IBM QRadar

Adapter Configuration Guide
December 2021

IBM

Note

Before you use this information and the product that it supports, read the information in "Notices" on page 53.

Contents

Introduction to configuring adapters for QRadar Risk Manager

IBM QRadar Risk Manager is an appliance that is used to monitor device configurations, simulate changes to your network environment, and prioritize risks and vulnerabilities. QRadar Risk Manager uses adapters to integrate with devices in your network.

Intended audience

Network administrators who are responsible for installing and configuring adapters must be familiar with network security concepts and device configurations.

Technical documentation

To find IBM Security QRadar product documentation on the web, including all translated documentation, access the IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome).

For information about how to access more technical documentation in the QRadar products library, see Accessing IBM Security QRadar Documentation (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).

Contacting customer support

For information about contacting customer support, see the Support and Download Technical Note (http://www.ibm.com/support/docview.wss?uid=swg21616144).

Statement of good security practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Please Note:

Use of this Program may implicate various laws or regulations, including those related to privacy, data protection, employment, and electronic communications and storage. IBM Security QRadar may be used only for lawful purposes and in a lawful manner. Customer agrees to use this Program pursuant to, and assumes all responsibility for complying with, applicable laws, regulations and policies. Licensee represents that it will obtain or has obtained any consents, permissions, or licenses required to enable its lawful use of IBM Security QRadar.

Chapter 1. Adapters overview

Use adapters to integrate IBM QRadar Risk Manager with your network devices. By configuring adapters, QRadar Risk Manager can interrogate and import the configuration parameters of network devices, such as firewalls, routers, and switches.

Network topology and configuration

QRadar Risk Manager uses adapters to collect network configurations. The adapters turn the configuration information into a standard format that is unified for supported device models, manufacturers, and types. QRadar Risk Manager uses the data to understand your network topology and configuration of your network devices.

To connect external devices in the network, QRadar Risk Manager must be able to access the devices. QRadar Risk Manager uses the user credentials that are configured in QRadar to access the device and to download the configurations.

Process for integrating network devices

To integrate network devices with QRadar Risk Manager, follow these steps:

1. Configure the network device to enable communication with QRadar Risk Manager.
2. Install the appropriate adapter for your network device on your QRadar Risk Manager appliance.
3. Use Configuration Monitor to add your network devices to QRadar Risk Manager.
4. Define the network protocol that is required for communication with your network devices.

    For more information, see the *IBM QRadar Risk Manager User Guide*.

Types of adapters

IBM QRadar Risk Manager supports several types of adapters.

The following adapters are supported:

- F5 BIG-IP
- Brocade vRouter
- Check Point SecurePlatform Appliances
- Check Point Security Management Server
- Cisco Catalyst (CatOS)
- Cisco Internet Operating System (IOS)
- Cisco Nexus
- Cisco Security Appliances
- Fortinet FortiOS
- HP Networking ProVision
- Juniper Networks ScreenOS
- Juniper Networks JUNOS
- Juniper Networks NSM
- Palo Alto
- Sourcefire 3D Sensor
- Generic SNMP
- TippingPoint IPS

- McAfee Sidewinder

Adapter features

Adapters come with many features to help you integrate your network devices with QRadar Risk Manager.

The following table lists common features for the supported adapters.

Table 1. Adapter features						
Adapter	**Versions**	**NAT**	**Routing**	**Tunnelling**	**Protocols**	**Other features**
Brocade vRouter	6.7 to 17.1		Static		Telnet, SSH	
Check Point Secure Platform	R65 to R77.30	Static Dynamic	Static		Telnet, SSH	
Check Point SMS OPSEC	NGX R60 to R77	Static Dynamic	Static		CPSMS	
Check Point SMS HTTPS	R80	Static Dynamic	Static		HTTPS	
Cisco ASA	ASA: 8.2, 8.4 to 9.1.7 PIX: 6.1, 6.3 FWSM: 3.1, 3.2	Static	Static EIGRP, OSPF		Telnet, SSH, SCP	
Cisco CatOS	Catalyst 6500 series chassis devices. 4.2, 6.4		Static		Telnet, SSH	
Cisco Nexus	Nexus 5548: OS level 6.0 Nexus 7000 series: OS level 6.2 Nexus 9000 series: OS level 6.1		Static EIGRP, OSPF		Telnet, SSH	
Cisco IOS	IOS 12.0 to 15.1 for routers and switches Cisco Catalyst 6500 switches with MSFC.	Static Dynamic	Static EIGRP, OSPF	VPN	Telnet, SSH	
F5 BIG-IP	10.1 - 13.1	Static Dynamic	Static	VPN	SSH	
Fortinet FortiOS	4.0 MR3 to 5.2.4	Static	Static		Telnet, SSH	
Generic SNMP	SNMPv1, v2 and v3					
HP ProCurve ProVision	HP Networking ProVision Switches K/KA.15.X		RIP		SSH	
IBM Proventia GX IPS	GX appliances that are managed by SiteProtector.				SQL	Applications
Juniper JUNOS	10.4, 11.2 to 12.3, and 13.2	Service-set NAT is supported on MX appliances.	Static OSPF		Telnet, SSH, SCP	
Juniper NSM	IDP appliances that are managed by NSM (Network and Security Manager)				HTTPS	

Table 1. Adapter features (continued)						
Adapter	Versions	NAT	Routing	Tunnelling	Protocols	Other features
Juniper ScreenOS	5.4, 6.2	Static Dynamic	Static		Telnet, SSH	
Sidewinder	8.3.2	Static	Static		Telnet, SSH	
Palo Alto Firewalls	PAN-OS Versions 5.0 to 7.0	Static Dynamic	Static	IPSEC	HTTPS	User/Groups Applications
SourceFire 3D Sensor	5.3			VPN	SSH	IPS
Tipping Point IPS	TOS 3.6 and SMS 4.2				Telnet, SSH, HTTPS	IPS

Adapter FAQs

QRadar Risk Manager uses adapters to connect and get configuration information from network devices.

- "Do adapters support all devices and versions that QRadar SIEM supports?" on page 3
- "Do all adapters support the same features, for example, OSPF routing?" on page 3
- "What user-access level does the adapter require to get device configuration?" on page 3
- "How do you configure credentials to access your network devices?" on page 3
- "What credential fields do you need to complete for each device?" on page 3
- "How do you configure protocols for your devices?" on page 4
- "How do you add your network devices to QRadar Risk Manager?" on page 4

Do adapters support all devices and versions that QRadar SIEM supports?

Adapters are a separate integration and are used by QRadar Risk Manager only to import device configurations. To view a list of supported adapters, see Chapter 5, "Supported adapters," on page 15.

Do all adapters support the same features, for example, OSPF routing?

The range of supported features such as routing support and NAT support vary with the adapters. See "Adapter features" on page 2.

What user-access level does the adapter require to get device configuration?

The required access level varies by adapter, but it is restricted to read-only for most adapters. See Chapter 5, "Supported adapters," on page 15 and view the user-access level requirements when you select an adapter.

How do you configure credentials to access your network devices?

You must configure credentials to allow QRadar Risk Manager to connect to devices in your network. Administrators use Configuration Monitor to input device credentials. Individual device credentials can be saved for a specific network device. If multiple network devices use the same credentials, you can assign credentials to a group. For more information, see the *IBM QRadar Risk Manager User Guide*.

What credential fields do you need to complete for each device?

Some adapters might require only a username and password while others might need extra credentials, for example, Cisco IOS might require an enable password. See Chapter 5, "Supported adapters," on page 15 and view the required credential parameters in the tables.

How do you configure protocols for your devices?

Use Network Groups, which contain protocols that you can use to enable connectivity to IP/CIDR/ address ranges for devices. For more information, see the *IBM QRadar Risk Manager User Guide*.

How do you add your network devices to QRadar Risk Manager?

Table 1 lists the methods for adding network devices to QRadar Risk Manager.

Table 2. Adding network devices	
Method	**Description**
Add devices individually	Use this method if you want to run a test backup of a few devices, for example, to check that your credentials and protocols are correctly configured.
Device discovery	Use this method if you have an IP/CIDR address range with SNMP community strings that are configured for each device and you want to find all devices in that address range.
	You must have SNMP get community strings defined in your credential set for device discovery to work.
Discovery from management device	Use this method for devices that are managed by a supported management system such as Check Point SMS.
Import devices	If you have several devices in your network, this method is the most reliable.

For information about adding network devices to QRadar Risk Manager, see the *IBM QRadar Risk Manager User Guide*.

(Back to top)

Chapter 2. Installing adapters

You must download the adapter files to your IBM QRadar SIEM Console, and then copy them to IBM QRadar Risk Manager.

Before you begin

After you establish the initial connection, QRadar SIEM Console is the only device that can communicate directly with QRadar Risk Manager.

Procedure

1. Using SSH, log in to your QRadar SIEM Console as the root user.
2. Download the compressed file for the QRadar Risk Manager adapters from <u>Fix Central</u> (www.ibm.com/support/fixcentral/) to your QRadar SIEM Console.
3. To copy the compressed file from your QRadar SIEM Console to QRadar Risk Manager, type the following command:

   `scp `*`adapters`*`.zip root@`*`IP_address`*`:`

   The *IP_address* option is the IP address or host name of QRadar Risk Manager.

