

IBM Security QRadar  
Version 7.2.3

*WinCollect User Guide V7.2.3*

**IBM**

**Note**

Before using this information and the product that it supports, read the information in “Notices” on page 63.

**Product information**

This document applies to IBM QRadar Security Intelligence Platform V7.2.5 and subsequent releases unless superseded by an updated version of this document.

© Copyright IBM Corporation 2011, 2016.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

---

# Contents

<b>About this WinCollect User Guide</b> . . . . .	<b>v</b>
<b>Chapter 1. What's new in WinCollect V7.2.3</b> . . . . .	<b>1</b>
<b>Chapter 2. WinCollect overview</b> . . . . .	<b>3</b>
<b>Chapter 3. Installation prerequisites for WinCollect</b> . . . . .	<b>7</b>
Communication between WinCollect agents and QRadar Event Collector . . . . .	8
Hardware and software requirements for the WinCollect host . . . . .	9
WinCollect agent installations and events per second . . . . .	10
Prerequisites for upgrading WinCollect agents . . . . .	11
<b>Chapter 4. WinCollect installations.</b> . . . . .	<b>13</b>
Installing and upgrading the WinCollect application on QRadar appliances . . . . .	13
Creating an authentication token for WinCollect agents. . . . .	14
Installing the WinCollect agent on a Windows host . . . . .	15
Installing a WinCollect agent from the command prompt . . . . .	17
Uninstalling a WinCollect agent from the command prompt . . . . .	21
Adding multiple destinations to WinCollect agents . . . . .	21
<b>Chapter 5. Configuring WinCollect agents after installation</b> . . . . .	<b>23</b>
Manually adding a WinCollect agent . . . . .	23
Deleting a WinCollect agent . . . . .	24
WinCollect destinations . . . . .	25
Adding a destination . . . . .	25
Deleting a destination from WinCollect . . . . .	26
Scheduling event forwarding and event storage for WinCollect agent . . . . .	27
Configuration options for systems with restricted policies for domain controller credentials . . . . .	27
Local installations with no remote polling . . . . .	28
Configuring access to the registry for remote polling . . . . .	28
Windows event subscriptions for WinCollect agents . . . . .	29
Forwarded events . . . . .	29
Domain controllers . . . . .	29
Supported software environments . . . . .	29
Troubleshooting event collection . . . . .	30
Using Microsoft event subscriptions . . . . .	30
WinCollect logs . . . . .	30
<b>Chapter 6. Log sources for WinCollect agents.</b> . . . . .	<b>33</b>
Common WinCollect log source parameters . . . . .	33
Adding a log source to a WinCollect agent . . . . .	37
Microsoft DHCP log source configuration options . . . . .	38
File Forwarder log source configuration options . . . . .	39
Microsoft IAS log source configuration options . . . . .	40
Microsoft IIS protocol configuration options . . . . .	42
Microsoft ISA log configuration options . . . . .	43
Juniper Steel-Belted Radius log source configuration options . . . . .	46
Microsoft SQL Server log source configuration options . . . . .	46
NetApp Data ONTAP configuration options . . . . .	49
XPath log source configuration options . . . . .	49
XPath queries. . . . .	50
Enabling remote log management on Windows 7. . . . .	50
Enabling remote log management on Windows 2008. . . . .	51
Enabling remote log management on Windows 2008R2. . . . .	51

Creating a custom view . . . . .	51
XPath query examples. . . . .	52
Bulk log sources for remote event collection . . . . .	54
Adding log sources in bulk for remote collection . . . . .	54
<b>Chapter 7. Stand-alone deployments and WinCollect Configuration Console. . . . .</b>	<b>57</b>
WinCollect Configuration Console overview . . . . .	57
Installing the configuration console . . . . .	58
Silently installing, upgrading, and uninstalling WinCollect software . . . . .	59
Creating a WinCollect credential . . . . .	60
Adding a destination to the WinCollect Configuration Console . . . . .	60
Adding a device to the WinCollect Configuration Console. . . . .	60
Sending encrypted events to QRadar . . . . .	61
Collecting local Windows logs . . . . .	61
Collecting remote Windows logs . . . . .	62
<b>Notices . . . . .</b>	<b>63</b>
Trademarks . . . . .	64
Privacy policy considerations . . . . .	65

---

## About this WinCollect User Guide

This documentation provides you with information that you need to install and configure WinCollect agents, and retrieve events from Windows-based event sources. WinCollect is supported by IBM Security QRadar SIEM and IBM Security QRadar Log Manager.

