

# Utilisateurs et groupes d'utilisateurs

Publié: 2024-02-13

Les utilisateurs peuvent accéder au système ExtraHop de trois manières : via un ensemble de comptes utilisateurs 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+.

## Utilisateurs locaux

Cette rubrique concerne les comptes locaux et par défaut. 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 connexion initiale.

### 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. Sur le plan physique capteurs, le mot de passe par défaut pour ce compte est le numéro de série inscrit sur le devant de l'appliance. Sur le virtuel capteurs, le mot de passe par défaut est `default`.

### coquille

Le `shell` Le compte, par défaut, a accès aux 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 inscrit sur le devant 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](#)

## 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 dotées de systèmes d'authentification tels que LDAP (OpenLDAP ou Active Directory, par exemple) de permettre à tous leurs utilisateurs ou à un sous-ensemble de leurs utilisateurs de se connecter au système avec leurs informations d'identification existantes.

L'authentification centralisée offre les avantages suivants :

- Synchronisation du mot 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](#)
- [Configuration de 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'activités 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. Ensuite, cochez la case à côté du nom du groupe d'utilisateurs et sélectionnez les utilisateurs dans **Filtrer les utilisateurs...** liste déroulante. 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 le 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.

#### Type

Affiche le type de groupe d'utilisateurs local ou distant.

#### 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. Lorsque le statut est `Disabled`, le groupe d'utilisateurs est considéré comme vide lors des vérifications d'adhésion ; toutefois, le groupe d'utilisateurs peut toujours être spécifié lors du partage de contenu.

## Membres actualisés (LDAP uniquement)

Affiche le temps écoulé depuis que l'adhésion au groupe a été actualisée. 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 le **Authentification à distance** > **Paramètres LDAP** page.
- Un administrateur actualise un groupe en cliquant sur **Actualiser tous les groupes d'utilisateurs** ou **Actualiser les utilisateurs du groupe**, ou par programmation via l'API REST. Vous pouvez actualiser un groupe à partir du Groupe d'utilisateurs ou depuis la page 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 privilège

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 accorder aux utilisateurs un accès basé sur les rôles à un ou à tous les modules NDR, NPM et Packet Forensics. Une licence de module est requise pour accéder aux fonctionnalités du module.

### Détection et réponse du réseau (NDR)

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

### Performances et surveillance du réseau (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.

### Criminalistique des paquets

Permet à l'utilisateur de visualiser et de télécharger des paquets et des clés de session, des paquets uniquement ou des tranches de paquets uniquement.

### Privilèges d'accès au système

Ces privilèges déterminent le niveau de fonctionnalité des utilisateurs dans les modules auxquels ils ont été autorisés à accéder.

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

Pour Reveal (x) 360, l'accès au système et les privilèges d'administration, l'accès aux modules sous licence, aux paquets et aux clés de session doivent être attribués séparément. Reveal (x) 360 propose également un compte d'administration système supplémentaire qui accorde des privilèges système complets, 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 du système et des accès	Administrati du système (Reveal (x) 360 uniquement)	Écriture complète	Écriture limitée	Rédaction personnelle	Lecture seule complète	Lecture seule restreinte
<b>Cartes d'activités</b>							
Création, affichage et chargement de cartes d'activités partagées	Y	Y	Y	Y	Y	Y	N
Enregistrer les cartes d'activités	Y	Y	Y	Y	Y	N	N
Partagez des cartes d'activités	Y	Y	Y	Y	N	N	N
<b>Alertes</b>	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
<b>Priorités d'analyse</b>							
Afficher la page des priorités d'analyse	Y	Y	Y	Y	Y	Y	N
Ajouter et modifier des niveaux d'analyse pour les groupes	Y	Y	Y	N	N	N	N
Ajouter des appareils à une liste de surveillance	Y	Y	Y	N	N	N	N

	Administrati du système et des accès	Administrati du système (Reveal (x) 360 uniquement)	Écriture complète	Écriture limitée	Rédaction personnelle	Lecture seule complète	Lecture seule restreinte
Gestion des priorités de transfert	Y	Y	Y	N	N	N	N
Bundles							
Création d'un bundle	Y	Y	Y	N	N	N	N
Téléchargez et appliquez un bundle	Y	Y	Y	N	N	N	N
Afficher la liste des offres groupées	Y	Y	Y	Y	Y	Y	N
Tableaux de bord	Licence et accès au module NPM requis pour créer et modifier des 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 visualiser et régler les détections de performances.						
Afficher les détections	Y	Y	Y	Y	Y	Y	Y
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

	Administrati du système et des accès	Administrati du système (Reveal (x) 360 uniquement)	Écriture complète	Écriture limitée	Rédaction personnelle	Lecture seule complète	Lecture seule restreinte
Création et modification d'enquêtes	Y	Y	Y	Y	N	N	N
Création et modification de règles de réglage	Y	Y	Y	N	N	N	N
Groupes d'appareils	Les administrateurs peuvent configurer <a href="#">Politique globale de contrôle des modifications par groupes d'appareils</a> pour indiquer si les utilisateurs disposant de droits 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 privileges globale est activée)	N	N	N
Métriques							
Afficher les métriques	Y	Y	Y	Y	Y	Y	N
Règles de notification	Licence et accès au module NDR requis pour créer et modifier les notifications relatives aux détections de sécurité et aux briefings sur les menaces.  Licence et accès au module NPM requis pour créer et modifier des notifications pour les détections de performances.						
Création et modification de règles de notification 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 du système et des accès	Administrati du système (Reveal (x) 360 uniquement)	Écriture complète	Écriture limitée	Rédaction personnelle	Lecture seule complète	Lecture seule restreinte
(Reveal (x) uniquement)							
Enregistrement	Recordstore 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
Création, modification et enregistrement de 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 du tableau de bord	Console requise.						
Création, affichage et gestion de 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
Afficher les renseignements sur les menaces	Y	Y	Y	Y	Y	Y	N
<b>DÉCLENCHEURS</b>							
Création et modification	Y	Y	Y	N	N	N	N

	Administrati du système et des accès	Administrati du système (Reveal (x) 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 d'autres appareils (console)	Y	Y	N	N	N	N	N
Gestion des utilisateurs et de l'accès aux API	Y	N	N	N	N	N	N