

Guide de configuration et d'administration de Reveal (x) 360

Publié: 2024-04-10

Après avoir reçu votre e-mail initial d'ExtraHop Networks, vous devez effectuer quelques procédures avant de pouvoir commencer à analyser votre trafic. Ce guide fournit les procédures de configuration et d'administration de base du système Reveal (x) 360.

 **Vidéo** consultez la formation associée : [Présentation de l'administration de Reveal \(x\) 360](#)

Activez votre compte administrateur

Le privilège d'administration du système et des accès est accordé à l'adresse e-mail que vous avez fournie lors de votre inscription.

1. Ouvrez votre e-mail Welcome to ExtraHop Reveal (x) 360.
2. Cliquez sur le lien URL de votre environnement Reveal (x) 360.
3. Sur la page de connexion, entrez votre adresse e-mail et le mot de passe temporaire inclus dans l'e-mail.
4. Cliquez **Connectez-vous**.
5. Sur l'écran Modifier le mot de passe, entrez un nouveau mot de passe dans les deux champs de mot de passe , puis cliquez sur **Envoyer**.
6. Sur la page de configuration de l'authentification multifactorielle, scannez le code QR ou saisissez manuellement le code qui apparaît dans votre application d'authentification.
7. Entrez le code fourni par votre application d'authentification dans **Code** champ, puis cliquez sur **Configuration complète**.
8. Sur la page Réussite, cliquez sur **Poursuivre**.

Configurez vos règles de pare-feu

Si votre système ExtraHop est déployé dans un environnement doté d'un pare-feu, vous devez ouvrir l'accès aux services cloud ExtraHop. Pour les systèmes Reveal (x) 360 connectés à des systèmes autogérés capteurs, vous devez également ouvrir l'accès à l'ExtraHop Cloud Recordstore.

Accès ouvert aux services cloud

Pour accéder aux services cloud ExtraHop, votre capteurs doit être capable de résoudre les requêtes DNS pour *.extrahop.com et d'accéder au protocole TCP 443 (HTTPS) à partir de l'adresse IP correspondant à votre sonde licence :

- 35.161.154.247 (Portland, États-Unis)
- 54.66.242,25 (Sydney, Australie)
- 52.59.110.168 (Francfort, Allemagne)

Accès ouvert au Cloud Recordstore

Pour accéder à l'ExtraHop Cloud Recordstore, votre capteurs doit être en mesure d'accéder au protocole TCP 443 (HTTPS) sortant à ces noms de domaine complets :


- bigquery.googleapis.com
- bigquerystorage.googleapis.com
- oauth2.googleapis.com

- www.googleapis.com
- www.mtls.googleapis.com
- iamcredentials.googleapis.com

Vous pouvez également consulter les conseils publics de Google à propos de [calcul des plages d'adresses IP possibles](#) pour googleapis.com.

Outre la configuration de l'accès à ces domaines, vous devez également configurer le [paramètres globaux du serveur proxy](#).

Ajouter et gérer des utilisateurs

1. Sur la page de présentation, cliquez sur **Paramètres du système**  puis cliquez sur **Accès utilisateur**.
2. Dans la section Utilisateurs, cliquez sur **Afficher les utilisateurs**.
3. Cliquez **Créer**.
4. Entrez l'adresse e-mail, le prénom et le nom de famille du nouvel utilisateur.
5. Dans la section Accès au système, sélectionnez l'un des privilèges suivants.

Privilège	Descriptif
Administration des systèmes et des accès	Créer et modifier tous les objets et paramètres, y compris les pages d'administration, dans Reveal (x) 360.
Administration du système	Créer et modifier des objets et des paramètres, à l'exception de l'accès utilisateur et de l'accès aux API sur la page Administration.
Écriture complète	Créer et modifier tous les objets et paramètres, à l'exception des pages d'administration.
Écriture limitée	Créer, modifier et partager des tableaux de bord. Créer et modifier des règles de réglage. Créer et modifier les règles de détection et de notification des informations sur les menaces.
Rédaction personnelle	Créer des tableaux de bord personnels et modifier les tableaux de bord partagés avec l'utilisateur connecté.
Lecture seule complète	Afficher les objets dans le système ExtraHop.
Lecture seule limitée	Afficher les tableaux de bord partagés avec cet utilisateur.