   For example:

   `scp adapters.bundle-2014-10-972165.zip root@192.0.2.0:`
4. On your QRadar Risk Manager appliance, type the password for the root user.
5. Using SSH from your QRadar SIEM Console, log in to your QRadar Risk Manager appliance as the root user.
6. To unpack and install the adapters, type the following commands from the root directory that contains the compressed file:

   `unzip `*`adapters`*`.zip`

   `yum install -y adapters*.rpm`

   For example:

   `unzip adapters.bundle-2014-10-972165.zip`

   `yum install -y adapters*.rpm`

   Important: For QRadar Risk Manager versions before V.7.2.8, use the **rpm** command. For example:

   `rpm -Uvh adapters*.rpm`
7. To restart the services for the ziptie server and complete the installation, type the following command:

   `service ziptie-server restart`

   Important: Restarting the services for the ziptie server interrupts any device backups that are in progress from Configuration Monitor.

Uninstalling an adapter

Use the **yum** command to remove an adapter from IBM QRadar Risk Manager.

Procedure

1. Using SSH, log in to the IBM QRadar SIEM Console as the root user.
2. To uninstall an adapter, type the following command:

```
yum remove -y adapter package
```

For example, `yum remove -y adapters.cisco.ios-2011_05-205181.noarch`

Important: For QRadar Risk Manager versions before V.7.2.8, use the **rpm** command. For example:

```
rpm -e adapter file
rpm -e adapters.cisco.ios-2011_05-205181.noarch.rpm
```

Chapter 3. Methods for adding network devices

Use Configuration Monitor to add network devices to IBM QRadar Risk Manager.

The following table describes the methods that you can use to add a network device.

Table 3. Methods for adding a network device to QRadar Risk Manager	
Method	**Description**
Add Device	Add one device.
Discover Devices	Add multiple devices.
Discover From NSM	Add devices that are managed by a Juniper Networks NSM console.
Discover Check Point SMS	Add devices that are managed by a Check Point Security Manager Server (CPSMS).
Discover From SiteProtector	Add devices from SiteProtector.
Discover from Palo Alto Panorama	Add devices from Palo Alto Panorama.
Discover From Defense Center	Add devices from Sourcefire Defense Center.
Discover From Firepower Management Center	Add devices from Cisco Firepower Management Center.

For more information, see Discovering devices in your network.

Chapter 4. Troubleshooting device discovery and backup

Fix issues with device discovery and backup. You can look at the details for logs and error and warning messages to help you troubleshoot.

Device backup failure

Check device login credentials.

1. On the **Risks** tab, click **Configuration Monitor**.
2. Verify that the credentials to access the target device are correct.
3. Test the credentials on the target device.

View device backup errors

To see backup errors, do the following steps:

1. On the **Risks** tab, click **Configuration Monitor**.
2. Click a device, and then click **View error**.

This table lists the error message identifier, the description of the message and the suggested troubleshooting action.

Table 4. Device backup errors		
Backup errors	**Error description**	**Suggested troubleshooting step**
UNEXPECTED_RESPONSE	Connection attempt timed out	Verify that you're using the correct adapter.
INVALID_CREDENTIALS	Credentials are incorrect	Check credentials in **Configuration Monitor**.
SSH_ERROR	Connection error	Check that the device is working and is connected to your network. Use other network connection protocols and troubleshooting tools to verify that the device is accessible. Verify that the SSH connection protocol is allowed and that it is configured correctly.
TELNET_ERROR	Connection error	Check that the device is working and is connected to your network. Use other network connection protocols and troubleshooting tools to verify that the device is accessible. Verify that the Telnet connection protocol is allowed and that it is configured correctly.

Table 4. Device backup errors (continued)		
Backup errors	**Error description**	**Suggested troubleshooting step**
SNMP_ERROR	Connection error	Check that the device is working and is connected to your network. Use other network connection protocols and troubleshooting tools to verify that the device is accessible. Verify that the SNMP is allowed and that it is configured correctly.
TOO_MANY_USERS	The number of users that are configured to access this device is exceeded.	Check the maximum number of users that are allowed to access the device by logging on to the device and checking the configuration for the maximum number of users that can access the device at the same time.
DEVICE_MEMORY_ERROR	Device configuration errors	Verify that the device is working correctly. Access the device and verify the configuration and check the logs for errors. Use your device documentation to help you to troubleshoot errors.
NVRAM_CORRUPTION_ERROR	Device access issues	In **Configuration Monitor**, check the access level of the user name that is configured to access the device.
INSUFFICIENT_PRIVILEGE	User that is configured to access the device has insufficient privilege	In **Configuration Monitor**, check the access level of the user name that is configured to access the device.
DEVICE_ISSUE	Error on the device	In **Configuration Monitor**, in the **Status** column, click **Failure**. On the **Recent Activity** page, click **View Log** to see more details.

Backup completes with parse warning

To view more detail about the warning, do the following steps:

1. Click the **Risks** tab.
2. From the navigation menu, click **Configuration Monitor**.
3. Click **See Log** for the selected device in the **Device List** table.

Verify whether you have the most recent adapter versions

To check your adapter versions, log in as root to the QRadar Risk Manager appliance and then type the following command:

```
yum list adapter\*
```

You can look for date information in the names of the adapters to help you determine the release dates.

To download the most recent adapter bundle, do the following steps:

1. Go to IBM Fix Central (https://www.ibm.com/support/fixcentral/).
2. In the **Product selector** field type Risk Manager to filter your selection.
3. Click IBM QRadar Risk Manager.

4. From the **Installed Version** list, select the version that is installed on your system.

5. From the **Platform** list, select the operating system that is installed on your system, and then click **Continue**.

6. Click **Browse for fixes**, and then click **Continue**.

7. To download the most recent adapter bundle, click the adapter-bundle link on the top of the **Adapter** list.

Verify whether your device backup is current

To verify whether you have a recent backup, do these steps:

1. Click the **Risks** tab.

2. From the navigation menu, click **Configuration Monitor**.

3. Double-click the device in the **Device List** table.

4. From the toolbar, click **History**. The most recent configuration that is imported is displayed.

If you don't think that you have the most recent configuration, verify by running the backup again.

Error when importing configurations from your devices

An incorrectly formatted CSV file can cause a device backup to fail. Do these steps to check the CSV file:

1. Review your CSV file to correct any errors.

2. Re-import your device configurations by using the updated CSV file.

Failure to discover devices from Check Point SMS (OPSEC)

Follow all steps in the "Adding devices that are managed by a CPSMS console" section of the *IBM QRadar Risk Manager Adapter Configuration Guide*, especially steps 7 and 8 where the OPSEC fields must be precise.

Device backup failure because of login message or message of the day

Adapters that use Telnet and SSH to connect to devices use regular expressions (regex) to match device prompts. If characters in the login message or the message of the day match the regex, then the backup process might fail.

For example, if you use the following login banner for the Cisco ASA, the backup fails because the adapter operates as if the *#* character in the login message is the device prompt when the regex *#\s*$* is matched.

################ Welcome to ASA ################

The following table lists the adapters and their regexes that are impacted by these backup failures:

Table 5. Adapters and their regexes	
Adapter	**Regexes (single quotes (') are used as delimiters)**

CheckPoint SecurePlatform	```'sername:|(?<!Last)\s+login:'```
	```'[Pp]assword:'```
	```'(#|\$|>)\s*$'```