### Intended audience

System administrators who are responsible for installing WinCollect must be familiar with network security concepts and device configurations.

### Technical documentation

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

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

### Contacting customer support

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

### Statement of good security practices

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



---

## Chapter 1. What's new in WinCollect V7.2.3


WinCollect V7.2.3 introduces improvements to disk space maintenance and enables disconnected WinCollect agents to support TLS Syslog.

### **Reduction in the disk space required for log maintenance**

WinCollect manages disk space for logs by compressing and archiving new versions of logs after they reach a certain size. WinCollect also archives the oldest patch checkpoint folder after 10 are created. When QRadar updates WinCollect with new code, the checkpoint folders store a backup of the replaced code. This feature is available automatically for new installations of WinCollect V7.2.3. Users that upgrade to WinCollect V7.2.3 can configure options that enable the log

rollover feature.  Learn more.

### **Stand-alone agents can send events using TLS Syslog**

Configure a log source in WinCollect stand-alone deployments to send encrypted events to IBM Security QRadar.  Learn more.





---

## Chapter 2. WinCollect overview

The WinCollect application is a Syslog event forwarder that administrators can use for Windows event collection with QRadar. The WinCollect application can collect events from systems with WinCollect software installed (local systems), or remotely poll other Windows systems for events.

WinCollect is one of many solutions for Windows event collection. For more information about alternatives to WinCollect, see the *IBM Security QRadar DSM Configuration Guide*.

### How does WinCollect Work?

WinCollect uses the Windows Event Log API to gather events, and then WinCollect sends the events to QRadar.

### WinCollect managed deployment

A managed WinCollect deployment has a QRadar appliance that shares information with the WinCollect agent installed on the Windows hosts that you want to monitor. The Windows host can either gather information from itself, the local host, and, or remote Windows hosts. Remote hosts don't have the WinCollect software installed. The Windows host with WinCollect software installed polls the remote hosts, and then sends event information to QRadar.

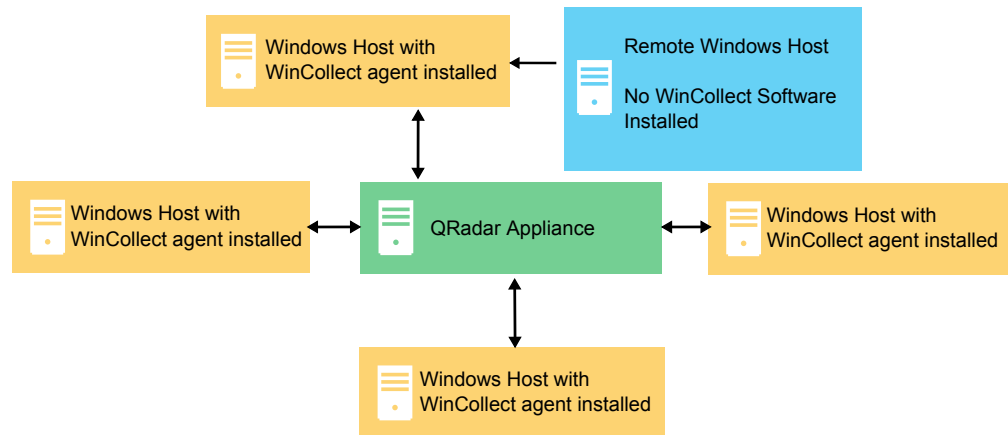


Figure 1. WinCollect managed deployment example

**Important:** In a managed deployment, the WinCollect agents that are installed on Windows hosts can be managed by either a QRadar console or a QRadar Managed Host.

WinCollect works best when a managed deployment monitors up to 500 Windows agents. If you want to monitor more than 500 Windows hosts, the suggested proven practice is to use the stand-alone WinCollect deployment. For more information, see Chapter 7, “Stand-alone deployments and WinCollect Configuration Console,” on page 57.