6. Dans la section Accès au module NDR, sélectionnez l'un des privilèges suivants.

Privilège	Descriptif
Accès complet	Accès aux détections du réseau.
Pas d'accès	Aucun accès aux détections du réseau.

7. Dans la section Accès au module NPM, sélectionnez l'un des privilèges suivants.

Privilège	Descriptif
Accès complet	Accès aux détections de performances.
Pas d'accès	Aucun accès aux détections de performances.

8. Dans le **Accès aux paquets et aux clés de session** section, sélectionnez l'un des privilèges suivants :

Privilège	Descriptif
Paquets et clés de session	Recherchez et téléchargez des paquets et des clés de session associées.
Paquets uniquement	Recherchez et téléchargez des paquets.
Tranches en sachets uniquement	Recherchez et téléchargez les 64 premiers octets d'un paquet.
Pas d'accès	Aucun accès aux paquets.

9. Cliquez **Enregistrer**.
L'utilisateur reçoit un e-mail contenant l'URL de l' environnement Reveal (x) 360 et son mot de passe temporaire. Le mot de passe temporaire expire au bout de 7 jours.
10. Cliquez **Terminé**.

Modifier les paramètres utilisateur

Vous pouvez modifier les niveaux de privilèges attribués, réinitialiser la configuration de l'authentification multifacteur ou supprimer l'utilisateur.

Modifier les privilèges des utilisateurs

1. Dans la section Utilisateurs, cliquez sur le nom de l'utilisateur que vous souhaitez modifier.
2. Dans le volet de gauche, sélectionnez le nouveau niveau de privilège pour l'utilisateur, puis cliquez sur **Enregistrer**.

Réinitialiser l'authentification multifacteur


1. Dans la section Utilisateurs, cliquez sur le nom de l'utilisateur que vous souhaitez modifier.
2. Effacez le **Réinitialiser la configuration MFA pour cet utilisateur** .
L'utilisateur doit configurer l'authentification multifacteur lors de sa prochaine connexion à Reveal (x) 360.

Supprimer un utilisateur

1. Dans la section Utilisateurs, cliquez sur le nom de l'utilisateur que vous souhaitez modifier.
2. Cliquez **Supprimer**.
3. Sélectionnez l'une des options suivantes :
 - **Transférez les tableaux de bord, les collections et les cartes d'activité appartenant à <username> à l' utilisateur suivant :** puis sélectionnez un nouvel utilisateur dans la liste déroulante.
 - **Supprimer tous les tableaux de bord, collections et cartes d'activité appartenant à <username>**
4. Cliquez **Supprimer**.

Gérez les politiques mondiales

Les administrateurs peuvent configurer des politiques globales qui s'appliquent à tous les utilisateurs qui accèdent au système.

1. Sur la page de présentation, cliquez sur **Paramètres du système**  puis cliquez sur **Accès utilisateur**.
2. Dans la section Politiques globales, spécifiez une ou plusieurs des options suivantes.


Option	Description
Contrôle d'édition des groupes d'appareils	Sélectionnez cette option pour contrôler si tous les utilisateurs disposant de privilèges d'écriture limités peuvent créer et modifier des groupes d'équipements. Lorsque cette politique est sélectionnée, tous les utilisateurs à écriture limitée peuvent créer des groupes d'appareils et

Option	Description
Tableau de bord par défaut	ajouter d'autres utilisateurs à écriture limitée en tant qu'éditeurs à leurs groupes d'appareils. Spécifiez le tableau de bord que les utilisateurs voient lorsqu'ils se connectent au système. Seuls les tableaux de bord partagés avec tous les utilisateurs peuvent être définis par défaut par défaut. Les utilisateurs peuvent modifier ce paramètre par défaut ↗ depuis le menu de commande de n'importe quel tableau de bord.

3. Cliquez **Enregistrer les modifications**.

Configurer une liste d'autorisations


Configurez une liste d'adresses IPv4 et de blocs CIDR autorisés à accéder à Reveal (x) 360.

1. Sur la page de présentation, cliquez sur **Paramètres du système**  puis cliquez sur **Accès utilisateur**.
2. Dans la section Liste des autorisations, cliquez sur **Activer la liste des autorisations**.
3. Tapez une liste séparée par des virgules des adresses IPv4 ou des blocs CIDR autorisés à accéder au système. Les adresses IPv6 ne sont pas prises en charge.
4. Cliquez **Enregistrer**. L'activation de la liste d'autorisation peut prendre plusieurs minutes.

