IBM Security QRadar SIEM
Version 7.1.0 (MR1)

Tuning Guide

IBM

Note: Before using this information and the product that it supports, read the information in Notices and Trademarks on page 35.

CONTENTS

A   IDENTIFYING NETWORK ASSETS

B   GLOSSARY

C   NOTICES AND TRADEMARKS

INDEX

ABOUT THIS GUIDE

The *IBM Security QRadar SIEMTuning Guide* provides information on tuning your QRadar SIEM deployment.

Intended Audience

This guide is intended for all users responsible for tuning QRadar SIEM. This guide assumes that you have QRadar SIEM access and a knowledge of your corporate network and networking technologies.

Conventions

The following conventions are used throughout this guide:

▶ Indicates that the procedure contains a single instruction.

NOTE

Indicates that the information provided is supplemental to the associated feature or instruction.

CAUTION

Indicates that the information is critical. A caution alerts you to potential loss of data or potential damage to an application, system, device, or network.

WARNING

Indicates that the information is critical. A warning alerts you to potential dangers, threats, or potential personal injury. Read any and all warnings carefully before proceeding.

Technical Documentation

For information on how to access more technical documentation, technical notes, and release notes, see the *Accessing IBM Security QRadar Documentation Technical Note*.
(http://www.ibm.com/support/docview.wss?rs=0&uid=swg21614644)

Contacting Customer Support

For information on contacting customer support, see the *Support and Download Technical Note*.
(http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861)

1 OVERVIEW

This document provides an overview of the steps to set up and tune your new IBM Security QRadar SIEM software. It assumes that your QRadar SIEM system is installed and functional. For more information on installing QRadar SIEM, see the *IBM Security QRadar SIEM Installation Guide*.

Tuning your QRadar SIEM system is completed in two phases; deployment and tuning. Table 1-1 describes the tasks required to complete each phase.

Table 1-1 Tuning Checklist

Phase	Task	Complete
Deployment	Create your network hierarchy.	
	Optional. Configure VA Scanners.	
	Update your Device Support Modules (DSMs).	
	Detecting Log Sources.	
	Establish and configure flow sources.	
	Configure your Asset Profile.	
	For more information, see **The Deployment Phase**.	
Tuning	Discover and validate servers.	
	Understanding and using rules and offenses.	
	Populating building blocks.	
	Tuning false positives.	
	Optimize Custom Rules	
	Cleaning the SIM model.	
	For more information, see **The Tuning Phase**.	

For assistance with tuning your QRadar SIEM system, contact Customer Support.

2 THE DEPLOYMENT PHASE

The Deployment Phase section describes the essential network, scanner, log source and asset configurations required to effectively tune your QRadar SIEM system.

This section includes the following topics:

- **Creating Your Network Hierarchy**
- **Configuring VA Scanners**
- **Updating Your DSMs**
- **Detecting Log Sources**
- **Establishing and Configuring Flow Sources**
- **Configuring Your Asset Profile**

Creating Your Network Hierarchy

QRadar SIEM uses the Network Hierarchy to:

- Determine which hosts are local and which are remote.
- Monitor specific logical groups or services in your network, such as marketing, Demilitarized Zones (DMZs), or Voice Over IP (VOIP).

We recommend that you define the following top level objects:

- DMZ: Internet facing IP address.
- Virtual Private Network (VPN): IP addresses used for remote access.
- Data centers and server networks.
- Network management and network devices.
- You must configure a weight value between 1 and 100 for each network component. This enables QRadar SIEM to determine the severity of the same event interacting with two different hosts.

NOTE

Assign higher weight values to servers that contain critical information.

NOTE
Ensure all internal address spaces, both routable and non-routable, are defined within your network hierarchy. Failure to do so could result in QRadar SIEM generating an excessive number of false positives.

Using the Admin tab, you can create your Network Hierarchy.

For more information on creating your network hierarchy, see the *IBM Security QRadar SIEM Administration Guide*.

Configuring VA Scanners

Vulnerability Integration Services (VIS) enable vulnerability assessment data to build profiles of attackers and targets. Vulnerability Assessment (VA) data uses correlated event data, network activity, and behavioral changes to remove false positives and determine the threat level for each critical business asset. To schedule scans and keep your VA data up-to-date, integrate QRadar SIEM with VA tools (third-party scanners).

For more information on configuring VA scanners, see the *Managing Vulnerability Assessment Guide.*

QRadar SIEM users VA information to determine a rank of magnitude for offenses on your network. Depending on the scanner type, QRadar SIEM imports scan results from the scanner server or remotely initiates a scan.

The results of a scan provide the system and version of each CIDR, server, and version of each port. This information describes the ports that are open and the vulnerabilities on the system.

NOTE
Ensure that you have downloaded and applied the latest scanner plug-ins from the Qmmunity website.

Updating Your DSMs

QRadar SIEM uses Device Support Modules (DSMs) to log and correlate the data sent to QRadar SIEM from various external log sources, such as security equipment (for example, firewalls) and network equipment (for example, switches and routers).

For a list of supported devices, see the *Configuring DSMs Guide*.

DSMs are regularly updated to ensure QRadar SIEM can properly interpret and parse security event information provided by external devices. DSMs can be updated both automatically and manually.

NOTE

Although most devices include native log sending capabilities, several devices require additional configuration, or an agent, or both, to send logs. Configuration varies between device types. You must ensure the devices are configured to send logs in a format that QRadar SIEM supports.

This section provides information on the following:

- **Automatically Updating DSMs**
- **Manually Updating DSMs**

Automatically Updating DSMs

The automatic DSM update function downloads and installs your DSM updates.

To configure automatic DSM updates:

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **Auto Update** icon.

Step 4 On the navigation menu, click **Change Settings**.

Step 5 From the Auto Update Schedule pane, select how frequently your DSM updates should be downloaded and installed:

   a **Frequency** - Select the frequency with which you want to receive updates.

   b **Hour** - Select the time of day you want your system to update.

   c **Week day** - Select this option if you have selected **Weekly** as the update frequency.

   d **Month Day** - This option is only active when you select **Monthly** as the update frequency.

Step 6 From the Update Types pane, select **Auto Install** from the **DSM, Scanner, Protocol Updates** drop-down list box.

