

Guia de Instalação  
IBM Security QRadar Risk Manager  
Versão 7.2.2

## *Guia de Instalação*



**Nota**

Antes de utilizar estas informações e o produto que elas suportam, leia as informações em “Avisos” na página 19.

---

# Índice

<b>Introdução à Instalação do IBM Security QRadar Risk Manager . . . . .</b>	<b>v</b>
<b>Capítulo 1. Prepare-se para instalar o IBM Security QRadar Risk Manager . . . . .</b>	<b>1</b>
Antes de instalar . . . . .	1
Identificar configurações de rede . . . . .	1
Configurar o acesso a portas em firewalls. . . . .	1
Recursos não suportados no QRadar Risk Manager . . . . .	2
Requisitos de Hardware Adicionais. . . . .	2
Requisitos de software adicionais . . . . .	2
Navegadores da web suportdos . . . . .	2
Ativar o modo de documento e modo de navegação no Internet Explorer . . . . .	3
<b>Capítulo 2. Instale os dispositivos IBM Security QRadar Risk Manager . . . . .</b>	<b>5</b>
Preparando seu dispositivo . . . . .	5
Acesse a interface com o usuário do IBM Security QRadar Risk Manager . . . . .	6
Informações de parâmetro de rede para o IPv4 . . . . .	6
Instalando o IBM Security QRadar Risk Manager . . . . .	6
Incluindo o QRadar Risk Manager no QRadar SIEM . . . . .	7
Limpando o cache do navegador da web . . . . .	8
Função de usuário do Risk Manager . . . . .	9
Designando a função de usuário do Risk Manager. . . . .	9
Guia Resolução de Problemas de Riscos . . . . .	10
Removendo um host gerenciado . . . . .	10
Reincluindo o QRadar Risk Manager como um host gerenciado . . . . .	10
<b>Capítulo 3. Reinstale o IBM Security QRadar Risk Manager a partir da partição de recuperação . . . . .</b>	<b>11</b>
Reinstalando o QRadar Risk Manager usando a reinstalação de factory . . . . .	11
<b>Capítulo 4. Altere as configurações de rede. . . . .</b>	<b>13</b>
Removendo um host gerenciado . . . . .	13
Alterando as configurações de rede . . . . .	13
Reincluindo o QRadar Risk Manager como um host gerenciado . . . . .	14
<b>Capítulo 5. Backup e restauração de dados . . . . .</b>	<b>15</b>
Pré-requisitos para backup e restauração de dados . . . . .	15
Fazendo backup de seus dados. . . . .	16
Restaurando dados . . . . .	16
<b>Avisos . . . . .</b>	<b>19</b>
Marcas Comerciais . . . . .	21
Considerações de política de privacidade . . . . .	21
<b>Índice Remissivo . . . . .</b>	<b>23</b>



---

# Introdução à Instalação do IBM Security QRadar Risk Manager

Estas informações se destinam ao uso com o IBM® Security QRadar Risk Manager. O QRadar Risk Manager é um dispositivo usado para monitorar configurações do dispositivo, simular mudanças em seu ambiente de rede e priorizar riscos e vulnerabilidades de sua rede.

Esse guia contém instruções para instalação do QRadar Risk Manager e inclusão do QRadar Risk Manager como um host gerenciado no console IBM Security QRadar SIEM.

Os dispositivos QRadar Risk Manager são pré-instalados com software e um sistema operacional Red Hat Enterprise Linux. Também é possível instalar o software QRadar Risk Manager em seu próprio hardware.

## Público alvo

Esse guia se destina a administradores de rede que são responsáveis pela instalação e configuração de sistemas QRadar Risk Manager em sua rede.

Os administradores precisam de um conhecimento de trabalho de rede e de sistemas Linux.

## Documentação técnica

Para obter informações sobre como acessar a documentação mais técnica, notas técnicas e notas sobre a liberação, consulte Acessando a nota de documentação técnica do IBM Security (<http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861>).

## Contatando o suporte ao cliente

Para obter informações sobre como entrar em contato com o suporte ao cliente, consulte o Suporte e download de nota técnica (<http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861>).

## Declaração de boas práticas de segurança

A segurança do sistema de TI envolve proteger sistemas e informações por meio de prevenção, detecção e resposta para acesso incorreto de dentro e de fora de sua empresa. O acesso incorreto pode resultar em alteração, destruição, desapropriação ou mal uso de informações ou pode resultar em danos ou mal uso dos sistemas, incluindo seu uso em ataques a outros sistemas. Nenhum sistema de TI ou produto deve ser considerado completamente seguro e nenhum único produto, serviço ou medida de segurança pode ser completamente efetivo(a) na prevenção de uso ou acesso impróprio. Os sistemas, produtos e serviços IBM são projetados para fazerem parte de uma abordagem de segurança abrangente, que envolverá, necessariamente, procedimentos operacionais adicionais e poderão requerer outros sistemas, produtos ou serviços para serem mais efetivos. A IBM NÃO GARANTE QUE NENHUM SISTEMA, PRODUTO OU SERVIÇO SEJA IMUNE OU TORNE A SUA EMPRESA IMUNE CONTRA A CONDUTA MALICIOSA OU ILEGAL DE TERCEIROS.



---

# Capítulo 1. Prepare-se para instalar o IBM Security QRadar Risk Manager

É possível instalar um dispositivo IBM Security QRadar Risk Manager como um host gerenciado no console do IBM Security QRadar SIEM. Pode existir somente um QRadar Risk Manager em um console QRadar SIEM.

A partir da versão 7.1 do QRadar Risk Manager, o QRadar SIEM e o QRadar Risk Manager usam o mesmo processo de instalação e ISO para instalação. Por essa razão, é possível usar o editor de implementação no QRadar SIEM para incluir o QRadar Risk Manager em sua implementação. Uma instalação do dispositivo QRadar Risk Manager inclui o software QRadar Risk Manager e um sistema operacional Red Hat Enterprise Linux.

