WinCollect User Guide

QRadar 7.1

September 2012

DO09242012-A

http://www.q1labs.com

Q1 Labs, Inc., an IBM Company
170 Tracer Lane
Waltham, MA 02451 USA

ABOUT THIS GUIDE

1 WINCOLLECT OVERVIEW

2 INSTALLING WINCOLLECT

3 MANAGING WINCOLLECT SOURCES

INDEX

ABOUT THIS GUIDE

The *WinCollect User Guide* provides you with information for installing and configuring WinCollect agents and Windows-based log sources for use with QRadar.

Intended Audience

This guide is intended for the system administrator responsible for setting up Windows event sources or WinCollect agents for QRadar in your network. This guide assumes that you have QRadar administrative 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

You can access technical documentation, technical notes, and release notes directly from the Qmmunity website at *https://qmmunity.q1labs.com/*. Once you access the Qmmunity website, locate the product and software release for which you require documentation.

Your comments are important to us. Please send your e-mail comments about this guide or any of the Q1 Labs documentation to:

documentation@q1labs.com.

Include the following information with your comments:

- Document title
- Page number

Contacting Customer Support

To help you resolve any issues that you may encounter when installing or maintaining QRadar, you can contact Customer Support as follows:

- Log a support request 24/7: *https://qmmunity.q1labs.com/support/*

  To request a new Qmmunity and Self-Service support account, send your request to *welcomecenter@q1labs.com*. You must provide your invoice number to process your account.
- Telephone assistance:
  - **US/Canada** - 1.866.377.7000
  - **International** - (01) 506.462.9117
  - **UK** - 028 9031 7991
- Forums: Access our Qmmunity Forums to benefit from our customer experiences.

Trademarks

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

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

1 WinCollect Overview

WinCollect is a stand-alone Windows application (agent), which resides on a host in your network to allow QRadar to manage and collect Windows-based events. The Wincollect agent collects Windows-based events from local or remote Windows systems by adding individual or bulk WinCollect log sources in QRadar. Your QRadar Console can provide centralized management and configurations your Windows-based log sources for a large number of WinCollect agents. All WinCollect agents deployed in your network are managed through the **Admin** tab on your QRadar Console. Each WinCollect agent deployed in your network can collect and forward events to your QRadar Console using syslog. The following image shows a typical WinCollect deployment of two WinCollect agents.

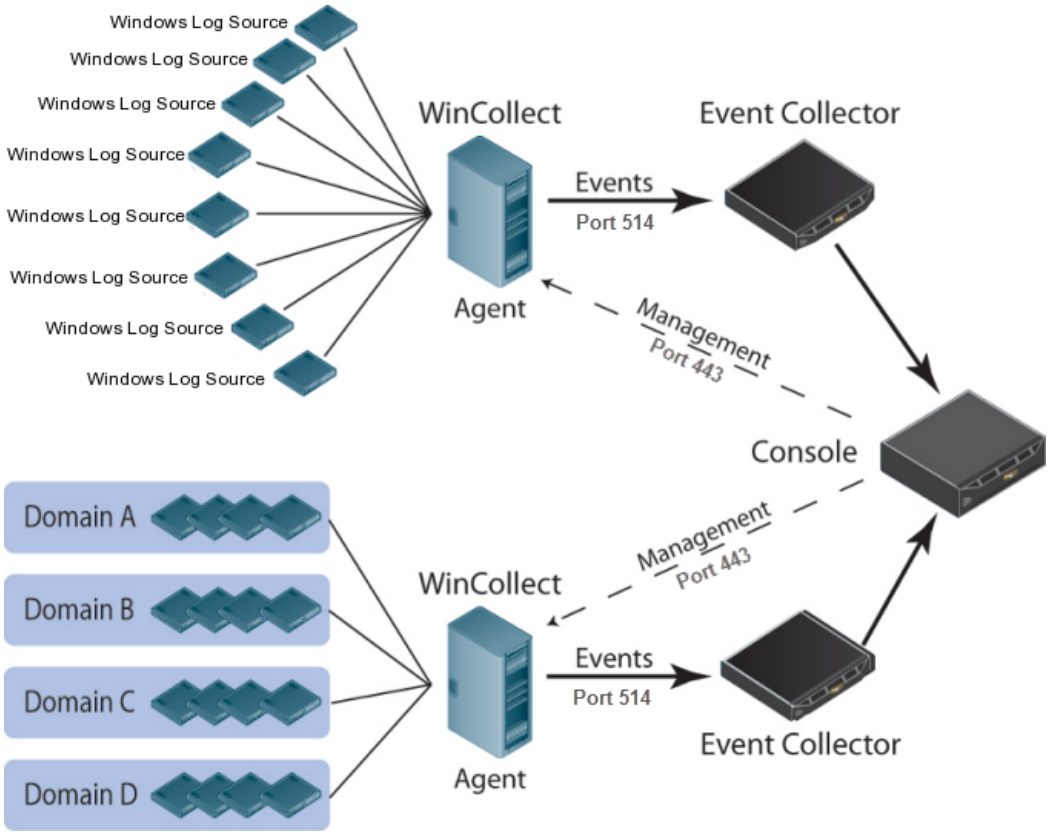

Figure 1-1 A standard WinCollect agent deployment reporting to the QRadar Console.

The Windows log sources can be added individually or bulk added to the WinCollect agent to capture information, warning, error, success audit, and failure audit severity messages.

The following Windows event types are collected:

- **Application Log** - Contains events logged by programs. For example, a database program recording a file error to the application log.
- **Security Log** - Contains security-based events and resource use events. For example, valid and invalid logon attempts or creating, opening, or deleting files from a resource.

  You must be an administrator or a member of the administrators group to enable, use, and specify the events you want to record in the security log.
- **System Log** - Contains events logged by Windows system components. For example, if a driver fails to load during startup, an event is recorded in the system log. Your Windows-based operating system is preconfigured with the events that are logged by system components.
- **Directory Service Log** - Contains events logged by the Active Directory domain controller. For example, authentication failures when users attempt to log in to a network resource.
- **DNS Server Log** - Contain events related to the resolution of DNS names to IP addresses. For example, if the DNS server was unable to open a socket for communication or if the DNS service is shut down.
- **File Replication Service Log** - Contains events related to replication between domain controllers. For example, if an error occurs when a volume attempts to replicate.

NOTE The WinCollect icon is located on the **Admin** tab of QRadar, but is only visible after you complete the installation of the WinCollect protocol.

You are ready to install the WinCollect components for your QRadar Console and install WinCollect agents in your network. For more information, see **Installing WinCollect**.

2 INSTALLING WINCOLLECT

The WinCollect agent can be installed on any Windows-based host in your network. WinCollect agents can be distributed in your organization in a remote collection configuration or installed on the local host. The installation and number of WinCollect agent installations in your deployment is dependant on the available resources in your network, as only one WinCollect agent can be installed on a host. The following WinCollect installation methods are available:

- **Local Collection** - The WinCollect agent is installed locally on several hosts and collecting events for the local host. This type of installation is common for network assets that are very busy or have limited resources.
- **Remote Collection** - The WinCollect agent is installed on a single host to collect events from multiple Windows systems. Remote collection allows you to easily scale the number of Windows log sources you can monitor by adding physical or virtual Windows hosts in your network that include a WinCollect agent. To collect from remote Windows-based operating systems, you must bulk add or individually add log sources to your WinCollect agent. The **Log Source Identifier** field determines which remote Windows sources the WinCollect agent polls for events. The log source must contain an identifier with the IP address or hostname for the remote Windows source and the proper credentials to poll for events.

NOTE To access event logs from a domain controller, you must configure the log source with a username and password containing domain administrator security credentials. This is required because domain controller logs are accessed from an administrative share.

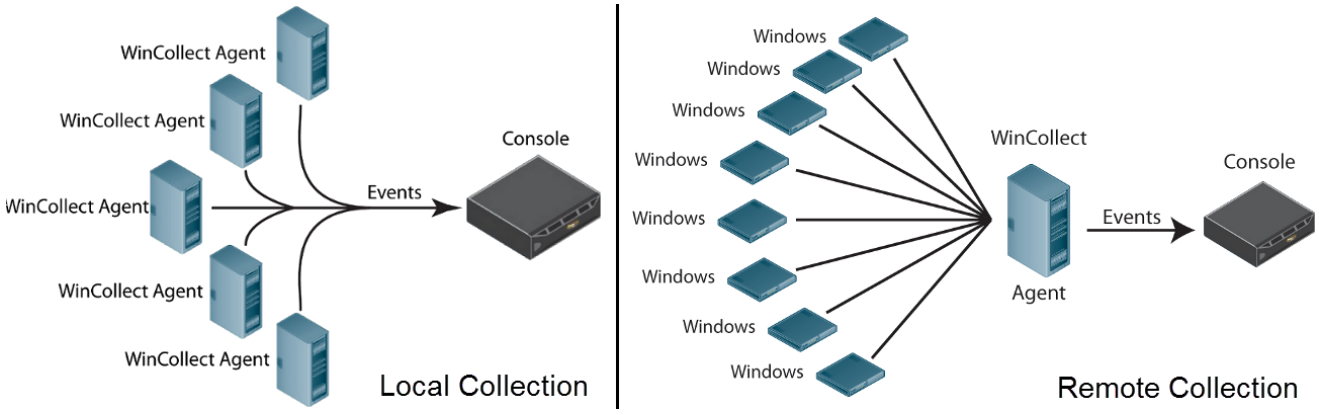

Figure 2-1 Two methods of gathering events are supported: local and remote collection.

This section includes the following topics:

Before You Begin

Before you can begin installing WinCollect agents, you must verify your deployment meets the installation criteria.

This section includes the following topics:

General Requirements

The QRadar Console must be installed with QRadar 7.1 or QRadar 7.0 Maintenance Release 5 Patch 2 (7.0.0.342942).