Step 7 Click **Save**.

For more information on configuring DSM updates, see the *IBM Security QRadar SIEM Administration Guide.*

Manually Updating DSMs

You can manually install DSM updates at any time irrespective of the automatic update schedule.

To manually install DSM updates:

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **Auto Update** icon.

Step 4 On the navigation menu, click **Check for Updates**.

Step 5 From the toolbar, select **Install > DSM, Scanner, Protocol Updates**.

Step 6 Click **OK**.

Detecting Log Sources

QRadar SIEM automatically detects log sources that send syslog messages to an Event Collector. QRadar SIEM detects the log sources after a specific number of identifiable syslog messages are received within a predfined time frame.

QRadar SIEM processes syslog messages through a Traffic Analysis function which identifies the DSMs installed on the system and assigns the appropriate DSM to the log source. Automatically discovered log sources are displayed in the Log Sources window. You can open this window by clicking on the **Admin** tab.

NOTE

QRadar SIEM is pre-configured with DSM's which interpret log source data. To ensure log source data is received by QRadar SIEM, we recommend that you ensure the correct DSMs are installed. For more information, see **Updating Your DSMs**.

For more information on automatically detecting log sources, see the *Log Sources Guide*.

Adding Log Sources Manually

Log sources with low activity levels do not send enough logs for QRadar SIEM to automatically detect them or they require QRadar SIEM to be configured to retrieve the data. These devices must be added manually.

To manually add a log source:

Step 1 Click the **Admin** tab.

Step 2 In the navigation menu, click **Data Sources**.

Step 3 Click the **Log Sources** icon.

Step 4 Click **Add**.

Step 5 Configure the parameters. For more information on the Log Source parameters, see the *Log Sources User Guide*.

Step 6 Click **Save**.

Step 7 On the **Admin** tab, click **Deploy Changes**.

For more information on adding log sources manually, see the *Log Sources User Guide*.

Establishing and Configuring Flow Sources

Flows provide network traffic information and can be sent simultaneously to QRadar SIEM in a variety of formats, including flowlog files, NetFlow, J-Flow, sFlow, and Packeteer. Flow information enables QRadar SIEM to detect threats and activity that would otherwise be missed by relying strictly on event information.

NetFlow, J-Flow and sFlow are protocols which collect flow data from network devices, such as routers, and send this data to QRadar SIEM. NetFlow, J-Flow, and sFlow are configured in a similar way, but each is deployed according to the protocol that each network device supports.

NOTE

If you are collecting NetFlow, J-Flow, or sFlow data, verify that QRadar SIEM is collecting complete flow sets. Incomplete or missing flows can make it difficult to analyze network activity.

This section provides information on the following:

- **Validating QRadar QFlow Collector Data Collection**
- **Configuring QFlow Collector Devices**
- **Validating NetFlow Data**
- **NetFlow Log Messages**

NOTE

If you require assistance validating your QFlow collection, contact your network administrator or Customer Support.

Validating QRadar QFlow Collector Data Collection

QRadar SIEM can capture traffic from mirror ports or taps within your network using an IBM Security QRadar QFlow Collector. The QFlow Collector is enabled by default, whilst the mirror port or tap is connected to a monitoring interface on your QRadar SIEM appliance. Common mirror port locations include core, DMZ, server, and application switches.

The QFlow Collector provides full application detection of network traffic regardless of the port on which the application is operating. For example, if the Internet Relay Chat (IRC) protocol is communicating on port 7500 TCP, the QFlow Collector will identify the traffic as IRC and provide a packet capture of the beginning of the conversation. This differs from NetFlow and J-Flow which indicate that there is traffic on port 7500 TCP without identifying the protocol.

To validate QFlow Data:

Step 1 Click the **Network Activity** tab.

Step 2 From the Network Activity toolbar, select **Search > New Search**.

Step 3 In the **Search Parameters** pane, add a flow source search filter:

   a From the first drop-down list down, select **Flow Source**.

   b From the third drop-down list box, select your QFlow interface name.

Step 4 Click **Add Filter**.

Step 5 In the **Search Parameters** pane, add a protocol search filter.

   a From the first drop-down list box, select **Protocol**.

   b From the third drop-down list box, select **TCP**.

Step 6 Click **Add Filter**.

Step 7 Click **Filter**.

Locate the **Source Bytes** and **Destination Bytes** columns. If either column displays a large volume of results with zero (0) bytes, this might indicate that your

network tap or span is not configured correctly. We recommend that you verify your QFlow configuration. For more information, see **Configuring QFlow Collector Devices**.

Configuring QFlow Collector Devices

To verify your QFlow configuration:

- Ensure that span ports or taps are configured correctly to process both received and transmitted packets.

- Ensure visibility into both sides of any asymmetric routes.

If you are running dynamic routing protocols, traffic might follow different paths to and from a host. If you have more than one traffic path or route at the locations where you are collecting flow data, check with your network administrator to ensure that you are collecting flows from all routers that the traffic can traverse.

Validating NetFlow Data

To ensure your NetFlow configuration is functioning correctly, we recommend that you validate your QRadar SIEM NetFlow Data. Netflow should be configured to send data to the nearest QFlow Collector or Flow Processor appliance.

We recommend that you configure NetFlow to send data as quickly as possible by configuring the external network device's ip-cache flow timeout value to one. Ensure ingress and egress traffic is forwarded from the router (not all routers can do this). If you are configuring a router that only provides a sample of data, configure the router to use the lowest possible sampling rate, without increasing the load on the switch.

NOTE

By default, QRadar SIEM listens on the management interface for NetFlow traffic on port 2055 UDP. You can assign additional NetFlow ports if necessary.

To validate NetFlow data:

Step 1   Click the **Network Activity** tab.

Step 2   From the Network Activity toolbar, select **Search > New Search**.

Step 3   In the **Search Parameters** pane, add a flow source search filter.

- **a**   From the first drop-down list box, select **Flow Source**.

- **b**   From the third drop-down list box, select your NetFlow router's name or IP address.

NOTE

If your NetFlow router is not displayed in the third drop-down list box, QRadar SIEM might have been unable to detect traffic from the router. For further assistance, contact Customer Support.

Step 4   Click **Add Filter**.

