

Leitfaden für den Schnelleinstieg

Dieser Leitfaden soll Ihnen die Standardinstallation erleichtern.

Versionen in anderen Sprachen: Drucken Sie die entsprechenden PDF-Dateien auf den Installationsmedien, wenn Sie das Dokument 'Leitfaden für den Schnelleinstieg' in anderen Sprachen lesen wollen.

Produktübersicht

IBM® QRadar Security Intelligence Platform-Produkte bieten eine einheitliche Architektur für die Integration des Sicherheitsinformations- und Ereignis-Managements (SIEM), des Protokollmanagements, der Anomalieerkennung, der Ereignis-Forensik und des Konfigurations- und Schwachstellenmanagements. Dieser Leitfaden für den Schnelleinstieg enthält Informationen zur Installation von IBM Security QRadar-Appliances.

Wichtig: Wenn QRadar auf Ihrer Appliance bereits installiert ist, halten Sie sich bei der Erstellung des Rootkennworts an folgende Regeln: Kennwörter müssen mindestens 5 Zeichen lang sein. Sie dürfen keine Leerzeichen enthalten, jedoch die folgenden Sonderzeichen: @, #, ^ und *.

1 Schritt 1: Auf Software und Dokumentation zugreifen



Lesen Sie die Releaseinformationen zu der QRadar-Komponente, die Sie installieren möchten.

Folgen Sie den Anweisungen im Downloaddokument (www.ibm.com/support/docview.wss?uid=swg24042706), um QRadar von IBM Passport Advantage herunterzuladen.

2 Schritt 2: Bedienfeldfunktionen und Funktionen an der Gehäuserückwand kennenlernen

Lesen Sie die Informationen zu den Bedienfeldfunktionen und den Funktionen an der Gehäuserückwand Ihrer Appliances, um eine korrekte Verbindung und Funktion sicherzustellen.

Sie finden weitere Informationen zu den Funktionen an der Gehäusevorder- und Gehäuserückwand für Appliances unter Funktionen an der Gehäusevorder- und Gehäuserückwand.

Der serielle und der Ethernet-Anschluss an der Gehäuserückwand der Appliances kann mit dem Integrated Management Module verwaltet werden. Weitere Informationen zum Integrated Management Module finden Sie im *Benutzerhandbuch zum Integrated Management Module*.

3 Schritt 3: Installationsvoraussetzungen



Stellen Sie sicher, dass folgende Voraussetzungen erfüllt sind:

- Die erforderliche Hardware ist installiert.
- Für QRadar-Appliances: Am seriellen Anschluss an der Rückseite der Appliance ist ein Notebook angeschlossen (oder Tastatur und Bildschirm sind angeschlossen).
- Sie sind als Rootbenutzer angemeldet.
- Der Aktivierungsschlüssel ist verfügbar.

Zur Sicherstellung einer erfolgreichen Installation von QRadar auf Ihrer Appliance muss das Betriebssystem Red Hat Enterprise Linux installiert sein. Außerdem müssen Sie sicherstellen, dass Ihre Appliance die Systemvoraussetzungen für QRadar-Implementierungen erfüllt. Weitere Informationen hierzu finden Sie im *QRadar Hardware Guide*.

4 Schritt 4: QRadar SIEM auf Ihrer Appliance installieren



Für QRadar Risk Manager und QRadar Incident Forensics ist jeweils eine eigene Lizenz erforderlich und beide Produkte müssen auf verschiedenen Appliances installiert sein. QRadar Risk Manager muss als verwalteter Host installiert werden. QRadar Vulnerability Manager kann auf einer All-in-One-Konsole auf demselben System wie die Konsole installiert werden.