Port Requirements

Ensure any firewalls located between the QRadar Console and WinCollect allows traffic on the following ports:

- **Port 443 (HTTPS)** - Port 443 is required for communication and management of the WinCollect agent from the QRadar Console. Port 443 is used for features such as the heartbeat and configuration updates.
- **Port 514 (Syslog Events)** - Port 514 is required for the WinCollect agent to forward syslog events. WinCollect log sources can be configured to provide events using TCP or UDP. Depending on your configuration requirements, you can decide which transmission protocol is required for each WinCollect log source.

WinCollect Host Requirements

The Windows system hosting the WinCollect agent must meet the following requirements:

- 8GB of RAM (2GB reserved for the WinCollect agent)
- Intel Core 2 Duo processor 2.0 GHz or better
- 3 GB of available disk space for software and log files
- At minimum, 20% of the available processor resources
- The physical or virtual host system for the WinCollect agent must be installed with one of the following operating systems:
  - Windows Server 2003
  - Windows Server 2008
  - Windows 7
  - Windows Vista
- Administrative privileges to install the WinCollect agent

NOTE

Only one WinCollect agent should be installed on a host at a time.

Tested Event Per Second Rates

Before you install WinCollect agents in your network, it is important to understand your expected event per second (EPS) rate. EPS rates can help you determine how many local or remote WinCollect agents you require in your network. The following table describes our test environment:

Table 2-1 WinCollect Test Environment

Installation Type	EPS	Log Sources
Remote Collection	10	100
Local Collection	250	1

The table above describes an environment where we configured a remote collection network and bulk added 100 Windows-systems as log sources that were providing 10 EPS each. We also tested installing the WinCollect agent to collect events from a single host that is providing 250 EPS. This table can be used as an initial guideline for planning your WinCollect agent deployment. This table represents our test environment. If your Windows log sources provide a higher or lower EPS rate, you can adjust the number of log sources managed by your WinCollect agent accordingly.

CAUTION

Exceeding these initial guidelines can cause you to experience performance issues or event loss, especially on busy systems. If your deployment is at the upper limit of these guidelines, we recommend installing additional physical or virtual systems for WinCollect agents in your network.

Collected Events

The WinCollect agent can only collect events from the following Windows operating systems:

- Windows Server 2003
- Windows Server 2008
- Windows 7
- Windows Vista
- Windows XP

NOTE

WinCollect does not support event collection from Windows 2000 operating systems.

Installing WinCollect Components for QRadar

Before you install WinCollect agents in your network, you must install the WinCollect DSM and WinCollect protocol on your QRadar Console.

The section includes the following topics:

- **Installing the WinCollect DSM**
- **Installing the WinCollect Protocol Manually**

Installing the WinCollect DSM

The WinCollect Device Support Module (DSM) allows QRadar to properly parse syslog events from WinCollect sources and categorize unique events from WinCollect agents by their QRadar Identification (QID) map. If your environment does not allow auto updates for DSMs and protocols, you might be required to manually install or update the WinCollect DSM.

To manually install the WinCollect DSM:

Step 1 Download the WinCollect DSM from the Qmmunity website to your QRadar Console.

https://qmmunity.q1labs.com/

For access to Qmmunity, contact Customer Support.

Step 2 Using SSH, log in to QRadar as the root user.

Username: **`root`**

Password: **`<password>`**

Step 3 Navigate to the directory that includes the WinCollect DSM.

Step 4 Type the following command:

```
rpm -Uvh <filename>
```

Where **`<filename>`** is the name of the WinCollect DSM. For example,

```
rpm -Uvh DSM-WinCollect-7.0.0-<version>.noarch.rpm
```

Step 5 Log in to QRadar.

https://**<IP Address>**

Where **<IP Address>** is the IP address of the QRadar Console.

Step 6 On the **Admin** tab, click **Deploy Changes**.

You are now ready to install the WinCollect protocol.

Installing the WinCollect Protocol Manually

Installing protocols allow you to access additional information or communicate with remote devices. The WinCollect protocol allows QRadar to communicate with the Windows-based operating systems hosting the WinCollect agent. The WinCollect protocol is also responsible for enabling the WinCollect icon from the **Admin** tab in QRadar. If your environment does not allow auto updates for DSMs and protocols, you might be required to manually install or update the WinCollect protocol.

To manually install the WinCollect protocol:

Step 1 Download the WinCollect protocol file from the Qmmunity website to your QRadar Console.

https://qmmunity.q1labs.com/

For access to Qmmunity, contact Customer Support.

Step 2 Using SSH, log in to your QRadar Console as the root user.

Username: **root**

Password: **<password>**

Step 3 Navigate to the directory that includes the WinCollect protocol.

Step 4 Type the following command:

rpm -Uvh <filename>

Where **<filename>** is the name of the downloaded file. For example:

rpm -Uvh PROTOCOL-WinCollect-2.0.noarch.rpm

Step 5 Log in to QRadar.

https://**<IP Address>**

Where **<IP Address>** is the IP address of the QRadar Console.

Username: **root**

Password: **<password>**

Step 6 Click the **Admin** tab.

Step 7 Select **Advanced > Deploy Full Configuration**.

CAUTION

*Selecting **Deploy Full Configuration** restarts multiple services on the QRadar system. Event collection is unavailable on QRadar until the deployment completes.*

Step 8 Using SSH, log in to your QRadar Console as a root user.

Step 9 Type the following command to restart the Tomcat service:

```
service tomcat restart
```

After the Tomcat service restarts, then the WinCollect protocol installation is complete. You are now ready to install the WinCollect agent on your Windows host.

Installing the WinCollect Agent

The command-line interface (CLI) allows you to install, uninstall, and update the WinCollect agent without the installation wizard. Command-line installations allow you to deploy WinCollect agents simultaneously to multiple remote systems using any third-party products that provide remote or batch installs, for example, MSI Packaging Tools, Message-Oriented Middleware (MOM), or System Center Configuration Manager (SCCM).

NOTE

Installing the WinCollect agent using the installation wizard is not a supported installation method. You must install the WinCollect agent using the command-line interface.

Installing a WinCollect agent from the command-line is a two-step process:

1. **Authorizing the WinCollect Agent**.
2. **Installing a WinCollect Agent Using the Command- line Interface**.

Authorizing the WinCollect Agent

Any third-party or external applications that interact with QRadar require authentication using authorized services in the **Admin** tab of QRadar. Before you install WinCollect, you must create an authentication token for the WinCollect agent. This authorization token is used in the command-line installation and allows WinCollect to authorize itself to the QRadar Console. You only need to create one authorization token for all of your WinCollect agents that communicate events to your QRadar Console.

To create an authentication token:

Step 1 Click the **Admin** tab.

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

The System Configuration pane is displayed.

Step 3 Click the **Authorized Services** icon.

The Manage Authorized Services window is displayed.

Step 4 Click **Add Authorized Service**.

The Add Authorized Service window is displayed.

Step 5 Configure the following parameters:

Table 2-2 Add Authorized Services Parameters

Parameter	Description
Service Name	Type a name for this authorized service. The name can be up to 255 characters in length. For example, WinCollect Agent.
User Role	From the list box, select **Admin** as the user role for the WinCollect Agent authorized service. The user roles assigned to an authorized service determine the functionality of a service in QRadar.
Expiry Date	Type of select an expiry date using the calendar provided. Alternatively, select the **No Expiry** check box to indicate you don't want this service to expire. The Expiry Date field allows you to define a date when you want this service to expire. If the date defined expires, the service is no longer authorized and a new authorization token needs to be generated by an administrator. By default, the authorized service is valid for 30 days.

Step 6 Click **Create Service**.

A confirmation message is displayed when an authorized service is added to QRadar. This message contains a token value that is required when you install WinCollect using the command-line.

NOTE

We recommend you copy or write down the authentication token as it is required for the WinCollect agent installation. You only need to create one authorization token for all of your WinCollect agents that communicate events to your QRadar Console.

You are now ready to install the WinCollect agent using the command-line interface.

Installing a WinCollect Agent Using the Command-line Interface

After you have created the authorized token, you are ready to install the WinCollect agent on your remote host. The installation must be completed by logging in to the remote host or accessing the WinCollect agent setup file from a shared network drive.

To install a WinCollect agent using the CLI:

Step 1 Download the WinCollect agent setup file from the Qmmunity website to the WinCollect agent host:

https://qmmunity.q1labs.com/

NOTE If you are installing a WinCollect agent remotely, you should verify that other active applications are closed on the remote host before installing the WinCollect.

Step 2 From the desktop, select **Start > Run**.

The Run window is displayed.

Step 3 Type the following command:

```
cmd
```

Step 4 Click **OK**.

The command-line interface (CLI) is displayed.

Step 5 Navigate to the download directory containing the WinCollect agent.

Step 6 Type the following command from the directory containing the WinCollect setup file:

```
AGENT-WinCollect-7.0.0.setup.exe /VERYSILENT /SUPPRESSMSGBOXES
/AUTH_TOKEN=<token> /HOST_IDENTIFIER=<host name>
/CONFIG_CONSOLE_ADDRESS=<QRadar Console>
```

Where:

`<token>` is the authorized token you created in **Step 6**, **Authorizing the WinCollect Agent**.

`<host name>` is the host name or IP address of the Windows system where the WinCollect agent is going to be installed.

`<QRadar Console>` is the IP address of your QRadar Console.

```
AGENT-WinCollect-7.0.0.setup.exe /VERYSILENT /SUPPRESSMSGBOXES
/AUTH_TOKEN=af111ff6-4f30-11eb-11fb-1fc117711111
/HOST_IDENTIFIER=100.100.100.100
/CONFIG_CONSOLE_ADDRESS=100.100.100.101
```

Table 2-3 WinCollect CLI Commands

Parameter	Description
`/VERYSILENT`	The /VERYSILENT command removes the installation progress indicators from the remote installation.
`/SUPPRESSMSGBOXES`	The /SUPPRESSMSGBOXES command suppresses popup message boxes from the installation.