Step 5   In the **Search Parameters** pane, add a protocol search filter.

- **a**   From the first drop-down list box, select **Protocol**.

- **b**   From the third drop-down list box, select **TCP**.

Step 6 Click **Add Filter**.

Step 7 Click **Filter**.

Locate the **Source Bytes** and **Destination Bytes** columns. If either column displays a large volume of results with zero (0) bytes, this might indicate that your NetFlow configuration is incomplete. We recommend that you verify your NetFlow configuration.

NetFlow Log Messages

If your NetFlow router is configured to sample flows, the following message can be logged in your QRadar SIEM log file:

```
Nov  3 16:01:03 qflowhost \[11519\] qflow115: \[WARNING\]
default_Netflow: Missed 30 flows from 10.10.1.1
(2061927611,2061927641)
```

This message indicates that the sequence number on the packet was missed. If the number of missed flows is consistent with your sampling rate, you can ignore this message.

To disable this message and prevent it from consuming log file space:

Step 1 Click the **Admin** tab.

Step 2 On the Admin toolbar, click **Deployment Editor**.

Step 3 Right-click the component specified in the error message and select **Configure**.

Step 4 On the toolbar, click **Advan.**

Step 5 From the **General Settings** expansion list, identify the **Verify NetFlow Sequence Numbers** field, and select **No** from the drop-down list box.

Step 6 Click **Save**.

Step 7 Click the **Saves recent changes and closes editor** icon to close the Deployment Editor.

Step 8 Click **Deploy Changes**.

Configuring Your Asset Profile

QRadar SIEM automatically discovers assets (servers and hosts) operating on your network, based on passive QFlow data and vulnerability data. QRadar SIEM then builds an asset profile that displays the services running on each asset. This profile data is used for correlation purposes to help reduce false positives. For example, if an attack attempts to exploit a specific service running on a specific asset, QRadar SIEM can determine if the asset is vulnerable to this attack by correlating the attack against the asset profile.

NOTE

Flow data or VA scanners must be configured for asset profiles to be displayed in the user interface. If no flow data or scanners are present, no data will exist to compile an asset profile.

You can define specific IP addresses (servers) as assets by importing existing assets in Comma-Separated Value (CSV) format. For more information, see **Importing Assets in CSV Format**. Adding an asset profile enables you to identify an IP address by name and provide a description and weight for the asset.

For more information on managing assets, see the *IBM Security QRadar SIEM Administration Guide*.

Importing Assets in CSV Format

When importing asset profile data in CSV format, the file must be in the following format:

```
ip,name,weight,description
```

Where:

- IP - Specifies any valid IP address in the dot decimal format. For example, 192.168.5.34.
- Name - Specifies the name of the asset up to 255 characters in length. Commas are not valid in this field and will invalidate the import process. For example, WebServer01.
- Weight - Specifies a number from 0 to 10, which indicates the importance of the asset on your network. A value of 0 denotes low importance, while 10 denotes a very high importance.
- Description - Specifies a textual description for this asset up to 255 characters in length. This value is optional.

Examples of Acceptable CSV Entries

The following entries can be included in a CSV file:

- 192.168.5.34,WebServer01,5,Main Production Web Server
- 192.168.5.35,MailServ01,0,

The CSV import process merges any asset profile information which is currently stored in your QRadar SIEM system.

For more information on configuring assets, see the *IBM Security QRadar SIEM Administration Guide*.

3 THE TUNING PHASE

The Tuning Phase section describes a number of procedures and best practices to optimize and tune your QRadar SIEM.

This section includes the following topics:

- **Discovering Servers**
- **Understanding and Using Rules and Offenses**
- **Populating Building Blocks**
- **Tuning False Positives**
- **Tuning Methodology**
- **False Positive Rule Chains**
- **Optimizing Custom Rules**
- **Cleaning the SIM Model**

Best Practices
Before you start this section, wait for 24 hours to allow QRadar SIEM *to detect the servers on the network, store events and flows, and create offenses based on existing rules.*

Discovering Servers
QRadar SIEM automatically discovers and classifies servers in your network, providing a faster initial deployment and easier tuning when network changes occur.

The Server Discovery function uses the asset profile database to discover many types of servers on your network. This function lists automatically discovered servers and enables you to select which servers you want to include in building blocks. For more information, see **Populating Building Blocks**.

For more information on server discovery, see the *IBM Security QRadar SIEM Administration Guide*.

NOTE

To discover servers, QRadar SIEM must receive vulnerability assessment (VA) scanner data or flow traffic. Server Discovery uses this data to configure port mappings in the asset profile. For more information on VA, see the *Managing Vulnerability Assessment Guide*.

QRadar SIEM uses building blocks to tune the system and allow additional correlation rules to be enabled. This reduces the number of false positives detected by QRadar SIEM, helping you to identify business critical assets. For more information on false positives, see **Tuning False Positives**.

This sections provides information on the following:

- **Best Practices in Discovering Servers**
- **Discovering Servers**

Best Practices in Discovering Servers

There are a number of best practices we recommend to determine which servers to discover:

- Allow the Server Discovery function to add servers, that you recognize as authorized infrastructure servers in your organization, to the selected building block. The Server Discovery function selects the correct building block or rule for the discovered servers. This enables QRadar SIEM to continue monitoring these servers while suppressing false positives that are specific to the server category.

- Some servers may be present in multiple categories. We recommend that you allow QRadar SIEM to place these servers in multiple building blocks. For example, active directory domain controllers may be identified as both Windows and DNS servers.

- After reviewing the server discovery list, not all servers displayed in the list may be familiar to you. These servers could be located in another business unit or function within a testing or staging environment. If you identify these servers as authorized, add them to the building block. For more information, see **Populating Building Blocks**.

- You can allow QRadar SIEM to categorize unauthorized servers or servers running unauthorized services into a related building block. For more information, see **Table 3-1**. If this generates an excessive number of offenses use the Server Discovery function to place these servers in a building block.

Discovering Servers

The Server Discovery function uses QRadar SIEM's Asset Profile database to discover different server types, based on port definitions. It enables you to select which servers to add to a server type building block. This feature makes the discovery and tuning process simpler and faster by providing a quick mechanism to insert servers into building blocks.