Cisco SecurityAppliance (ASA)	```'sername:|ogin:'```
	```'[Pp]assword:'```
	```'>\s*$'```
	```'#\s*$'```

Table 5. Adapters and their regexes (continued)	
Adapter	**Regexes (single quotes (') are used as delimiters)**

Cisco Nexus	`'sername:\s*'`
	`'assword:\s*'`
	`'(^|\n|\r)[^#^\n^\r]+#\s*$|[^#^\n^\r]+#\s*\S+#\s*$'`
	`'\/hello>\W+?'`

Cisco IOS	`'maximum number of telnet'`
	`'assword required, but none se'`
	`'sername:'`
	`'assword:'`
	`'PASSCODE:'`
	`'(?m)^\w\S*#\s*(?![\n\r])$'`
	`'(?m)^\w\S*>\s*(?![\n\r])$'`
	`'any key to'`
	`'User Interface Menu'`

Cisco CatOS	`'sername:|ogin:'`
	`'[Pp]assword:'`
	`'\n\S+\s$'`
	`'\(enable\)\s*$'`
	`'(^|\n|\r)[^>^(\n|\r)]+>\s*$'`

HP ProVision	`'\S+>'`
	`'\S+#'`
	`'sername:\s*\Z'`
	`'ogin as:'`

TippingPoint IPS	`'sername:|ogin:'`
	`'assword:'`
	`'(#|\$|>)\s*$'`

CheckPoint OPSEC	`'sername:|(?<!Last)\s+login:'`
	`'[Pp]assword:'`
	`'(#|\$|>)\s*$'`

McAfee Sidewinder	`'sername:|(?<!Last)\s+login:|(login:\s+)$'`
	`'[Pp]assword:'`
	`'(#|\$|>|%)\s*$'`

Juniper ScreenOS	`'sername:|ogin:'`
	`'[Pp]assword:'`
	`'(#|>)\s*$'`

Juniper JUNOS	`'^\s*login:'`
	`'assword'`
	`'%'`
	`'.+>'`

Juniper NSM	`'sername:|(?<!Last)\s+login:'`
	`'[Pp]assword:'`
	`'(#|\$|>)\s*$'`

Sourcefire 3D	`'(#|\$|\>)\s*$'`
	`'(\>\s*expert\a?)\s*$'`
	`'([Pp]assword)\s*\:\s*$'`

Table 5. Adapters and their regexes (continued)	
Adapter	**Regexes (single quotes (') are used as delimiters)**
F5 BIG-IP	``` 'sername:|ogin:\s*$' 'continue connecting \(yes\/no\)\?\s*$' '[Pp]assword:\s*$' '(#\|\$)\s*$' ```
Fortinet FortiOS	``` 'sername:|(?<!Last)\s+login:' '[Pp]assword:' '(#|\$|>)\s*$' ```
Nokia CheckPoint	``` 'sername:\s*$\|ogin:\s*$' '[Pp]assword:' 'Terminal\s+type\?' '(#|\$|>)\s*$' ```

Chapter 5. Supported adapters

IBM QRadar Risk Manager integrates with many manufacturers and vendors of security products.

The following information is provided for each supported adapter:

Supported versions

Specifies the product name and version supported.

Supports neighbor data

Specifies whether neighbor data is supported for this adapter. If your device supports neighbor data, then you get neighbor data from a device by using Simple Network Management Protocol (SNMP) and a command-line interface (CLI).

SNMP discovery

Specifies whether the device allows discovery by using SNMP.

Devices must support standard MIB-2 for SNMP discovery to take place, and the device's SNMP configuration must be supported and configured correctly.

Required credential parameters

Specifies the necessary access requirements for QRadar Risk Manager and the device to connect.

Ensure that the device credentials configured in QRadar Risk Manager and in the device are the same.

If a parameter is not required, you can leave that field blank.

To add credentials in QRadar, log in as an administrator and use **Configuration Monitor** on the **Risks** tab.

Connection protocols

Specifies the supported protocols for the network device.

To add protocols in QRadar, log in as an administrator and use **Configuration Monitor** on the **Risks** tab.

Required commands

Specifies the list of commands that the adapter requires to log in and collect data.

To run the listed commands on the adapter, the credentials that are provided in QRadar Risk Manager must have the appropriate privileges.

Files collected

Specifies the list of files that the adapter must be able to access. To access these files, the appropriate credentials must be configured for the adapter.

Brocade vRouter

IBM QRadar Risk Manager supports the Brocade Virtual Router (vRouter) adapter.

The static routing feature is available with the Brocade vRouter adapter.

The integration requirements for the Brocade vRouter adapter are described in the following table:

Table 6. Brocade vRouter adapter	
Integration Requirement	**Description**
Supported versions	6.7 to 17.1

Table 6. Brocade vRouter adapter (continued)	
Integration Requirement	**Description**
Minimum user access level	Operator or Admin
Required credential parameters	**Username** **Password**
Supported connection protocols	Use one of the following supported connection protocols: **SSH** **Telnet**

Commands that the adapter requires to log in and collect data	```show version```
	 ```show host name```
	 ```show system memory```
	 ``show configuration all
		no-more```
		 ``show interfaces
			no-more```

Check Point SecurePlatform Appliances

IBM QRadar Risk Manager supports the Check Point SecurePlatform Appliances adapter.

The following features are available with the Check Point SecurePlatform Appliances adapter:

- Dynamic NAT
- Static NAT
- SNMP discovery
- Static routing
- Telnet and SSH connection protocols

The following table describes the integration requirements for the Check Point SecurePlatform Appliances adapter.

Table 7. Integration requirements for the Check Point SecurePlatform Appliances adapter	
Integration requirement	**Description**
Versions	R65 to R77.30 **Restriction:** Nokia IPSO appliances are not supported for backup.
SNMP discovery	Matches NGX in SNMP sysDescr.
Required credential parameters To add credentials in QRadar, log in as an administrator and use **Configuration Monitor** on the **Risks** tab.	**Username** **Password** **Enable Password** (expert mode)
Supported connection protocols To add protocols in QRadar, log in as an administrator and use **Configuration Monitor** on the **Risks** tab.	Use any one of the following supported connection protocols: **Telnet** **SSH**

Table 7. Integration requirements for the Check Point SecurePlatform Appliances adapter (continued)	
Integration requirement	**Description**

Commands that the adapter requires to log in and collect data	`hostname`
	`dmidecode`
	`ver`
	`uptime`
	`dmesg`
	`route -n`
	`show users`
	`ifconfig -a`
	`echo $FWDIR`

Files collected	`rules.C`
	`objects.C`
	`implied_rules.C`
	`Standard.pf`
	`snmpd.com`

Check Point Security Management Server adapter

Use the Check Point adapter to discover and backup end nodes that are managed by the Security Management Server (CPSMS).

Choose one of the following adapters to discover and backup end nodes that are managed by the CPSMS.

Check Point Security Management Server OPSEC adapter

Use the Check Point Security Management Server OPSEC adapter to discover and backup end nodes that are managed by the CPSMS versions NGX R60 to R77.

The following features are available with the Check Point Security Management Server OPSEC adapter:

- OPSEC protocol
- Dynamic NAT
- Static NAT
- Static routing

The CPSMS adapter is built on the OPSEC SDK 6.0, which supports Check Point products that are configured to use certificates that are signed by using SHA-1 only.

The following table describes the integration requirements for the CPSMS adapter.

Table 8. Integration requirements for the CPSMS adapter	
Integration requirement	**Description**
Versions	NGX R60 to R77

Table 8. Integration requirements for the CPSMS adapter (continued)	
Integration requirement	**Description**
Required credential parameters To add credentials in QRadar, log in as an administrator and use **Configuration Monitor** on the **Risks** tab.	Use the credentials that are set from Discovering devices in your network.
Supported connection protocols To add protocols in QRadar, log in as an administrator and use **Configuration Monitor** on the **Risks** tab.	**CPSMS**
Configuration requirements	To allow the `cpsms_client` to communicate with Check Point Management Server, the `$CPDIR/conf/sic_policy.conf` on CPSMS must include the following line: `# OPSEC applications defaultANY ; SAM_clients ; ANY ; sam ; sslca, local, sslca_comp# sam proxyANY ; Modules, DN_Mgmt ; ANY; sam ; sslcaANY ; ELA_clients ; ANY ; ela ; sslca, local, sslca_compANY ; LEA_clients ; ANY ; lea ; sslca, local, sslca_compANY ; CPMI_clients; ANY ; cpmi ; sslca, local, sslca_comp`
Required ports	The following ports are used by QRadar Risk Manager and must be open on CPSMS: Port 18190 for the Check Point Management Interface service (or CPMI) Port 18210 for the Check Point Internal CA Pull Certificate Service (or FW1_ica_pull) If you cannot use 18190 as a listening port for CPMI, then the CPSMS adapter port number must be similar to the value listed in the `$FWDIR/conf/fwopsec.conf` file for CPMI on CPSMS. For example, `cpmi_server auth_port 18190`.

Check Point Security Management Server HTTPS adapter

Use the Check Point Security Management Server HTTPS adapter to discover and backup end nodes that are connected to firewall blades that are managed by the Security Management Server or a Domain Management Server version R80 or later.

Tip: Discovery from the multi-domain server is not supported. Instead, target the virtual Domain Management Server.

The following features are available with the Check Point Security Management Server HTTPS adapter:

- Static NAT
- Static routing
- HTTPS connection protocol

The following features are not supported by the Check Point Security Management Server adapter:

- Dynamic objects (network objects)
- Security Zones (network objects)
- RPC objects (services)
- DCE-RPC objects (services)
- ICMP services (services)
- GTP objects (services)
- Compound TCP objects (services)
- Citrix TCP objects (services)
- Other services (services)
- User objects
- Time objects
- Access Control Policy criteria negation

Important: If you upgrade to the Check Point Security Management Server R80 or later from a previous version of Check Point SMS, you must rediscover your devices by using the **Discover From Check Point HTTPS** discovery method, even if your devices are recorded by Configuration Monitor.

The following table describes the integration requirements for the Check Point Security Management Server adapter.

Table 9. Integration requirements for the Check Point Security Management Server adapter	
Integration requirement	**Description**
API process must be running on the SMS	To check the API status, log in to the Management Server and type the following command on the cli: `api status`
API must allow requests from the QRadar IP address	If all IP addresses are not allowed to access the Management API, you must give QRadar Risk Manager access to it. To configure access on the SMS, go to **Manage & Settings** > **Blades** > **Management API** > **Advanced Settings**.
Versions	R80–R81.10
Required credential parameters To add credentials in QRadar, log in as an administrator and use **Configuration Monitor** on the **Risks** tab. **Important:** You must add the credentials for the Check Point Security Management Server before you configure device discovery.	**Enable Username** - Used for the domain of a Domain Management Server. **Username** **Password**
Device discovery configuration To configure device discovery in QRadar, log in as an administrator and use **Configuration Monitor** on the **Risks** tab. To configure the discovery method, click **Discover From Check Point HTTPS**, enter the IP address of the Check Point Security Management Server, and then click **OK**.	Discover From Check Point HTTPS

Table 9. Integration requirements for the Check Point Security Management Server adapter (continued)	
Integration requirement	**Description**
Supported connection protocols To add protocols in QRadar, log in as an administrator and use **Configuration Monitor** on the **Risks** tab.	HTTPS
User access level requirements	Read-write access all

Requested API endpoints	Use the following format to issue the listed commands to devices:
	
	`https://<managemenet server>:<port>/web_api/`
	`<command>`
	
	`show-simple-gateways`
	
	`show-hosts`
	
	`show-networks`
	
	`show-address-ranges`
	
	`show-groups`
	
	`show-groups-with-exclusion`
	
	`show-services-tcp`
	
	`show-services-udp`
	
	`show-service-groups`
	
	`show-packages`
	
	`show-access-rulebase`
	
	`show-nat-rulebase`
	
	`run-script`
	
	`show-task`

Important:

- The adapter cannot retrieve all the necessary data directly from the Check Point REST API. To obtain all the necessary data, the adapter uses the run-script endpoint to run the following Check Point CLI commands:

