

Utilisateurs et groupes d'utilisateurs

Publié: 2025-03-28

Les utilisateurs peuvent accéder au système ExtraHop de trois manières : via un ensemble de comptes utilisateur préconfigurés, via des comptes utilisateurs locaux configurés sur l'appliance ou via des comptes utilisateurs distants configurés sur des serveurs d'authentification existants, tels que LDAP, SAML, Radius et TACACS+. Pour RevealX 360, vous pouvez ajouter des groupes d'utilisateurs via l'API



Consultez les formations associées :

- [Administration des utilisateurs](#)
- [Groupes d'utilisateurs](#)

Utilisateurs locaux

Cette rubrique concerne les comptes par défaut et locaux. Voir [Authentification à distance](#) pour savoir comment configurer des comptes distants.

Les comptes suivants sont configurés par défaut sur les systèmes ExtraHop mais n'apparaissent pas dans la liste des noms de la page Utilisateurs. Ces comptes ne peuvent pas être supprimés et vous devez modifier le mot de passe par défaut lors de la première connexion.

installation

Ce compte fournit des privilèges complets de lecture et d'écriture du système à l'interface utilisateur basée sur le navigateur et à l'interface de ligne de commande (CLI) ExtraHop. Pour les informations de connexion et de mot de passe par défaut, voir [FAQ sur les comptes utilisateurs par défaut](#).

coquille

Le `shell` Par défaut, le compte a accès à des commandes shell non administratives dans l'interface de ligne de commande ExtraHop. Sur les capteurs physiques, le mot de passe par défaut pour ce compte est le numéro de série figurant sur la face avant de l'appliance. Sur les capteurs virtuels, le mot de passe par défaut est `default`.



Note: Le mot de passe ExtraHop par défaut pour l'un ou l'autre des comptes lorsqu'il est déployé dans Amazon Web Services (AWS) et Google Cloud Platform (GCP) est l'ID d'instance de la machine virtuelle.

Prochaines étapes

- [Ajouter un compte utilisateur local à une console ou à une sonde](#)
- [Ajouter un compte utilisateur local à un espace de stockage des enregistrements ou à un magasin de paquets](#)

Authentification à distance

Le système ExtraHop prend en charge l'authentification à distance pour l'accès des utilisateurs. L'authentification à distance permet aux organisations qui disposent de systèmes d'authentification tels que LDAP (OpenLDAP ou Active Directory, par exemple) de permettre à l'ensemble ou à un sous-ensemble de leurs utilisateurs de se connecter au système à l'aide de leurs informations d'identification existantes.



Important: Les sélections de menu varient en fonction du type d'appliance que vous configurez. Par exemple, SAML n'est disponible que pour les capteurs et les consoles.

L'authentification centralisée offre les avantages suivants :

- Synchronisation des mots de passe utilisateur.
- Création automatique de comptes ExtraHop pour les utilisateurs sans intervention de l'administrateur.
- Gestion des privilèges ExtraHop en fonction des groupes d'utilisateurs.

- Les administrateurs peuvent accorder l'accès à tous les utilisateurs connus ou restreindre l'accès en appliquant des filtres LDAP .

Prochaines étapes

- [Configuration de l'authentification à distance via LDAP](#)
- [Configuration de l'authentification à distance via SAML](#) (Capteurs et consoles uniquement)
- [Configurer l'authentification à distance via TACACS+](#)
- [Configuration de l'authentification à distance via RADIUS](#)

Utilisateurs distants

Si votre système ExtraHop est configuré pour l'authentification à distance SAML ou LDAP, vous pouvez créer un compte pour ces utilisateurs distants. La préconfiguration des comptes sur le système ExtraHop pour les utilisateurs distants vous permet de partager les personnalisations du système avec ces utilisateurs avant qu'ils ne se connectent.

Si vous choisissez de provisionner automatiquement les utilisateurs lorsque vous configurez l'authentification SAML, l'utilisateur est automatiquement ajouté à la liste des utilisateurs locaux lorsqu'il se connecte pour la première fois. Cependant, vous pouvez créer un compte utilisateur SAML distant sur le système ExtraHop lorsque vous souhaitez approvisionner un utilisateur distant avant que celui-ci ne se soit connecté au système. Les privilèges sont attribués à l'utilisateur par le fournisseur. Une fois l'utilisateur créé, vous pouvez l'ajouter aux groupes d'utilisateurs locaux.