To discover servers:

Step 1 Click the **Assets** tab.

Step 2 On the navigation menu click **Server Discovery**.

The Server Discovery page is displayed.

Step 3 From the **Server Type** drop-down list box, select the server type you want to discover. The default is **Database Servers**.

Step 4 Select the option to determine the servers you want to discover:

- **All** - Search all servers in your deployment with the currently selected server type.

- **Assigned** - Search servers in your deployment that have been previously assigned to the currently selected server type.

- **Unassigned** - Search servers in your deployment that have not been previously assigned.

Step 5 From the **Network** drop-down list box, select the network you want to search.

Step 6 Click **Discover Servers**.

All discovered servers are displayed.

Step 7 Click **Approve Selected Servers**.

Step 8 In the Matching Servers table, select the check box or boxes of all the servers you want to assign to the server role.

NOTE

If you want to modify the search criteria, click either **Edit Ports** or **Edit Definition**. The Rules Wizard is displayed. For more information on the rules wizard, see the *IBM Security QRadar SIEM Users Guide*.

For more information on discovering servers, see the *IBM Security QRadar SIEM Administration Guide*.

Understanding and Using Rules and Offenses

QRadar SIEM generates offenses using the rule configuration defined in its Custom Rules Engine (CRE). This displays all the rules and building blocks in the system. Rules and building blocks are stored in two separate lists, because they function differently. For more information on building blocks, see **Populating Building Blocks**.

Understanding Rules

A rule is a collection of tests that perform an action when certain conditions are met. Each rule can be configured to capture and respond to a specific event, sequence of events, flow sequence, or offense. The actions which can be triggered can include sending an email or generating a syslog message. A rule can reference multiple building blocks by using the tests found in the function sections of the test groups within the Rule Editor.

Understanding Offenses

As event and flow data passes through the CRE, it is correlated using the rules setup on your QRadar SIEM system. Depending on how each rule is configured, an offense can be generated based on this correlation. These Offenses are displayed using the Offenses tab. For more information on offenses, see **Investigating Offenses**.

For more information on Rules and Offenses, see the *IBM Security QRadar SIEM Administration Guide*.

This sections includes the following topics:

- **Viewing your Current CRE Configuration**
- **Investigating Offenses**

Viewing your Current CRE Configuration

From the Offenses tab you can view all the rules that are deployed in your QRadar SIEM. This provides information about how the rules are grouped, the types of tests the rule performs, for example Flow or Event tests, and the responses each rule generates. Double-click any rule to display the Rule Wizard. This displays the tests associated with each rule and enables you to configure the response to each rule.

To view your current CRE configuration:

Step 1 Click the **Offenses** tab.

Step 2 On the navigation menu click **Rules**.

For more information on your CRE configuration, see the *IBM Security QRadar SIEM Users Guide*.

NOTE

To determine which rules are most active in generating offenses, from the rules page click **Offense Count** to reorder the column. This displays the rules which are generating offenses in descending order.

Investigating Offenses

QRadar SIEM generates offenses by testing event and flow conditions. We recommend that you investigate QRadar SIEM offenses, by viewing the rules that created the offense.

To investigate offenses:

Step 1 Click the **Offenses** tab.

Step 2 On the navigation menu click **All Offenses**.

Step 3 Double-click the offense you are interested in.

Step 4 From the All Offenses Summary toolbar, select **Display > Rules**.

Step 5 From the **List of Rules Contributing to Offense** pane, double-click the **Rule Name** you are interested in.

The Rule Wizard - Rule Test Stack Editor is displayed.

NOTE

The All Offenses Rules pane can display multiple Rule Names, since the offense generated by QRadar SIEM might have been triggered by a series of different tests.

For more information on investigating offenses, see the *IBM Security QRadar SIEM Users Guide*.

Populating Building Blocks

Building blocks use the same tests as rules, but have no actions associated with them. Building blocks group together commonly used tests, to build complex logic, so they can be used in rules. Building blocks are often configured to test groups of IP addresses, privileged usernames, or collections of event names. For example, you might create a building block that includes the IP addresses of all mail servers in your network, then use that building block in another rule, to exclude those hosts. The building block defaults are provided as guidelines, which should be reviewed and edited based on the needs of your network.

You can configure the host definition building blocks (BB:HostDefinition) to enable QRadar SIEM to discover and classify additional servers on your network. If a particular server is not automatically detected, you can manually add the server to its corresponding host definition building block. This ensures that the appropriate rules are applied to the particular server type. You can also manually add entire address ranges as opposed to individual devices.

This section includes the following topics:

- **Commonly Edited Building Blocks**
- **Building Block Tuning**
- **Editing a Building Block**

Commonly Edited Building Blocks

Proxy servers and virus servers can generate high volumes of traffic. To reduce the offenses created by these server types, edit the following building blocks to reduce the number of offenses:

- BB:HostDefinition: VA Scanner Source IP
- BB:HostDefinition: Network Management Servers
- BB:HostDefinition: Virus Definition and Other Update Servers
- BB:HostDefinition: Proxy Servers
- BB:NetworkDefinition: NAT Address Range
- BB:NetworkDefinition: TrustedNetwork

Building Block Tuning

Table 3-1 provides the full list of building blocks that we recommend you edit to reduce the number of false positives generated by QRadar SIEM. For more information on false positives, see **Tuning False Positives**.

You can edit the building blocks listed in the table if you have certain server types present on the networks that you want to monitor. If you do not have these server types on the network you want to monitor, you can choose to skip this step.

To edit these building blocks, you must add the IP address or IP addresses of the server or servers into the appropriate building blocks.

For more information, see the *IBM Security QRadar SIEM Administration Guide*. Also, see **Identifying Network Assets**.

Table 3-1 List of Recommended Building Blocks to Edit.

