur de test** et cliquez sur **Rechercher un utilisateur**. Le texte saisi dans le champ **Nom d'utilisateur de test** doit correspondre au format de texte de l'attribut Active Directory. Par exemple, si le nom d'utilisateur est défini sur :
   - « SAMAccountName », alors les données de test seront probablement au format *domain\user*.
   - « name », alors les données de test seront probablement au format *user*.

   Les informations associées seront récupérées et renseignées dans les champs d'attributs correspondants, par exemple :



6. Cliquez sur **Créer une connexion d'authentification**.

   Un message de notification s'affiche pour confirmer que la connexion est établie et vous êtes invité à importer des utilisateurs.

7. Cliquez sur **Oui** pour synchroniser maintenant. Sinon, vous pouvez sélectionner **Non** et synchroniser ultérieurement à l'aide du processus dans Synchroniser les utilisateurs Active Directory sur la page 52.

   Un message s'affiche indiquant le nombre d'utilisateurs trouvés.

   ⚠ Si vous importez un grand nombre d'utilisateurs (par exemple, des dizaines de milliers), la taille des fichiers log des transactions de la base de données pour AuthenticationServerDB, HubDB et InteractDB augmente. Si la taille du fichier log des transactions de l'une de ces trois bases de données est limitée par une taille de fichier maximale trop petite, ou si la taille de fichier ne peut pas être augmentée, l'importation peut échouer. Il est donc recommandé d'activer le réglage de croissance automatique pour les fichiers log des transactions de la base de données et de définir le paramètre de croissance sur 1 024 Mo, tout en veillant à ce qu'une taille maximale suffisante soit définie pour éviter l'échec de l'importation. Pour plus d'informations sur la croissance automatique, consultez la documentation de Microsoft.

8. Cliquez sur **Continuer**.

   La liste des utilisateurs s'affiche. Ceux-ci n'ont pas encore été importés dans Hub, car vous devez configurer les permissions et les rôles pour les utilisateurs requis.

9. Sélectionnez un utilisateur à importer et attribuez les rôles Hub appropriés et/ou toute responsabilité Interact.

   > Si vous configurez un utilisateur pour qu'il ait un rôle d'administrateur Hub, il aura accès à tous les plug-ins et fonctionnalités de Hub, y compris la possibilité de créer de nouvelles connexions de base de données et LDAP et d'autres fonctionnalités de sécurité. Il est donc important d'attribuer ce rôle avec soin.

10. Répétez l'opération pour tous les utilisateurs requis.
11. Cliquez sur **Enregistrer l'accès et les rôles**.

    Seuls les utilisateurs pour lesquels les rôles et permissions ont été définis sont enregistrés et la page Utilisateurs s'affiche avec les nouveaux utilisateurs affichés.

Modifier une connexion

1. Sur la page LDAP, sélectionnez l'icône de **crayon** pour la connexion requise.
2. Modifiez les informations comme requis. Vous ne pouvez pas modifier le domaine, le serveur LDAP, le numéro de port ou le DN de base.
3. Cliquez sur **Enregistrer**.

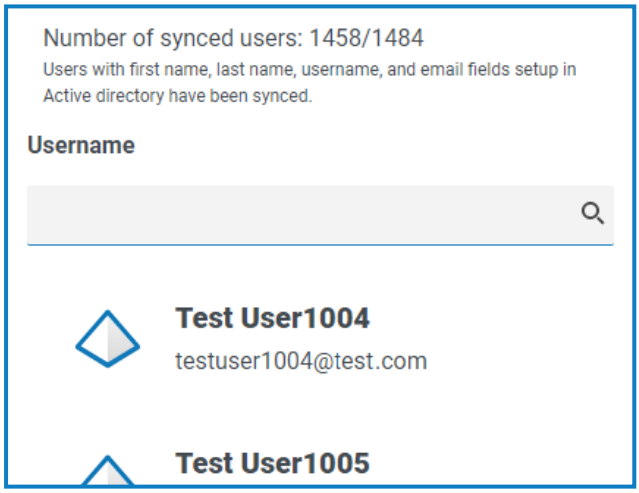
Synchroniser les utilisateurs Active Directory

⚠ Si vous importez un grand nombre d'utilisateurs (par exemple, des dizaines de milliers), la taille des fichiers log des transactions de la base de données pour AuthenticationServerDB, HubDB et InteractDB augmente. Si la taille du fichier log des transactions de l'une de ces trois bases de données est limitée par une taille de fichier maximale trop petite, ou si la taille de fichier ne peut pas être augmentée, l'importation peut échouer. Il est donc recommandé d'activer le réglage de croissance automatique pour les fichiers log des transactions de la base de données et de définir le paramètre de croissance sur 1 024 Mo, tout en veillant à ce qu'une taille maximale suffisante soit définie pour éviter l'échec de l'importation. Pour plus d'informations sur la croissance automatique, consultez la documentation de Microsoft.