Configurer l'heure du système

La page Heure du système affiche les paramètres d'heure système par défaut et l'heure d'affichage par défaut configurée pour votre système ExtraHop.


Voici quelques considérations concernant les paramètres de l'heure du système dans Reveal (x) 360 :

- Vous devez disposer de privilèges d'administrateur système ou d'une version supérieure pour effectuer des modifications.
 - L'heure système par défaut est un fuseau horaire global appliqué à votre système ExtraHop.
 - L'heure d'affichage par défaut pour les utilisateurs est le fuseau horaire que tous les utilisateurs voient dans le système ExtraHop, à moins qu'un utilisateur ne modifie manuellement son **fuseau horaire affiché** [↗](#).
1. Sur la page de présentation, cliquez sur **Paramètres du système**  puis cliquez sur **Toute l'administration**.
 2. Dans la section Paramètres de la console, cliquez sur **Heure du système**.
 3. À partir du Heure système par défaut liste déroulante, sélectionnez le fuseau horaire de votre choix.
 4. À partir du Heure d'affichage par défaut pour les utilisateurs section, sélectionnez l'une des options suivantes :
 - Heure du navigateur
 - Heure du système
 - UTC
 5. Cliquez **Enregistrer les modifications**.

Activer l'assistant de recherche AI

L'assistant de recherche AI vous permet de rechercher des appareils contenant des questions ou des invites rédigées dans un langage naturel et courant afin de créer rapidement des requêtes complexes.

L'assistant de recherche AI s'appuie sur un LLM tiers. Les instructions des utilisateurs ne sont pas fournies pour la formation LLM ni stockées par le LLM, mais peuvent être conservées par le système ExtraHop à des fins d'amélioration du produit. Consultez les [FAQ sur l'assistant de recherche AI](#) pour plus d'informations.


1. Sur la page Vue d'ensemble, cliquez sur **Paramètres du système** icône  puis cliquez sur **Toute l'administration**.
2. Dans la section Paramètres de la console, cliquez sur **Assistant de recherche IA**.
3. Activez l'assistant de recherche AI en sélectionnant **J'accepte d'activer l'assistant de recherche AI et d'envoyer des recherches en langage naturel à ExtraHop Cloud Services**.
4. Cliquez **Enregistrer les modifications**.

Prochaines étapes

[Trouvez des appareils avec AI Search Assistant](#)

Configurer la priorité des noms d'équipements

Les appareils découverts sont automatiquement nommés en fonction de plusieurs sources de données réseau. Lorsque plusieurs noms sont trouvés pour un équipement, un ordre de priorité par défaut est appliqué. Vous pouvez modifier l'ordre de priorité.

1. Sur la page de présentation, cliquez sur **Paramètres du système**  puis cliquez sur **Toute l'administration**.
2. Dans la section Paramètres de la console, cliquez sur **Priorité du nom de l'appareil**.
3. Cliquez et faites glisser les noms des équipements pour créer un nouvel ordre de priorité.
4. Cliquez **Enregistrer**.
Cliquez **Revenir à la valeur par défaut** pour annuler vos modifications.


Activer le suivi des détections

Le suivi des détections vous permet d'attribuer une détection à un utilisateur, de définir son statut et d'ajouter des notes. Vous pouvez suivre les détections directement dans le système ExtraHop, avec un système de billetterie externe tiers, ou avec les deux méthodes.



Note: Vous devez activer le suivi des tickets sur tous les capteurs connectés.

Avant de commencer

- Vous devez avoir accès à un système ExtraHop avec un compte utilisateur doté de **Privilèges d'administration**.
 - Après avoir activé le suivi externe des tickets, vous devez **configurer le suivi des tickets par des tiers** en écrivant un déclencheur pour créer et mettre à jour des tickets sur votre système de billetterie, puis activez les mises à jour des tickets sur votre système ExtraHop via l'API REST.
 - Si vous désactivez le suivi externe des tickets, les informations de statut et de ticket des destinataires précédemment stockées sont converties en suivi de détection ExtraHop. Si le suivi de détection depuis le système ExtraHop est activé, vous pourrez consulter les tickets qui existaient déjà lorsque vous avez désactivé le suivi des tickets externes, mais les modifications apportées à ce ticket externe n'apparaîtront pas dans le système ExtraHop.
1. Sur la page de présentation, cliquez sur **Paramètres du système**  puis cliquez sur **Toute l'administration**.
 2. Dans la section Paramètres de la console, cliquez sur **Suivi de la détection**.
 3. Sélectionnez l'une des méthodes suivantes ou les deux pour suivre les détections :
 - Sélectionnez **Permettre aux utilisateurs d'ExtraHop de suivre les détections depuis le système ExtraHop**.