---

## Antes de instalar

Você deve concluir o processo de instalação de um console IBM Security QRadar SIEM antes de instalar o IBM Security QRadar Risk Manager. Como uma melhor prática, instale o QRadar SIEM e o QRadar Risk Manager no mesmo computador de rede.

Para obter informações sobre a instalação do QRadar SIEM, inclusive os requisitos de hardware e software, consulte o *Guia de Instalação do IBM Security QRadar SIEM*.

Como o dispositivo IBM Security QRadar Risk Manager é de 64 bits, certifique-se de fazer download do software correto de instalação para seu sistema operacional.

## Identificar configurações de rede

Deve-se reunir informações sobre suas configurações de rede antes de iniciar o processo de instalação.

Reúna as seguintes informações para suas configurações de rede:

- Nome do host
- endereço IP
- Endereço da máscara de rede
- Máscara de sub-rede
- Endereço de gateway padrão
- Endereço do servidor Sistema de Nomes de Domínio (DNS) principal
- Endereço do servidor DNS secundário (opcional)
- Endereço IP público para redes que usem nome de servidor de email de Conversão de Endereço de Rede (NAT)
- Nome do servidor de e-mail
- Servidor Network Time Protocol (NTP) (Console somente) ou nome do servidor de horário

## Configurar o acesso a portas em firewalls

Os firewalls entre o console IBM Security QRadar SIEM e o IBM Security QRadar Risk Manager devem permitir tráfego em determinadas portas.

Assegure-se de que qualquer firewall localizado entre o console QRadar SIEM e o QRadar Risk Manager permita tráfego nas seguintes portas:

- Porta 443 (HTTPS)
- Porta 22 (SSH)
- Porta 37 UDP (Horário)

## Recursos não suportados no QRadar Risk Manager

É importante estar ciente dos recursos que não são suportados pelo IBM Security QRadar Risk Manager.

Os recursos a seguir não são suportados no QRadar Risk Manager:

- Alta disponibilidade (HA)
- Roteamento Dinâmico para Protocolo de Roteamento de Borda (BGP), Open Shortest Path First (OSPF) ou Protocolo de Informações de Roteamento (RIP)
- IPv6
- Máscaras de rede não contíguas
- Rotas de carga balanceada
- Mapas de referência
- Armazenamento e Encaminhamento

---

## Requisitos de Hardware Adicionais

Hardware adicional é requerido antes de poder instalar o IBM Security QRadar Risk Manager.

Antes de instalar os sistemas IBM QRadar Risk Manager, é necessário acessar os seguintes componentes de hardware:

- monitor e teclado ou um console serial
- Fonte de Alimentação Ininterrupta (UPS)

Sistemas ou dispositivos QRadar Risk Manager que estão executando o software QRadar Risk Manager que armazena dados devem ser equipados com uma Fonte de Alimentação Ininterrupta (UPS). O uso de uma UPS garante que os dados do QRadar Risk Manager, como consoles, processadores de eventos e Coletores QFlow, sejam preservados durante uma falha de energia.

---

## Requisitos de software adicionais

É requerido software adicional antes de poder instalar o IBM Security QRadar Risk Manager.

O software a seguir deve ser instalado no sistema desktop que você usa para acessar a interface com o usuário do QRadar Risk Manager:

- Java™ Runtime Environment
- Adobe Flash, versão 10 ou superior

---

## Navegadores da web suportados

Para os recursos nos produtos IBM Security QRadar funcionarem de forma adequada, você deve usar um navegador da web suportado.



Ao acessar o sistema QRadar, será solicitado que você forneça um nome de usuário e uma senha. O nome de usuário e senha devem ser configurados com antecedência pelo administrador.

A tabela a seguir lista as versões suportadas dos navegadores da web.

*Tabela 1. Navegadores da web suportados para produtos QRadar*

<b>Navegador da web</b>	<b>Versão suportada</b>
Mozilla Firefox	17,0 Extended Support Release 24.0 Extended Support Release
Microsoft Internet Explorer de 32 bits, com o modo de documento e modo de navegação ativados	9.0
Google Chrome	A versão atual a partir da data da liberação dos produtos IBM Security QRadar V7.2.2

## **Ativar o modo de documento e modo de navegação no Internet Explorer**

Se você usar o Microsoft Internet Explorer para acessar os produtos IBM Security QRadar, você deve ativar o modo de navegação e o modo de documento.

### **Procedimento**

1. Em seu navegador da web Internet Explorer, pressione F12 para abrir a janela Ferramentas de Desenvolvedor.
2. Clique em **Modo de Navegador** e selecione a versão do seu navegador da web.
3. Clique em **Modo de Documento**.
  - Para o Internet Explorer V9.0, selecione **Internet Explorer 9**
  - Para o Internet Explorer V8.0, selecione **Internet Explorer 7.0 Standards**



---

## Capítulo 2. Instale os dispositivos IBM Security QRadar Risk Manager

Uma implementação do IBM Security QRadar Risk Manager inclui um IBM Security QRadar SIEM Console e o dispositivo QRadar Risk Manager como um host gerenciado.

A instalação do QRadar Risk Manager envolve as seguintes etapas:

1. Preparando seu dispositivo.
2. Instalando o QRadar Risk Manager.
3. Incluindo o QRadar Risk Manager no QRadar SIEM.

---

### Preparando seu dispositivo

Você deve preparar seu dispositivo antes de instalar um dispositivo IBM Security QRadar Risk Manager.

#### Antes de Iniciar

Deve-se instalar todo o hardware necessário e você precisa de uma chave de ativação. A chave de ativação é uma sequência alfanumérica de 24 dígitos, com quatro partes, que você recebe da IBM. É possível localizar a chave de ativação:

- Impresso em uma etiqueta e colocado fisicamente em seu dispositivo.
- Incluído com o código da embalagem; todos os dispositivos são listados juntamente com suas chaves associadas.

Para evitar erros de digitação, a letra I e o número 1 (um) são tratados da mesma forma, assim como a letra O e o número 0 (zero).

Se você não tiver uma chave de ativação para o dispositivo QRadar Risk Manager, entre em contato com o suporte ao cliente (<http://www.ibm.com/support>).