Table 2-3 WinCollect CLI Commands (continued)

Parameter	Description
/AUTH_TOKEN=<token>	The /AUTH_TOKEN command is required by QRadar to authorize the WinCollect service. This parameter is required to install the WinCollect agent. For example, **/AUTH_TOKEN=af111ff6-4f30-11eb-11fb-1fc117711111** For more information on creating an authorization token for WinCollect, see **Authorizing the WinCollect Agent**. ***Note:*** *If the AUTH_TOKEN command is not present, the installation is cancelled. For more information on installation errors, see* **Installation Troubleshooting***.*
/HOST_IDENTIFIER=<host name>	The /HOST_IDENTIFIER command sets the installation location for the WinCollect agent. This parameter is required to install the WinCollect agent. We recommend you use a unique identifier, such as an identifiable name, IP address, or hostname. It is important to clearly identify your WinCollect agents, so you can manage large WinCollect agent deployments. For example, **/HOST_IDENTIFIER=100.10.10.255** or **/HOST_IDENTIFIER=%host%** or **/HOST_IDENTIFIER=VMRack2** ***Note:*** *The at symbol (@) is not allowed in the host identifier field.*
/CONFIG_CONSOLE_ADDRESS=<QRadar Console>	The /CONFIG_CONSOLE_ADDRESS command sets the IP address of your QRadar Console. This parameter is required to install the WinCollect agent. For example, **/CONFIG_CONSOLE_ADDRESS=100.10.10.1** or **/CONFIG_CONSOLE_ADDRESS=hostname** ***Note:*** *This parameter is intended for the QRadar Console only. Do not specify an Event Collector or non-Console appliance in this field. If the CONFIG_CONSOLE_ADDRESS is not present, the installation is cancelled. For more information on installation errors, see* **Installation Troubleshooting***.*

Step 7 Press Enter to install the WinCollect agent on the remote Windows host.

The WinCollect agent is installed on your host. Since the WinCollect is managed through the QRadar Console an interface is not installed on the host for the WinCollect agent.

You are now ready to manage your WinCollect agent and add log sources to QRadar. For more information on managing WinCollect agents, see **Managing WinCollect Sources**.

Uninstalling WinCollect

To uninstall a WinCollect agent from a Windows host:

Step 1 Ensure all applications on your Windows host are closed.

Step 2 From desktop of the WinCollect host, select **Start > Programs > WinCollect > Utility > Uninstall WinCollect**.

A confirmation message is displayed.

Step 3 Click **Yes** to continue.

Once the process is complete, a message is displayed to indicate that WinCollect was removed from your Windows host.

Step 4 Click **OK**.

The WinCollect agent is uninstalled from the host.

Upgrading your WinCollect Agent

As updates and features are added to WinCollect, you might be required to update your WinCollect agents installed on your Windows hosts. To update a WinCollect agent, you must uninstall the existing WinCollect agent from the host, then reinstall the WinCollect agent using the command-line installation instructions.

NOTE Future versions of the WinCollect agent are going to include the ability to update your installations directly through an rpm file installed to the QRadar Console.

Log sources you configured are maintained by the QRadar Console. You are not required to reconfigure log sources after reinstalling an updated WinCollect agent if you use the same WinCollect agent hostname during the WinCollect agent update.

To update a WinCollect agent:

Step 1 Uninstall the WinCollect agent from the remote host. For more information, see **Uninstalling WinCollect**.

Step 2 Download the latest WinCollect agent setup file from the Qmmunity website and copy the files to your WinCollect host:

https://qmmunity.q1labs.com/

NOTE
If you are installing a WinCollect agent remotely, you should verify that other active applications are closed on the remote host before installing the WinCollect.

Step 3 Log in to QRadar.

Step 4 Click the **Admin** tab.

Step 5 On the navigation menu, click **Data Sources**.

The Data Sources pane is displayed.

Step 6 Click the **WinCollect** icon.

The WinCollect agent list is displayed.

Step 7 From the Host Name column, record the name of the WinCollect agent you want to update.

The host name is required later during the reinstallation of the WinCollect agent.

Step 8 Log in to the host for your WinCollect agent.

Step 9 From the desktop, select **Start > Run**.

The Run window is displayed.

Step 10 Type the following command:

```
cmd
```

Step 11 Click **OK**.

The command-line interface (CLI) is displayed.

Step 12 Navigate to the download directory containing the WinCollect agent setup file.

Step 13 Type the following command from the directory containing the WinCollect setup file:

```
AGENT-WinCollect-7.0.0.setup.exe /VERYSILENT /SUPPRESSMSGBOXES
/AUTH_TOKEN=<token> /HOST_IDENTIFIER=<host name>
/CONFIG_CONSOLE_ADDRESS=<QRadar Console>
```

Where:

<token> is the authorized token you created in **Step 6**, **Authorizing the WinCollect Agent**.

<host name> is the host name or IP address of the Windows system where the WinCollect agent is going to be installed.

NOTE
The host name must be identical to the previous WinCollect agent installation on the host. If the name differs, QRadar adds a new WinCollect agent. Using the previous host name allows QRadar to populate the WinCollect agent with the log sources already configured.

<QRadar Console> is the IP address of your QRadar Console.

```
AGENT-WinCollect-7.0.0.setup.exe /VERYSILENT /SUPPRESSMSGBOXES
/AUTH_TOKEN=af111ff6-4f30-11eb-11fb-1fc117711111
```

```
/HOST_IDENTIFIER=100.100.100.100
/CONFIG_CONSOLE_ADDRESS=100.100.100.101
```

Step 14 Press Enter to reinstall the WinCollect agent on the remote Windows host.

The WinCollect agent is installed on your host. After several minutes, QRadar Console copies the saved log source configurations to the updated WinCollect agent on your host.

For more information on installing WinCollect using the command-line, see **Installing a WinCollect Agent Using the Command- line Interface**.

Installation Troubleshooting

The WinCollect agent creates an installation log during the installation process for both standard and command-line installations. The log file contains the installation failure message and pertinent installation information.

The section includes the following topics:

- **Viewing the Installation Log**
- **Installation Log Examples**

Viewing the Installation Log

To view the WinCollect installation log, perform the following steps:

Step 1 Log in to the host of your WinCollect agent.

Step 1 On the desktop, select **Start > Run**.

The Run window is displayed.

Step 2 Type the following:

```
%TEMP%
```

Step 3 Click **OK**.

The Windows Explorer displays the temporary directory.

Step 4 Open the WinCollect installation log from the temporary directory.

```
Setup Log <Date> <#00X>.txt
```

Where:

`<Date>` is the installation date of the WinCollect agent.

`<#00X>` is the incremental log number file. Incremental log files are created with every installation, regardless of success or failure.

Step 5 Review the log file to determine the installation failure.

You can find several examples of installation error messages in the next section.

Installation Log Examples

The installation log captures the install process for WinCollect and includes information on finding the installation failure. The information contained in the setup log file is required to troubleshoot WinCollect installations with Customer Support.

This section includes the following installation error examples:

- **Missing Authorization or Console IP Address**
- **Installation Aborted by User**
- **Installation File in Use Error**

Missing Authorization or Console IP Address

The following text shows the error message generated when the AUTH_TOKEN or CONFIG_CONSOLE_ADDRESS is missing from the command-line installation:

```
2012-01-27 14:40:29.189   Log opened. (Time zone: UTC-04:00)
2012-01-27 14:40:29.189   Setup version: Inno Setup version
2012-01-27 14:40:29.189   Original Setup EXE: C:\AGENT-WinCollect-setup.exe
2012-01-27 14:40:29.189   Setup command line:
/SL5="$231104,11092567,54272,C:\AGENT-WinCollect-setup.exe" /SILENT
/CONFIG_CONSOLE_ADDRESS=100.100.100.100
2012-01-27 14:40:29.189   Windows version: 6.1.7601 SP1(NT platform: Yes)
2012-01-27 14:40:29.189   64-bit Windows: Yes
2012-01-27 14:40:29.189   Processor architecture: x64
2012-01-27 14:40:29.189   User privileges: Administrative
2012-01-27 14:40:29.191   64-bit install mode: No
2012-01-27 14:40:29.192   Created temporary directory:
C:\Users\IBM_AD~1\AppData\Local\Temp\is-OPP3D.tmp
2012-01-27 14:40:29.261   INFO: Host identifier not specified; generating appropriate
default...
2012-01-27 14:40:29.261   INFO: Generated default host identifier of WinUser
2012-01-27 14:40:29.261   ERROR: Installation was aborted because only one of
/AUTH_TOKEN and /CONFIG_CONSOLE_ADDRESS were specified. Both must be specified (for
remote configuration management) or neither specified (for stand-alone operation)
2012-01-27 14:40:29.261   InitializeSetup returned False; aborting.
2012-01-27 14:40:29.261   Got EAbort exception.
2012-01-27 14:40:29.261   Deinitializing Setup.
2012-01-27 14:40:29.262   Log closed.
```

Installation Aborted by User

The following text shows the message generated when a standard installation is aborted by the user:

```
2012-03-01 18:29:49.619   Log opened. (Time zone: UTC-04:00)
2012-03-01 18:29:49.619   Setup version: Inno Setup version 5.4.2 (a)
2012-03-01 18:29:49.619   Original Setup EXE:
C:\Users\jonathan.pechta\Desktop\AGENT-WinCollect-7.0.0.beta-setup.exe
2012-03-01 18:29:49.619   Setup command line:
/SL5="$70132,11199106,54272,C:\AGENT-WinCollect-setup.exe"
2012-03-01 18:29:49.619   Windows version: 6.1.7601 SP1 (NT platform: Yes)
```

```
2012-03-01 18:29:49.619   64-bit Windows: Yes
2012-03-01 18:29:49.619   Processor architecture: x64
2012-03-01 18:29:49.619   User privileges: Administrative
2012-03-01 18:29:49.619   64-bit install mode: No
2012-03-01 18:29:49.619   Created temporary directory:
C:\Users\Admin\AppData\Local\Temp\is-AF5L2.tmp
2012-03-01 18:29:56.510   Message box (Yes/No):
Setup is not complete. If you exit now, the program will not be installed.
You may run Setup again at another time to complete the installation.

Exit Setup?
2012-03-01 18:29:57.870   User chose Yes.
2012-03-01 18:29:57.870   Deinitializing Setup.
2012-03-01 18:29:57.916   Log closed.
```