Building Block	Description
BB:NetworkDefinition: NAT Address Range	Edit the **and where either the source or destination IP is one of the following** test to include the IP addresses of the Network Address Translation (NAT) servers.
	We recommend that you only edit this building block if you have detection in the non-NATd address space. Editing this building block means that offenses are not created for attacks targeted or sourced from this IP address range.
BB:HostDefinition: Network Management Servers	Network management systems create traffic, such as ICMP (Internet Control Message Protocol) sweeps, to discover hosts. QRadar SIEM may consider this threatening traffic. To ignore this behavior and define network management systems, edit the **and when either the source or destination IP is one of the following** test to include the IP addresses of the following:
	• Network Management Servers (NMS).
	• Other hosts that normally perform network discovery or monitoring.
BB:HostDefinition: Proxy Servers	Edit the **and when either the source or destination IP is one of the following** test to include the IP addresses of the proxy servers.
	We recommend that you edit this building block if you have sufficient detection on the proxy server. Editing this building block prevents offense creation for attacks targeted or sourced from the proxy server.This is useful when hundreds of hosts use a single proxy server and that single IP address of the proxy server may be infected with spyware.
BB:HostDefinition: VA Scanner Source IP	Vulnerability assessment products launch attacks that can result in offense creation. To avoid this behavior and define vulnerability assessment products or any server you want to ignore as a source, edit the **and when the source IP is one of the following** test to include the IP addresses of the following:
	• VA Scanners
	• Authorized Scanners
BB:HostDefinition: Virus Definition and Other Update Servers	Edit the **and when either the source or destination IP is one of the following** test to include the IP addresses of virus protection and update function servers.

Table 3-1 List of Recommended Building Blocks to Edit.

Building Block	Description
BB:Category Definition: Countries with no Remote Access	Edit the **and when the source is located in** test to include geographic locations which should be prevented from accessing your network. This enables the use of rules, such as **anomaly: Remote Access from Foreign Country** to create an offense when successful logins have been detected from remote locations.
BB:ComplianceDefinition: GLBA Servers	Edit the **and when either the source or destination IP is one of the following** test to include the IP addresses of servers used for GLBA (Gramm-Leach-Bliley Act) compliance. By populating this building block you can use rules such as **Compliance: Excessive Failed Logins to Compliance IS**, which create offenses for compliance and regulation based situations.
BB:ComplianceDefinition: HIPAA Servers	Edit the **and when either the source or destination IP is one of the following** test to include the IP addresses of servers used for HIPAA (Health Insurance Portability and Accountability Act) Compliance. By populating this building block, you can use rules, such as **Compliance: Excessive Failed Logins to Compliance IS**, which creates offenses for compliance and regulation based situations.
BB:ComplianceDefinition: SOX Servers	Edit the **and when either the source or destination IP is one of the following** test to include the IP addresses of servers used for SOX (Sarbanes-Oxley Act) Compliance. By populating this building block, you can use rules, such as **Compliance: Excessive Failed Logins to Compliance IS**, which creates offenses for compliance and regulation based situations.
BB:ComplianceDefinition:PCI DSS Servers	Edit the **and when either the source or destination IP is one of the following** test to include the IP addresses of servers used for PCI DSS (Payment Card Industry Data Security Standards) Compliance. By populating this building block, you can use rules such as **Compliance: Excessive Failed Logins to Compliance IS**, which creates offenses for compliance and regulation based situations.
BB:NetworkDefinition: Broadcast Address Space	Edit the **and when either the source or destination IP is one of the following** test to include the broadcast addresses of your network. This removes false positive events that may be caused by the use of broadcast messages.
BB:NetworkDefinition: Client Networks	Edit the **and when the local network is** test to include workstation networks that users are operating.
BB:NetworkDefinition: Server Networks	Edit the **when the local network is** test to include any server networks.
BB:NetworkDefinition: Darknet Addresses	Edit the **and when the local network is** test to include the IP addresses that are considered a Darknet. Any traffic or events directed towards a Darknet is considered suspicious as no hosts should be on the network.

Table 3-1 List of Recommended Building Blocks to Edit.

Building Block	Description
BB:NetworkDefinition: DLP Addresses	Edit the **and when the any IP is a part of any of the following** test to include the remote services that may be used to obtain information from the network. This can include services, such as webmail hosts or file sharing sites.
BB:NetworkDefinition: DMZ Addresses	Edit the **and when the local network** test to include networks that are considered to be part of the network's DMZ.
BB:PortDefinition: Authorized L2R Ports	Edit the **and when the destination port is one of the following** test to include common ports that are allowed outbound on the network.
BB:NetworkDefinition: Watch List Addresses	Edit the **and when the local network is** to include the remote networks that are considered to be on a watch list. This enables you to identify when events occur with hosts of interest.
BB:FalsePositive: User Defined Server Type False Positive Category	Edit this building block to include any categories you want to consider false positives for hosts defined in the BB:HostDefinition: User Defined Server Type building block.
BB:FalsePositive: User Defined Server Type False Positive Events	Edit this building block to include any events you want to consider false positives for hosts defined in the BB:HostDefinition: User Defined Server Type building block.
BB:HostDefinition: User Defined Server Type	Edit this building block to include the IP address of your custom server type. After you have added the servers, add any events or categories you want to consider false positives to this server as defined in the BB:FalsePositives: User Defined Server Type False Positive Category or the BB:False Positives: User Defined Server Type False Positive Events building blocks.

NOTE

You can include a CIDR range or subnet in any of the building blocks instead of listing the IP addresses. For example:192.168.1/24 includes addresses 192.168.1.0 to 192.168.1.255. You can also include CIDR ranges in any of the BB:HostDefinition building blocks.

Editing a Building Block

To edit a building block:

Step 1 Click the **Offenses** tab.

Step 2 On the navigation menu, click **Rules**.

Step 3 From the **Display** drop-down list box, select **Building Blocks**.

Step 4 Double-click the building block you want to edit. See **Table 3-1** for a list of building blocks we recommend that you populate with your network information.

The Rule Wizard window is displayed.

Step 5 Update the building block as required.

Step 6 Click **Finish**.

Tuning Methodology How you tune QRadar SIEM depends on different scenarios and whether you have one target or many targets within your network. The following table provides guidance on how to tune false positives according to these differing scenarios:

Table 3-2 Tuning Methodology.