Lorsque des utilisateurs supplémentaires sont ajoutés à Active Directory, ces utilisateurs doivent être synchronisés avec Hub.

1. Sur la page LDAP, cliquez sur l'icône de **resynchronisation** dans la ligne pour la connexion requise.

   Un message s'affiche au-dessus de la liste des utilisateurs indiquant le nombre d'utilisateurs synchronisés (ceux avec des informations valides dans Active Directory, prénom, nom, nom d'utilisateur et adresse e-mail) par rapport au nombre total d'utilisateurs trouvés. Seuls les utilisateurs synchronisés sont affichés dans la liste. Vous devrez configurer les permissions et les rôles pour les utilisateurs requis.



   Pour plus d'informations sur les attributs Active Directory qui fournissent à Hub le prénom, le nom, le nom d'utilisateur et l'adresse e-mail, voir Ajouter une nouvelle connexion sur la page 48. Hub synchronisera uniquement les utilisateurs qui ont des informations dans tous les attributs mappés.

2. Sélectionnez l'utilisateur requis à ajouter à la base d'utilisateurs Hub, en attribuant les rôles Hub appropriés et/ou toutes les responsabilités Interact.
3. Répétez l'opération pour tous les utilisateurs requis.
4. Cliquez sur **Enregistrer l'accès et les rôles**.

   Seuls les utilisateurs pour lesquels les rôles et permissions ont été définis sont enregistrés et la page Utilisateurs s'affiche avec les nouveaux utilisateurs affichés.

Classer et rétablir une connexion

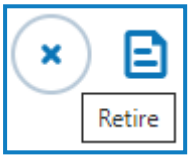
La suppression d'une connexion n'affecte pas le statut des utilisateurs associés. Les utilisateurs peuvent toujours se connecter et utiliser les applications. Tous les utilisateurs associés à une connexion LDAP peuvent être retirés en supprimant la connexion.

1. Sur la page LDAP, sélectionnez l'icône **Classer/Rétablir** pour la connexion requise.

   Si le statut de la connexion est :

   - En mode Actif, l'icône **Classer/Rétablir** s'affiche sous forme de croix.
   - En mode Classé, l'icône **Classer/Rétablir** s'affiche sous forme de coche.

2. Pour classer une connexion :
   a. Cliquez sur la croix.

   Un message s'affiche vous demandant de confirmer.
   b. Cliquez sur **Oui**.

   La connexion est classée et la croix devient une coche.

3. Pour activer une connexion classée, cliquez sur la coche.

   La connexion est instantanément rétablie et la coche devient une croix.

   Vous pouvez utiliser le filtre **Actif** pour filtrer la liste des connexions classées.

Supprimer une connexion

Vous pouvez uniquement supprimer une connexion classée.

1. Sur la page LDAP, sélectionnez **Supprimer** (la corbeille) pour la connexion requise.

   Un message s'affiche vous demandant de confirmer.

2. Cliquez sur **Oui**.

   La connexion est supprimée et tous les utilisateurs qui lui sont associés sont classés.

Utiliser les filtres sur la LDAPpage

Les filtres vous permettent de trouver facilement une connexion spécifique ou des connexions similaires en fonction des critères sélectionnés.

1. Sur la LDAPpage, cliquez sur **Filtrer** pour ouvrir le panneau Filtrer.
2. Utilisez le bouton bascule pour activer le filtre requis et renseignez les informations pour trouver la connexion requise. Vous pouvez appliquer plusieurs filtres en même temps.