- Sélectionnez **Activez des intégrations externes, telles que les systèmes SOAR ou de suivi des tickets, pour suivre les détections via l'API ExtraHop Rest**.
4. Optionnel : Après avoir sélectionné l'option permettant d'activer les intégrations externes, spécifiez le modèle d'URL pour votre système de billetterie et ajoutez le `$ticket_id` variable à l'endroit approprié. Par exemple, saisissez une URL complète telle que `https://jira.example.com/browse/$ticket_id`. Le `$ticket_id` La variable est remplacée par l'identifiant du ticket associé à la détection. Une fois le modèle d'URL configuré, vous pouvez cliquer sur l'ID du ticket dans une détection pour ouvrir le ticket dans un nouvel onglet de navigateur.

The screenshot displays a security alert in the ExtraHop interface. On the left, a sidebar shows the time 'Today 14:00 lasting an hour', a risk level of 83 (RISK), and a 'LATERAL MOVEMENT' indicator. Below this, the ticket status is 'CLOSED', the ticket ID is 'EX-4437', and the assignee is 'hopuser'. The main alert area is titled 'Suspicious CIFS Client File Share Access on AccountingLaptop' and contains the following text: 'This device sent an excessive number of read requests over the Common Internet File System (CIFS) protocol. This anomaly indicates that the device might be compromised and is preparing files for data exfiltration.' Below the text, it lists the 'Server linked to this anomaly' as 'corpshare.example.com (192.168.6.179)'. At the bottom, there is a table for 'AccountingLaptop' with an 'Activity Map' link.

CIFS Metric	6-hour Snapshot	Peak Value	Expected Range	Deviation
Reads		1.13 K	0-1	112,500%

Prochaines étapes

Si vous avez activé les intégrations externes de suivi des tickets, vous devez passer à la tâche suivante :

- [Configurer le suivi des tickets par des tiers pour les détections](#)

Configurer le suivi des tickets par des tiers pour les détections

Le suivi des tickets vous permet de connecter les tickets, les alarmes ou les dossiers de votre système de suivi du travail aux détections ExtraHop. Tout système de billetterie tiers capable d'accepter les requêtes Open Data Stream (ODS), tel que Jira ou Salesforce, peut être lié aux détections ExtraHop.

Avant de commencer

- Tu dois avoir [a sélectionné l'option de suivi de la détection par des tiers dans les paramètres d'administration](#).
- Vous devez avoir accès à un système ExtraHop avec un compte utilisateur doté de [Privilèges d'administration du système et des accès](#).
- Vous devez être familiarisé avec l'écriture de ExtraHop Triggers. Voir [déclencheurs](#) et les procédures de [Créer un déclencheur](#).
- Vous devez créer une cible ODS pour votre serveur de suivi des tickets. Consultez les rubriques suivantes concernant la configuration des cibles ODS : [HTTP](#), [Kafka](#), [MongoDB](#), [syslog](#), ou [données brutes](#).
- Vous devez être familiarisé avec l'écriture de scripts d'API REST et disposer d'une clé d'API valide pour effectuer les procédures ci-dessous. Voir [Génération d'une clé d'API](#).


Rédigez un déclencheur pour créer et mettre à jour des tickets concernant les détections sur votre système de billetterie

Cet exemple montre comment créer un déclencheur qui exécute les actions suivantes :


- Créez un nouveau ticket dans le système de billetterie chaque fois qu'une nouvelle détection apparaît sur le système ExtraHop.
- Attribuer de nouveaux tickets à un utilisateur nommé `escalations_team` dans le système de billetterie.

- Exécuté chaque fois qu'une détection est mise à jour sur le système ExtraHop.
- Envoyez des mises à jour de détection via un flux de données ouvert (ODS) HTTP au système de billetterie.

L'exemple de script complet est disponible à la fin de cette rubrique.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône des paramètres système  puis cliquez sur **DÉCLENCHEURS**.
3. Cliquez **Nouveau**.
4. Spécifiez un nom et une description facultative pour le déclencheur.
5. Dans la liste des événements, sélectionnez **MISE À JOUR DE DÉTECTION**.