Prochaines étapes

- [Ajouter un compte pour un utilisateur distant](#)

Groupes d'utilisateurs

Les groupes d'utilisateurs vous permettent de gérer l'accès au contenu partagé par groupe plutôt que par utilisateur individuel. Les objets personnalisés tels que les cartes d'activité peuvent être partagés avec un groupe d'utilisateurs, et tout utilisateur ajouté au groupe y a automatiquement accès. Vous pouvez créer un groupe d'utilisateurs local, qui peut inclure des utilisateurs locaux et distants. Sinon, si votre système ExtraHop est configuré pour l'authentification à distance via LDAP, vous pouvez configurer les paramètres pour importer vos groupes d'utilisateurs LDAP .

- Cliquez **Créer un groupe d'utilisateurs** pour créer un groupe local. Le groupe d'utilisateurs apparaît dans la liste. Cochez ensuite la case à côté du nom du groupe d'utilisateurs et sélectionnez les utilisateurs dans le **Filtrer les utilisateurs...** menu déroulant. Cliquez **Ajouter des utilisateurs au groupe**.
- (LDAP uniquement) Cliquez sur **Actualiser tous les groupes d'utilisateurs** ou sélectionnez plusieurs groupes d'utilisateurs LDAP et cliquez sur **Actualiser les utilisateurs dans les groupes**.
- Cliquez **Réinitialiser le groupe d'utilisateurs** pour supprimer tout le contenu partagé d'un groupe d'utilisateurs sélectionné. Si le groupe n'existe plus sur le serveur LDAP distant, il est supprimé de la liste des groupes d'utilisateurs.
- Cliquez **Activer le groupe d'utilisateurs** ou **Désactiver le groupe d'utilisateurs** pour contrôler si un membre du groupe peut accéder au contenu partagé pour le groupe d'utilisateurs sélectionné.
- Cliquez **Supprimer un groupe d'utilisateurs** pour supprimer le groupe d'utilisateurs sélectionné du système.
- Consultez les propriétés suivantes pour les groupes d'utilisateurs répertoriés :

Nom du groupe

Affiche le nom du groupe. Pour afficher les membres du groupe, cliquez sur le nom du groupe.

Tapez

Affiche Local ou Remote comme type de groupe d'utilisateurs.

Membres

Affiche le nombre d'utilisateurs du groupe.

Contenu partagé

Affiche le nombre d'objets créés par l'utilisateur qui sont partagés avec le groupe.

État

Indique si le groupe est activé ou désactivé sur le système. Quand le statut est `Disabled`, le groupe d'utilisateurs est considéré comme vide lors des vérifications d'appartenance ; toutefois, le groupe d'utilisateurs peut toujours être spécifié lors du partage de contenu.

Membres actualisés (LDAP uniquement)

Affiche le temps écoulé depuis l'actualisation de l'appartenance au groupe. Les groupes d'utilisateurs sont actualisés dans les conditions suivantes :

- Une fois par heure, par défaut. Le réglage de l'intervalle de rafraîchissement peut être modifié sur **Authentification à distance** > **Paramètres LDAP** page.
- Un administrateur actualise un groupe en cliquant sur **Actualiser tous les groupes d'utilisateurs** ou **Rafraîchir les utilisateurs du groupe**, ou par programmation via l'API REST. Vous pouvez actualiser un groupe à partir du Groupe d'utilisateurs page ou depuis Liste des membres page.
- Un utilisateur distant se connecte au système ExtraHop pour la première fois.
- Un utilisateur tente de charger un tableau de bord partagé auquel il n'a pas accès.

Privilèges utilisateur

Les administrateurs déterminent le niveau d'accès au module pour les utilisateurs du système ExtraHop.

Pour plus d'informations sur les privilèges utilisateur pour l'API REST, consultez le [Guide de l'API REST](#).

Pour plus d'informations sur les privilèges des utilisateurs distants, consultez les guides de configuration pour [LDAP](#), [RAYON](#), [SAML](#), et [TACACS+](#).