Les filtres disponibles sont les suivants :

Filtrer	Description
Actif	Sélectionnez le statut de la connexion parmi les options suivantes : • **En direct** : affiche les connexions actives, à savoir celles qui n'ont pas été classées. • **Classé** : affiche les connexions qui ont été classées par un administrateur.
Nom de la connexion	Saisissez le nom complet ou partiel de la connexion.
Serveur LDAP	Saisissez le nom d'hôte du serveur, ou une partie du nom d'hôte du serveur.
Nom distinctif de la base	Saisissez le DN de base, ou une partie du DN de base à rechercher.
Domaine	Saisissez le nom complet ou partiel du domaine.
Nombre d'importations de l'utilisateur	Saisissez une plage numérique : • Dans le premier champ, saisissez le plus petit nombre d'importations. • Dans le second champ, saisissez le plus grand nombre d'importations. Cela affiche toutes les connexions qui comportent des utilisateurs importés dans cette plage.
Dernière synchronisation	Saisissez une plage de dates : • Dans le premier champ, sélectionnez la date la plus proche. • Dans le second champ, sélectionnez la date la plus lointaine. • Si nécessaire, ajustez les champs d'heure. Par défaut, l'heure de la date antérieure est 00:00:00 et celle de la date ultérieure est 23:59:59, incluant ainsi la journée complète. Cela affiche toutes les connexions qui ont été synchronisées pendant cette période.
Synchronisé par	Saisissez le nom d'utilisateur d'un utilisateur, ou une partie de son nom d'utilisateur. Si vous avez saisi une partie d'un nom d'utilisateur, les résultats s'affichent pour toutes les correspondances partielles. Elles peuvent être destinées à d'autres utilisateurs ainsi qu'à celui que vous vouliez.

Les informations sur la LDAPpage sont immédiatement filtrées.

Si vous avez défini les filtres, mais que vous souhaitez afficher à nouveau les informations non filtrées, désactivez les filtres requis ou supprimez tous les réglages du filtre afin qu'il soit vide.

3. Cliquez sur **Fermer le tiroir** pour fermer le panneau Filtrer.

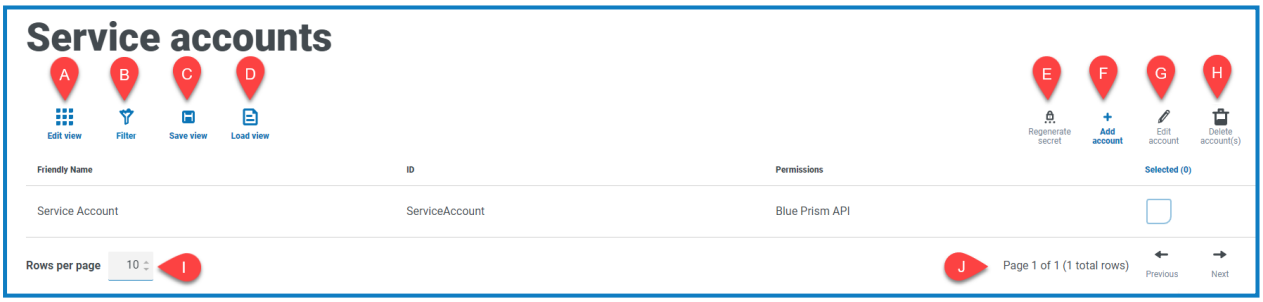
Comptes de service

La page Comptes de service permet de gérer les comptes d'application authentifiés. Cette zone n'est disponible que si vous êtes un administrateur.

Les comptes de service sont utilisés par les applications qui ont besoin d'obtenir des jetons d'accès pour leur propre utilisation plutôt que pour le compte d'un utilisateur. Ces jetons d'accès peuvent ensuite être utilisés pour effectuer des requêtes authentifiées aux API. Les API pour lesquelles les comptes de service peuvent obtenir des jetons d'accès sont les suivantes :

- **API Authentication Server** : un compte de service doit être créé pour toutes les applications qui s'intègrent à l'API Authentication Server. Pour en savoir plus, consultez le guide de configuration d'Authentication Server.
- **Blue Prism API** : un compte de service doit être créé pour toutes les applications tierces qui s'intègrent à Blue Prism API. Pour en savoir plus, consultez le guide d'installation de Blue Prism API.
- **API Decision** : un compte de service doit être créé pour que Blue Prism puisse utiliser les modèles Decision qui ont été entraînés et étalonnés dans le plug-in Decision. Pour en savoir plus, consultez le guide d'installation de Blue Prism Decision.
- **API Interact Remote API** : un compte de service doit être créé pour toutes les applications qui s'intègrent à l'API Interact Remote API, comme le client interactif Blue Prism. Pour en savoir plus, consultez le guide de l'utilisateur du service API Web Interact.