1. Wenn Sie eine eigene Appliance verwenden, hängen Sie das QRadar-ISO-Image an:
 - a. Erstellen Sie das Verzeichnis "/media/cdrom" mit folgendem Befehl:

```
mkdir /media/cdrom
```
 - b. Hängen Sie das QRadar-ISO-Image mit folgendem Befehl an:

```
mount -o loop <Pfad zu QRadar-ISO> /media/cdrom
```
 - c. Geben Sie zur Ausführung der Installation folgenden Befehl ein:

```
/media/cdrom/setup
```
2. Wählen Sie als Appliance-Typ **Non-Software Appliance** (Nicht-Software-Appliance) aus.
3. Wählen Sie in der Liste den Appliance-Typ aus oder geben Sie **Strg+K** ein, um einen Aktivierungsschlüssel einzugeben. Dies ist die aus 24 Zeichen und vier Teilen bestehende alphanumerische Zeichenfolge, die Sie von IBM erhalten haben. Der Buchstabe **I** und die Zahl **1** (eins) werden gleich behandelt. Ebenso werden der Buchstabe **O** und die Zahl **0** (null) gleich behandelt.
4. Wählen Sie als Installationstyp **Normal** aus.
5. Richten Sie das Datum und die Uhrzeit ein.
6. Wählen Sie den Typ der IP-Adresse aus.
7. Geben Sie im Assistenten im Feld **Hostname** den vollständig qualifizierten Domännennamen ein.
8. Geben Sie im Feld **IP-Adresse** eine statische IP-Adresse ein oder übernehmen Sie die von DHCP zugewiesene IP-Adresse.
Informationen zur Einrichtung des primären oder sekundären IPv6-Hosts finden Sie im *IBM Security QRadar High Availability Guide*.
9. Wenn Sie keinen E-Mail-Server haben, geben Sie im Feld **E-Mail-Servername** `localhost` ein.
10. Erstellen Sie Root- und Administrator-Kennwörter. Kennwörter müssen mindestens 5 Zeichen lang sein. Sie dürfen keine Leerzeichen enthalten, jedoch die folgenden Sonderzeichen: `@`, `#`, `^` und `*`.
11. Befolgen Sie die Anweisungen im Installationsassistenten, um die Installation abzuschließen. Der Installationsprozess kann mehrere Minuten dauern.

5 Schritt 5: Lizenzschlüssel anwenden



1. Melden Sie sich bei QRadar an:

```
https://IP-Adresse_QRadar
```


Der standardmäßige **Benutzername** lautet `admin`. Das **Kennwort** ist das des Rootbenutzer-Kontos.
2. Klicken Sie auf die Registerkarte **Verwaltung**.
3. Klicken Sie im Navigationsbereich auf **Systemkonfiguration**.
4. Klicken Sie auf das Symbol **System- und Lizenzverwaltung**.
5. Wählen Sie im Listenfeld **Anzeige** die Option **Lizenzen** aus und laden Sie Ihren Lizenzschlüssel hoch.
6. Wählen Sie die freigegebene Lizenz aus und klicken Sie auf **System einer Lizenz zuordnen**.
7. Wählen Sie in der Lizenzliste die Lizenz aus und klicken Sie auf **Lizenz dem System zuordnen**.

6 Schritt 6: Erste Schritte



Weitere Informationen zu den ersten Schritten mit Ihren QRadar-Komponenten finden Sie in folgenden Ressourcen:

- Erste Schritte mit IBM Security QRadar SIEM
- Erste Schritte mit IBM Security QRadar Risk Manager
- Erste Schritte mit IBM Security QRadar Vulnerability Manager
- Erste Schritte mit IBM Security QRadar Incident Forensics
- Erste Schritte mit IBM Security QRadar Packet Capture
- Erste Schritte mit IBM QRadar Network Packet Capture

Weitere Informationen



Sie finden die vollständige Produktdokumentation im IBM Knowledge Center für IBM QRadar Security Intelligence Platform. Laden Sie die Dokumentation im PDF-Format von der Webseite [Accessing IBM Security QRadar documentation](https://www.ibm.com/legal/copytrade.shtml) herunter.