L'événement `DETECTION_UPDATE` s'exécute chaque fois qu'une détection est créée ou mise à jour dans le système ExtraHop.

6. Dans le volet droit, spécifiez **Classe de détection**  paramètres d'un objet JavaScript. Ces paramètres déterminent les informations envoyées à votre système de billetterie.

L'exemple de code suivant ajoute l'identifiant de détection, la description, le titre, les catégories, les techniques et tactiques MITRE, ainsi que l'indice de risque à un objet JavaScript appelé `payload`:

```
const summary = "ExtraHop Detection: " + Detection.id + ": " +
  Detection.title;
const description = "ExtraHop has detected the following event on your
network: " + Detection.description
const payload = {
  "fields": {
    "summary": summary,
    "assignee": {
      "name": "escalations_team"
    },
    "reporter": {
      "name": "ExtraHop"
    },
    "priority": {
      "id": Detection.riskScore
    },
    "labels": Detection.categories,
    "mitreCategories": Detection.mitreCategories,
    "description": description
  }
};
```

7. Définissez ensuite les paramètres de requête HTTP dans un objet JavaScript situé sous l'objet JavaScript précédent.

L'exemple de code suivant définit une requête HTTP pour la charge utile décrite dans l'exemple précédent : définit une requête avec une charge utile JSON :

```
const req = {
  'path': '/rest/api/issue',
  'headers': {
    'Content-Type': 'application/json'
  },
  'payload': JSON.stringify(payload)
};
```

Pour plus d'informations sur les objets de requête ODS, voir **Classes de flux de données ouvertes** .

8. Enfin, spécifiez la requête HTTP POST qui envoie les informations à la cible ODS. L'exemple de code suivant envoie la requête HTTP décrite dans l'exemple précédent à une cible ODS nommée ticket-server :

```
Remote.HTTP('ticket-server').post(req);
```

Le code du déclencheur complet doit ressembler à l'exemple suivant :

```
const summary = "ExtraHop Detection: " + Detection.id + ": " +
  Detection.title;
const description = "ExtraHop has detected the following event on your
  network: " + Detection.description
const payload = {
  "fields": {
    "summary": summary,
    "assignee": {
      "name": "escalations_team"
    },
    "reporter": {
      "name": "ExtraHop"
    },
    "priority": {
      "id": Detection.riskScore
    },
    "labels": Detection.categories,
    "mitreCategories": Detection.mitreCategories,
    "description": description
  }
};

const req = {
  'path': '/rest/api/issue',
  'headers': {
    'Content-Type': 'application/json'
  },
  'payload': JSON.stringify(payload)
};

Remote.HTTP('ticket-server').post(req);
```

Envoyer les informations des tickets aux détections via l'API REST

Après avoir configuré un déclencheur pour créer des tickets pour les détections dans votre système de suivi des tickets, vous pouvez mettre à jour les informations des tickets sur votre système ExtraHop via l'API REST .

Les informations du ticket apparaissent dans les détections sur la page des détections du système ExtraHop. Pour plus d'informations, consultez le [Détections](#) sujet.

L'exemple de script Python suivant prend les informations de ticket d'un tableau Python et met à jour les détections associées sur le système ExtraHop.

```
#!/usr/bin/python3

import json
import requests
import csv

API_KEY = '123456789abcdefghijklmnop'
HOST = 'https://extrahop.example.com/'

# Method that updates detections on an ExtraHop system
def updateDetection(detection):
```



```

url = HOST + 'api/v1/detections/' + detection['detection_id']
del detection['detection_id']
data = json.dumps(detection)
headers = {'Content-Type': 'application/json',
           'Accept': 'application/json',
           'Authorization': 'ExtraHop apikey=%s' % API_KEY}
r = requests.patch(url, data=data, headers=headers)
print(r.status_code)
print(r.text)

# Array of detection information
detections = [
    {
        "detection_id": "1",
        "ticket_id": "TK-16982",
        "status": "new",
        "assignee": "sally",
        "resolution": None,
    },
    {
        "detection_id": "2",
        "ticket_id": "TK-2078",
        "status": None,
        "assignee": "jim",
        "resolution": None,
    },
    {
        "detection_id": "3",
        "ticket_id": "TK-3452",
        "status": None,
        "assignee": "alex",
        "resolution": None,
    }
]

for detection in detections:
    updateDetection(detection)