Scenario	One Target	Many Targets
One attacker, one event	Use the False Positive Wizard to tune this specific event.	Use the False Positive Wizard to tune specific event.
One attacker, many unique events in the same category	Use the False Positive Wizard to tune the category.	Use the False Positive Wizard to tune the category.
Many attackers, one event	Use the False Positive Wizard to tune the specific event.	Edit building blocks using the Custom Rules Editor to tune specific event.
Many attackers, many events in the same category	Use the False Positive Wizard to tune the category.	Edit building blocks using the Custom Rules Editor to tune the category.
One attacker, many unique events in different categories	Investigate the offense and determine the nature of the attacker. If the offense or offenses can be tuned out, edit building blocks using the Custom Rules Editor to tune categories for the host IP.	Investigate the offense and determine the nature of the attacker. If the offense or offenses can be tuned out, edit building blocks using the Custom Rules Editor to tune categories for the host IP.
Many attackers, many unique events in different categories	Edit building blocks using the Custom Rules Editor to tune the categories.	Edit building blocks using the Custom Rules Editor to tune the categories.

Tuning False Positives You can use the False Positive Tuning function to tune out false positive events and flows from creating offenses. You must have appropriate permissions for creating customized rules to tune false positives. For more information on roles and permissions, see the *IBM Security QRadar SIEM Administration Guide*.

To tune a false positive event or flow:

Step 1 Click the **Log Activity** tab, or alternatively click the **Network Activity** tab.

Step 2 Select the event or flow you want to tune.

Step 3 Click **False Positive**.

NOTE
If you are viewing events or flows in streaming mode, you must pause streaming before you click **False Positive**.

The False Positive page is displayed with information derived from the selected event or flow.

Step 4 Select one of the following **Event** or **Flow Property** options:

- Event/Flow(s) with a specific QID of <Event>
- Any Event/Flow(s) with a low-level category of <Event>
- Any Event/Flow(s) with a high-level category of <Event>

Step 5 Select one of the **Traffic Direction** options:

- <Source IP Address> to <Destination IP Address>.
- <Source IP Address> to Any Destination
- Any Source to <Destination IP Address>
- Any Source to any Destination

Step 6 Click **Tune**.

NOTE
QRadar SIEM prevents you from selecting **Any Events/Flow(s)** and **Any Source To Any Destination**. This creates a custom rule and prevents QRadar SIEM from creating offenses.

For more information on tuning false positives, see the *IBM Security QRadar SIEM Users Guide*.

Best Practices: Tuning Methodology

To ensure reliable system performance, we recommend you consider the following best practice guidelines:

- Disable rules that produce numerous unwanted offenses.
- To tune CRE rules, increase the rule threshold by doubling the numeric parameters and time interval.
- Consider modifying rules to consider local rather than remote network context.
- When you edit a rule with the **attach events for the next 300 seconds** option enabled, wait 300 seconds before closing the related offenses.

False Positive Rule Chains

The rule **FalsePositive: False Positive Rules and Building Blocks** is the first rule to execute in the CRE. When it loads, all of its dependencies are loaded and tested.

If the rule is successfully matched in QRadar SIEM, the rule drops the detected event or flow. This stops the event or flow from progressing through the CRE and prevents the flow or event from creating an offense.

False Positive Rule Chains

When creating false positive building blocks within QRadar SIEM, we recommend the following:

- Mirror a methodology similar to the default rule set by creating new building blocks with the following naming convention:

  <CustomerName>-BB:False Positive: All False Positive Building Blocks.

  Where <CustomerName> is a name you assign to the false positive building block.

- Building blocks should contain the test **and when a flow or an event matches any of the following rules**. This is used as a collection point for all the false positive building blocks and will enable you to quickly find and identify the customizations within your site.

- When the <CustomerName>-BB:False Positive: All False Positive Building Block is created, add it to the test in the rule **FalsePositive: False Positive Rules and Building Blocks**.

- When the new false positive building block is created, you can create new building blocks to match the traffic you want to prevent from creating offenses. Add these building blocks to the <CustomerName>-BB:False Positive: All False Positive Building block.

NOTE

To prevent events from creating offenses, the most accurate method is to create a new building block that matches the exact traffic you are interested in. Save this as a building block <CustomerName>-BB:False Positive: <name of rule>, then edit <CustomerName>-BB:False Positive: All False Positive building blocks, to include the rule that you created.

CAUTION

If you add a rule or building block that includes a rule to the FalsePositive: False Positive Rules and Building Blocks rule, the rule you have added will execute before the event is dropped by the CRE and could create offenses by overriding the false positive test.

Optimizing Custom Rules

When building custom rules, we recommend that you optimize the order of the testing. This ensures that the rules do not slow down the CRE. The tests in a rule are executed in the order in which they are displayed in the user interface.

The most memory intensive tests for the CRE are the payload and regular expression searches. To ensure these tests run against a smaller subset of data and execute faster, we strongly recommend you first include one of the following tests:

- **when the event(s) were detected by one or more of these log source types**
- **when the event QID is one of the following QIDs**
- **when the source IP is one of the following IP addresses**
- **when the destination IP is one of the following IP addresses**
- **when the local IP is one of the following IP addresses**
- **when the remote IP is one of the following IP addresses**
- **when either the source or destination IP is one of the following IP addresses**
- **when the event(s) were detected by one of more of these log sources**

NOTE

You can further optimize QRadar SIEM by exporting common tests to building blocks. Building Blocks execute per event as opposed to multiple times if tests are individually included in a rule.

For more information on optimizing custom rules, see the *IBM Security QRadar SIEM Users Guide*.

Creating an OR Condition within the CRE

As you add more tests to a rule, each test can only be an AND or AND NOT conditional test. To create an OR condition within the CRE put each separate set of conditions into a building block and then create a new rule or building block that utilizes the **And When An Event Matches Any Of The Following Rules** rule. This will ensure both Building Blocks are loaded when the test is applied.

To create an OR condition:

Step 1   Click the **Offenses** tab.

Step 2   On the navigation menu, click **Rules**.

Step 3   From the **Actions** list box, select one of the following options:

- **New Event Rule** - Select this option to configure a rule for events.
- **New Flow Rule** - Select this option to configure a rule for flows.
- **New Common Rule** - Select this option to configure a rule for events and flows.
- **New Offense Rule** - Select this option to configure a rule for offenses.

The Rule Wizard window is displayed.

NOTE

If you do not want to view the Welcome message on the Rules Wizard page again, select the **Skip this page when running the rules wizard** check box.

Step 4   Read the introductory text. Click **Next**.