Para obter informações sobre seu dispositivo, consulte o *Guia de Instalação do Hardware IBM Security QRadar*.

#### Procedimento

1. Escolha uma das opções a seguir:
  - Conecte um notebook à porta serial na parte traseira do dispositivo.  
Se você usar um notebook para conectar ao sistema, deverá usar um programa de terminal, como HyperTerminal, para conectar ao sistema. Certifique-se de configurar **Conectar Usando** à porta COM adequada do conector serial e **Bits por segundo** para 9600. Deve-se também configurar **Bits de Parada** (1), **Bits de Dados** (8) e **Paridade** (Nenhuma).
  - Conecte um teclado e monitor a suas respectivas portas.
2. Ligue o sistema e efetue login. O nome do usuário, que distingue maiúsculas e minúsculas, é raiz.
3. Pressione Enter.
4. Leia as informações na janela. Pressione a Barra de Espaço para avançar cada janela até atingir o fim do documento.

5. Digite yes para aceitar o acordo e, em seguida, pressione Enter.
6. Digite sua chave de ativação e pressione Enter.

---

## Acesse a interface com o usuário do IBM Security QRadar Risk Manager

O IBM Security QRadar Risk Manager usa informações de login padrão para a URL, nome de usuário e senha.

Acesse o IBM Security QRadar Risk Manager por meio do console QRadar SIEM. Use as informações da tabela a seguir quando efetuar login no console IBM Security QRadar SIEM.

*Tabela 2. Informações de login padrão para o QRadar Risk Manager*

Informações de login	Padrão
URL	https://<IP address>, em que <IP address> é o endereço IP do console QRadar SIEM.
Nome de usuário	admin
Senha	A senha que é designada para o QRadar Risk Manager durante o processo de instalação.
Chave de licença	Uma chave de licença padrão fornece acesso ao sistema por 5 semanas.

---

## Informações de parâmetro de rede para o IPv4

Informações de rede para configurações de rede do Protocolo da Internet versão 4 (IPv4) são requeridas ao instalar o IBM Security QRadar Risk Manager ou quando você alterar as configurações de rede.

Informações de rede são requeridas ao instalar ou reinstalar o IBM Security QRadar Risk Manager ou quando você precisar alterar configurações de rede.

A configuração de rede IP Pública é opcional. Esse endereço IP secundário é usado para acessar o servidor, geralmente de uma rede diferente ou da Internet e é gerenciado por seu administrador de rede. O endereço IP Público geralmente é configurado usando os serviços de Conversão de Endereço de Rede (NAT) nas configurações de rede ou do firewall em sua rede. O NAT converte um endereço IP em uma rede para um endereço IP diferente em outra rede.

---

## Instalando o IBM Security QRadar Risk Manager

É possível instalar o IBM Security QRadar Risk Manager após preparar seu dispositivo.

### Antes de Iniciar

Você deve concluir as etapas de preparação antes de instalar o QRadar Risk Manager.

### Procedimento

1. Selecione normal para o tipo de configuração. Selecione **Avançar** e pressione Enter.

2. Selecione o continente ou área do fuso horário. Selecione **Avançar** e pressione Enter.
3. Selecione a região do fuso horário. Selecione **Avançar** e pressione Enter.
4. Selecione uma versão do protocolo da Internet. Selecione **Avançar** e pressione Enter.
5. Selecione a interface que você deseja especificar como a interface de gerenciamento. Selecione **Avançar** e pressione Enter.
6. Digite seu nome de host, endereço IP, máscara de rede, gateway, DNS primário, DNS secundário, IP público e servidor de email. Para obter informações do parâmetro de rede, consulte “Informações de parâmetro de rede para o IPv4” na página 6.
7. Selecione **Avançar** e pressione Enter.
8. Digite uma senha para configurar a senha raiz do QRadar Risk Manager.
9. Selecione **Avançar** e pressione Enter.
10. Redigite sua nova senha para confirmar. Selecione **Concluir** e pressione Enter. Esse processo geralmente leva vários minutos.

## O que Fazer Depois

Use o editor de implementação para incluir o QRadar Risk Manager como um host gerenciado em seu console QRadar SIEM.

---

## Incluindo o QRadar Risk Manager no QRadar SIEM

Você deve incluir o IBM Security QRadar Risk Manager como um host gerenciado no IBM Security QRadar SIEM.

### Antes de Iniciar

Se desejar ativar a compactação, a versão mínima para cada host gerenciado deve ser QRadar SIEM 7.1 ou QRadar Risk Manager 7.1.

Para incluir um host gerenciado não NATed em sua implementação quando o Console for NATed, deve-se alterar o console QRadar SIEM para um host NATed. Deve-se alterar o console antes de incluir o host gerenciado em sua implementação. Para obter mais informações, consulte o *Guia de Administração do IBM Security QRadar SIEM*.

### Procedimento

1. Abra seu navegador da web.
2. Digite a URL, `https://<Endereço IP>`, em que o <Endereço IP> é o endereço IP do console QRadar SIEM.
3. Digite seu nome de usuário e senha.
4. Na guia **Admin**, clique em **Editor de Implementação**.
5. No menu, selecione **Ações** e, em seguida, selecione **Incluir um Host Gerenciado**.
6. Clique em **Avançar**.
7. Inserir valores para o parâmetros a seguir:

Opção	Descrição
Insira o IP do servidor ou dispositivo para incluir	O endereço IP do QRadar Risk Manager.

Opção	Descrição
Insira a senha raiz do host	A senha raiz para o host.
Confirme a senha raiz do host	Confirmação para sua senha.
O host é NATed	Para ativar NAT para um host gerenciado, a rede NATed deve estar usando tradução estática NAT. Para obter informações adicionais, consulte o Guia de Administração do <i>IBM Security QRadar SIEM</i> .
Ativar Criptografia	Cria um túnel de criptografia SSH para o host. Para ativar a criptografia entre dois hosts gerenciados, cada host gerenciado deve estar executando o QRadar SIEM 7.1 ou QRadar Risk Manager 7.1.
Ativar Compactação	Ativa a compactação de dados entre dois hosts gerenciados.