Installation File in Use Error

The WinCollect agent cannot be installed while the WinCollect service is running. To avoid an installation issue, we recommend you stop the WinCollect service before attempting to reinstall the WinCollect agent on your host. The following text displays the message error message when an installation file is in use:

```
2012-03-01 18:37:02.021   Log opened. (Time zone: UTC-04:00)
2012-03-01 18:37:02.021   Setup version: Inno Setup version 5.4.2 (a)
2012-03-01 18:37:02.021   Original Setup EXE: C:\AGENT-WinCollect-setup.exe
2012-03-01 18:37:02.021   Setup command line:
/SL5="$90134,11199106,54272,C:\AGENT-WinCollect-setup.exe" /VERYSILENT
/SUPPRESSMSGBOXES /CONFIG_CONSOLE_ADDRESS 10.100.125.101
2012-03-01 18:37:02.037   Windows version: 6.1.7601 SP1  (NT platform: Yes)
2012-03-01 18:37:02.037   64-bit Windows: Yes
2012-03-01 18:37:02.037   Processor architecture: x64
2012-03-01 18:37:02.037   User privileges: Administrative
2012-03-01 18:37:02.037   64-bit install mode: No
2012-03-01 18:37:02.037   Created temporary directory:
C:\Users\Admin\AppData\Local\Temp\is-2DKPC.tmp
2012-03-01 18:37:02.130   Starting the installation process.
2012-03-01 18:37:02.130   Directory for uninstall files: C:\Program Files
(x86)\WinCollect
2012-03-01 18:37:02.130   Will append to existing uninstall log: C:\Program Files
(x86)\WinCollect\unins000.dat
2012-03-01 18:37:02.130   -- File entry --
2012-03-01 18:37:02.130   Dest filename: C:\Program Files
(x86)\WinCollect\unins000.exe
2012-03-01 18:37:02.130   Time stamp of our file: 2012-03-01 18:37:01.927
2012-03-01 18:37:02.130   Dest file exists.
2012-03-01 18:37:02.130   Time stamp of existing file: 2012-03-01 18:30:07.010
2012-03-01 18:37:02.146   Version of our file: 51.52.0.0
2012-03-01 18:37:02.146   Version of existing file: 51.52.0.0
2012-03-01 18:37:02.146   Installing the file.
2012-03-01 18:37:02.146   Uninstaller requires administrator: Yes
2012-03-01 18:37:02.146   Leaving temporary file in place for now.
```

```
2012-03-01 18:37:02.146   -- File entry --
2012-03-01 18:37:02.146   Dest filename: C:\Program Files
(x86)\WinCollect\bin\WinCollect.exe
2012-03-01 18:37:02.146   Time stamp of our file: 2012-03-01 09:52:18.000
2012-03-01 18:37:02.146   Dest file exists.
2012-03-01 18:37:02.146   Time stamp of existing file: 2012-03-01 09:52:18.000
2012-03-01 18:37:02.146   Installing the file.
2012-03-01 18:37:02.162   The existing file appears to be in use (5). Retrying.
2012-03-01 18:37:03.162   The existing file appears to be in use (5). Retrying.
2012-03-01 18:37:04.162   The existing file appears to be in use (5). Retrying.
2012-03-01 18:37:05.162   The existing file appears to be in use (5). Retrying.
2012-03-01 18:37:06.162   Defaulting to Abort for suppressed message box
(Abort/Retry/Ignore):
C:\Program Files (x86)\WinCollect\bin\WinCollect.exe

An error occurred while trying to replace the existing file:

DeleteFile failed; code 5.

Access is denied.

Click Retry to try again, Ignore to skip this file (not recommended), or Abort to
cancel installation.
2012-03-01 18:37:06.162   User canceled the installation process.
2012-03-01 18:37:06.162   Rolling back changes.
2012-03-01 18:37:06.162   Starting the uninstallation process.
2012-03-01 18:37:06.162   Uninstallation process succeeded.
2012-03-01 18:37:06.162   Deinitializing Setup.
2012-03-01 18:37:06.162   Log closed.
```

3 MANAGING WINCOLLECT SOURCES

The WinCollect agent is responsible for communicating to the individual log sources, parsing events, and forwarding the event information to QRadar using syslog. After you have installed the WinCollect agent on your Windows host, you can wait for the WinCollect agent to auto discover. If you prefer not to wait for the WinCollect agent to auto discover, you can manually add your WinCollect agent to your QRadar Console using the **Admin** tab. The WinCollect agent auto discovery process typically takes a few minutes to complete.

This section includes the following topics:

Managing WinCollect Agents

The QRadar Console can manage an entire deployment of WinCollect agents using the WinCollect agent user interface. This allows you to view installed agents and the log sources the WinCollect agent manages in your deployment.

NOTE If you have multiple QRadar Consoles in your deployment, your WinCollect agents can only be added to and managed by one QRadar Console. Adding a WinCollect agent to multiple QRadar Consoles is prohibited.

This section includes the following topics:

- To view the list of installed WinCollect agents, see **Viewing the Agent List**.
- To add a WinCollect agent, see **Adding a WinCollect Agent**.
- To edit an existing WinCollect agent, see **Editing a WinCollect Agent**.
- To view your WinCollect agents, see **Viewing WinCollect Agents**.
- To enable or disable a WinCollect agent, see **Enabling or Disabling a WinCollect Agent**.
- To delete a WinCollect agent, see **Deleting a WinCollect Agent**.

Viewing the Agent List

The WinCollect agent user interface allows you to manage and view the status of each WinCollect agent in your deployment. All of the WinCollect agents installed in your deployment are displayed in a searchable agent list.

This section includes the following topics:

- **Viewing Your WinCollect Agent Status**
- **Using the WinCollect Toolbar**

Viewing Your WinCollect Agent Status

The status of each WinCollect agent is displayed in the WinCollect agent list when you launch the WinCollect icon from the **Admin** tab. The WinCollect agent list displays the following information for each agent in your deployment:

Table 3-1 WinCollect Agent Status

Control	Description
Name	Displays the name of the WinCollect agents in your deployment. If the WinCollect agent is auto discovered, the name contains WinCollect @ **<Host Name>**. Where **<Host Name>** is the IP address or host name of the system hosting the WinCollect agent.
Host Name	Displays the IP address or host name of the WinCollect agent.
Description	Displays the description for the WinCollect agent. If your WinCollect agent is auto discovered the description displays **WinCollect agent installed on <Host Name>**. Where **<Host Name>** is the IP address or host name of the system hosting the WinCollect agent.
Version	Displays the version of the WinCollect agent installed on the Windows host.
OS Version	Displays the Windows operating system version the WinCollect agent is installed on.
Last Heart Beat	Displays the time heart beat successfully communicated from the WinCollect agent to the QRadar Console.

Table 3-1 WinCollect Agent Status (continued)

Control	Description
Status	Allows you to view the status of your WinCollect agent. The options include: • **Running** - The WinCollect agent is active on the Windows host. • **Stopped** - The WinCollect agent is stopped. If the WinCollect service is stopped, then events from the log sources managed by the agent are not forwarded to the QRadar Console. • **Unavailable** - The WinCollect service that reports on the status of the WinCollect agent has been stopped or restarted, so it can no longer report the agent status. • **No Communication from Agent** - The WinCollect agent has not established communication to the QRadar Console. If you manually added the WinCollect agent, verify the **Host Name** parameter is correct. You can also verify that there are no firewalls blocking communication between the WinCollect agent and the QRadar Console.
Enabled	Allows you to view the status of your WinCollect agent. Click **Enable/Disable** to toggle the agent's status. The options include: • **True** - The WinCollect agent is enabled. • **False** - The WinCollect agent is disabled. All log sources managed by the WinCollect agent are also disabled.

Using the WinCollect Toolbar

You can manage your WinCollect agents using the buttons available on the toolbar. To use the toolbar to manage a WinCollect agent, you must first select a WinCollect agent from the list.

Table 3-2 WinCollect Toolbar Controls

Control	Description
Add	Allows you to manually add a WinCollect agent.
Edit	Allows you to edit the configuration of the selected WinCollect agent.
Delete	Deletes the selected WinCollect agent and disables all of the log sources the WinCollect agent manages.
Log Sources	Allows you to configure Windows-based log sources for your WinCollect agent.
Show Events	Allows you to view events coming from the WinCollect agent.
Enable/Disable	Enables or disables the WinCollect agent. All log sources managed by the WinCollect agent are also disabled. Disabling the WinCollect agent stops the forwarding of events to the QRadar Console.

Table 3-2 WinCollect Toolbar Controls (continued)

Control	Description
Search	Allows you to search the list of WinCollect agents. The search term attempts to match any information found in the name, description, or hostname from the list of WinCollect agents.

Adding a WinCollect Agent

If your WinCollect agent does not automatically discover and add an entry in the WinCollect agent list, you can manually add your WinCollect agent. The auto discovery process typically takes a few minutes to complete, but the registration request to the QRadar Console can be blocked by firewalls in your network.

To add a WinCollect agent, perform the following steps:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

Step 3 Click the **WinCollect** icon.

The WinCollect window is displayed.

Step 4 Click **Add**.

The Configure a WinCollect Agent window is displayed.

Step 5 Type values for the following parameters:

Table 3-3 Configure a WinCollect Agent Parameters

Parameter	Description
Name	Type a suitable name for your WinCollect agent. The name must be unique to the WinCollect agent. The name can be up to 255 characters in length.
Host Name	Type the IP address or host name used when installing the WinCollect agent. The host name can be up to 255 characters in length. The information must match the IP address or host name specified during the agent installation for the **`/HOST_IDENTIFIER=<host name>`** parameter. The IP address or host name must be unique to the WinCollect agent. For more information, see **Installing the WinCollect Agent**, **Step 6**.
Description	Optional. Type a description for the WinCollect agent. If you specified IP addresses for the WinCollect agent, you might consider adding a descriptive message to identify the WinCollect agent or the log sources the WinCollect agent is managing. These messages are often helpful for other QRadar administrators, if a WinCollect agent requires managing.