```



Note: Si le script renvoie un message d'erreur indiquant que la vérification du certificat SSL a échoué, assurez-vous que **un certificat fiable a été ajouté à votre sonde ou à votre console** [🔗](#). Vous pouvez également ajouter le `verify=False` option permettant de contourner la vérification des certificats. Cependant, cette méthode n'est pas sûre et n'est pas recommandée. Le code suivant envoie une requête HTTP GET sans vérification du certificat :

```
requests.get(url, headers=headers, verify=False)
```

Une fois le suivi des tickets configuré, les détails des tickets sont affichés dans le volet gauche des détails de détection, comme dans la figure suivante :

The screenshot displays a detection alert in the ExtraHop interface. On the left, a sidebar shows the ticket status as 'CLOSED', the ticket ID as 'EX-4437', and the assignee as 'hopuser'. The main panel shows the alert title 'Suspicious CIFS Client File Share Access on AccountingLaptop' with a risk score of 83 and a 'LATERAL MOVEMENT' indicator. The alert description states: 'This device sent an excessive number of read requests over the Common Internet File System (CIFS) protocol. This anomaly indicates that the device might be compromised and is preparing files for data exfiltration.' Below this, it lists the server linked to the anomaly: 'corpshare.example.com (192.168.6.179)'. At the bottom, a table provides CIFS metrics for 'AccountingLaptop'.

CIFS Metric	6-hour Snapshot	Peak Value	Expected Range	Deviation
Reads		1.13 K	0-1	112,500%

État

État du ticket associé à la détection. Le suivi des tickets prend en charge les statuts suivants :

- Nouveau
- En cours
- Fermé
- Fermé avec action prise
- Fermé sans qu'aucune mesure n'ait été prise

Identifiant du billet

L'identifiant du ticket associé à la détection dans votre système de suivi du travail. Si vous avez configuré un modèle d'URL, vous pouvez cliquer sur l'identifiant du ticket pour ouvrir le ticket dans votre système de suivi du travail.

Cessionnaire

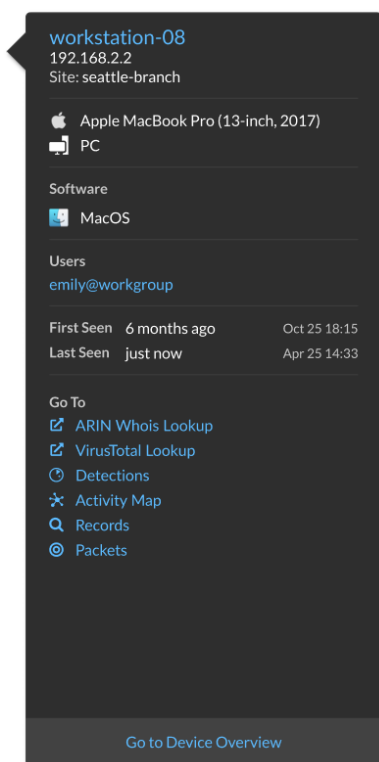
Le nom d'utilisateur attribué au ticket associé à la détection. Les noms d'utilisateur en gris indiquent un compte non-ExtraHop.


Configurer les liens de recherche du point de terminaison

La recherche de point de terminaison vous permet de spécifier des outils d'adresse IP externes disponibles pour récupérer des informations sur les points de terminaison au sein du système ExtraHop. Par exemple, lorsque vous cliquez ou placez le pointeur sur une adresse IP, les liens des outils de recherche s'affichent afin que vous puissiez facilement trouver des informations sur ce point de terminaison.

Les liens de recherche suivants sont configurés par défaut et peuvent être modifiés ou supprimés :

- Recherche Whois ARIN
- Recherche VirusTotal



1. Sur la page de présentation, cliquez sur **Paramètres du système**  puis cliquez sur **Toute l'administration**.
2. Dans la section Paramètres de la console, cliquez sur **Recherche de terminaux**.
3. Dans le **Modèle d'URL** dans ce champ, saisissez l'URL de l'outil de recherche.
L'URL doit inclure `$ip` variable, qui est remplacée par l'adresse IP du point de terminaison lors de la recherche. Par exemple, `https://search.arin.net/rdap/?query=$ip`
4. Dans le **Nom d'affichage** dans ce champ, tapez le lien du nom tel que vous souhaitez qu'il apparaisse.
5. Sélectionnez l'une des options suivantes Options d'affichage:
 - Afficher ce lien sur tous les terminaux
 - Afficher ce lien sur les points de terminaison externes
 - Afficher ce lien sur les points de terminaison internes
 - Ne pas afficher ce lien
6. Cliquez **Enregistrer**.