Pour ouvrir la page Comptes de service, cliquez sur l'icône de votre profil pour ouvrir la page Réglages, puis sur **Comptes de service**.



La page Comptes de service vous fournit les informations et fonctions suivantes :

A. **Modifier l'affichage** : définissez les colonnes qui sont affichées. Vous pouvez ensuite afficher ou masquer les colonnes à l'aide des boutons à bascule.

B. **Filtrer** : filtrez les informations qui sont affichées. Vous pouvez ensuite activer les filtres requis et saisir ou sélectionner les informations appropriées pour l'affichage. Vous pouvez, par exemple, activer le Filtre **Permissions** et sélectionner **Blue Prism API**.

C. **Enregistrer l'affichage** : enregistrez les réglages de vos colonnes actuelles. Vous pouvez entrer un nom pour votre affichage afin de le rendre facilement identifiable lors du chargement des affichages.

D. **Charger l'affichage** : chargez un affichage enregistré. Vous pouvez sélectionner l'affichage requis et cliquer sur **Appliquer**.

E. **Regénérer le secret** : pour créer un secret pour un compte de service existant.

F. **Ajouter un compte** : pour ajouter un nouveau compte de service.

G. **Modifier le compte** : pour modifier les détails d'un compte de service existant.

H. **Supprimer le(s) compte(s)** : pour supprimer un ou plusieurs comptes de service.

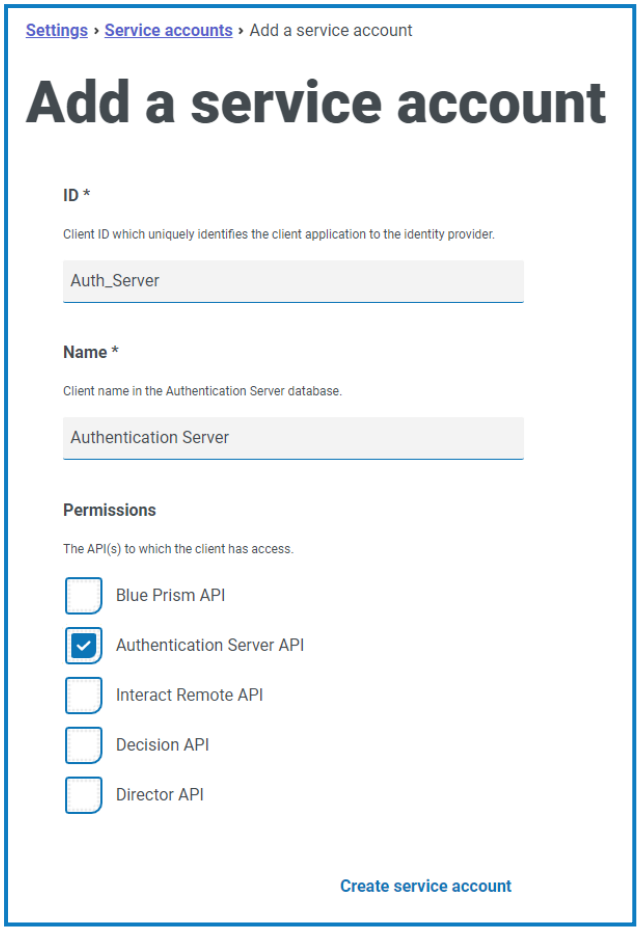
I. **Lignes par page** : saisissez un nombre, ou utilisez les flèches haut et bas, pour modifier le nombre de lignes affichées sur une page.

J. **Précédent et Suivant** : cliquez sur **Précédent** ou **Suivant** pour vous déplacer dans les pages. de comptes de service.