Niveaux de privilèges

Définissez le niveau de privilège de votre utilisateur afin de déterminer les zones du système ExtraHop auxquelles il peut accéder.

Privilèges d'accès aux modules

Ces privilèges déterminent les fonctionnalités auxquelles les utilisateurs peuvent accéder dans le système ExtraHop. Les administrateurs peuvent activer le contrôle d'accès basé sur les rôles (RBAC) en accordant aux utilisateurs l'accès à un ou à tous les modules Network Detection and Response (NDR), Network Performance and Monitoring (NPM) et Packet Forensics. Une licence de module est requise pour accéder aux fonctionnalités du module.

Accès au module NDR

Permet à l'utilisateur d'accéder à des fonctionnalités de sécurité telles que la détection des attaques, les enquêtes et les briefings sur les menaces.

Accès au module NPM

Permet à l'utilisateur d'accéder à des fonctionnalités de performance telles que la détection des opérations et la possibilité de créer des tableaux de bord personnalisés.

Accès aux paquets et aux clés de session

Permet à l'utilisateur de visualiser et de télécharger des paquets et des clés de session, des paquets uniquement, des en-têtes de paquets uniquement ou des tranches de paquets uniquement. Permet également à l'utilisateur d'extraire les fichiers associés aux paquets.

Privilèges d'accès au système

Ces privilèges déterminent le niveau de fonctionnalité dont disposent les utilisateurs dans les modules auxquels l'accès leur a été accordé.

Pour RevealX Enterprise, les utilisateurs disposant de privilèges d'accès au système et d'administration peuvent accéder à toutes les fonctionnalités, paquets et clés de session de leurs modules sous licence.

Pour RevealX 360, les privilèges d'accès au système et d'administration, l'accès aux modules sous licence, aux paquets et aux clés de session doivent être attribués séparément. RevealX 360 propose également un compte d'administration système supplémentaire qui accorde tous les privilèges du système, à l'exception de la possibilité de gérer les utilisateurs et l'accès aux API.

Le tableau suivant contient les fonctionnalités d'ExtraHop et leurs privilèges requis. Si aucune exigence de module n'est notée, la fonctionnalité est disponible à la fois dans les modules NDR et NDM.

	Administrati des systèmes et des accès	Administrati du système (RevealX 360 uniquement)	Écriture complète	Écriture limitée	Rédaction personnelle	Lecture seule complète	Lecture seule restreinte
Cartes d'activités							
Créer, visualiser et charger des cartes d'activités partagées	Y	Y	Y	Y	Y	Y	N
Enregistrer des cartes d'activité	Y	Y	Y	Y	Y	N	N
Partager des cartes d'activités	Y	Y	Y	Y	N	N	N
Alertes	Licence et accès au module NPM requis.						
Afficher les alertes	Y	Y	Y	Y	Y	Y	Y
Création et modification d'alertes	Y	Y	Y	N	N	N	N
Priorités d'analyse							
Afficher la page Priorités d'analyse	Y	Y	Y	Y	Y	Y	N
Ajouter et modifier des niveaux d'analyse	Y	Y	Y	N	N	N	N

	Administrati des systèmes et des accès	Administrati du système (RevealX 360 uniquement)	Écriture complète	Écriture limitée	Rédaction personnelle	Lecture seule complète	Lecture seule restreinte
pour les groupes							
Ajouter des appareils à une liste de surveillance	Y	Y	Y	N	N	N	N
Gestion des priorités de transfert	Y	Y	Y	N	N	N	N
Lots							
Création d'un bundle	Y	Y	Y	N	N	N	N
Téléchargez et appliquez un bundle	Y	Y	Y	N	N	N	N
Téléchargez un bundle	Y	Y	Y	Y	Y	N	N
Afficher la liste des offres groupées	Y	Y	Y	Y	Y	Y	N
Tableaux de bord							
Afficher et organiser les tableaux de bord	Y	Y	Y	Y	Y	Y	Y
Création et modification de tableaux de bord	Y	Y	Y	Y	Y	N	N
Partagez des tableaux de bord	Y	Y	Y	Y	N	N	N
Détections	Licence et accès au module NDR nécessaires pour visualiser et régler les détections de sécurité et créer des enquêtes.						
	Licence et accès au module NPM requis pour afficher et régler les détections de performances.						
Afficher les détections	Y	Y	Y	Y	Y	Y	Y