8. Escolha uma das opções a seguir:

- Se você tiver marcado a caixa de seleção **Host é NATed**, deverá inserir valores para os parâmetros NAT.

Opção	Descrição
Insira o IP público do servidor ou dispositivo a incluir	O endereço IP público do host gerenciado. O host gerenciado usa esse endereço IP para se comunicar com outros hosts gerenciados em diferentes redes que usam NAT.
Selecione rede NATed	A rede que você deseja que este host gerenciado use.  Se o host gerenciado estiver na mesma sub-rede que o console QRadar SIEM, selecione o console da rede NATed.  Se o host gerenciado não estiver na mesma sub-rede que o console QRadar SIEM, selecione o host gerenciado da rede NATed.

- Se você não tiver marcado a caixa de seleção **O Host é NATed**, clique em **Avançar**.

9. Clique em **Concluir**. Este processo pode levar vários minutos para ser concluído. Se a sua implementação incluir mudanças, você deverá implementar todas as mudanças.

10. Clique em **Implementar**.

## O que Fazer Depois

Limpe o cache do navegador da web e, em seguida, efetue login no QRadar SIEM. A guia **Riscos** agora está disponível.

---

## Limpendo o cache do navegador da web

Você deve limpar o cache do navegador da web antes de poder acessar a guia **Riscos** no QRadar SIEM.

## Antes de Iniciar

Assegure-se de que somente um navegador da web esteja aberto. Se você tiver vários navegadores abertos, o cache poderá falhar na limpeza adequada.

Se você estiver usando um navegador da web Mozilla Firefox, você deverá limpar o cache de seu navegador da web Microsoft Internet Explorer também.

## Procedimento

1. Abra seu navegador da web.
2. Limpe o cache do navegador da web. Para obter instruções, consulte a documentação do navegador da web.

---

## Função de usuário do Risk Manager

Deve-se designar a função de usuário do Risk Manager para usuários que necessitem de acesso à guia **Riscos**.

Uma conta de usuário define a senha padrão e o endereço de email para um usuário. É necessário designar uma função de usuário e perfil de segurança para cada nova conta de usuário.

Antes de poder permitir acesso à funcionalidade IBM Security QRadar Risk Manager para outros usuários de sua organização, deve-se designar as permissões adequadas de função de usuário. Por padrão, o QRadar SIEM fornece uma função administrativa padrão, que fornece acesso a todas as áreas do QRadar Risk Manager.

Para obter informações sobre a criação e gerenciamento de funções do usuário, consulte o *Guia de Administração do IBM Security QRadar SIEM*.

## Designando a função de usuário do Risk Manager

É possível designar a função de usuário do Risk Manager para usuários que precisem de acesso à guia **Risco**.

## Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do Sistema**.
3. Na área de janela **Gerenciamento do Usuário**, clique no ícone **Funções do Usuário**.
4. Clique no ícone **Editar** ao lado da função do usuário que você deseja editar.
5. Marque a caixa de seleção **Risk Manager**.
6. Clique em **Avançar**. Se você incluir Risk Manager na função de um usuário que tenha a permissão de Atividade de Log, você deverá, então, definir as origens de log que a função do usuário pode acessar. É possível incluir um grupo de origem de log inteiro clicando no ícone **Incluir** na área de janela **Grupo de Origem de Log**. É possível selecionar várias origens de log segurando a tecla Control e selecionando cada origem de log que você deseja incluir.
7. Clique em **Retornar**.
8. No menu da guia **Administração**, clique em **Implementar Mudanças**.

---

## Guia Resolução de Problemas de Riscos

É possível resolver problemas se a guia **Riscos** não for exibida adequadamente ou estiver inacessível.

Quando a guia Riscos não for exibida adequadamente ou estiver inacessível, remova e reinclua o IBM Security QRadar Risk Manager como um host gerenciado.

### Removendo um host gerenciado

É possível remover o host gerenciado IBM Security QRadar Risk Manager do IBM Security QRadar SIEM para alterar as configurações de rede ou se houver um problema com a guia **Riscos**.

#### Procedimento

1. Abra seu navegador da web.
2. Digite a URL `https://<IP Address>`, em que <IP Address> é o endereço IP do console QRadar SIEM.
3. Digite seu nome de usuário e senha.  
Para obter informações de login padrão, consulte Tabela 2 na página 6.
4. Na guia **Admin**, clique em **Editor de Implementação**.
5. Clique na guia **Visualização do sistema**.
6. Clique com o botão direito do mouse no host gerenciado que deseja excluir e selecione **Excluir**. Repita para cada host gerenciado que não seja do Console até que todos os hosts sejam excluídos.
7. Clique em **Salvar**.
8. Feche o editor de implementação.
9. Na guia **Admin**, clique em **Implementar Mudanças**.

### Reincluindo o QRadar Risk Manager como um host gerenciado

É possível reincluir o QRadar Risk Manager como um host gerenciado após ele ser removido.

#### Procedimento

1. Abra seu navegador da web.
2. Digite a URL `https://<IP Address>`, em que <IP Address> é o endereço IP do console QRadar SIEM.
3. Digite seu nome de usuário e senha.  
Para obter informações de login padrão, consulte Tabela 2 na página 6.
4. Na guia **Admin**, clique em **Editor de Implementação**.
5. Clique na guia **Visualização do sistema**.
6. No menu, selecione **Ações > Incluir um host gerenciado**.
7. Clique em **Avançar**.
8. Inserir valores na janela Incluir novo host gerenciado.
9. Clique em **Avançar**.
10. Clique em **Concluir**. O processo de inclusão do QRadar Risk Manager pode levar vários minutos para ser concluído.
11. Feche o editor de implementação.
12. Na guia **Admin**, clique em **Implementar Mudanças**.