```
ip address
```

```
hostname
```

```
route -n
```

- The default permission profile "Read Only All" does not have one of the privileges that are required to integrate the HTTPS Adapter. You must add the "Run One Time Script" privilege to a permission profile. You can create a custom permission profile that is less permissive than "Read Write All" and "Read Only All," but contains the required permission. For more information, see "Create a Check Point custom permission profile to permit QRadar Risk Manager access" on page 21.

Create a Check Point custom permission profile to permit QRadar Risk Manager access

To enable QRadar Risk Manager access to the Check Point SMS HTTPS adapter API, you must create a permission profile on the Check Point Multi-Domain Server that includes the "Run One Time Script" permission.

About this task

You can create a custom permission profile that includes this permission, but is less permissive than the "Read Write All" or "Read Only All" profile.

Procedure

1. On the SMS Console with SmartDashboard, click **Manage & Settings** > **Permissions & Administrators** > **Permission Profiles**.
2. Click **Create New Profile**.
3. On the **Overview** tab, select **Customized**.
4. On the **Gateways** tab, select **One Time Script**.
5. On the **Access Control** tab, select the following options:
   - **Show Policy**
   - **Edit layers by the Software Blades** – Leave the check boxes cleared.
   - **NAT Policy** – Set the permission to **Read**.
   - **Access Control Objects and Settings** – Set the permission to **Read**.
6. On the **Threat Prevention** tab, select **Settings** and set the permission to **Read**.
7. On the **Others** tab, select the following options:
   - **Common Objects** – Set the permission to **Read**.
   - **Check Point Users Database** – Set the permission to **Read**.
8. On the **Monitoring and Logging** tab, leave the check boxes cleared.
9. On the **Management** tab, select **Management API Login**.

   Important: Ensure that any options that are not listed in Steps 3 – 9 are not selected.
10. Click **OK** and assign your user to this new permission profile.

Create a Check Point custom permission profile for a multi-domain server

To enable QRadar Risk Manager access to the Check Point SMS HTTPS adapter API, you must create a permission profile on the Check Point Multi-Domain Server that includes the "Run One Time Script" permission.

About this task

You can create a custom permission profile that includes this permission, but is less permissive than the "Read Write All" or "Read Only All" profile.

Procedure

1. On the MDS Console with SmartDashboard, click **Manage & Settings** > **Permissions & Administrators** > **Permission Profiles**.
2. Click **New Domain Permissions Profile**.
3. On the **Overview** tab, select **Customized**.
4. On the **Gateways** tab, select **One Time Script**.
5. On the **Access Control** tab, select the following options:

- **Show Policy**
- **Edit layers by the Software Blades** – Leave the check boxes cleared.
- **NAT Policy** – Set the permission to **Read**.
- **Access Control Objects and Settings** – Set the permission to **Read**.

6. On the **Threat Prevention** tab, select **Settings** and set the permission to **Read**.
7. On the **Others** tab, select the following options:

- **Common Objects** – Set the permission to **Read**.
- **Check Point Users Database** – Set the permission to **Read**.

8. On the **Monitoring and Logging** tab, leave the check boxes cleared.

   Important: Ensure that any options that are not listed in Steps 3 – 8 are not selected.
9. Click **OK** to finish the Domain Permission Profile and return to the **Permission Profiles** page.
10. Click **New Multi-Domain Permissions Profile**.
11. Under **Multi-Domain Levels**, select **Domain Level Only**.
12. Under **Multi-Domain Management**, select **Management API Login**.
13. Under **Global Management**, select **View global objects in domain**.
14. Under **Domain Management**, select **Default profile for all Domains**, and select the **Domain Profile** you created in steps 2 – 9.
15. Click **OK** and assign your user to this new permission profile.

Cisco CatOS

IBM QRadar Risk Manager supports the Cisco Catalyst (CatOS) adapter.

The Cisco CatOS adapter collects device configurations by backing up CatOS network devices that QRadar Risk Manager can access.

The following features are available with the Cisco CatOS adapter:

- Neighbor data support
- SNMP discovery
- Static routing
- Telnet and SSH connection protocols

The following table describes the integration requirements for the Cisco CatOS adapter.

Table 10. Integration requirements for the Cisco CatOS adapter	
Integration requirement	**Description**
Versions	Catalyst 6500 series chassis devices.
	4.2
	6.4
	Restriction: The adapter for CatOS backs up only the essential switching port structure.
	Multilayer Switch Feature Card (MSFC) CatOS adapters are backed up by Cisco IOS adapters.
	Firewall Services Module (FWSM) CatOS adapters are backed up by Cisco ASA adapters.
SNMP discovery	Matches CATOS or Catalyst Operating System in SNMP sysDescr.

Table 10. Integration requirements for the Cisco CatOS adapter (continued)	
Integration requirement	**Description**
Required credential parameters To add credentials in QRadar, log in as an administrator and use **Configuration Monitor** on the **Risks** tab.	**Username** **Password** **Enable Password**
Supported connection protocols To add protocols in QRadar, log in as an administrator and use **Configuration Monitor** on the **Risks** tab.	Use any one of the following supported connection protocols: **Telnet** **SSH**

Commands that the adapter requires to log in and collect data	`show version`
	`whichboot`
	`show module`
	`show mod ver`
	`show system`
	`show flash devices`
	`show flash ...`
	`show snmp ifalias`
	`show port ifindex`
	`show interface`
	`show port`
	`show spantree`
	`show ip route`
	`show vlan`
	`show vtp domain`
	`show arp`
	`show cdp`
	`show cam dynamic`
	`show port status`
	`show counters`

Cisco IOS

IBM QRadar Risk Manager supports the Cisco Internet Operating System (IOS) adapter.

The Cisco IOS adapter collects device configurations by backing up IOS-based network switches and routers.

The following features are available with the Cisco IOS adapter:

- Neighbor data support
- Dynamic NAT
- Static NAT

- SNMP discovery
- Static routing
- EIGRP and OSPF dynamic routing
- P2P Tunneling/VPN
- Telnet and SSH connection protocols

The following table describes the integration requirements for Cisco IOS.

Table 11. Integration requirements for Cisco IOS

Integration requirement	Description
Versions	IOS 12.0 to 16.12 for routers and switches. Cisco Catalyst 6500 switches with MSFC. Use the Cisco IOS adapter to back up the configuration and state of the MSFC card services. If a Cisco IOS 7600 series router has an FWSM, use the Cisco ASA adapter to back up the FWSM.
User Access Level	A user with command exec privilege level for each command that the adapter requires to log in and collect data. For example, you can configure a custom privilege level 10 user that uses local database authentication. The following example sets all show ip commands, to privilege level 10. `privilege exec level 10 show ip`
SNMP discovery	Matches ISO or Cisco Internet Operation System in SNMP sysDescr.
Required credential parameters To add credentials in QRadar, log in as an administrator and use **Configuration Monitor** on the **Risks** tab.	**Username** **Password** **Enable Username** (Optional) Use this field, if the user needs to enter a specific privilege level when logging in to the device. Use the format `level-<n>` where *n* is a privilege level [0-15]. For example, to enter privilege level 10, enter the following command: `level-10` This results in sending the **enable 10** command to the Cisco device. **Enable Password** (Optional)
Supported connection protocols To add protocols in QRadar, log in as an administrator and use **Configuration Monitor** on the **Risks** tab.	Use any one of the following supported connection protocols: **Telnet** **SSH**

Table 11. Integration requirements for Cisco IOS (continued)	
Integration requirement	**Description**
Commands that the adapter requires to log in and collect data	`terminal length 0` `show startup-config` `show ip arp` `show cdp neighbors detail` `show mac address-table dynamic` `show ip ospf neighbor` `show ip eigrp neighbors` `show ip bgp neighbors` `show interfaces` `show standby` `show version` `show interfaces` `show access-lists` `show ip route	exclude ^B'`  `show ip route bgp	include 0.0.0.0/0`  `show ipv6 route	exclude ^B`  `show ipv6 route bgp	include 0.0.0.0/0`  `show ipv6 routers`  `show ipv6 interface`  `show ipv6 access-list`  `show object-group`  `show vlan`  `show vlans`  Try to use the `show vlan` command first. If the `show vlan` command is not available, use the `show vlans` command.  The `show vlans` command is used for Catalyst 6500 series switches and Cisco 7600 series routers.