Connecter les capteurs

Ajouter capteurs à Reveal (x) 360 pour surveiller le trafic de votre réseau.

Reveal (x) géré par ExtraHop capteurs pour AWS peut être sélectionné et déployé depuis la console Reveal (x) 360.

- [Déployez les capteurs Reveal \(x\) 360 pour AWS](#) 

Autogéré capteurs et les packetstores peuvent également être connectés depuis la console Reveal (x) 360. Notez que si vous possédez déjà une console, vous devez la déconnecter avant de connecter votre console autogérée capteurs vers Reveal (x) 360.

- [Connectez-vous à Reveal \(x\) 360 à partir de capteurs autogérés](#) 

Intégrations

La page Intégrations affiche un catalogue de produits et de solutions de fournisseurs tiers qui fonctionnent avec le système ExtraHop. Les intégrations peuvent fournir des informations sur la façon dont vos appareils communiquent dans votre environnement ou améliorer votre capacité à enquêter sur les menaces et les problèmes.

Les exigences et les configurations varient en fonction de l'intégration. Certaines intégrations nécessitent l'installation et la configuration d'une application ou d'un module complémentaire, et la plupart des intégrations nécessitent la création d'informations d'identification pour accéder au [API REST ExtraHop](#).

Cliquez sur une vignette pour afficher plus d'informations sur l'intégration.

Authentification multifactorielle

L'authentification multifactorielle (MFA) est une amélioration de la sécurité qui vous oblige à fournir deux types d'informations d'identification lorsque vous vous connectez à votre compte. En plus de vos informations d'identification ExtraHop, vous devez fournir des informations d'identification provenant d'une application d'authentification tierce.

Sélectionnez et téléchargez une application d'authentification sur votre équipement et générez des codes sécurisés à six chiffres lorsque vous vous connectez à votre système Reveal (x) 360.

Il existe de nombreuses applications d'authentification parmi lesquelles choisir. Les étapes suivantes sont des directives générales, mais vous devez également consulter la documentation d'aide de l'application que vous sélectionnez.

1. Choisissez un équipement, tel qu'un ordinateur ou un équipement mobile (téléphone ou tablette), sur lequel vous pouvez installer des applications.
2. Téléchargez et installez une application d'authentification sur l'équipement. Voici quelques options populaires :
 - Android et iOS : Google Authenticator, Authy
 - Windows et macOS : 1Password, OTP Manager
 - Extensions Chrome : Authenticator
3. Ouvrez un nouveau navigateur et connectez-vous à votre système ExtraHop Reveal (x) 360.
4. Suivez les instructions pour scanner ou entrez le code qui apparaît sur l'écran de configuration de l'authentification multifactorielle ExtraHop, puis entrez les informations d'identification fournies par votre application d'authentification.

Améliorez les capteurs connectés dans Reveal (x) 360

Les administrateurs peuvent mettre à niveau capteurs connectés à Reveal (x) 360.

Avant de commencer

- Votre compte utilisateur doit disposer de privilèges sur Reveal (x) 360 pour l'administration du système et des accès ou l'administration du système.

Voici quelques considérations concernant la mise à niveau des capteurs :

- Les capteurs doivent être connectés aux services cloud ExtraHop
- Les notifications apparaissent lorsqu'une nouvelle version du firmware est disponible
- Vous pouvez mettre à niveau plusieurs capteurs en même temps

1. Sur la page de présentation, cliquez sur **Paramètres du système**  puis cliquez sur **Capteurs**.

Les capteurs éligibles à la mise à niveau affichent une flèche vers le haut dans Version du capteur champ.

Name	Sensor Model	Status	License	Sensor Version	Date Added
sensor-1	EDA1100V	Online	Valid	1 8.8.0.1362	2022-03-16 10:15:53
sensor-2	EDA1100V	Online	Valid	1 8.8.0.1414	2022-03-11 08:43:58

2. Cochez la case à côté de chaque sonde que vous souhaitez mettre à niveau.
3. Dans le Détails du capteur volet, sélectionnez la version du microprogramme dans le **Micrologiciel disponible** liste déroulante.

La liste déroulante affiche uniquement les versions compatibles avec les capteurs.