---

## Capítulo 3. Reinstale o IBM Security QRadar Risk Manager a partir da partição de recuperação

Ao reinstalar o IBM Security QRadar Risk Manager do IBM Security QRadar SIEM ISO na partição de recuperação, seu sistema será restaurado de volta para a configuração padrão de fábrica. Isso significa que seus arquivos de dados e de configuração atuais são sobrescritos.

Essas informações se aplicam às novas instalações ou upgrades do QRadar Risk Manager das novas instalações do QRadar Risk Manager nos dispositivos QRadar Risk Manager. Quando você instala o QRadar Risk Manager, o instalador (QRadar SIEM ISO) é copiado para a partição de recuperação. A partir dessa partição, é possível reinstalar o QRadar Risk Manager, que restaura o QRadar Risk Manager para padrões de fábrica.

**Nota:** Se você fizer upgrade de seu software após instalar o QRadar Risk Manager, o arquivo ISO será substituído pela versão mais nova.

Quando você reinicializar o dispositivo QRadar Risk Manager, será apresentada uma opção de reinstalar o software. Como o QRadar SIEM e o QRadar Risk Manager usam o mesmo arquivo de instalação ISO, o nome do QRadar SIEM ISO é exibido.

Se você não responder ao prompt após 5 segundos, o sistema reinicializará normalmente, o que mantém seus arquivos de dados e de configuração. Se você escolher reinstalar o QRadar SIEM ISO, uma mensagem de aviso será exibida e você deverá confirmar que deseja reinstalar o software. Após a confirmação, o instalador é executado e é possível seguir os prompts no processo de instalação.

Após uma falha no disco rígido, não é possível reinstalar a partir da partição de recuperação, porque não está mais disponível. Se você experimentar uma falha de disco rígido, entre em contato com o suporte ao cliente para obter assistência.

---

### Reinstalando o QRadar Risk Manager usando a reinstalação de factory

É possível reinicializar e reinstalar o dispositivo QRadar Risk Manager usando a opção de reinstalação de factory.

#### Antes de Iniciar

Assegure-se de ter sua chave de ativação, que é uma sequência alfanumérica de 24 dígitos e quatro partes, que você recebe da IBM. É possível localizar a chave:

- Impresso em uma etiqueta e colocado fisicamente em seu dispositivo.
- Incluído com o código da embalagem; os dispositivos são listados juntamente com suas chaves associadas.

Para evitar erros de digitação, a letra I e o número 1 (um) são tratados da mesma forma, assim como a letra O e o número 0 (zero).

Se você não tiver uma chave de ativação para o dispositivo QRadar Risk Manager, entre em contato com o suporte ao cliente (<http://www.ibm.com/support>).

As chaves de ativação de software não requerem números de série.

## Procedimento

1. Reinicialize o dispositivo QRadar Risk Manager.
2. Selecione **reinstalação de factory**.
3. Digite **comprimir** para continuar. O disco rígido é particionado e reformatado, o SO é instalado e, em seguida, o QRadar Risk Manager é reinstalado. Você deve aguardar a conclusão do processo de compressão. Esse processo pode levar vários minutos, dependendo de seu sistema.
4. Digite **SETUP**.
5. Efetue login no QRadar Risk Manager como usuário raiz.
6. Leia as informações na janela. Pressione a Barra de Espaço para avançar cada janela até atingir o fim do documento. Digite **yes** para aceitar o acordo e, em seguida, pressione **Enter**.
7. Digite sua chave de ativação e pressione **Enter**.
8. Selecione **normal** para o tipo de configuração. Selecione **Avançar** e pressione **Enter**.
9. Selecione o continente ou área do fuso horário. Selecione **Avançar** e pressione **Enter**.
10. Selecione a região do fuso horário. Selecione **Avançar** e pressione **Enter**.
11. Selecione uma versão do protocolo da Internet. Selecione **Avançar** e pressione **Enter**.
12. Selecione a interface que você deseja especificar como a interface de gerenciamento. Selecione **Avançar** e pressione **Enter**.
13. Insira as informações para o nome do host, endereço IP, máscara de rede, gateway, DNS primário, DNS secundário, IP público e servidor de email. Para obter informações de rede, consulte “Informações de parâmetro de rede para o IPv4” na página 6.
14. Digite uma senha para configurar a senha raiz do QRadar Risk Manager.
15. Selecione **Avançar** e pressione **Enter**.
16. Redigite sua nova senha para confirmar. Selecione **Concluir** e pressione **Enter**. Esse processo geralmente leva vários minutos.
17. Pressione **Enter** para selecionar **OK**.
18. Pressione **Enter** para selecionar **OK**.

## O que Fazer Depois

Use o editor de implementação para incluir o QRadar Risk Manager como um host gerenciado em seu console QRadar SIEM.

---

## Capítulo 4. Altere as configurações de rede

É possível alterar as configurações de rede de um dispositivo IBM Security QRadar Risk Manager que esteja anexado a um Console IBM Security QRadar SIEM.

Se você precisar alterar as configurações de rede, você deverá, em seguida, concluir estas tarefas na seguinte ordem:

1. Remova o QRadar Risk Manager como um host gerenciado.
2. Altere as configurações de rede.
3. Reinclua o QRadar Risk Manager como um host gerenciado.

---

### Removendo um host gerenciado

É possível remover o host gerenciado IBM Security QRadar Risk Manager do IBM Security QRadar SIEM para alterar as configurações de rede ou se houver um problema com a guia **Riscos**.

#### Procedimento

1. Abra seu navegador da web.
2. Digite a URL `https://<IP Address>`, em que <IP Address> é o endereço IP do console QRadar SIEM.
3. Digite seu nome de usuário e senha.  
Para obter informações de login padrão, consulte Tabela 2 na página 6.
4. Na guia **Admin**, clique em **Editor de Implementação**.
5. Clique na guia **Visualização do sistema**.
6. Clique com o botão direito do mouse no host gerenciado que deseja excluir e selecione **Excluir**. Repita para cada host gerenciado que não seja do Console até que todos os hosts sejam excluídos.
7. Clique em **Salvar**.
8. Feche o editor de implementação.
9. Na guia **Admin**, clique em **Implementar Mudanças**.