Ajouter un compte de service

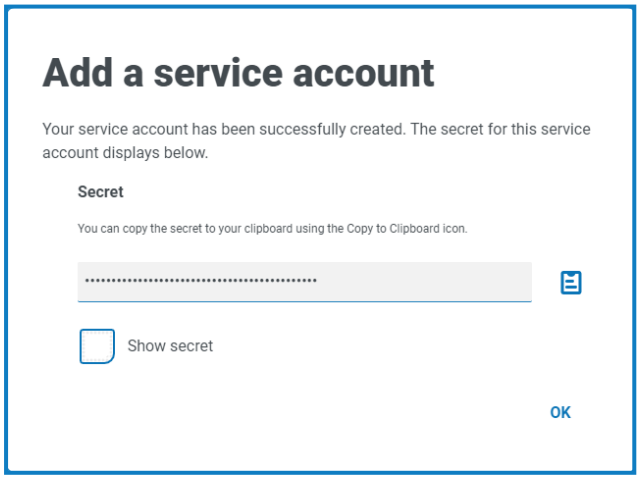
1. Sur la page Comptes de service, cliquez sur **Ajouter un compte**.
2. Saisissez un ID unique pour l'application client et un nom convivial pour le client dans la base de données Authentication Server.
3. Sous **Permissions**, sélectionnez l'option appropriée :
   - **Blue Prism API** : le secret du compte de service est utilisé pour obtenir un jeton d'accès afin de s'authentifier avec Blue Prism API.
   - **API Authentication Server** : le secret du compte de service est utilisé pour envoyer des requêtes authentifiées à l'API Authentication Server.
   - **Interact Remote API** : le secret du compte de service est utilisé pour obtenir un jeton d'accès afin de s'authentifier avec Interact Remote API.
   - **API Decision** : le secret du compte de service permet d'obtenir un jeton d'accès afin de s'authentifier avec l'API Web Decision.
   - **API Directeur** : cette permission n'a pas de fonction. Elle est réservée aux fonctionnalités futures.

4. Cliquez sur **Créer un compte de service**.



La boîte de dialogue Ajouter un compte de service s'affiche avec un secret généré, qui sera utilisé pour obtenir le jeton d'accès à l'API ou aux API sélectionnées.

5. Cliquez sur l'icône Copier dans le presse-papiers pour copier le secret généré dans votre presse-papiers.



6. Cliquez sur **OK** pour fermer la boîte de dialogue.

La page Comptes de service s'affiche avec le compte nouvellement créé.

Regénérer le secret

Si vous avez égaré un secret généré précédemment pour un compte de service existant, vous pouvez en générer un nouveau.

1. Sur la page Comptes de service, sélectionnez le compte de service requis et cliquez sur **Regénérer le secret**.

   Le nouveau secret pour le compte de service s'affiche.
2. Cliquez sur l'icône Copier dans le presse-papiers pour copier le secret généré dans votre presse-papiers.
3. Cliquez sur **OK** pour fermer la boîte de dialogue.

Modifier un compte de service

1. Sur la page Comptes de service, sélectionnez le compte de service requis et cliquez sur **Modifier le compte**.
2. Modifiez les informations comme requis.

   Vous ne pouvez pas modifier l'ID client d'un compte de service.
3. Cliquez sur **Enregistrer** pour appliquer vos modifications.

Supprimer des comptes de service

1. Sur la page Comptes de service, sélectionnez le(s) compte(s) de service requis et cliquez sur **Supprimer le(s) compte(s)**.

   Un message s'affiche vous demandant de confirmer la suppression.
2. Cliquez sur **Oui** pour supprimer le(s) compte(s) sélectionné(s) ou sur **Non** pour annuler.

Utiliser les filtres sur la page Comptes de service

Les filtres vous permettent de trouver facilement un compte de service spécifique en fonction des critères sélectionnés.

1. Sur la page Comptes de service, cliquez sur **Filtrer** pour ouvrir le panneau Filtrer.
2. Utilisez le bouton bascule pour activer le filtre requis et renseignez les informations pour trouver le compte de service. Vous pouvez appliquer plusieurs filtres en même temps.

   Les filtres disponibles sont les suivants :

Filtrer	Description
Nom convivial	Saisissez le nom du compte de service, ou une partie du nom.
ID	Saisissez l'identifiant du compte de service, ou une partie de l'identifiant.
Permissions	Sélectionnez l'option de niveau de permission appropriée. Vous pouvez sélectionner plusieurs options. Si vous ne sélectionnez aucun niveau de permission, tous les niveaux sont inclus sur la page Comptes de service.

   Les informations sur la page Comptes de service sont immédiatement filtrées.

   
   Si vous avez défini les filtres, mais que vous souhaitez afficher à nouveau les informations non filtrées, désactivez les filtres requis ou supprimez tous les réglages du filtre afin qu'il soit vide.

3. Cliquez sur **Fermer le tiroir** pour fermer le panneau Filtrer.