The managed WinCollect deployment has the following capabilities:

- Central management from the QRadar Console.
- Automatic local log source creation at the time of installation.
- Event storage to ensure that no events are dropped.
- Collects forwarded events from Microsoft Subscriptions.
- Filters events by using XPath queries or exclusion filters.
- Supports more remote Windows sources than the Adaptive Log Exporter.
- Supports virtual machine installations.
- Console can send software updates to remote WinCollect agents without you reinstalling agents in your network.
- Forwards events on a set schedule (Store and Forward)

## WinCollect stand-alone deployment

If you need to collect Windows events from more than 500 hosts, use the stand-alone WinCollect deployment. A stand-alone deployment is a Windows host in unmanaged mode with WinCollect software installed. The Windows host can either gather information from itself, the local host, and, or remote Windows hosts. Remote hosts don't have the WinCollect software installed. The Windows host with WinCollect software installed polls the remote hosts, and then sends event information to QRadar. To save time when you configure more than 500 Windows hosts, you can use a solution such as IBM Endpoint Manager. Automation can help you manage stand-alone instances.

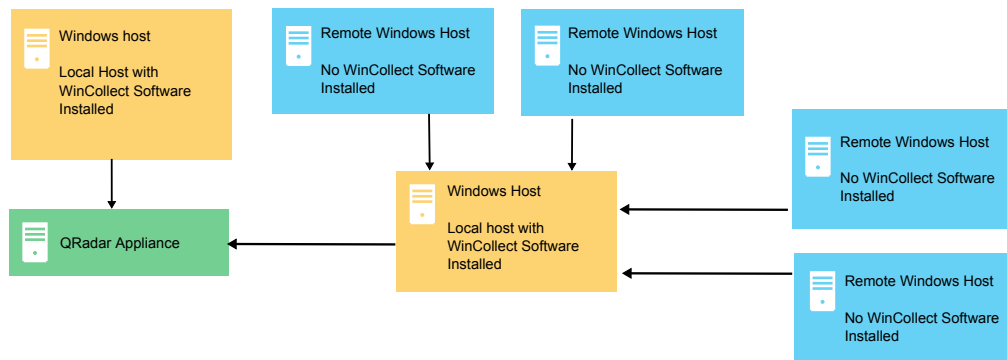


Figure 2. WinCollect stand-alone deployment example

You can also deploy stand-alone WinCollect to consolidate event data on one Windows host, where WinCollect collects events to send to QRadar.

Stand-alone WinCollect mode has the following capabilities:

- You can configure each WinCollect agent by using the WinCollect Configuration Console.
- You can update WinCollect software with the software update installer.
- Event storage to ensure that no events are dropped.
- Capable of collecting “Forwarded” events from Microsoft Subscriptions.
- Capable of filtering events by using XPath queries or exclusion filters.
- Supports more remote Windows sources than the Adaptive Log Exporter.
- Officially supports virtual machine installs.

**Important:** Managed WinCollect deployments are not supported on IBM Security Intelligence on Cloud.

## Setting up a Managed WinCollect deployment

For a managed deployment, you follow these steps:

1. Understand the prerequisites for managed WinCollect, which ports to use, what hardware is required, how to upgrade. For more information, see Chapter 3, “Installation prerequisites for WinCollect,” on page 7.
2. Install the WinCollect application on the QRadar console that is used to monitor your Windows hosts. For more information, see “Installing and upgrading the WinCollect application on QRadar appliances” on page 13.
3. Create an authentication token so that the Windows hosts can send information to QRadar. For more information, see “Creating an authentication token for WinCollect agents” on page 14.
4. Install the WinCollect agent on the Windows hosts. For more information, see one of the following options:
  - “Installing the WinCollect agent on a Windows host” on page 15
  - “Installing a WinCollect agent from the command prompt” on page 17, or
  - “Manually adding a WinCollect agent” on page 23
5. If you want to add bulk log sources by using domain controllers in your deployment, see “Bulk log sources for remote event collection” on page 54.
6. If you want to configure forwarded events, or event subscriptions, see “Windows event subscriptions for WinCollect agents” on page 29.
7. If you want to tune your WinCollect installation, see the event tuning profile section in “Common WinCollect log source parameters” on page 33.
8. If you want to set up multiple QRadar destinations in case one fails, see “Adding multiple destinations to WinCollect agents” on page 21.