Table 3-3 Configure a WinCollect Agent Parameters (continued)

Parameter	Description
WinCollect Configuration Pane	
Enabled	Select this check box to enable the WinCollect agent. If this check box is cleared, then events are not forwarded from the WinCollect agent to the QRadar Console for any of the log sources the WinCollect agent manages.
Heart Beat Interval	From the list box, select a heart beat interval for WinCollect. This option defines how often the WinCollect agent communicates its status to the QRadar Console. The interval ranges from 0 seconds (Off) to 20 minutes.
Configuration Poll Interval	From the list box, select an interval to poll for configuration updates to WinCollect agents. This option defines how often the WinCollect agent polls the QRadar Console for updated log source configuration information. The interval ranges from 0 seconds (Off) to 20 minutes.
WinCollect Details Pane	
Auto discovered	Displays if the WinCollect agent was auto discovered. • **True** - The WinCollect agent was auto discovered. • **False** - The WinCollect agent was not auto discovered or added manually.
WinCollect Version	Optional. Type the WinCollect version of the system hosting the WinCollect agent.
OS Version	Optional. Type the OS version of the system hosting the WinCollect agent.

Step 6 Click **Save**.

The WinCollect agent list is displayed.

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

Editing a WinCollect Agent

To edit the agent name, description, host IP address, or group of a log source, double-click a WinCollect agent from the agent list.

To edit a WinCollect agent:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

Step 3 Click the **WinCollect** icon.

The WinCollect window is displayed.

Step 4 Select the WinCollect agent to edit.

Step 5 Click **Edit**.

The Configure a WinCollect agent window is displayed.

Step 6 Edit values for the parameters, as necessary:

Table 3-4 Edit a Log Source Parameters

Parameter	Description
Name	Type a suitable name for the WinCollect agent. The name must be unique to the WinCollect agent. The name can be up to 255 characters in length.
Host Name	Type the IP address or host name of the system hosting the WinCollect agent. The IP address or host name must be unique to the WinCollect agent. The host name can be up to 255 characters in length.
Description	Optional. Type a description for the WinCollect agent.
WinCollect Configuration Pane	
Enabled	Select this check box to enable the WinCollect agent. If this check box is cleared, then events are not forwarded from the WinCollect agent to the QRadar Console.
Heart Beat Interval	From the list box, select a heart beat interval for WinCollect. This option defines how often the WinCollect agent communicates to the QRadar Console. The interval ranges from 0 seconds (Off) to 20 minutes.
Configuration Poll Interval	From the list box, select an interval to poll for configuration updates to WinCollect agents. This option defines how often the WinCollect agent polls the QRadar Console for updated log source configuration information. The interval ranges from 0 seconds (Off) to 20 minutes.
WinCollect Details Pane	
Auto discovered	Displays if the WinCollect agent was auto discovered. • **True** - The WinCollect agent was auto discovered. • **False** - The WinCollect agent was not auto discovered or added manually.
WinCollect Version	Optional. Type the WinCollect version of the system hosting the WinCollect agent.
OS Version	Optional. Type the OS version of the system hosting the WinCollect agent.

Table 3-4 Edit a Log Source Parameters (continued)

Parameter	Description
Status	The status of the WinCollect agent is displayed. The options include: • **Running** - The WinCollect agent is active on the Windows host. • **Stopped** - The WinCollect agent is stopped. If the WinCollect service is stopped, then events from the log sources managed by the agent are not forwarded to the QRadar Console. Verify the status of the WinCollect host and the WinCollect service. • **Unavailable** - The WinCollect service that reports on the status of the WinCollect agent has been stopped or restarted, so it can no longer report the agent status. • **No Communication from Agent** - The WinCollect agent has not established communication to the QRadar Console. If you manually added the WinCollect agent, verify the **Host Name** parameter is correct or verify that there are no firewalls blocking communication between the Windows Host and the QRadar Console.
Last Heart Beat	The timestamp of the last successful heart beat.
Last Configuration	The timestamp of the last successful configuration update from the QRadar Console.
Log Sources	The number of log sources the agent manages.

Step 7 Click **Save**.

Any changes that have been made to the configuration take place immediately. The WinCollect agent list is displayed.

Viewing WinCollect Agents

The WinCollect page allows you to manage WinCollect agents that have been added or auto discovered by the QRadar Console. The WinCollect page displays all of the agents and their current status.

To view WinCollect agents, perform the following steps:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

Step 3 Click the **WinCollect** icon.

The WinCollect window is displayed.

If a WinCollect agent has not connected to the QRadar Console, the Status column displays No Communication.

NOTE

The WinCollect icon is only viewable from the **Admin** tab after you complete the installation of the WinCollect agent and QRadar components.

Enabling or Disabling a WinCollect Agent

The WinCollect agent installed on the host can be disabled remotely from the QRadar Console. Disabling a WinCollect agent stops all events from the log sources that agent managed. The individual log sources are enabled, but the agent is disabled from sending events.

To enable or disable a WinCollect agent, perform the following steps:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

Step 3 Click the **WinCollect** icon.

The WinCollect window is displayed.

Step 4 Select the WinCollect agent that you want to enable or disable.

Step 5 Click **Enable/Disable**.

When an agent is enabled, the Enabled column indicates true. When disabled, the Enabled column indicates false.

NOTE

If you enable a WinCollect agent, the log sources managed by the WinCollect agent are also enabled. These log sources count toward your log source license limit. If several log sources remain disabled, you might have exceeded your log source license restriction. For more information about your license limits, see the Managing the System chapter of the *QRadar Administration Guide*. If you require additional license limits, contact your sales representative.

Deleting a WinCollect Agent

Deleting a WinCollect agent not only removes the agent, but disables the log sources the agent manages. WinCollect agents that are deleted do not auto discover and must be manually added to the QRadar Console.

For example, if you delete a WinCollect agent with a host identifier name VMRack1, then delete the agent and reinstall using VMRack1 as a host identifier name, then the WinCollect agent does not automatically discover. You must add the WinCollect agent manually.

To delete a WinCollect agent, perform the following steps:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

Step 3 Click the **WinCollect** icon.

The WinCollect window is displayed.

Step 4 Select any agents you want to delete.

Step 5 Click **Delete**.

A confirmation window is displayed.

Step 6 Click **OK**.

NOTE To delete multiple WinCollect agents, press the Ctrl key to select multiple agents and clicking **Delete**.

Managing WinCollect Log Sources

After your WinCollect agents have been added, you can assign log sources to the agent. A single WinCollect agent can manage and forward events from a number of Windows-based log sources and operating systems. Log sources communicating through a WinCollect agent can be added individually or if the log sources contain similar configurations, then you can add multiple log sources using the bulk add or bulk edit feature. Changes to individually added log sources are managed individually, but changes made to bulk log sources are made to all of the log sources in the bulk added group.

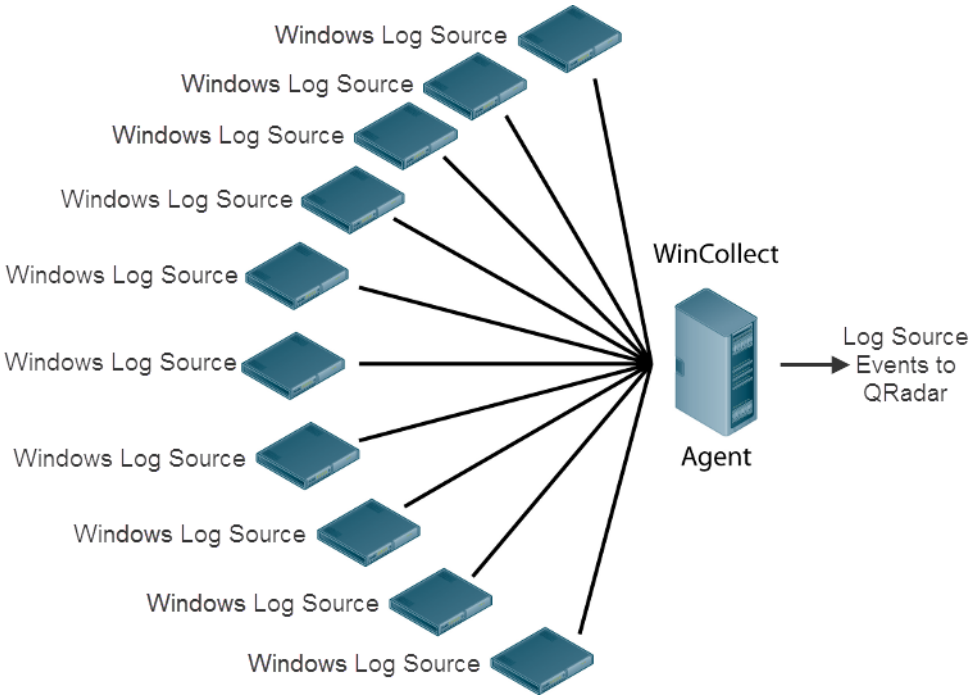

Figure 3-1 A single WinCollect agent configured for remote collection and forward Windows events to the QRadar Console.

This section includes the following topics:

- To view a log source managed by WinCollect, see **Viewing Log Sources**.
- To add an individual log source, see **Adding a Log Source**.
- To edit an individual log source, see **Editing a Log Source**.
- To enable or disable a log source, see **Enabling/Disabling a Log Source**.
- To delete an individual log source from your WinCollect agent, see **Deleting a Log Source**.
- To bulk add similar log sources, see **Adding Multiple Log Sources**.
- To bulk edit similar log sources, see **Editing Multiple Log Sources**

Viewing Log Sources

To view log source status or manage WinCollect log sources, perform the following steps:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

Step 3 Click the **WinCollect** icon.

The WinCollect window is displayed.

Step 4 Select the WinCollect agent, and click **Log Sources**.

The Log Sources window is displayed and filtered by the WinCollect agent.

If a log source has not received any events within the configured syslog timeout period, the Status column displays Error. If you manually configure a log source that uses syslog, the Status column displays a status of Error until that log source has received an event. For more information about the Syslog Event Timeout parameter, see the *QRadar Administration Guide*.

NOTE

Bulk added log sources display N/A in the Status column.

Adding a Log Source

To add an individual log source to your WinCollect:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

Step 3 Click the **WinCollect** icon.