Cisco Nexus

To integrate IBM QRadar Risk Manager with your network devices, ensure that you review the requirements for the Cisco Nexus adapter.

The following features are available with the Cisco Nexus adapter:

- Neighbor data support
- SNMP discovery
- EIGRP and OSPF dynamic routing
- Static routing
- Telnet and SSH connection protocols

The following table describes the integration requirements for the Cisco Nexus adapter.

Integration requirement	Description
Table 12. Integration requirements for the Cisco Nexus adapter	
Integration requirement	**Description**
Versions and supported OS levels	Nexus 5xxx series: 7.3 and earlier Nexus 7xxx series: 8.4 and earlier Nexus 9xxx series: 9.2 and earlier
SNMP discovery	Matches *Cisco NX-OS* and an optional qualification string that ends with *Software* in the SNMP sysDescr. **Example:** *(Cisco NX\-OS.* Software)*
Required credential parameters To add credentials in QRadar, log in as an administrator and use **Configuration Monitor** on the **Risks** tab.	**Username** **Password** **Enable Password** **If you add virtual device contexts (VDCs) as individual devices, ensure that the required credentials allow the following actions:** Access the account that is enabled for the VDCs. Use the required commands in that virtual context.
Supported connection protocols To add protocols in QRadar, log in as an administrator and use **Configuration Monitor** on the **Risks** tab.	Use any one of the following supported connection protocols: **Telnet** **SSH**

Table 12. Integration requirements for the Cisco Nexus adapter (continued)	
Integration requirement	**Description**

Commands that the adapter requires to log in and collect data	`show hostname`
	
	`show version`
	
	`show vdc`
	
	`show vdc current-vdc`
	
	`switchto vdc <vdc>` where *vdc* is an active vdc that is listed when you enter the command, `show vdc`.
	
	`dir <filesystem>` where *filesystem* is `bootflash`, `slot0`, `volatile`, `log`, `logflash`, or `system`.
	
	`show running-config`
	
	`show startup-config`
	
	`show module`
	
	`show interface brief`
	
	`show interface snmp-ifindex`
	
	`show ip access-lists`
	
	`show vlan`
	
	`show object-group`
	
	`show interface <interface>` where *interface* is any interface that is listed when you enter the command, `show running-config`.
	
	`show ip eigrp`
	
	`show ip route eigrp`
	
	`show ip ospf`
	
	`show ip route ospf`
	
	`show ip rip`
	
	`show ip route rip`

Telemetry commands	`terminal length 0`
	
	`show hostname`
	
	`show vdc`
	
	`switchto vdc <vdc>` where *vdc* is an active vdc that is listed when you enter the command, `show vdc`.
	
	`show cdp entry all`
	
	`show interface brief`
	
	`show ip arp`
	
	`show mac address-table`
	
	`show ip route`

Methods for adding VDCs for Cisco Nexus devices

Use Configuration Monitor to add Nexus network devices and Virtual Device Contexts (VDC) to IBM QRadar SIEM. There are two ways to add multiple VDCs to IBM QRadar Risk Manager.

You can add VDCs as subdevices of the Nexus device or as individual devices.

View Virtual Device Contexts

If you add VDCs as individual devices, then each VDC is displayed as a device in the topology.

If you add VDCs as subdevices, they are not displayed in the topology. You can view the VDCs in the **Configuration Monitor** window.

Adding VDCs as subdevices of your Cisco Nexus device

Use Configuration Monitor to add VDCs as subdevices of your Cisco Nexus device.

Procedure

1. Enable the following commands for the user that is specified in the credentials:
   - `show vdc` (admin context)
   - `switchto vdc` *x*, where *x* is the VDC that is supported.

   In **Configuration Monitor**, you can view the Nexus device in the topology and the VDC subdevices. For more information about viewing devices, see the *IBM QRadar Risk Manager User Guide*.
2. Use Configuration Monitor to add the *admin context* IP address of the Nexus device.

Adding VDCs as individual devices

Use Configuration Monitor to add each (virtual device context) VDC as a separate device. When you use this method, the Nexus device and the VDCs are displayed in the topology.

When you view your Cisco Nexus device and VDCs in the topology, the chassis containment is represented separately.

Procedure

1. Use Configuration Monitor to add the admin IP address of each VDC.
2. Use Configuration Monitor to obtain the configuration information for your VDCs.
3. On the Cisco Nexus device, use the Cisco Nexus CLI to disable the **switchto vdc** command for the username that is associated with the adapter.

   Example: If the username for a Cisco Nexus device is *qrmuser*, type the following commands:

   ```
   NexusDevice(config)# role name qrmuser
   NexusDevice(config-role)# rule 1 deny command switchto vdc
   NexusDevice(config-role)# rule 2 permit command show *
   NexusDevice(config-role)# rule 3 permit command terminal
   NexusDevice(config-role)# rule 4 permit command dir
   ```

Cisco NGIPS

To integrate IBM QRadar Risk Manager with your network devices, ensure that you review the requirements for the Cisco Next-Generation Intrusion Prevention System (NGIPS) adapter.

The following features are available with the Cisco NGIPS adapter:
- IPS
- SSH connection protocol

Limitations:

- Intrusion policies attached to individual access control rules are not used by QRadar Risk Manager. Only the default intrusion policy is supported.
- NAT and VPN are not supported.

The following table describes the integration requirements for the Cisco NGIPS adapter.

Table 13. Integration requirements for the Cisco NGIPS adapter	
Integration requirement	**Description**
Versions	6.2.0
SNMP discovery	No
Required credential parameters To add credentials in QRadar, log in as an administrator and use **Configuration Monitor** on the **Risks** tab.	**Username** **Password**
Supported connection protocols To add protocols in QRadar, log in as an administrator and use **Configuration Monitor** on the **Risks** tab.	**SSH**

Commands that the adapter requires to log in and collect data.	`show version`
	`show memory`
	`show network`
	`show interfaces`
	`expert`
	`sudo`
	`su`
	`df`
	`hostname`
	`ip addr`
	`route`
	`cat`
	`find`
	`head`
	`mysql`

Commands that the adapter uses to read configuration information:
 	
To get hardware information.
To get the system host name.
To get routing information.
	`sudo su df`
	`sudo su hostname`
	`sudo su route -n`

Table 13. Integration requirements for the Cisco NGIPS adapter (continued)	
Integration requirement	**Description**
Use the cat or head command to read files and get configurations.	`/etc/sf/ims.conf`
Read to get the base directory for the SNORT instance, which is referenced as $DE_DIR in the following three examples:	`$SNORT_DIR/fwcfg/affinity.conf`
Read the IPS rules and objects.	`$DE_DIR/policyText_full.yaml`
Read the SNORT configuration.	`$DE_DIR/snort.conf`
Files are read in dynamically when they are referenced in the `policyText_full.yaml` file.	`$DE_DIR/*`
The adapter uses the **find** command is to search for IP reputation files in this directory.	`$SNORT_DIR/iprep_download`
File that is read to get the database connection credentials.	`/etc/sf/ims-data.conf`

Cisco Security Appliances

To integrate IBM QRadar Risk Manager with your network devices, ensure that you review the requirements for the Cisco Security Appliances adapter.

The following features are available with the Cisco Security Appliances adapter:

- Neighbor data support
- Static NAT
- SNMP discovery
- EIGRP and OSPF dynamic routing
- Static routing
- IPSEC tunneling
- Telnet and SSH connection protocols

The Cisco Security Appliances adapter collects device configurations by backing up Cisco family devices. The Cisco Security Appliances adapter supports the following firewalls:

- Cisco Adaptive Security Appliances (ASA) 5500 series
- Firewall Service Module (FWSM)
- Module in a Catalyst chassis
- Established Private Internet Exchange (PIX) device.

Note: Cisco ASA transparent contexts cannot be placed in the QRadar Risk Manager topology, and you cannot do path searches across these transparent contexts.

The following table describes the integration requirements for the Cisco Security Appliances adapter.

Table 14. Integration requirements for the Cisco Security Appliances adapter	
Integration requirement	**Description**
Versions	ASA:
	8.2 to 9.13
Minimum User Access Level	privilege level 5
	You can back up devices with privilege level 5 access level. For example, you can configure a level 5 user that uses local database authentication by running the following commands:
	`aaa authorization command LOCAL`
	`aaa authentication enable console LOCAL`