	Administrati des systèmes et des accès	Administrati du système (RevealX 360 uniquement)	Écriture complète	Écriture limitée	Rédaction personnelle	Lecture seule complète	Lecture seule restreinte
Reconnaître les détections	Y	Y	Y	Y	Y	N	N
Modifier l'état de détection et les notes	Y	Y	Y	Y	N	N	N
Création et modification d'enquêtes	Y	Y	Y	Y	N	N	N
Création et modification de règles d'exceptions	Y	Y	Y	N	N	N	N
Groupes d'appareils	Les administrateurs peuvent configurer le Politique globale de contrôle des modifications des groupes d'appareils  pour spécifier si les utilisateurs disposant de privilèges d'écriture limités peuvent créer et modifier des groupes d'équipements.						
Création et modification de groupes d'équipements	Y	Y	Y	Y (Si la politique de privilèges globale est activée)	N	N	N
Intégrations	RevealX 360 uniquement						
Configuration et modification des intégrations	Y	Y	N	N	N	N	N
Analyse de fichiers							
Configuration des paramètres et des règles d'analyse des fichiers	Y	Y	N	N	N	N	N
Métriques							
Afficher les statistiques	Y	Y	Y	Y	Y	Y	N
Règles de notification	Licence et accès au module NDR requis pour créer et modifier des notifications pour les détections de sécurité, le catalogue des détections de sécurité et les briefings sur les menaces.						

	Administrati des systèmes et des accès	Administrati du système (RevealX 360 uniquement)	Écriture complète	Écriture limitée	Rédaction personnelle	Lecture seule complète	Lecture seule restreinte
	Licence et accès au module NPM requis pour créer et modifier des notifications pour les détections de performances et le catalogue de détection des performances.						
Création et modification de règles de notification de détection	Y	Y	Y	N	N	N	N
Création et modification de règles de notification de détection pour les intégrations SIEM (RevealX 360 uniquement)	Y	Y	N	N	N	N	N
Création et modification des règles de notification du catalogue de détection	Y	Y	Y	N	N	N	N
Création et modification des règles de notification des informations sur les menaces	Y	Y	Y	N	N	N	N
Création et modification des règles de notification du système	Y	Y	N	N	N	N	N

	Administrati des systèmes et des accès	Administrati du système (RevealX 360 uniquement)	Écriture complète	Écriture limitée	Rédaction personnelle	Lecture seule complète	Lecture seule restreinte
Disques	Disquaire requis.						
Afficher les requêtes d'enregistrement	Y	Y	Y	Y	Y	Y	N
Afficher les formats d'enregistrement	Y	Y	Y	Y	Y	Y	N
Créer, modifier et enregistrer des requêtes d'enregistrement	Y	Y	Y	N	N	N	N
Création, modification et enregistrement de formats d'enregistrement	Y	Y	Y	N	N	N	N
Rapports planifiés	Console requise.						
Créer, consultez et gérez des rapports planifiés	Y	Y	Y	Y	N	N	N
Renseignements sur les menaces	Licence et accès au module NDR requis.						
Gérez les collections de menaces	Y	Y	N	N	N	N	N
Gérer les flux TAXII	Y	Y	N	N	N	N	N
Afficher les renseignements sur les menaces	Y	Y	Y	Y	Y	Y	N
éléments déclencheurs							
Création et modification	Y	Y	Y	N	N	N	N

	Administrati des systèmes et des accès	Administrati du système (RevealX 360 uniquement)	Écriture complète	Écriture limitée	Rédaction personnelle	Lecture seule complète	Lecture seule restreinte
de déclencheurs							
Privilèges administratifs							
Accédez aux paramètres d'administration d'ExtraHop	Y	Y	N	N	N	N	N
Connexion à d'autres appareils	Y	Y	N	N	N	N	N
Gérer les autres appareils (console)	Y	Y	N	N	N	N	N
Gérez les utilisateurs et l'accès aux API	Y	N	N	N	N	N	N