The WinCollect window is displayed.

NOTE

You can also use the Log Sources icon to add or edit a log source.

Step 4 Select the WinCollect agent, and click **Log Sources**.

Step 5 Click **Add**.

The Add a log source window is displayed.

Step 6 From the **Log Source Type** drop-down list box, select **Microsoft Windows Security Event Log**.

Step 7 From the **Protocol Configuration** drop-down list box, select **WinCollect**.

Step 8 Configure values for the following parameters:

Table 3-5 WinCollect Protocol Parameters

Parameter	Description
Log Source Name	Type a suitable name for the log source. The name can be up to 255 characters in length.
Log Source Description	Type a description for the log source (optional).
Log Source Type	From the list, select **Microsoft Windows Security Event Log.**
Protocol Configuration	From the list box, select **WinCollect**.
Log Source Identifier	Type the IP address or hostname of a remote Windows operating system from which you want to collect Windows-based events. The log source identifier must be unique for the log source type. ***Note:*** *The Log Source Identifier field in a WinCollect log source is used for polling events from remote sources. This field is used in the same manner as the Remote Machine field in the Adaptive Log Exporter.*
Domain	Type the Windows domain that includes the Windows log source. This parameter is optional.
User Name	Type the username required to access the Windows host. ***Note:*** *If your WinCollect agent is installed on a domain controller, you must provide domain administrator credentials for the user name and password fields.*
Password	Type the password required to access the Windows host. ***Note:*** *The password must be 15 characters or less.*
Confirm Password	Confirm the password required to access the Windows host.

Table 3-5 WinCollect Protocol Parameters (continued)

Parameter	Description
Standard Log Types	Select any check boxes for the Windows log type you want QRadar to monitor. At least one check box must be selected. The log types include: • Security • System • Application • DNS Server • File Replication Service • Directory Service
Event Types	Select any check boxes for the event type you want QRadar to monitor. At least one check box must be selected. The event types include: • Informational • Warning • Error • Success Audit • Failure Audit
WinCollect Agent	From the list box, select the WinCollect agent to manage this log source.
Transport Protocol	From the list box, select the protocol the WinCollect agent uses to communicate via syslog to QRadar. The options include: • **UDP** - The WinCollect agent communicates syslog events to QRadar using UDP. • **TCP** - The WinCollect agent communicates syslog events to QRadar using TCP.

Table 3-5 WinCollect Protocol Parameters (continued)

Parameter	Description
Remote Machine Poll Interval (in milliseconds)	Type the polling interval, which is the number of milliseconds between queries to the remote Windows host to poll for new events. • **7500** - A polling interval of 7500 should be used where the WinCollect agent collects events from a large number of remote computers that have a low event per second rate. For example, collecting from 100 remote computers that provide 10 events per second or less. • **3500** - A polling interval of 3500 should be used where the WinCollect agent collects events from a large number of remote computers that have a low event per second rate. For example, collecting from 50 remote computers that provide 20 events per second or less. • **1000** - A polling interval of 1000 should be used where the WinCollect agent collects events from a small number of remote computers that have a high event per second rate. For example, collecting from 10 remote computers that provide 100 events per second or less. The minimum polling interval is 100 milliseconds (.1 seconds). The default is 7500 milliseconds or 7.5 seconds.
XPath Query	XPath queries are structured XML expressions that you can include to retrieve customized events from the Microsoft Windows Security Event Log. If you specify an XPath Query to filter incoming events, any check boxes you selected from the **Standard Log Type** or **Event Type** are ignored and the events collected by QRadar use the contents of the XPath Query. You might be required to enable Remote Event Log Management on Windows 2008 to collect information using an XPath Query. For more information, see **XPath Queries**. ***Note:*** *Microsoft Server 2003 does not support XPath Queries for events. This field should be left blank for WinCollect agents collecting from Windows Server 2003.*
Enabled	Select this check box to enable the log source. By default, this check box is selected.

Table 3-5 WinCollect Protocol Parameters (continued)

Parameter	Description
Credibility	From the list box, select the credibility of the log source. The range is 0 to 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Event Collector	From the list box, select the Event Collector to use as the target for the log source.
Coalescing Events	Select this check box to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the **Coalescing Events** list box from the System Settings in QRadar. However, when you create or edit a log source, you can select the **Coalescing Events** check box to coalesce events for an individual log source. For more information, see the *QRadar Administration Guide*.
Store Event Payload	Select this check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the **Store Event Payload** list box from the System Settings in QRadar. However, when you create or edit a log source, you can select the **Store Event Payload** check box to retain the event payload for an individual log source. For more information, see the *QRadar Administration Guide*.
Groups	Select one or more groups for the log source.

Step 9 Click **Save**.

The Log Sources window is displayed.

Step 10 On the **Admin** tab, click **Deploy Changes**.

Repeat these steps to add additional log sources to your WinCollect agent. If the configurations are similar and only differ by IP address or hostname of the remote source, you can add multiple log sources using the bulk add feature. For more information, see **Adding Multiple Log Sources**.

The log source configuration is complete.

Editing a Log Source

Editing a log source enables you to change most of the configurable log source parameters, such as credentials, IP address, domain. This provides you with the ability to update log sources as your network changes. All of the log course parameters are editable, with the exception of the Log Source Type and the Protocol Configuration parameters.

CAUTION

Editing a WinCollect log source forces QRadar to update the WinCollect agent with the latest configuration information. During this configuration update, the WinCollect agent cannot collect events and events might be missed.

To edit a log source, perform the following steps:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

Step 3 Click the **WinCollect** icon.

The WinCollect window is displayed.

NOTE

You can also use the Log Sources icon to add or edit a log source.

Step 4 Select the WinCollect agent, and click **Log Sources**.

The Log Sources window is displayed.

Step 5 Select the log source to edit.

NOTE

You can also double-click any log source to edit the configuration parameters.

Step 6 Click **Edit**.

The Edit a log source window is displayed.

Step 7 Edit the log source parameters, as necessary:

Table 3-6 Edit a Log Source Parameters

Parameter	Description
Log Source Name	Type a suitable name for the log source. The name can be up to 255 characters in length.
Log Source Description	Type a description for the log source (optional).
Log Source Type	The **Microsoft Windows Security Event Log** is displayed. The log source type is not editable after the log source has been added and deployed.
Protocol Configuration	The protocol configuration is displayed. The log source type is not editable field after the log source has been added and deployed.

Table 3-6 Edit a Log Source Parameters (continued)

Parameter	Description
Log Source Identifier	Type the IP address or hostname of the Windows host. The log source identifier must be unique for the log source type.
Domain	Type the Windows domain that includes the log source. This parameter is optional.
User Name	Type the username required to access the Windows host. ***Note:*** *If your WinCollect agent is installed on a domain controller, you must provide domain administrator credentials for the user name and password fields.*
Password	Type the password required to access the Windows host. ***Note:*** *The password must be 15 characters or less.*
Confirm Password	Confirm the password required to access the Windows host.
Standard Log Types	Select any check boxes for the Windows log type you want QRadar to monitor. At least one check box must be selected. The log types include: • Security • System • Application • DNS Server • File Replication Service • Directory Service
Event Types	Select any check boxes for the event type you want QRadar to monitor. At least one check box must be selected. The event types include: • Informational • Warning • Error • Success Audit • Failure Audit
WinCollect Agent	From the drop-down list box, select the WinCollect agent to manage this log source.

Table 3-6 Edit a Log Source Parameters (continued)

Parameter	Description
Transport Protocol	From the drop-down list box, select the protocol the WinCollect agent uses to communicate via syslog to QRadar. The options include: • **UDP** - The log source communicates with the WinCollect agent using UDP. • **TCP** - The log source communicates with the WinCollect agent using TCP.
Remote Machine Poll Interval (in milliseconds)	Type the polling interval, which is the number of milliseconds between queries to the remote Windows host to poll for new events. Type the polling interval, which is the number of milliseconds between queries to the remote Windows host to poll for new events. • **7500** - A polling interval of 7500 should be used where the WinCollect agent collects events from a large number of remote computers that have a low event per second rate. For example, collecting from 100 remote computers that provide 10 events per second or less. • **3500** - A polling interval of 3500 should be used where the WinCollect agent collects events from a large number of remote computers that have a low event per second rate. For example, collecting from 50 remote computers that provide 20 events per second or less. • **1000** - A polling interval of 1000 should be used where the WinCollect agent collects events from a small number of remote computers that have a high event per second rate. For example, collecting from 10 remote computers that provide 100 events per second or less. The minimum polling interval is 100 milliseconds (.1 seconds). The default is 7500 milliseconds or 7.5 seconds.

Step 8 Click **Save**.

The Log Sources window is displayed.

Enabling/Disabling a Log Source

To enable or disable a log source:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

Step 3 Click the **WinCollect** icon.

The WinCollect window is displayed.

Step 4 Select the WinCollect agent, and click **Log Sources**.

The Log Sources window is displayed.

Step 5 Select the log source that you want to enable or disable.

Step 6 Click **Enable/Disable**.

When a log source is enabled, the Enabled column indicates true. When a log source is disabled, the **Status** column indicates **Disabled**.

NOTE

If you cannot enable a log source, you might have exceeded your license restrictions. For more information about your license limits, see the Managing the System chapter of the *QRadar Administration Guide*. If you require additional license limits, contact your sales representative.

Deleting a Log Source

To delete a log source:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

Step 3 Click the **WinCollect** icon.

The WinCollect window is displayed.

Step 4 Select the WinCollect agent, and click **Log Sources**.

The Log Sources window is displayed.

Step 5 Select the log source you want to delete.

Step 6 Click **Delete**.

A confirmation window is displayed.

Step 7 Click **OK**.

You can delete multiple log sources by holding the Shift key to select multiple log sources and click **Delete**.

Adding Multiple Log Sources

You can add multiple log sources to QRadar that share a configuration protocol for remote collection with your WinCollect agent. Log sources allow you to bulk add and configure hosts by uploading a text file, using a domain query, or typing a host name or IP address. A maximum of 500 active hosts or IP addresses can share a single protocol configuration. If you attempt to add more than 500 hosts, an error message is displayed.