You are prompted to choose the source from which you want this rule to apply. The default is the rule type you selected on the **Offenses** tab.

Step 5   If required, select the rule type you want to apply to the rule. Click **Next**.

The Rule Wizard - Rule Test Stack Editor is displayed.

Step 6   Locate the **when an event matches any/all of the following rules** test and click the **+** icon beside the test.

The selected test is displayed in the Rule pane.

Step 7   On the **and when an event matches any of the following rules** test, click **rules.**

The Rule Wizard window is displayed.

Step 8   From the **Select the rule(s) to match and click 'Add'** field, select multiple building blocks by holding down the Ctrl key and click **Add +**.

The selected building blocks are displayed in the Selected Items pane.

Step 9   Click **Submit**.

The selected building blocks are displayed in the Rule pane.

Making Searches Faster

When you are performing data searches with QRadar SIEM's Event and Flow viewer, we recommend adding filters to search indexed fields. This will minimize the search time.

Table 3-3 provides information on the fields that are indexed:

Table 3-3   Log Viewer and Flow Viewer Indexed Fields

QRadar SIEM **Tab**	**Indexed Filter**
Log Activity tab (Events)	Username
	Source or Destination IP
	Destination Port
	Has Identity
	Device Type
	Device ID
	Category
	Matches Custom Rule
Network Activity tab (Flows)	Application
	Source or Destination IP
	Destination Port

NOTE

You can monitor the performance of your search by expanding the **Current Statistics** option on the **Search** page, this will display how much data is being loaded from data files and indexes. If your search is not displaying a count in the index file count, add an indexed filter to the search. For more information, see **Adding Indexed Filters**.

Adding Indexed Filters

Indexed filters can be added to both log activity and network activity data.

To add indexed filters:

Step 1 Click the **Log Activity** tab, or alternatively click the **Network Activity** tab.

Step 2 On the toolbar, click **Add Filter**.

Step 3 From the first drop-down list box, select your preferred index filter.

For more information on the indexed fields used to filter events and flows, see table **Table 3-3**.

Step 4 From the second drop-down list box, select the modifier you want to use.

Step 5 Type or select the specific information for your filter. The controls that are displayed depend on the index filter you selected in **Step 3**.

Step 6 Click **Add Filter**.

Quick Filter Option For installations of QRadar SIEM 7.0 MR3 and above, you can enable a new feature called Quick Filter. This option must be enabled in the System Settings page. For more information, see **Enable Quick Filter Option**.

You can use the new Quick Filter option in the Event and Flow viewer. The quick filter searches the payload in the events or flows and returns matching results. Since this search is a free text search you can type your exact search criteria.

Enable Quick Filter Option

To enable the quick filter option:

Step 1 Click the **Admin** tab.

Step 2 Click **System Settings**.

Step 3 From the **Beta Features** panel select the following options:

a **Event Payload Indexing - Yes**

b **Flow Payload Indexing - Yes**

c **Payload Index Retention - <Time Period>**

Where **<Time Period>** is the amount of time you want to store event and payload indexes. The default setting is 1 week.

Step 4 Click **Save** to close the System Settings window.

Step 5 Click **Deploy Changes**.

Report Optimization The reporting engine functions similarly to the log viewer. By optimizing your searches to include indexed fields, you can reduce the impact of generating reports. Report Generation times do not need to be staggered as they are executed serially by the reporting engine.

Custom Extracted Properties The Custom Extracted Properties function in QRadar SIEM is used to expand normalized fields by adding numerous custom fields for reports, searches, and the CRE. For example, to extract proxy URLs, virus names, or secondary usernames.

When creating extracted properties in QRadar SIEM, we recommend that they are restricted to a particular log source type or individual log source.

NOTE

If your extracted property is only applicable to certain events, you can reduce the workload on your QRadar SIEM system by limiting the extracted property to only that event type.

By using the extracted properties function to optimize for rules, reports and searches, the custom property can be used by the custom rules engine. This moves the processing of the extracted property to the time when the event is collected, as opposed to when it is searched (by default custom extracted properties are processed when they are searched or displayed). Enabling the

optimize feature for an extracted property minimizes the search time against the property.

NOTE
The extracted property field is not indexed, but if an event matches the property, it will store an index to the offset and length of the property which reduces the amount of data that has to be searched.

Cleaning the SIM Model

When the tuning process is complete, we recommend that you clean the SIM model. This ensures that QRadar SIEM only displays recent offenses. This function ensures that offenses are based on the most current rules, discovered servers, and network hierarchy. When you clean the SIM model, all existing offenses are closed, but this does not affect existing events and flows.

NOTE
False positive offenses could have occurred before you performed the tuning tasks. We recommend that you clean the SIM model to ensure each host on the network creates new offenses based on the current configuration.

To clean the SIM model:

Step 1 Click the **Admin** tab.

Step 2 From the Admin toolbar, select **Advanced > Clean SIM Model**.

Step 3 Select the **Hard Clean** option.

Step 4 Select the **Are you sure you want to reset the data model?** check box.

Step 5 Click **Proceed**.

A message is displayed indicating that the SIM reset process has started. This process may take several minutes, depending on the volume of data in your system.

Step 6 When the SIM reset process is complete, refresh your browser.

NOTE
If you attempt to navigate to other areas of the user interface during the SIM reset process, an error message is displayed.

A   IDENTIFYING NETWORK ASSETS

This section provides a reference for identifying network assets that you might want to include in building blocks.

Table 5-4   Identifying Network Assets

Category	How to Identify and Examples	Building Block
NAT Address	IP addresses and/or CIDR blocks used for Network Address Translation (NAT). These are commonly configured on firewalls and routers.	BB-NetworkDefinition: NAT Address Range.
Network and Desktop Management Servers	Altiris, BindView, CA Unicenter, CiscoWorks, Dell OpenManage, HP OpenView, IBM Director, Marimba, McAfee ePolicy Orchestrator, Norton Antivirus server, Tivoli, Sitescope, Sophos server, SMS, What's Up Gold	BB-HostDefinition:Network Management Servers.
Proxy Servers	In-Line PaloAlto firewalls, Sidewinder, ISA, Bluecoat, Microsoft Proxy Server, Squid, Websense, Wingate	BB-HostDefinition: Proxy Servers.
Server Networks	CIDRs used by data centers or server populations.	BB-HostDefinition: Server Networks.
Vulnerability/ Security Scanners	Acunetix, CyberCop Scanner, Foundstone, HackerShield, ISS Internet Scanner, Nessus, Retina, nCircle, Nmap.	BB-HostDefinition: VA Scanner Source ID.