	`privilege cmd level 5 mode exec command terminal`
	`privilege cmd level 5 mode exec command changeto` (*multi-context* only)
	`privilege show level 5 mode exec command running-config`
	`privilege show level 5 mode exec command startup-config`
	`privilege show level 5 mode exec command version`
	`privilege show level 5 mode exec command shun`
	`privilege show level 5 mode exec command names`
	`privilege show level 5 mode exec command interface`
	`privilege show level 5 mode exec command pager`
	`privilege show level 5 mode exec command arp`
	`privilege show level 5 mode exec command route`
	`privilege show level 5 mode exec command context`
	`privilege show level 5 mode exec command mac-address-table`
SNMP discovery	Matches PIX or Adaptive Security Appliance or Firewall Service Module in SNMP sysDescr.
Required credential parameters To add credentials in QRadar, log in as an administrator and use **Configuration Monitor** on the **Risks** tab.	**Username** **Password** **Enable Password** You can specify the enable level of the user that you configure to access the ASA device from QRadar Risk Manager. For example, use the enable username of **level-5** to make the adapter run **enable 5** to enter privileged mode, instead of the higher level enable mode.

Table 14. Integration requirements for the Cisco Security Appliances adapter (continued)	
Integration requirement	**Description**
Supported connection protocols To add protocols in QRadar, log in as an administrator and use **Configuration Monitor** on the **Risks** tab.	Use any one of the following supported connection protocols: **Telnet** **SSH** **SCP**

Required commands that the adapter requires to log in and collect data	`changeto context <context>`
	`changeto system`
	`show running-config`
	`show startup-config`
	`show arp`
	`show context`
	`show interface`
	`show mac-address-table`
	`show names`
	`show ospf neighbor`
	`show route`
	`show shun`
	`show version`
	`terminal pager 0`
	`show interface detail`
	`show crypto ipsec sa`
	`show eigrp topology`
	`show eigrp neighbors`
	`show firewall`
	`show dns`
	
	The `changeto context <context>` command is used for each context on the ASA device.
	
	The `changeto system` command detects whether the system has *multi-context* configurations and determines the *admin-context*.
	
	The `changeto context` command is required if the `changeto system` command has a *multi-context* configuration or *admin-configuration* context.
	
	The `terminal pager` command is used to turn off paging behavior.

F5 BIG-IP

IBM QRadar Risk Manager supports the F5 BIG-IP adapter.

The following features are available with the F5 BIG-IP adapter:

- Neighbor data support
- Dynamic NAT
- Static NAT
- SNMP discovery
- Static routing

F5 BIG-IP load balancer appliances that run the Local Traffic Manager (LTM) are supported.

The following table describes the integration requirements for the F5 BIG-IP adapter.

Table 15. Integration requirements for the F5 BIG-IP adapter	
Integration requirement	**Description**
Versions	10.1 - 13.1
SNMP discovery	Matches F5 BIG-IP in sysOid containing 1.3.6.1.4.1.3375.2
Required credential parameters To add credentials in QRadar, log in as an administrator and use **Configuration Monitor** on the **Risks** tab.	**Username** **Password**
Supported connection protocols To add protocols in QRadar, log in as an administrator and use **Configuration Monitor** on the **Risks** tab.	**SSH**

Table 15. Integration requirements for the F5 BIG-IP adapter (continued)	
Integration requirement	**Description**

Version 10 (Bigpipe) backup commands
 	
Note: On version 10, the adapter sends Bigpipe commands. On versions 11 and later, the adapter sends tmsh commands.
	`bigpipe global`
	`bigpipe system hostname`
	`bigpipe platform`
	`uptime`
	`bigpipe version show`
	`cat /config/bigip.license`
	`bigpipe db packetfilter`
	`bigpipe db packetfilter.defaultaction`
	`bigpipe packet filter list`
	`bigpipe nat list all`
	`bigpipe vlan show all`
	`bigpipe vlangroup list all`
	`bigpipe vlangroup`
	`ip addr list`
	`bigpipe interface show all`
	`bigpipe interface all media speed`
	`bigpipe trunk all interfaces`
	`route -n`
	`bigpipe route all list all`
	`bigpipe mgmt show all`
	`bigpipe mgmt route show all`
	`bigpipe pool`
	`bigpipe self`
	`bigpipe virtual list all`
	`bigpipe snat list all`
	`bigpipe snatpool list all`
	`b db snat.anyipprotocol`

Table 15. Integration requirements for the F5 BIG-IP adapter (continued)	
Integration requirement	**Description**

Version 11 and later (tmsh) backup commands
 	
Note: On version 10, the adapter sends Bigpipe commands. On versions 11 and later, the adapter sends tmsh commands.
	`list sys global-settings hostname`
	`list sys management-ip`
	`show sys memory`
	`show sys hardware`
	`show sys version`
	`list sys db packetfilter`
	`list sys db packetfilter.defaultaction`
	`list sys db snat.anyipprotocol`
	`list net interface all-properties`
	`list net trunk`
	`list net packet-filter`
	`list net vlan all-properties`
	`show net vlan`
	`list net vlan-group all all-properties`
	`show net vlan-group`
	`list ltm virtual`
	`list ltm nat`
	`list ltm snatpool`
	`list ltm snat`
	`list net route`
	`list ltm pool`
	`list net self`
	`list net ipsec`
	`list net tunnels`

Fortinet FortiOS

IBM QRadar Risk Manager adapter for Fortinet FortiOS supports Fortinet FortiGate appliances that run the Fortinet operating system (FortiOS).

The following features are available with the Fortinet FortiOS adapter:

- Static NAT
- Static routing
- Telnet and SSH connection protocols

The Fortinet FortiOS adapter interacts with FortiOS over Telnet or SSH. The following list describes some limitations of QRadar Risk Manager and the Fortinet FortiOS adapter:

- Geography-based addresses and referenced policies are not supported by QRadar Risk Manager.
- Identity-based, VPN, and Internet Protocol Security policies are not supported by QRadar Risk Manager.

- Policies that use Unified Threat Management (UTM) profiles are not supported by the Fortinet FortiOS adapter. Only layer 3 firewall policies are supported.
- Policy Routes are not supported.
- Virtual Domains with Virtual Links that have partial IP addresses or no IP addresses are not supported.

The integration requirements for the Fortinet FortiOS adapter are described in following table:

Table 16. Integration requirements for the Fortinet FortiOS adapter	
Integration Requirement	**Description**
Version	6.4.6 or earlier
SNMP discovery	No
Required credential parameters To add credentials in QRadar, log in as an administrator and use **Configuration Monitor** on the **Risks** tab.	**Username** **Password**
Supported connection protocols To add protocols in QRadar, log in as an administrator and use **Configuration Monitor** on the **Risks** tab.	Use any one of the following supported connection protocols: **Telnet** **SSH**
User access level requirements	Read-write access for Fortinet firewalls that have VDOMs enabled. Read-only access for Fortinet firewalls that don't have VDOMs enabled.

Table 16. Integration requirements for the Fortinet FortiOS adapter (continued)	
Integration Requirement	**Description**

Commands that the adapter requires to log in and collect data	`config system console`
	
	`set output standard`
	
	Note: The `config system console` and `set output standard` commands require a user with read/write access to system configuration. If you use a read-only user with pagination enabled when you back up a Fortigate device, the performance is impaired significantly.
	
	`show system interface`
	
	`get hardware nic <variable>`
	
	`get system status`
	
	`get system performance status`
	
	`get router info routing-table static`
	
	`get test dnsproxy 6`
	
	`show firewall addrgrp`
	
	`show firewall address`
	
	`show full-configuration`
	
	`get firewall service predefined <variable>`
	
	`show firewall service custom`
	
	`show firewall service group`
	
	`show firewall policy`
	
	`show system zone`
	
	`show firewall vip`
	
	`show firewall vipgrp`
	
	`show firewall ippool`

Commands to use with VDOMs	`config global` to enter global configuration mode `config vdom; edit <vdom-name>` to switch between VDOMs

Generic SNMP adapter

IBM QRadar Risk Manager supports appliances that run an SNMP agent with the generic SNMP adapter.

This adapter interacts with the SNMP agent by using SNMP queries.

The object identifiers (OIDs) are contained in SNMP MIB-2, and you can expect all SNMP agents to expose these OIDs.

The following are adapter limitations:

- Collects basic interface and basic system information only. Rules and routing information are not collected.
- Even though displayed in Configuration Monitor, with SNMPv3, the adapter does not support AES encryption.

- The adapter does not support AES encryption with SNMPv3, even though it might appear to support it in the **Configuration Monitor** window.