---

### Alterando as configurações de rede

É possível alterar as configurações de rede de um dispositivo IBM Security QRadar Risk Manager que esteja anexado a um Console IBM Security QRadar SIEM.

#### Antes de Iniciar

Deve-se remover o host gerenciado do QRadar Risk Manager do QRadar SIEM antes de alterar as configurações de rede.

#### Procedimento

1. Usando SSH, efetue login no QRadar Risk Manager como usuário raiz.
2. Digite o comando, `qchange_netsetup`.
3. Selecione uma versão do protocolo da Internet. Selecione **Avançar** e pressione Enter. Dependendo de sua configuração de hardware, a janela exibe até um máximo de quatro interfaces. Cada interface com um link físico é denotada com um símbolo de mais (+).

4. Selecione a interface que você deseja especificar como a interface de gerenciamento. Selecione **Avançar** e pressione Enter.
5. Insira as informações para o nome do host, endereço IP, máscara de rede, gateway, DNS primário, DNS secundário, IP público e servidor de email. Para obter informações de rede, consulte “Informações de parâmetro de rede para o IPv4” na página 6.
6. Digite uma senha para configurar a senha raiz do QRadar Risk Manager.
7. Selecione **Avançar** e pressione Enter.
8. Redigite sua nova senha para confirmar. Selecione **Concluir** e pressione Enter. Esse processo geralmente leva vários minutos.

---

## Reincluindo o QRadar Risk Manager como um host gerenciado

É possível reincluir o QRadar Risk Manager como um host gerenciado após ele ser removido.

### Procedimento

1. Abra seu navegador da web.
2. Digite a URL `https://<IP Address>`, em que <IP Address> é o endereço IP do console QRadar SIEM.
3. Digite seu nome de usuário e senha.  
Para obter informações de login padrão, consulte Tabela 2 na página 6.
4. Na guia **Admin**, clique em **Editor de Implementação**.
5. Clique na guia **Visualização do sistema**.
6. No menu, selecione **Ações > Incluir um host gerenciado**.
7. Clique em **Avançar**.
8. Inserir valores na janela Incluir novo host gerenciado.
9. Clique em **Avançar**.
10. Clique em **Concluir**. O processo de inclusão do QRadar Risk Manager pode levar vários minutos para ser concluído.
11. Feche o editor de implementação.
12. Na guia **Admin**, clique em **Implementar Mudanças**.

---

## Capítulo 5. Backup e restauração de dados

É possível usar um script da interface com a linha de comandos (CLI) para fazer backup de dados armazenados nos hosts gerenciados pelo IBM Security QRadar SIEM.

É possível usar o script CLI para restaurar o IBM Security QRadar Risk Manager após uma falha de dados ou falha de hardware no dispositivo.

Um script de backup é incluído no QRadar Risk Manager, que pode ser programado usando crontab. O script cria automaticamente um archive diário dos dados do QRadar Risk Manager às 3h da manhã. Por padrão, o QRadar Risk Manager mantém os cinco últimos backups. Se você tiver rede ou armazenamento anexado, você deverá criar uma tarefa cron para copiar os archives de fundo do QRadar Risk Manager de para um local de armazenamento de rede.

O archive de backup inclui os seguintes dados:

- Configurações do dispositivo QRadar Risk Manager
- Dados de conexão
- Dados de topologia
- Perguntas do Monitor de Política
- Tabelas do banco de dados do QRadar Risk Manager

Para obter informações sobre migração do QRadar Risk Manager Maintenance Liberação 5 para esta liberação atual, consulte o *Guia de Migração do IBM Security QRadar Risk Manager*.

---

### Pré-requisitos para backup e restauração de dados

Deve-se entender como ocorre o backup dos dados, como são armazenados e arquivados antes de poder fazer backup e restaurar seus dados.

#### Local de backup de dados

O backup de dados ocorre no diretório local `/store/qrm_backups`. Seu sistema pode incluir uma montagem `/store/backup` de um SAN externo ou serviço NAS. Os serviços externos fornecem retenção de dados offline de longo prazo. O armazenamento de longo prazo pode ser requerido por regulamentos de conformidade, como padrões Payment Card Industry (PCI).

#### Versão do dispositivo

A versão do dispositivo que criou o backup no archive está armazenada. Um backup somente pode ser restaurado em um dispositivo QRadar Risk Manager se for da mesma versão.

#### Frequência de backup de dados e informações de archive

Backups diários de dados são criados às 3h. Somente os últimos cinco arquivos de backup são armazenados. Um archive de backup é criado se houver espaço livre suficiente no QRadar Risk Manager.

## Formato dos arquivos de backup

Use o seguinte formato para salvar arquivos de backup: backup-<target date>-<timestamp>.tgz

Em que:

<data prevista> é a data em que o arquivo de backup foi criado.

O formato da data de destino é <dia>\_<mês>\_<ano>. <registro de data e hora> é o horário em que o arquivo de backup foi criado. O formato do registro de data e hora é <hora>\_<minuto>\_<segundo>.

---

## Fazendo backup de seus dados

O backup automático ocorre diariamente, às 3h da manhã, ou é possível iniciar o processo de backup manualmente.

### Procedimento

1. Usando SSH, efetue login no console QRadar SIEM como usuário raiz.
2. Usando SSH no console QRadar SIEM, efetue login no QRadar Risk Manager como usuário raiz.
3. Inicie um backup do QRadar Risk Manager digitando `/opt/qradar/bin/dbmaint/risk_manager_backup.sh`

### Resultados

O script que é usado para iniciar o processo de backup pode levar vários minutos para iniciar.

Após o script concluir o processo de backup, é exibida a mensagem a seguir:

```
Ter 11 de set 10:14:41 EDT 2012
- Backup do Risk Manager concluído,
wrote /store/qrm_backups/backup-2012-09-11-10-14-39.tgz
```

---

## Restaurando dados

É possível usar um script de restauração para restaurar dados a partir de um backup do QRadar Risk Manager.