NOTE

Adding multiple log sources forces QRadar to connect to and retrieve all existing events from your remote sources. Depending on the number of WinCollect log

sources added, it can take an extended period of time for the WinCollect agent to access and collect all outstanding Windows events. For more information, see **Device Polling Overdue**.

To add multiple log sources to your deployment:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

Step 3 Click the **WinCollect** icon.

The WinCollect window is displayed.

Step 4 Select the WinCollect agent, and click **Log Sources**.

The Log Sources window is displayed.

Step 5 Using the **Bulk Actions** drop-down menu, select **Bulk Add**.

The Add a bulk log source window is displayed.

Step 6 Type values for the parameters, as necessary:

Table 3-7 Adding a Bulk Log Source Parameters

Parameter	Description
Bulk Log Source Name	Type a suitable name for the group or bulk log source. The name can be up to 255 characters in length. ***Note:*** *Adding a bulk log source automatically creates a log source group using the name you input into this field.*
Log Source Type	From the list box, select **Microsoft Windows Security Event Log**.
Protocol Configuration	From the list box, select **WinCollect**.
Domain	Type the Windows domain that includes the log source. This parameter is optional.
User Name	Type the username required to access the Windows host. ***Note:*** *If you bulk add a list of log sources, we recommend that the list does not contain domain controllers. Domain controllers should be added individually as they require domain administrator credentials in the user name and password fields.*
Password	Type the password required to access the Windows host. ***Note:*** *The password must be 15 characters or less.*
Confirm Password	Confirm the password required to access the Windows host.

Table 3-7 Adding a Bulk Log Source Parameters (continued)

Parameter	Description
Standard Log Types	Select any check boxes for the Windows log type you want QRadar to monitor. At least one check box must be selected. The log types include: • Security • System • Application • DNS Server • File Replication Service • Directory Service
Event Types	Select any check boxes for the event type you want QRadar to monitor. At least one check box must be selected. The event types include: • Informational • Warning • Error • Success Audit • Failure Audit
WinCollect Agent	From the list box, select the WinCollect agent to manage this log source.
Transport Protocol	From the list box, select the protocol the WinCollect agent uses to communicate via syslog to QRadar. The options include: • **UDP** - The log source communicates with the WinCollect agent using UDP. • **TCP** - The log source communicates with the WinCollect agent using TCP.

Table 3-7 Adding a Bulk Log Source Parameters (continued)

Parameter	Description
Remote Machine Poll Interval (in milliseconds)	Type the polling interval, which is the number of milliseconds between queries to the remote Windows host to poll for new events. Type the polling interval, which is the number of milliseconds between queries to the remote Windows host to poll for new events. • **7500** - A polling interval of 7500 should be used where the WinCollect agent collects events from a large number of remote computers that have a low event per second rate. For example, collecting from 100 remote computers that provide 10 events per second or less. • **3500** - A polling interval of 3500 should be used where the WinCollect agent collects events from a large number of remote computers that have a low event per second rate. For example, collecting from 50 remote computers that provide 20 events per second or less. • **1000** - A polling interval of 1000 should be used where the WinCollect agent collects events from a small number of remote computers that have a high event per second rate. For example, collecting from 10 remote computers that provide 100 events per second or less. The minimum polling interval is 100 milliseconds (.1 seconds). The default is 7500 milliseconds or 7.5 seconds.
XPath Query	XPath queries are structured XML expressions that you can include to retrieve customized events from the Microsoft Windows Security Event Log. If you specify an XPath Query to filter incoming events, any check boxes you selected from the **Standard Log Type** or **Event Type** are ignored and the events collect by QRadar use the contents of the XPath Query. ***Note:*** *Microsoft Server 2003 does not support XPath Queries for events. This field should be left blank for WinCollect agents collecting from Windows Server 2003* For more information on XPath Queries, see **XPath Queries**.
Enabled	Select this check box to enable the log source. By default, this check box is selected.

Table 3-7 Adding a Bulk Log Source Parameters (continued)

Parameter	Description
Credibility	From the drop-down list box, select the credibility of the bulk log source. The range is 0 to 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Event Collector	From the drop-down list box, select the Event Collector to use as the target for the log source.
Coalescing Events	Select this check box to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the **Coalescing Events** list box from the System Settings in QRadar. However, when you create or edit a log source, you can select the **Coalescing Events** check box to coalesce events for an individual log source. For more information, see the *QRadar Administration Guide*.
Store Event Payload	Select this check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the **Store Event Payload** list box from the System Settings in QRadar. However, when you create or edit a log source, you can select the **Store Event Payload** check box to retain the event payload for an individual log source. For more information, see the *QRadar Administration Guide*.
File Upload	
Bulk Import File	Select a text file containing a maximum of 500 IP addresses or host names of log sources you want to bulk add. The text file should contain one IP address or host name per line. Extra characters after an IP address or host names longer than 255 characters result in an error, indicating a log source from the host list could not be added.
Domain Query	
Domain Controller	Type the IP address of the domain controller. To search a domain you must add the domain, username, and password for the log source before polling the domain for hosts to add.
Full Domain Name	Type the fully qualified domain name (FQDN) of the domain controller. To search a domain you must add the domain, username, and password for the log source before polling the domain for hosts to add.

Table 3-7 Adding a Bulk Log Source Parameters (continued)

Parameter	Description
Manual	
Host	Type an individual IP address or host name to add to the host list.
Add Host	Click **Add Host** to add an IP address or host name to the host list. The **Add Host** check box is only displayed when you have at least one log source in the host list. By default, this check box is selected. Clearing the check box from the add field allows you to ignore a log source. ***Note:*** *You are not required to clear check boxes for log sources that already exist. Duplicate host names or IP addresses are ignored from the host list.*

Step 7 Click **Save**.

A summary of the added log sources is displayed.

Step 8 Click **Continue**.

The log sources are added to your WinCollect agent.

Editing Multiple Log Sources

Log sources that share a common protocol can be edited as a group as they share a configuration. You can use bulk editing to update host names, IP addresses, or add additional log sources to an existing log source group. This provides you with the ability to update log sources as your network changes.

CAUTION

Editing a WinCollect log source forces QRadar to update the WinCollect agent with the latest configuration information. During this momentary configuration update, the WinCollect agent cannot collect events and events might be missed.

To edit a bulk log source in your deployment, perform the following steps:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

Step 3 Click the **WinCollect** icon.

The WinCollect window is displayed.

Step 4 Select the WinCollect agent, and click **Log Sources**.

The Log Sources window is displayed.

Step 5 Select a bulk log source to edit from the list.

You must select one or more bulk log sources from your active log sources list for the **Bulk Edit** drop-down menu to be available.

NOTE

To edit the log source name, log source description, log source identifier, or group, double-click the bulk log source.

Step 6 Using the **Bulk Actions** drop-down menu, select **Bulk Edit**.

The Edit a bulk log source window is displayed.

Step 7 Type values for the parameters you want to edit.

For more information, see **Adding a Bulk Log Source Parameters**.

Step 8 Click **Save**.

A summary of the added log sources is displayed.

Step 9 Click **Continue**.

The Log sources window is displayed.

Grouping Log Sources

Categorizing your log sources into groups allows you to efficiently view and track the log sources managed by WinCollect agents. By default, when a WinCollect agent is added the log sources managed by the agent are added to the WinCollect group. This enables you to efficiently view log sources based on functional groups. For example, you can filter the log sources by WinCollect agent name. Each group can display a maximum of 1,000 log sources.

You must have administrative access to create, edit, or delete groups. For more information on user roles, see the *QRadar Administration Guide*.

This section includes the following topics:

- **Viewing Log Sources By Group**
- **Creating a Group**
- **Editing a Group**
- **Copying a Log Source to Another Group**
- **Removing a Log Source From a Group**

Viewing Log Sources By Group

To view WinCollect log sources by group, perform the following steps:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

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

The Log Sources window is displayed.

Step 4 From the **Search For** drop-down list box, select **Group**.

Step 5 From the group criteria, select **WinCollect**.

Step 6 Click **Go**.

The log sources associated with the group WinCollect are displayed.

Creating a Group

By default, when a WinCollect agent is added the log sources managed by the agent are added to the WinCollect group. To create a unique group, perform the following steps:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

Step 3 Click the **Log Source Groups** icon.

The Log Source Groups window is displayed.

Step 4 From the menu tree, select the group under which you want to create a new group.

NOTE Alternatively, click **Assign** to access the log source group menu option.

Step 5 Click **New Group**.

The Group Properties window is displayed.

Step 6 Define values for the parameters:

- **Name** - Type a name to assign to the new group. The name can be up to 255 characters in length and is case sensitive.
- **Description** - Type a description to assign to this group. The description can be up to 255 characters in length.

Step 7 Click **OK**.

Step 8 To change the location of the new group, click the new group and drag the folder to a chosen location in your menu tree.

Step 9 Close the Groups Properties window.

NOTE When you create the group, you can drag and drop menu tree items to change the organization of the tree items.

Editing a Group

To edit a group, perform the following steps:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

Step 3 Click the **Log Source Groups** icon.

The Log Source Groups window is displayed.

Step 4 From the menu tree, select the group to edit.

Step 5 Click **Edit**.

The Group Properties window is displayed.

Step 6 Update values for the parameters, as necessary:

- **Name** - Type a name to assign to the new group. The name can be up to 255 characters in length and is case sensitive.
- **Description** - Type a description to assign to this group. The description can be up to 255 characters in length.

Step 7 Click **OK**.

Step 8 To change the location of the group, click the new group and drag the folder to the chosen location in your menu tree.

Step 9 Close the Groups window.

Copying a Log Source to Another Group

Using the groups functionality, you can copy a log source to one or more groups.

To copy a log source:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

Step 3 Click the **Log Source Groups** icon.

The Log Source Groups window is displayed.

Step 4 From the Log Source Groups tree, select the group from which you want to copy the log source.

A list of log sources is displayed in the Group Content Frame.

Step 5 From the Group Content Frame, select the log source you want to copy to another group.

Step 6 Click **Copy**.

The Choose Group window is displayed.