The integration requirements for the generic SNMP adapter are described in following table:

Integration Requirement	Description
Version	SNMPv1, SNMPv2c, SNMPv3
Neighbor data support	No
SNMP discovery	No
Required credential parameters To add credentials in QRadar, log in as an administrator and use **Configuration Monitor** on the **Risks** tab.	SNMPv1 and SNMPv2c require **SNMP Get Community** SNMPv3 requires **SNMPv3 Authentication Username** SNMPv3 can have either one of the following credentials: **SNMPv3 Authentication Password** **SNMPv3 Privacy Password**
Supported connection protocols To add protocols in QRadar, log in as an administrator and use **Configuration Monitor** on the **Risks** tab.	Use any one of the following supported connection protocols: **SNMPv1** **SNMPv2c** **SNMPv3 using MD5** **SHA with DES**
Commands that the adapter requires to log in and collect data	SNMP Get commands .1.3.6.1.2.1.1.1.0 .1.3.6.1.2.1.1.2.0 .1.3.6.1.2.1.1.3.0 .1.3.6.1.2.1.1.4.0 .1.3.6.1.2.1.1.5.0 .1.3.6.1.2.1.1.6.0 SNMP Walk commands .1.3.6.1.2.1.2.2.1.2 .1.3.6.1.2.1.2.2.1.3 .1.3.6.1.2.1.2.2.1.4 .1.3.6.1.2.1.2.2.1.5 .1.3.6.1.2.1.2.2.1.6 .1.3.6.1.2.1.2.2.1.7 .1.3.6.1.2.1.4.20

HP Networking ProVision

IBM QRadar Risk Manager supports the HP Networking ProVision adapter.

The following features are available with the HP Networking ProVision adapter:

- Neighbor data support
- SNMP discovery
- RIP dynamic routing
- Telnet and SSH connection protocols

The following table describes the integration requirements for the HP Networking ProVision adapter.

Table 17. Integration requirements for the HP Networking ProVision adapter	
Integration requirement	**Description**
Versions	HP Networking ProVision Switches K/KA.15.X **Restriction:** HP switches that run a Comware operating system are not supported by this adapter.
SNMP discovery	Matches version numbers with the format `HP(.*)Switch(.*)(revision [A-Z]{1,2}\.(\d+)\.(\d+))` in sysDescr.
Required credential parameters To add credentials in QRadar, log in as an administrator and use **Configuration Monitor** on the **Risks** tab.	**Username** **Password** **Enable Password**
Supported connection protocols To add protocols in QRadar, log in as an administrator and use **Configuration Monitor** on the **Risks** tab.	**SSH**

Table 17. Integration requirements for the HP Networking ProVision adapter (continued)	
Integration requirement	**Description**
Backup operation commands that are issued by the adapter to the device	`dmesgshow system power-supply`
	`getmib`
	`show access-list vlan <vlan id>`
	`show access-list`
	`show access-list <name or number>`
	`show access-list ports <port number>`
	`show config`
	`show filter`
	`show filter <id>`
	`show running-config`
	`show interfaces brief`
	`show interfaces <interface id>` For each interface.
	`show jumbos`
	`show trunks`
	`show lacp`
	`show module`
	`show snmp-server`
	`show spanning-tree`
	`show spanning-tree config`
	`show spanning-tree instance <id or list>` (for each spanning-tree that is configured on the device)
	`show spanning-tree mst-config`
	`show system information`
	`show version`
	`show vlans`
	`show vlans <id>` (for each vlan)
	`show vrrp`
	`walkmib`
`show ip` backup operation commands that are issued by the adapter to the device	`show ip`
	`show ip route`
	`show ip odpf`
	`show ip odpf redistribute`
	`show ip rip`
	`show ip rip redistribute`

Table 17. Integration requirements for the HP Networking ProVision adapter (continued)	
Integration requirement	**Description**
Telemetry and neighbor data commands	`getmib`
	`show arp`
	`show cdp neighbors`
	`show cdp neighbors detail <port number>`
	`show interfaces brief`
	`show interface`
	`show ip route`
	`show lldp info remote-device`
	`show lldp info remote-device <port number>`
	`show mac-address or show mac address`
	`show system information`
	`show vlans`
	`show vlans custom id state ipaddr ipmask`
	`walkmib`

Juniper Networks JUNOS

To integrate IBM QRadar Risk Manager with your network devices, ensure that you review the requirements for the Juniper Networks JUNOS adapter.

The following features are available with the Juniper Networks JUNOS adapter:

- Neighbor data support
- SNMP discovery
- OSPF dynamic routing
- Static routing
- Telnet and SSH connection protocols
- Service-set NAT

The following table describes the integration requirements for the Juniper Networks JUNOS adapter.

Table 18. Integration requirements for the Juniper Networks JUNOS adapter	
Integration requirement	**Description**
Versions	10.4 to 19.4
SNMP discovery	Matches SNMP sysOID: 1.3.6.1.4.1.2636
Required credential parameters To add credentials in QRadar, log in as an administrator and use **Configuration Monitor** on the **Risks** tab.	**Username** **Password**

Table 18. Integration requirements for the Juniper Networks JUNOS adapter (continued)	
Integration requirement	**Description**
Supported connection protocols To add protocols in QRadar, log in as an administrator and use **Configuration Monitor** on the **Risks** tab.	Use any one of the following supported connection protocols: **Telnet** **SSH** **SCP**

Commands that the adapter requires to log in and collect data
 	
Note: A login announcement must end with \n. For example, set system login announcement "Login announcement\n". If it does not end with \n, then the backup fails.
	``
	set cli screen-length 0
	show version
	show chassis hardware | display xml
	show chassis mac-addresses
	show configuration interfaces | display xml
	show interfaces | display xml
	show system uptime
	show chassis firmware
	show chassis routing-engine
	show configuration snmp | display xml
	show configuration firewall | display xml
	show configuration firewall family inet6
	show configuration security | display xml
	show configuration security zones | display xml
	show configuration applications | display xml
	show configuration firewall
	show interfaces filters | display xml
	show configuration routing-options | display xml
	show ospf route | display xml
	show route protocol bgp 0.0.0.0 | display xml
	show configuration routing-instances <vrf> | display xml
	`` (where *<vrf>* is the name of a VRF)
	``
	show configuration
	show arp no-resolve
	show ospf neighbor
	show ospf rip neighbor
	show ospf bgp neighbor
	show configuration services | display xml
	``

Juniper Networks NSM

IBM QRadar Risk Manager adapter supports Juniper Networks NSM (Network and Security Manager).

You can use the QRadar Risk Manager to back up a single Juniper Networks device or obtain device information from a Juniper Networks NSM console.

The Juniper Networks NSM (Network and Security Manager) console contains the configuration and device information for Juniper Networks routers and switches that are managed by the Juniper Networks NSM console.

You can use HTTPS and SOAP connection protocols with Juniper Networks NSM.

The following table describes the supported environments for Juniper Networks NSM.

Table 19. QRadar Risk Manager adapter supported environments for Juniper Networks NSM	
Supported environment	**Description**
Versions	IDP appliances that are managed by NSM (Network and Security Manager)
SNMP discovery	Not supported
Required credential parameters To add credentials in QRadar, log in as an administrator and use **Configuration Monitor** on the **Risks** tab.	**Username** **Password**
Supported connection protocols To add protocols in QRadar, log in as an administrator and use **Configuration Monitor** on the **Risks** tab.	Use any one of the following supported connection protocols: **SOAP** **HTTP**

Juniper Networks ScreenOS

To integrate IBM QRadar Risk Manager with your network devices, ensure that you review the requirements for the Juniper Networks ScreenOS adapter.

The following features are available with the Juniper Networks ScreenOS adapter:

- Neighbor data support
- Dynamic NAT
- Static NAT
- SNMP discovery
- Static routing
- Telnet and SSH connection protocols

The following table describes the integration requirements for the Juniper Networks ScreenOS adapter.

Table 20. Integration requirements for the Juniper Networks ScreenOS adapter	
Integration requirement	**Description**
Versions	5.4 6.2

Integration requirement	Description
Table 20. Integration requirements for the Juniper Networks ScreenOS adapter (continued)	
Integration requirement	**Description**
SNMP discovery	Matches netscreen or SSG in SNMP sysDescr.
Required credential parameters	**Username** **Password**
Supported connection protocols	Use any one of the following supported connection protocols: **Telnet** **SSH**

Commands that the adapter requires to log in and collect data	```set console page 0```
	```get system```
	```get config```
	```get snmp```
	```get memory```
	```get file info```
	```get file```
	```get service```
	```get group address zone group```
	```get address```