## Setting up a stand-alone WinCollect deployment

For a stand-alone deployment, follow these steps:

1. Install the WinCollect software on the Windows host or hosts that send Windows events to QRadar. For more information, see “Installing the WinCollect agent on a Windows host” on page 15.
2. Install the WinCollect configuration console and, or the WinCollect software update. For more information, see “Installing the configuration console” on page 58 or “Silently installing, upgrading, and uninstalling WinCollect software” on page 59.
3. Configure the destination, or the QRadar appliance where the Windows hosts send Windows events. For more information, see “Adding a destination to the WinCollect Configuration Console” on page 60.
4. If you collect events from remote hosts, create credentials so that WinCollect can log in to the remote hosts. See “Creating a WinCollect credential” on page 60.
5. Set up the devices that send Windows events to WinCollect. For more information, see “Adding a device to the WinCollect Configuration Console” on page 60.



---

## Chapter 3. Installation prerequisites for WinCollect

Before you can install WinCollect agents, you must verify that your deployment meets the installation requirements.

### Distribution options for WinCollect agents

WinCollect agents can be distributed in a remote collection configuration or installed on the local host. The following WinCollect collection methods are available: local and remote.

#### Local collection

The WinCollect agent collects events only for the host on which it is installed. You can use this collection method on a Windows host that is busy or has limited resources, for example, domain controllers.

**Important:** Domain Controllers must have WinCollect software installed. Do not poll Domain Controllers as remote hosts.

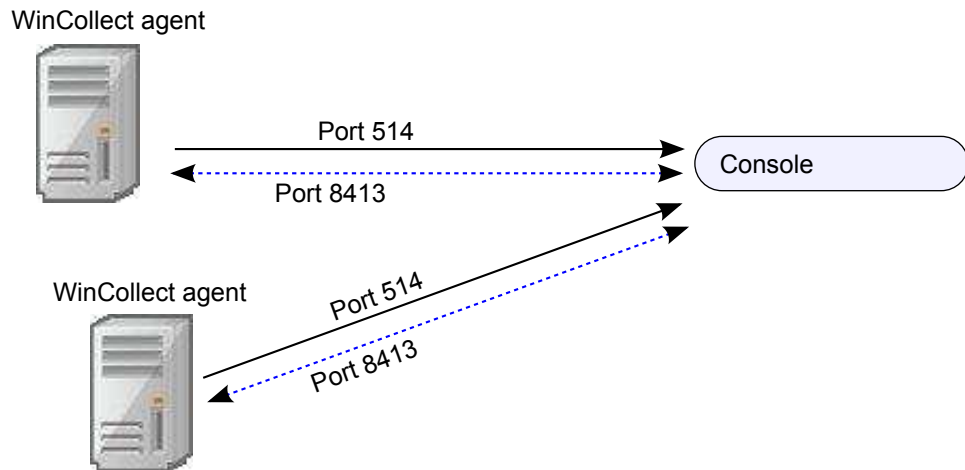


Figure 3. Local collection for WinCollect agents

#### Remote Collection

The WinCollect agent is installed on a single host and collects events from multiple Windows systems. Use remote collection to easily scale the number of Windows log sources that you can monitor.

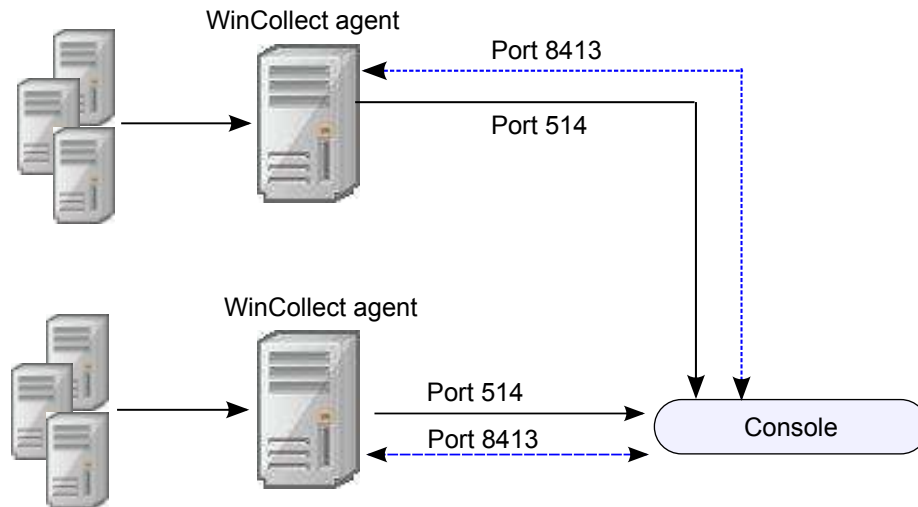


Figure 4. Remote collection for WinCollect agents

## System performance and deployment strategies

Use the following strategies to reduce the impact to system performance:

- To reduce the total number of agents, use remote collection where one agent monitors many endpoints.
- If you update a group of WinCollect agents, do it during off-peak operating hours.
- Deploy and manage the WinCollect agents in groups of 100 and monitor system performance for issues.

---

## Communication between WinCollect agents and QRadar Event Collector

Open ports are required for data communication between WinCollect agents and the QRadar host, and between WinCollect agents and the hosts that they remotely poll.

### WinCollect agent communication to QRadar Console and Event Collectors

All WinCollect agents communicate with the QRadar Console and Event Collectors to forward events to QRadar and request updated information. You must ensure firewalls that are between the QRadar Event Collectors and your WinCollect agents allow traffic on the following ports:

#### Port 8413

This port is required for managing the WinCollect agents. Port 8413 is used for features such as configuration updates. Traffic is always initiated from the WinCollect agent. This traffic is sent over TCP and communication is encrypted.

#### Port 514

This port is used by the WinCollect agent to forward syslog events to QRadar. You can configure WinCollect log sources to provide events by using TCP or UDP. You can decide which transmission protocol is required for each WinCollect log source. Port 514 traffic is always initiated from the WinCollect agent.

### WinCollect local port usage on the Windows host

The WinCollect service (WinCollectSvc.exe) uses port 12345 locally on the Windows host to listen for notifications from the WinCollect application (WinCollect.exe). If another Windows application uses port 12345, the WinCollect service encounters a port conflict, which can prevent the service from starting. To diagnose and troubleshoot this issue, see [www.ibm.com/support \(http://www-01.ibm.com/support/docview.wss?uid=swg21967256\)](http://www.ibm.com/support/docview.wss?uid=swg21967256).

### WinCollect agents remotely polling Windows event sources

WinCollect agents that remotely poll other Windows operating systems for events that include extra port requirements. The following ports are used when WinCollect agents remotely poll for Windows-based events:

*Table 1. Port usage for WinCollect remote polling*

Port	Protocol	Usage
135	TCP	Microsoft Endpoint Mapper
137	UDP	NetBIOS name service
138	UDP	NetBIOS datagram service
139	TCP	NetBIOS session service
445	TCP	Microsoft Directory Services for file transfers that use Windows share

Collecting events by polling remote Windows systems uses dynamic RPC. To use dynamic RPC, you must allow inbound traffic to the Windows system that WinCollect attempts to poll for events on port 135. Port 135 is used for Endpoint Mapping by Windows.

If you remotely poll any Windows operating system other than the Windows Vista operating system, you might need to allow ports in the range between 1024 and port 5000. You can configure Windows to restrict the communication to specific ports for the older versions of Windows Firewall. For more information, see your Windows documentation.

**Important:** To limit the number of events that are sent to QRadar, administrators can use exclusion filters for an event based on the EventID or Process. For more information about WinCollect filtering, see WinCollect Event Filtering (<http://www.ibm.com/support/docview.wss?uid=swg21672656>).

---

## Hardware and software requirements for the WinCollect host

Ensure that the Windows-based computer that hosts the WinCollect agent meets the minimum hardware and software requirements

The following table describes the minimum hardware requirements:

*Table 2. Hardware requirements for WinCollect*

Requirement	Description
Memory	8 GB 2 GB reserved for the WinCollect agent

Table 2. Hardware requirements for WinCollect (continued)

Requirement	Description
Processing	Intel Core 2 Duo processor 2.0 GHz
Disk space	3 GB of available disk space for software and log files.  6 GB might be required if events are stored on a schedule.
Available processor resources	20%

The following table describes the supported software:

Table 3. Software requirements

Requirement	Description
Operating system	Windows Server 2008 (most recent)  Windows Server 2012 (most recent)  Windows 7 (most recent)  Windows 8 (most recent)  Windows Vista (most recent)
Distribution	One WinCollect agent for each Windows host.
Required user role permissions for installation	Administrator, or local administrator  Administrative permissions are not required for remote collection.