Step 7 Select the group to which you want to copy the log source.

Step 8 Click **Assign Groups**.

Step 9 Close the Groups window.

Removing a Log Source From a Group

Removing a log source group does not delete the log source from QRadar, just removes the group association. To remove a log source from a group:

Step 1 Click the **Admin** tab.

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

The Data Sources pane is displayed.

Step 3 Click the **Log Source Groups** icon.

The Log Source Groups window is displayed.

Step 4 From the menu tree, select the a group with items to be removed.

Step 5 From the **Group Content Frame**, select the item to remove.

Step 6 Click **Remove**.

A confirmation window is displayed.

Step 7 Click **OK**.

Step 8 Close the Groups window.

Device Troubleshooting

The WinCollect agent creates an device log that stores configuration information and warnings about log sources configured for each WinCollect agent. Each time the WinCollect service is restarted or the date changes, a new log is created.

This section includes the following topics:

- **Viewing the Device Log**
- **Device Polling Overdue**

Viewing the Device Log

The device log captures log source configuration information for WinCollect and includes information on finding log source issues. The information contained in the device log file can be helpful when troubleshooting log source with Customer Support.

To view the WinCollect device log, perform the following steps:

Step 1 Log in to the host of your WinCollect agent.

Step 2 Navigate to the following directory on the WinCollect host:

```
C:\Program Files\WinCollect\logs\
```

On 64-bit operating systems, this file location can be the following:

```
C:\Program Files (x86)\WinCollect\logs\
```

Step 3 Open the following file:

```
WinCollect_Device.<date> <identifier>.txt
```

Where:

`<date>` indicates the date the device log is created.

`<version>` indicates the version of the device log file. The version increments by one each time the WinCollect Service is restarted or when adding or changing the configuration of a log source managed by the WinCollect agent.

Device Polling Overdue

The following warning for device polling overdue is displayed when the WinCollect agent is waiting to remotely collect events from a log source managed by the WinCollect agent, but the device is in queue. This warning message can occur when adding or editing a WinCollect agent with a large number of remotely collected log sources. Each time the log source is edited, the service is restarted on the WinCollect agent and each log source is polled for updated events. Log

sources near the bottom of the list can be in queue waiting to be polled. If this occurs, then the following message is displayed in the device log:

```
2012-09-02 12:50:11,328 WARN Device.WindowsLog.EventLogMonitor.OnTimerExpired :
Event log 10.100.100.10 [\\10.100.100.10:Application] is seriously overdue to be
polled (interval approx 500 millisec, overdue = 45005 millisec).
```

This message does not indicate that any events are dropped, but that the WinCollect agent is waiting to poll the remote log source for events.

A XPATH QUERIES

An XPath Query is a new log source parameter that allows you to filter (or path to) specific events when communicating with a Windows 2008-based event log. XPath queries use XML notation and are available in QRadar when retrieving events using the WinCollect protocol. The most common method of creating an XPath query is to use the Microsoft Event Viewer to create a custom view. The custom view you create in the Event Viewer for specific events can generate XPath notations. You can then copy this XPath notation generated for you in your XPath query to filter your incoming log source events for specific event data.

NOTE We do not recommend that you create your XPath queries manually unless you are proficient with XPath 1.0 and creating XPath queries.

This section includes the following topics:

Enabling Remote Log Management

Windows 2008 and newer operating systems that allow the use of XPath queries require that you enable remote event log management. Enabling remote log management is only required when you are using the XPath Query field in your WinCollect log source.

Select your operating system to configure remote event log management:

Windows 2008

To enable remote log management for Windows 2008:

Step 1 On your desktop, select **Start > Control Panel**.

Step 2 Click the **Security** icon.

Step 3 Click **Allow a program through Windows Firewall**.

Step 4 If prompted by User Account Control, click **Continue**.

The Windows Firewall Settings window is displayed.

Step 5 From the **Exceptions** tab, select **Remote Event Log Management**.

Step 6 Click **OK**.

Remote event log management is now enabled for Windows 2008.

Windows 2008R2 To enable remote log management for Windows 2008R2:

Step 1 On your desktop, select **Start > Control Panel**.

Step 2 Click the **Windows Firewall** icon.

Step 3 From the menu, click **Allow a program or feature through Windows Firewall**.

Step 4 If prompted by User Account Control, click **Continue**.

The Allowed Programs window is displayed.

Step 5 Click **Change Settings**.

Step 6 From the Allowed programs and features pane, select the **Remote Event Log Management** check box.

This also selects a check box for a network type. Depending on your network, you may need to correct or select additional network types.

Step 7 Click **OK**.

Remote event log management is now enabled for Windows 2008R2.

Windows 7 To enable remote log management for Windows 7:

Step 1 On your desktop, select **Start > Control Panel**.

Step 2 Click the **System and Security** icon.

Step 3 From the Windows Firewall pane, click **Allow a program through Windows Firewall**.

Step 4 If prompted by User Account Control, click **Continue**.

The Windows Firewall Settings window is displayed.

Step 5 Click **Change Settings**.

Step 6 From the Allowed programs and features pane, select the **Remote Event Log Management** check box.

This also selects a check box for a network type. Depending on your network, you may need to correct or select additional network types.

Step 7 Click **OK**.

Remote event log management is now enabled for Windows 7.

Creating Custom Views

The Microsoft Event Viewer allows you to create custom views, which can filter events for severity, source, category, keywords, or specific users. WinCollect log sources can use XPath filters to capture specific events from your logs. To create the XML for your XPath Query parameter, you must create a custom view. You must log in as an administrator to use the Microsoft Event Viewer.

CAUTION

XPath queries used with the WinCollect protocol do not support the filtering of events by time range using the TimeCreated notation. Filtering events by a time range can lead to events not collecting properly.

To create a custom view, perform the following steps:

Step 1 On your desktop, select **Start > Run**.

The Run window is displayed.

Step 2 Type the following:

```
Eventvwr.msc
```

Step 3 Click **OK**.

Step 4 If you are prompted, type your administrator password and press Enter.

The Event Viewer is displayed.

Step 5 On the **Action** menu, select **Create Custom View**.

The Create Custom View window is displayed.

CAUTION

*When creating a custom view, do not select a time range from the **Logged** drop-down list box. The **Logged** drop-down list box includes the TimeCreated element, which is not supported in XPath Queries for the WinCollect protocol.*

Step 6 In **Event Level**, select the check boxes for the severity of events you want to include in your custom view.

Step 7 Select one of the following event sources:

- **By Log** - From the **Event Logs** drop-down list box, select the log types you want to monitor.
- **By Source** - From the **Event Sources** drop-down list box, select the event sources you want to monitor.

Step 8 Type the event IDs you want to filter from the event or log source.

Event IDs can be typed individually using comma-separated IDs or as a range. For example 4133, 4511-4522.

Step 9 From the **Task Category** drop-down list box, select the categories you want to filter from the event or log source.

Step 10 From the **Keywords** drop-down list box, select any keywords you want to filter from the event or log source.

Step 11 Type the user name you want to filter from the event or log source.

Step 12 Type the computer or computers you want to filter from the event or log source.

Step 13 Click the **XML** tab.

The XML is displayed for your XPath Query.

Step 14 Copy and paste the XML to the XPath Query field of your WinCollect protocol configuration.

NOTE If you specify an XPath Query that for your log source, only the events specified in the query are retrieved by the WinCollect protocol and forwarded to QRadar. Any check boxes you select from the **Standard Log Type** or **Event Type** are ignored by the log source configuration.

XPath Query Examples

The following information contains XPath examples you might use with the WinCollect protocol. There are thousands of examples that can be created and customized for your specific network policy. We suggest you only use these Xpath examples as reference information.

Monitor Events for a Specific User

This example retrieves events from all Windows event logs for the user Guest.

```
<QueryList>
<Query Id="0" Path="Application">
<Select Path="Application">*[System[(Level=4 or Level=0) and
Security[@UserID='S-1-5-21-3709697454-1862423022-1906558702-501
']]]</Select>
<Select Path="Security">*[System[(Level=4 or Level=0) and
Security[@UserID='S-1-5-21-3709697454-1862423022-1906558702-501
']]]</Select>
<Select Path="Setup">*[System[(Level=4 or Level=0) and
Security[@UserID='S-1-5-21-3709697454-1862423022-1906558702-501
']]]</Select>
<Select Path="System">*[System[(Level=4 or Level=0) and
Security[@UserID='S-1-5-21-3709697454-1862423022-1906558702-501
']]]</Select>
<Select Path="ForwardedEvents">*[System[(Level=4 or Level=0) and
Security[@UserID='S-1-5-21-3709697454-1862423022-1906558702-501
']]]</Select>
</Query>
</QueryList>
```

Credential Logon for Windows 2008

This example retrieves events from the security log for Information level events pertaining to the account authentication in Windows 2008 using, specific event IDs.

```
<QueryList>
<Query Id="0" Path="Security">
      <Select Path="Security">*[System[(Level=4 or Level=0) and
( (EventID &gt;= 4776 and EventID &lt;= 4777) )]]</Select>
</Query>
</QueryList>
```

Table B-1 Event IDs in this example

ID	Description
4776	The domain controller attempted to validate credentials for an account.
4777	The domain controller failed to validate credentials for an account.

Account Creation on a Sensitive Asset

This example looks at event IDs to pull specific events when a user account is created on a fictional computer that contains a user password database.

```
<QueryList>
  <Query Id="0" Path="Security">
<Select Path="Security">*[System[(Computer='Password_DB') and
(Level=4 or Level=0) and (EventID=4720 or  (EventID &gt;= 4722
and EventID &lt;= 4726)  or  (EventID &gt;= 4741 and EventID
&lt;= 4743) )]]</Select>
  </Query>
</QueryList>
```

Table B-2 Event IDs in this example

ID	Description
4720	A user account was created.
4722	A user account was enabled.
4723	An attempt was made to change an account's password.
4724	An attempt was made to reset an account's password.
4725	A user account was disabled.
4726	A user account was deleted.
4741	A computer account was created.
4742	A computer account was changed.
4743	A computer account was deleted.

INDEX

W

X