### Antes de Iniciar

O dispositivo QRadar Risk Manager e o archive de backup devem ser da mesma versão do QRadar Risk Manager. Se o script detectar uma diferença de versão entre o archive e o host gerenciado do QRadar Risk Manager, será exibido um erro.

### Sobre Esta Tarefa

Use o script de restauração para especificar o archive que você está restaurando para o QRadar Risk Manager. Esse processo requer que você pare os serviços no QRadar Risk Manager. Parar os serviços desconecta todos os usuários do QRadar Risk Manager e para vários processos.

A tabela a seguir descreve os parâmetros que é possível usar para restaurar um archive de backup.

Tabela 3. Os parâmetros usados para restaurar um archive de backup para o QRadar Risk Manager

Opção	Descrição
<b>-f</b>	Sobrescreve todos os dados existentes do QRadar Risk Manager em seu sistema com os dados do arquivo de restauração. A seleção desse parâmetro permite que o script sobrescreva quaisquer configurações existentes do dispositivo no Gerenciamento de Origem de Configuração com as configurações do dispositivo do arquivo de backup.
<b>-w</b>	Não exclua diretórios antes de restaurar os dados do QRadar Risk Manager.
<b>-h</b>	A ajuda para o script de restauração.

### Procedimento

1. Usando SSH, efetue login no console QRadar SIEM como usuário raiz.
2. Usando SSH no console QRadar SIEM, efetue login no QRadar Risk Manager como usuário raiz.
3. Pare o contexto do host digitando `service hostcontext stop`.
4. Digite o seguinte comando para restaurar um archive de backup para o QRadar Risk Manager: `/opt/qradar/bin/risk_manager_restore.sh -r /store/qrm_backups/<backup>`. Em que <backup> é o archive QRadar Risk Manager que você deseja restaurar.  
Por exemplo, `backup-2012-09-11-10-14-39.tgz`.
5. Inicie o contexto do host digitando `service hostcontext start`.





---

## Avisos

Estas informações foram desenvolvidas para produtos e serviços oferecidos nos Estados Unidos.

É possível que a IBM não ofereça os produtos, serviços ou recursos discutidos nesta documentação em outros países. Consulte seu representante IBM local para obter informações sobre os produtos e serviços disponíveis atualmente em sua área. Qualquer referência a produtos, programas ou serviços IBM não significa que apenas produtos, programas ou serviços IBM possam ser utilizados. Qualquer produto, programa ou serviço funcionalmente equivalente, que não infrinja nenhum direito de propriedade intelectual da IBM poderá ser utilizado em substituição a este produto, programa ou serviço. Entretanto, a avaliação e verificação da operação de qualquer produto, programa ou serviço não IBM são de responsabilidade do Cliente.

A IBM pode ter patentes ou solicitações de patentes pendentes relativas a assuntos tratados nesta publicação. O fornecimento desta publicação não garante ao Cliente nenhum direito sobre tais patentes. Pedidos de licença devem ser enviados, por escrito, para:

Gerência de Relações Comerciais e Industriais da IBM Brasil  
Av. Pasteur, 138-146  
Botafogo  
Rio de Janeiro, RJ  
CEP 22290-240

Para consultas sobre licenças a respeito de informações do conjunto de caracteres de byte duplo (DBCS), entre em contato com o Departamento de Propriedade Intelectual da IBM em seu país ou envie consultas, por escrito, para:

Intellectual Property Licensing  
Legal and Intellectual Property Law  
IBM Japan Ltd.  
19-21, Nihonbashi-Hakozakicho, Chuo-ku  
Tokyo 103-8510, Japan

**O parágrafo a seguir não se aplica ao Reino Unido ou a qualquer país em que tais disposições não estejam de acordo com a legislação local:**

A INTERNATIONAL BUSINESS MACHINES CORPORATION FORNECE ESTA PUBLICAÇÃO "NO ESTADO EM QUE SE ENCONTRA" SEM GARANTIA DE NENHUM TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS A ELAS NÃO SE LIMITANDO, AS GARANTIAS IMPLÍCITAS DE NÃO INFRAÇÃO, COMERCIALIZAÇÃO OU ADEQUAÇÃO A UM DETERMINADO PROPÓSITO. Alguns estados não permitem a exclusão de garantias expressas ou implícitas em certas transações; portanto, esta disposição pode não se aplicar ao Cliente.

Estas informações podem incluir imprecisões técnicas ou erros tipográficos. São feitas alterações periódicas nas informações aqui contidas; tais alterações serão incorporadas em futuras edições desta publicação. A IBM pode, a qualquer momento, aperfeiçoar e/ou alterar os produtos e/ou programas descritos nesta publicação, sem aviso prévio.

Quaisquer referências nestas informações a websites não IBM são fornecidas apenas por conveniência e não representam de forma alguma um endosso a estes websites. Os materiais contidos nesses websites não fazem parte dos materiais desse produto IBM e a utilização desses websites é de inteira responsabilidade do Cliente.

A IBM pode utilizar ou distribuir as informações fornecidas da forma que julgar apropriada sem incorrer em qualquer obrigação para com o Cliente.

Os licenciados deste programa que desejarem obter informações sobre ele para o propósito de ativação: (i) a troca de informações entre programas criados independentemente e outros programas (incluindo este) e (ii) o uso mútuo das informações que foram trocadas, devem entrar em contato com:

Gerência de Relações Comerciais e Industriais da IBM Brasil  
Av. Pasteur, 138-14  
Botafogo  
Rio de Janeiro, RJ  
CEP 22290-240

Tais informações podem estar disponíveis, sujeitas a termos e condições apropriados, incluindo em alguns casos o pagamento de uma taxa.

O programa licenciado descrito nesta publicação e todo o material licenciado disponível são fornecidos pela IBM sob os termos do IBM Customer Agreement, do Contrato Internacional de Licença do Programa IBM ou de qualquer outro contrato equivalente.