Seuls les sélectionnés capteurs pour lesquels une mise à niveau du microprogramme est disponible apparaissent dans Sonde Volet de détails.

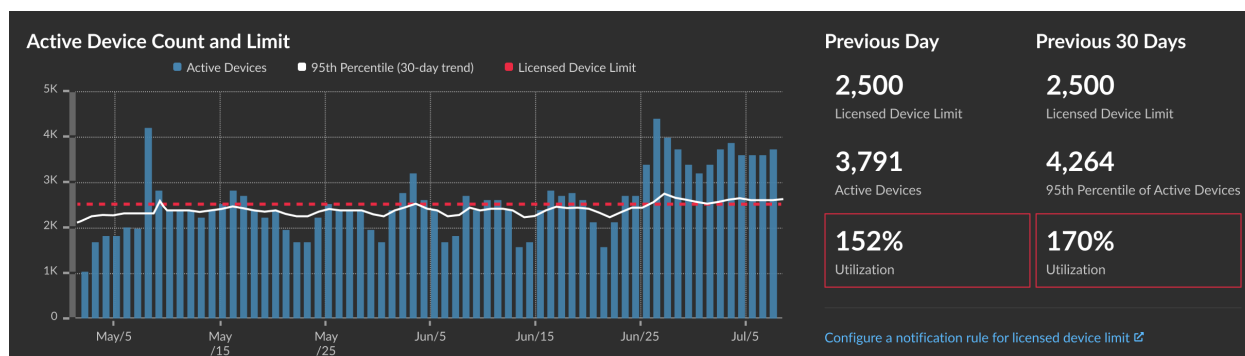
4. Cliquez **Installer le microprogramme**.

Une fois la mise à niveau terminée, Version du capteur le champ est mis à jour avec la nouvelle version du firmware.

Nombre et limite d'équipements actifs

Le graphique du nombre et des limites d'appareils actifs sur la page d'administration principale vous permet de vérifier si le nombre d'appareils actifs a dépassé la limite autorisée. Par exemple, un système ExtraHop avec une bande de 20 000 à 50 000 appareils est autorisé jusqu'à 50 000 appareils.

Cliquez **Paramètres du système** puis cliquez sur **Toute l'administration** pour consulter le graphique.



Le graphique du nombre et de la limite d'appareils actifs affiche les mesures suivantes :

- La ligne rouge pointillée représente **limite d'équipements sous licence**.
- La ligne noire continue représente le 95e percentile des dispositifs actifs observés chaque jour au cours des 30 derniers jours.
- Les barres bleues représentent le nombre maximum d'appareils actifs observés chaque jour au cours des 30 derniers jours.

Cette page affiche également les statistiques suivantes :

- La limite d'équipements homologués pour la veille et les 30 derniers jours.
- Le nombre d'appareils actifs observés la veille.
- Le 95e percentile des dispositifs actifs observés au cours des 30 derniers jours.
- Pourcentage d'utilisation de la limite d'équipement sous licence pour la veille et les 30 derniers jours. L'utilisation est le nombre d'équipements actifs divisé par la limite autorisée.

Tu peux [créer une règle de notification système](#) pour vous avertir si l'utilisation est proche (supérieure à 80 %) ou supérieure (supérieure à 100 %) de la limite d'équipement sous licence. Les pourcentages limites sont personnalisables lorsque vous créez une règle. Si vous constatez que vous approchez ou dépassez régulièrement la limite de votre licence, nous vous recommandons de travailler avec votre équipe commerciale pour passer à la prochaine plage de capacité disponible.

Enregistrer l'ingestion et la capacité

Le tableau d'ingestion et de capacité des enregistrements sur la page d'administration principale vous permet de surveiller les niveaux d'ingestion et de capacité des enregistrements et de confirmer que la limite de capacité est optimale pour votre environnement.

La ligne rouge en pointillés sur le graphique représente la capacité d'enregistrement de votre abonnement, et les barres bleues représentent le montant d'ingestion effectué chaque jour jusqu'aux 60 derniers jours.

Tu peux [créer une règle de notification du système](#) pour vous avertir si l'espace de stockage des enregistrements est proche (supérieur à 80 %) ou supérieur (supérieur à 100 %) de votre capacité quotidienne d'ingestion d'enregistrements.

Si vous constatez que vous dépassez régulièrement la capacité qui vous est allouée, contactez votre représentant commercial ExtraHop.