Commands that the adapter requires to log in and collect data (continued)	```get service group```
	```get service group variable```
	```get interface```
	```get interface variable```
	```get policy all```
	```get policy id variable```
	```get admin user```
	```get route```
	```get arp```
	```get mac-learn```
	```get counter statistics interface variable```
	Where, *zone* is the zone data that is returned from the get config command.
	group is the group data that is returned from the get config command.
	variable is a list of returned data from a get service group, get interface, or get policy id command.

Palo Alto

IBM QRadar Risk Manager supports the Palo Alto adapter. The Palo Alto adapter uses the PAN-OS XML-based Rest API to communicate with Palo Alto firewall devices.

The following features are available with the Palo Alto adapter:

- Neighbor data support
- Dynamic NAT
- Static NAT
- Static routing
- SNMP discovery
- IPSEC Tunneling/VPN
- Applications
- User/Groups
- HTTPS connection protocol

The following table describes the integration requirements for the Palo Alto adapter.

Table 21. Integration requirements for the Palo Alto adapter

Integration requirement	Description
Versions	PAN-OS Versions 10.2.2 or earlier
Minimum user access level	Superuser (full access) is required for PA devices with External Dynamic Lists or Full Qualified Domain Name (FQDN) objects to perform system-level commands. Superuser (read-only) for all other PA devices.
SNMP discovery	SysDescr matches 'Palo Alto Networks(.*)series firewall' or sysOid matches 'panPA'
Required credential parameters To add credentials in QRadar, log in as an administrator and use **Configuration Monitor** on the **Risks** tab.	**Username** **Password**
Supported connection protocols To add protocols in QRadar, log in as an administrator and use **Configuration Monitor** on the **Risks** tab.	**HTTPS**

Required commands to use for the backup operation.	`/api/?type=op&cmd=<show><system><info></info></system>/show>`
	
	`/api/?type=op&cmd=<show><config><running></running></config></show>`
	
	`/api/?type=op&cmd=<show><interface>all</interface></show>`

Integration requirement	Description
Optional commands to use for the backup operation.	`/api/?type=op&cmd=<show><system><resources></resources></system></show>`
	`/api/?type=op&cmd=/config/predefined/service`
	For PAN-OS versions 7.0 and earlier: `/api/?type=op&cmd=<request><system><external-list><show><name>$listName</name>< /show></external-list></system></request>`, where *$listName* is a variable in this command, which is run multiple times.
	For PAN-OS versions 7.1 and higher: `/api/?type=op&cmd=<request><system><external-list><show><type><ip><name>$listName</name></ip></type></show></external-list></system></request>`, where *$listName* is a variable in this command, which is run multiple times.
	`/api/?type=op&cmd=<show><object><dynamic-address-group><all></all></dynamic-address-group></object></show>`
	`/api/?type=config&action=get&xpath=/config/predefined/application`
	`/api/?type=op&cmd=<request><system><external-list><show><type><predefined-ip><name>$listName</name></predefined-ip></type></show></external-list></system></request>`, where *$listName* is a variable in this command, which is run multiple times.
	`/api/?type=config&action=get&xpath=/config/predefined/service`
	`/api/?type=config&action=get&xpath=/config/panorama`
	`/api/?type=op&cmd=<request><system><fqdn><show-object><vsys>$vsysId</vsys><name>$FQDN</name></show-object></fqdn></system></request>`, where *$vsysId* is the virtual system the FQDN object resides on, and *$FQDN* is the required fully qualified domain name, which is run multiple times.
Required commands to use for telemetry and neighbor data.	`/api/?type=op&cmd=<show><system><info></info></system></show>`
	`/api/?type=op&cmd=<show><interface>all</interface></show>`
	`/api/?type=op&cmd=<show><routing><interface></interface></routing></show>`

Table 21. Integration requirements for the Palo Alto adapter (continued)

Table 21. Integration requirements for the Palo Alto adapter (continued)	
Integration requirement	**Description**

Optional commands to use for telemetry and neighbor data.	`/api/? type=op&cmd=<show><counter><interface>all</ interface></counter></show>`
	
	`/api/?type=op&cmd=<show><arp>all</arp></show></ p><p><show><mac>all</mac></show>`
	
	`/api/?type=op&cmd=<show><arp><entry name='all'/></arp></show>`
	
	`/api/?type=op&cmd=<show><routing><route></ route></routing></show>`

Required commands to use for the GetApplication.	`/api/?type=config&action=get&xpath=/config/ predefined/application`

Sidewinder

IBM QRadar Risk Manager supports McAfee Enterprise Firewall (Sidewinder) appliances that run SecureOS.

The following features are available with the Sidewinder adapter:

- Static NAT
- Static routing
- Telnet and SSH connection protocols

The Sidewinder adapter interacts with the CLI-based McAfee operating system (SecureOS) over Telnet or SSH.

Sidewinder adapter has the following limitations:

- Only Layer 3 firewall policies are supported because the Layer 7 policies that use Sidewinder application defenses are unsupported.
- Identity-based, geography-based, and IPv6 policies are dropped, because these policies are unsupported by QRadar Risk Manager.

The integration requirements for the Sidewinder adapter are described in the following table:

Table 22. Sidewinder adapter	
Integration Requirement	**Description**
Supported versions	8.3.2
Minimum user access level	admin The admin user access level is required to retrieve predefined services information from the database by using the **cf appdb list verbose=on** command.
SNMP discovery	No
Required credential parameters	**Username** **Password**

Table 22. Sidewinder adapter (continued)	
Integration Requirement	**Description**
Supported connection protocols	Use any one of the following supported connection protocols: **SSH** **Telnet**

Commands that the adapter requires to log in and collect data	`hostname`
	`uname -r`
	`uptime`
	`cf license q`
	`cf route status`
	`cf ipaddr q`
	`cf iprange q`
	`cf subnet q`
	`cf domain q`
	Use `"dig $address +noall +answer"`
	for each domain output from: `cf domain q`
	`cf host q`
	`cf netmap q`
	`cf netgroup q`
	`cf appdb list verbose=on`
	`cf application q`
	`cf appgroup q`
	`cf policy q`
	`cf interface q`
	`cf zone q`

Sourcefire 3D Sensor

To integrate IBM QRadar Risk Manager with your network devices, ensure that you review the requirements for the Sourcefire 3D Sensor adapter.

The following features are available with the Sourcefire 3D Sensor adapter:

• IPS
• SSH connection protocol

Limitations:

• Intrusion policies attached to individual access control rules are not used by QRadar Risk Manager. Only the default intrusion policy is supported.
• NAT and VPN are not supported.

The following table describes the integration requirements for the Sourcefire 3D Sensor adapter.

Table 23. Integration requirements for the Sourcefire 3D Sensor adapter	
Integration requirement	**Description**
Versions	5.2
Supported 3D sensors (Series 2 devices)	3D500 3D1000 3D2000 3D2100 3D2500 3D3500 3D4500 3D6500 3D9900
SNMP discovery	No
Required credential parameters To add credentials in QRadar, log in as an administrator and use **Configuration Monitor** on the **Risks** tab.	**Username** **Password**
Supported connection protocols To add protocols in QRadar, log in as an administrator and use **Configuration Monitor** on the **Risks** tab.	**SSH**

Commands that the adapter requires to log in and collect data	`show version`
	`show memory`
	`show network`
	`show interfaces`
	`expert`
	`sudo`
	`su`
	`df`
	`hostname`
	`ip addr`
	`route`
	`cat`
	`find`
	`head`
	`mysql`

Table 23. Integration requirements for the Sourcefire 3D Sensor adapter (continued)	
Integration requirement	**Description**
Commands that the adapter uses to read configuration information:	
To get hardware information.	`sudo su df`
To get the system host name.	`sudo su hostname`
To get routing information.	`sudo su route -n`
Use the cat or head command to read files and get configurations.	`/etc/sf/ims.conf`
Read to get the base directory for the SNORT instance, which is referenced as $DE_DIR in the following three examples:	`$SNORT_DIR/fwcfg/affinity.conf`
Read the IPS rules and objects.	`$DE_DIR/policyText_full.yaml`
Read the SNORT configuration.	`$DE_DIR/snort.conf`
Files are read in dynamically when they are referenced in the `policyText_full.yaml` file.	`$DE_DIR/*`
The adapter uses the **find** command is to search for IP reputation files in this directory.	`$SNORT_DIR/iprep_download`
File that is read to get the database connection credentials.	`/etc/sf/ims-data.conf`

TippingPoint IPS adapter

IBM QRadar Risk Manager supports TippingPoint IPS (intrusion prevention system) appliances that run TOS and that are under SMS control.

The following features are available with the TippingPoint IPS adapter:

- IPS
- Telnet, SSH+HTTPS connection protocols

This adapter requires interaction with the following devices:

- IPS directly by using the TippingPoint operating system (TOS) over Telnet or SSH.
- TippingPoint Secure Management Server (SMS) via the web services API over HTTPS.

A connection to the TippingPoint SMS is required to get the most recent Digital Vaccines signatures, which are managed by the SMS.

This adapter works only with IPS devices under SMS control. The SMS web services must be enabled for a successful backup.

This list is limitations of the TippingPoint adapter:

- QRadar Risk Manager doesn't process source or destination IP addresses in IPS rules or filters. The following TippingPoint features are not supported:
  - Traffic management filters
  - Profile or filter exceptions and restrictions
  - User-defined filters

- IPS filters without an associated CVE are not modeled because the IPS cannot be mapped to any QRadar vulnerabilities.

The integration requirements for the TippingPoint adapter are described in following table:

Table 24. TippingPoint IPS Adapter	
Integration Requirement	**Description**
Supported Versions	TOS 3.6 and SMS 4.2
Minimum User Access Level	IPS: Operator SMS: Operator (custom) A user who belongs to a group with a *custom operator* role, that has `Access SMS Web Services` option enabled .
SNMP discovery	No
Required credential parameters To add credentials in QRadar, log in as an administrator and use **Configuration Monitor** on the **Risks** tab.	Enter the following credentials: **Username**: *<IPS CLI username>* **Password**: *<IPS CLI password>* **Enable Username**: *<SMS username>* **Enable Password**: *<SMS password>*
Supported connection protocols To add protocols in QRadar, log in as an administrator and use **Configuration Monitor** on the **Risks** tab.	Use any one of the following supported connection protocols: **Telnet** for IPS CLI **SSH** for IPS CLI **HTTPS** for SMS

Commands that the adapter requires to log in and collect data	`show config`
	
	`show version`
	
	`show interface`
	
	`show host`
	
	`show sms`
	
	`show filter $filterNumber` (for each signature found in Digital Vaccine)

API commands that are sent to the SMS to retrieve the most recent signatures	`https://`*<sms_server>*`/dbAccess/ tptDBServlet?method=DataDictionary&table=SIGNATURE&format=xml`

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

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

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

53

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions..

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

IBM Online Privacy Statement

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user's session id for purposes of session management and authentication. These cookies can be disabled, but disabling them will also eliminate the functionality they enable.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, See IBM's Privacy Policy at http://www.ibm.com/privacy and IBM's Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled "Cookies, Web Beacons and Other Technologies" and the "IBM Software Products and Software-as-a-Service Privacy Statement" at http://www.ibm.com/software/info/product-privacy.