B GLOSSARY

CIDR See Classless Inter-Domain Routing (CIDR).

Classless Inter-Domain Routing (CIDR) Addressing scheme for the internet, which allocates and specifies internet addresses used in inter-domain routing. With CIDR, a single IP address can be used to designate many unique IP addresses.

CRE See Custom Rules Engine (CRE)

Custom Rules Engine The collection of rules that QRadar SIEM uses to correlate event and flow information into offenses.

Demilitarized Zone (DMZ) A demilitarized zone, or perimeter network, is a network area located between an organization's internal network and external network, usually the internet. It is separated by a firewall which only allows certain types of network traffic to enter or leave.

Device Support Module (DSM) Device Support Modules (DSMs) allow you to integrate QRadar SIEM with log sources.

DNS See Domain Name System (DNS).

Domain Name System An online, distributed database used to map human-readable machine names into an IP address for resolving machine names to IP addresses.

DSM See Device Support Module (DSM).

egress traffic Network traffic that begins inside a network and proceeds to a destination somewhere outside of the network.

event Record from a device that describes an action on a network or host.

Event Collector Collects security events and flows from various types of devices in your network. The Event Collector gathers events and flows from local, remote, and device sources. The Event Collector then normalizes the events and flows, and sends the information to the Event Processor.

Event Processor	Processes events collected from one or more Event Collector(s). The events are bundled once again to conserve network usage. Once received, the Event Processor correlates the information from QRadar SIEM and distributed to the appropriate area, depending on the type of event.
false positive	When an event is tuned as a false positive, the event no longer contributes to custom rules. Therefore, offenses do not generate based on the false positive event. The event is still stored in the database and contributes to reports.
flow	Communication session between two hosts. Describes how traffic is communicated, what was communicated (if content capture option has been selected), and includes such details as when, who, how much, protocols, priorities, or options.
flow data	Specific properties of a flow including: IP addresses, ports, protocol, bytes, packets, flags, direction, application ID, and payload data (optional).
flow logs	Record of flows that enables the system to understand the context of a particular transmission over the network. Flows are stored in flow logs.
flow sources	Source of flows that the QFlow Collector receives. Using the deployment editor, you can add internal and external flow sources from either the System or Event Views in the deployment editor.
GLBA	See Gramm-Leach-Bliley Act (GLBA).
Gramm-Leach-Bliley Act	Also known as the Financial Services Modernization Act of 1999, GLBA allows banking, securities and insurance companies to combine investment banking, commercial banking, and insurance activities.
Health Insurance Portability and Accountability Act (HIPPA)	A series of laws and regulations, organizations must comply with to demonstrate they are protecting the private health information of patients and customers.
HIPPA	See Health Insurance Portability and Accountability Act (HIPPA).
ICMP	See Internet Control Message Protocol (ICMP).
Internet Control Message Protocol (ICMP)	Part of the internet protocol suite, normally used by the operating systems of networked computers to send error messages.
Ingress Traffic	Network traffic originating from outside of the network and proceeding to a destination inside of the network.
Internet Protocol (IP)	The method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP

address that uniquely identifies it from all other systems on the Internet. An IP address includes a network address and a host address. An IP address can also be divided by using classless addressing or subnetting.

Internet Relay Chat	A set of scripts or an independent program that connects to internet relay chat as a client, and so appears to other IRC users as another user.
IP	See Internet Protocol.
IRC	See Internet Relay Chat (IRC).
J-Flow	A proprietary accounting technology used by Juniper® Networks that allows you to collect IP traffic flow statistics.
log source	Log sources are external event log sources such as security equipment (for example, firewalls and IDSs) and network equipment (for example, switches and routers).
NetFlow	A proprietary accounting technology developed by Cisco Systems® Inc. that monitors traffic flows through a switch or router, interprets the client, server, protocol, and port used, counts the number of bytes and packets, and sends that data to a NetFlow collector. You can configure QRadar SIEM to accept NDE's and thus become a NetFlow collector.
offense	A message sent or event generated in response to a monitored condition. For example, an offense informs you if a policy has been breached or the network is under attack.
Packeteer	Packeteer devices collect, aggregate, and store network performance data. Once you configure an external flow source for Packeteer, you can send flow information from a Packeteer device to QRadar SIEM.
Payment Card Industry Data Security Standard (PCI DSS)	An information security standard for organizations handling payment card information. It is used to increase controls and demonstrate compliance in the handling of sensitive data.
PCI DSS	See Payment Card Industry Data Security Standard (PCI DSS).
QFlow Collector	Collects data from devices and various live or recorded data feeds, such as, network taps, span/mirror ports, NetFlow, and QRadar SIEM flow logs.
Sarbanes-Oxley (SOX)	Legislation that protects shareholders and the general public from accounting errors and fraudulent practice by defining rules around the storage and handling of electronic records and data.

sFlow	A multi-vendor and end-user standard for sampling technology that provides continuous monitoring of application level traffic flows on all interfaces simultaneously.
SOX	See Sarbanes-Oxley Act (SOX).
UDP	See User Datagram Protocol (UDP).
User Datagram Protocol	A connectionless transport layer protocol which provides a simple message service for transaction-oriented services.
Virtual Private Network	A Virtual Private Network simulates a private network over the public internet by encrypting communications between the two private end-points.
Voice Over IP	VOIP uses the internet protocol to transmit voice as packets over an IP network.
VOIP	See Voice Over IP (VOIP).
VPN	See Virtual Private Network (VPN).

C NOTICES AND TRADEMARKS

What's in this appendix:

- **Notices**
- **Trademarks**

This section describes some important notices, trademarks, and compliance information.

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

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

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 states 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 Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply 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 Corporation
170 Tracer Lane,
Waltham MA 02451, USA

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

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.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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.

All 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 the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

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*.

The following terms are trademarks or registered trademarks of other companies:

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

INDEX