Todos os dados sobre desempenho aqui contidos foram determinados em um ambiente controlado. Portanto, os resultados obtidos em outros ambientes operacionais poderão variar significativamente. Algumas medidas podem ter sido tomadas em sistemas em nível de desenvolvimento e não há garantia de que estas medidas serão as mesmas em sistemas disponíveis em geral. Além disso, algumas medidas podem ter sido estimadas por meio de extrapolação. Os resultados reais podem variar. Os usuários deste documento devem verificar os dados aplicáveis para seu ambiente específico.

As informações relativas a produtos não IBM foram obtidas junto aos fornecedores dos respectivos produtos, de seus anúncios publicados ou de outras fontes disponíveis publicamente. A IBM não testou estes produtos e não pode confirmar a precisão de seu desempenho, compatibilidade nem qualquer outra reivindicação relacionada a produtos não IBM. Dúvidas sobre os recursos de produtos não IBM devem ser encaminhadas diretamente a seus fornecedores.

Todas as instruções relativas às direções ou intenções futuras da IBM estão sujeitas a mudanças ou retirada sem aviso prévio, e apenas representam metas e objetivos.

Todos os preços IBM mostrados são preços de varejo sugeridos pela IBM, são atuais e estão sujeitos a mudança sem aviso. Os preços dos revendedores podem variar.

Essas informações contêm exemplos de dados e relatórios usados em operações diárias de negócios. Para ilustrá-los da forma mais completa possível, os exemplos podem incluir nomes de indivíduos, empresas, marcas e produtos. Todos estes nomes são fictícios e qualquer semelhança com nomes e endereços utilizados por uma empresa real é mera coincidência.

Se estas informações estiverem sendo exibidas em formato eletrônico, as fotografias e ilustrações coloridas podem não aparecer.

---

## Marcas Comerciais

IBM, o logotipo IBM e [ibm.com](http://ibm.com) são marcas ou marcas comerciais da International Business Machines Corporation nos Estados Unidos e/ou em outros países. Se estes e outros termos de marca registrada da IBM estiverem marcados em sua primeira ocorrência nestas informações com um símbolo de marca registrada (® ou ™), esses símbolos indicarão marcas registradas ou de direito consuetudinário dos Estados Unidos, de propriedade da IBM no momento em que estas informações foram publicadas. Estas marcas comerciais também podem ser marcas registradas ou marcas comerciais de direito consuetudinário em outros países. Uma lista atual de marcas registradas da IBM está disponível na web em Informações de copyright e de marca registrada ([www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml)).

Adobe e Acrobat e todas as marcas comerciais baseadas em Adobe são marcas registradas ou marcas comerciais da Adobe Systems Incorporated nos Estados Unidos e/ou em outros países.

Java e todas as marcas registradas e logotipos baseados em Java são marcas ou marcas registradas da Sun Microsystems, Inc. nos Estados Unidos e/ou em outros



Linux é uma marca registrada de Linus Torvalds nos Estados Unidos e/ou em outros países.

Microsoft, Windows, Windows NT e o logotipo Windows são marcas comerciais da Microsoft Corporation nos Estados Unidos e/ou em outros países.

Outros nomes de empresas, produtos e serviços podem ser marcas comerciais ou marcas de serviço de terceiros.

---

## Considerações de política de privacidade

Os produtos de Software IBM, incluindo soluções de software as a service, (“Ofertas de Software”) podem usar cookies ou outras tecnologias para coletar informações sobre o uso do produto, para ajudar a melhorar a experiência do usuário final, ajustar as interações com o usuário final ou para outras finalidades. Em muitos casos, nenhuma informação de identificação pessoal é coletada pelas Ofertas de Software. Algumas de nossas Ofertas de Software podem ajudar a permitir que você colete informações pessoalmente identificáveis. Se esta Oferta de Software usar cookies para coletar as informações pessoalmente identificáveis, as informações específicas sobre o uso de cookies desta oferta serão apresentadas a seguir.

Dependendo das configurações implementadas, essa Oferta de Software poderá usar cookies de sessão que coletam o ID da sessão de cada usuário para fins de gerenciamento de sessões e autenticação. Estes cookies podem ser desativados, mas desativá-los também eliminará a funcionalidade que eles ativam.

Se as configurações implementadas para esta Oferta de Software fornecerem a capacidade de coletar, como cliente, informações pessoalmente identificáveis dos usuários finais por meio de cookies e outras tecnologias, deve-se consultar seu próprio conselho jurídico a respeito das leis aplicáveis a essa coleta de dados, incluindo quaisquer requisitos de aviso e consentimento.

Para obter mais informações sobre o uso de várias tecnologias, incluindo cookies, para esses propósitos, consulte a Política de Privacidade da IBM em <http://www.ibm.com/privacy>, a seção intitulada “Cookies, Web Beacons e Outras Tecnologias”, na Declaração de Privacidade Online da IBM em <http://www.ibm.com/privacy/details/br/pt/> e “IBM Software Products and Software-as-a-Service Privacy Statement” em <http://www.ibm.com/software/info/product-privacy>.

---

# Índice Remissivo

## A

administrador da rede v  
alta disponibilidade (HA) 2

## C

chave de ativação 5

## D

dados de backup 15  
dados de restauração 15

## E

endereço da máscara de rede 1  
endereço do gateway 1  
endereço IP 1

## F

Função de usuário do Risk Manager 9  
função do usuário 9

## H

host gerenciado 7

## I

Incluir o QRadar Risk Manager 7  
informações de login 6  
informações de login padrão 6  
informações de rede 1  
instale o QRadar Risk Manager 6  
introdução v  
IPv6 2

## M

máscara de sub-rede 1  
máscaras de rede não contíguas 2  
modo de documento  
    Navegador da web do Internet  
    Explorer 3  
modo do navegador  
    Navegador da web do Internet  
    Explorer 3  
mudanças de configuração de rede 13

## N

Navegador da web  
    versões suportadas 3

nome de usuário 6

## P

perfil de segurança 9  
porta 22 2  
porta 37 2  
porta 443 2  
preparação do dispositivo 5  
preparando para instalação 1, 5

## R

recursos não suportados 2  
requisitos de porta 2  
roteamento dinâmico 2

## S

senha 6  
servidor NTP 1