

# IBM QRadar Security Intelligence Platform

---

Guide de démarrage rapide

Version 7.4.3

Le présent guide explique comment effectuer une installation classique.

Pour obtenir le Guide de démarrage rapide dans une autre langue, imprimez le PDF correspondant depuis le support d'installation.

## Remarque :

IBM® QRadar 7.4.3 Éléments sous licence - Propriété d'IBM. © Copyright IBM Corp. 2012, 2020. US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

IBM, le logo IBM et ibm.com sont des marques d'International Business Machines Corporation dans de nombreux pays. Les autres noms de produits et de services peuvent être des marques d'IBM ou d'autres sociétés. La liste actualisée de toutes les marques d'IBM est disponible sur la page web "[Copyright and trademark information](http://www.ibm.com/legal/copytrade.shtml)" ([www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml)).

## Pourquoi et quand exécuter cette tâche

Présentation du produit

Les produits IBM QRadar Security Intelligence Platform fournissent une architecture unifiée pour l'intégration de la gestion des événements et des informations de sécurité (SIEM), la gestion des journaux, la détection des anomalies, l'analyse d'incidents et la gestion de la configuration et des vulnérabilités. Le présent Guide de démarrage rapide contient des informations sur l'installation des dispositifs IBM QRadar.

**Important :** Si QRadar est déjà installé sur votre dispositif, respectez les règles suivantes lors de la création du mot de passe root : le mot de passe doit contenir au moins cinq caractères, sans espaces, et peut contenir les caractères suivants : @, #, ^ et \*.

**Important :** Vous pouvez utiliser l'outil de vérification de signature pour valider l'intégrité de vos téléchargements à partir de IBM Fix Central ou de Passport Advantage. Pour plus d'informations, voir [Comment vérifier que les téléchargements à partir de IBM Fix Central sont sécurisés et signés avec un code.](#)

## Procédure

### 1. Accès aux logiciels et à la documentation

Consultez les [notes sur l'édition](#) du composant QRadar que vous souhaitez installer.

Suivez les instructions dans le [document relatif au téléchargement](#) (<http://www.ibm.com/support/pages/node/6435171>) pour télécharger QRadar depuis IBM Passport Advantage.

### 2. Aperçu des panneaux avant et arrière

Passez en revue les informations relatives aux fonctionnalités des panneaux avant et arrière des dispositifs et vérifiez leur connectivité et leur bon fonctionnement.

Pour plus d'informations sur les fonctionnalités des panneaux avant et arrière des dispositifs, voir le document *IBM QRadar Hardware Guide*.

Sur le panneau arrière de chaque type de dispositif, le connecteur série et les connecteurs Ethernet peuvent être gérés à l'aide du module IMM. Pour plus de détails sur le module IMM, voir le manuel *Integrated Management Module User's Guide*.

### 3. Conditions préalables à l'installation

Assurez-vous que les exigences suivantes sont respectées :

- Le matériel requis est installé.
- Un ordinateur portable est connecté au port série à l'arrière du dispositif, ou un clavier et un écran sont connectés.
- Vous êtes connecté en tant qu'utilisateur root.
- Vous disposez d'une clé de licence valide.

**Conseil :** Pour acquérir une clé de licence, envoyez un message à l'adresse [q1pd@us.ibm.com](mailto:q1pd@us.ibm.com). Si vous êtes un client Cloud Pak for Security, vous devez fournir la quantité de systèmes QRadar MVS Event Analytics ou EPS que vous avez achetée. Si vous avez également acheté QRadar Flow Analytics, vous devez également fournir la quantité de systèmes MVS ou FPM.

#### 4. Installation d'un dispositif QRadar

Pour des informations sur les licences QRadar Risk Manager et QRadar Vulnerability Manager, voir [QRadar Risk Manager et QRadar Vulnerability Manager](#).

Pour des informations sur les licences QRadar Incident Forensics, voir [Présentation de l'installation de QRadar Incident Forensics](#).

a. Montez l'image ISO QRadar :

i) Créez le répertoire `/media/cdrom` en entrant la commande suivante :

```
mkdir /media/cdrom
```

ii) Montez l'image ISO de QRadar en tapant a commande suivante :

```
mount -o loop <path_to_the_QRadars_ISO> /media/cdrom
```

b. Pour commencer l'installation, entrez la commande suivante :

```
/media/cdrom/setup
```

- Sélectionnez l'option **Appliance Install** correspondant au type de dispositif.
- Sélectionnez le type de dispositif dans la liste.
- Sélectionnez le type d'installation **normal**.
- Définissez la date et l'heure.
- Sélectionnez le type d'adresse IP.
- Dans l'assistant, entrez un nom de domaine complet dans la zone **Hostname**.
- Dans la zone **IP address**, entrez une adresse IP statique, ou utilisez l'adresse IP affectée par le DHCP.  
  
Pour plus d'informations sur la définition de l'hôte principal ou secondaire IPv6, voir *IBM QRadar High Availability Guide*.
- Si vous ne disposez pas d'un serveur de messagerie, entrez `localhost` dans la zone **Email server name**.
- Créez les mots de passe root et administrateur. Le mot de passe administrateur doit respecter la longueur minimale ainsi que les exigences de complexité imposées.
- Pour effectuer l'installation, suivez les instructions de l'assistant d'installation. La procédure d'installation peut prendre quelques minutes.

#### 5. Application de votre clé de licence

a. Connectez-vous à QRadar en tant qu'administrateur :

```
https://<QRadar_IP_Address>
```

b. Cliquez sur l'onglet **Admin**.

c. Cliquez sur l'icône **Gestion du système et de la licence**.

d. Cliquez sur **Télécharger la licence** et téléchargez votre clé de licence.

e. Sélectionnez la licence et cliquez sur **Allouer un système à la licence**.

f. Sélectionnez une licence dans la liste des licences et cliquez sur **Allouer une licence au système**.

## 6. Initiation

Pour plus d'informations sur la mise en route de vos composants QRadar, consultez les ressources suivantes :

- [Initiation à IBM QRadar SIEM](#)
- [Initiation à IBM QRadar Risk Manager](#)
- [Initiation à IBM QRadar Vulnerability Manager](#)
- [Initiation à IBM QRadar Incident Forensics](#)
- [Initiation à IBM QRadar Network Insights](#)
- [Initiation à IBM QRadar Network Packet Capture](#)
- [Initiation à IBM QRadar Packet Capture](#)

## Que faire ensuite

Informations complémentaires

Pour obtenir la documentation complète du produit, voir IBM QRadar Security Intelligence Platform l'[IBM Knowledge Center](#). Vous pouvez télécharger la documentation au format PDF depuis la page [Téléchargement de la documentation IBM Security QRadar](#).