**Important:** WinCollect is not supported on versions of Windows that have been moved to End Of Life by Microsoft. After software is beyond the Extended Support End Date the product might still function as expected, however, IBM will not make code or vulnerability fixes to resolve WinCollect issues for older operating systems. For example, Microsoft Windows Server 2003 R2 and Microsoft Windows XP are operating systems that are beyond the 'Extended Support End Date'. Any questions about this announcement can be discussed in the IBM Security QRadar Collecting Windows Events (WMI/ALE/WinCollect) forum. For more information, see <https://support.microsoft.com/en-us/lifecycle/search> (<https://support.microsoft.com/en-us/lifecycle/search>).

---

## WinCollect agent installations and events per second

Before you install your WinCollect agents, it is important to understand the number of events that can be collected by a WinCollect agent.

The event per second (EPS) rates in the following table represent a test network. This information can help you determine the number of WinCollect agents that you need to install on your network. WinCollect supports default EPS rates and also supports tuning. Tuning can help you to improve the performance of a single WinCollect agent.



Exceeding these EPS rates without tuning can cause you to experience performance issues or event loss, especially on busy systems. The following table describes the default EPS rate in the test environment:

*Table 4. EPS rates in a test environment*

Installation type	Tuning	EPS	Log sources	Total events per second (EPS)
Local Collection	Default	250	1	250
Local Collection	Tuned	5000	1	5000
Remote Collection	Default	5 - 10	500	2500
Remote Collection	Tuned	varies	varies	2500+

Tuning an agent to increase the EPS rates for remote event collection depends on your network, the number of log sources that you assign to the agent, and the number of events that are generated by each log source. For more information about events and tuning, see Log Source Event Rates and Tuning Profiles (<http://www.ibm.com/support/docview.wss?uid=swg21672193>).

---

## Prerequisites for upgrading WinCollect agents

Before you upgrade WinCollect agents, ensure that your software meets the version requirements.

### WinCollect and QRadar software versions

The version of the installed WinCollect depends on the version of QRadar that you are running.

*Table 5. Software version matrix*

QRadar Version	Minimum WinCollect Version	RPM Minimum Version
QRadar V7.1 (MR2)	WinCollect 7.2.2-2	AGENT-WINCOLLECT-7.1-1018604.noarch
QRadar V7.2.x or later	WinCollect 7.2.2-2	AGENT-WINCOLLECT-7.2-1018607.noarch

### Checking the installed version of the WinCollect agent

You can check the version of the installed WinCollect agent by using one of the following methods:

1. In QRadar, select **Help > About**
2. Select the **Additional Release Information** link.
3. If you want to verify the WinCollect agent release, use ssh to log in to the QRadar Console as the root user, and run the following command:

```
rpm -qa | grep -i AGENT-WINCOLLECT
```



---

## Chapter 4. WinCollect installations

To install WinCollect, you must download and install a WinCollect agent on your QRadar system, create an authentication token, and then install a WinCollect agent on each Windows host that you want to collect events from. You can also install the WinCollect agent on a Windows host that you want to use to remotely collect events from other Windows hosts.

---

### Installing and upgrading the WinCollect application on QRadar appliances

To manage a deployment of WinCollect agents from the QRadar user interface, you must first install the WinCollect application on your QRadar Console. This application includes the required protocols to enable communication between the QRadar system and the managed WinCollect hosts. You can use the WinCollect installation file to initially install a WinCollect application on your QRadar host and to upgrade your WinCollect agents to newer versions.

#### About this task

**Important:** For information about upgrading WinCollect versions 7.0 through 7.1.0, see [www.ibm.com/support](http://www.ibm.com/support) (<http://www-01.ibm.com/support/docview.wss?uid=swg21698127>).

When you upgrade a WinCollect application file, the QRadar host automatically updates all WinCollect agents that are enabled to receive automatic updates from the Console. WinCollect agents request updated configurations from the QRadar host on a frequency that is determined by the configuration polling interval. If new WinCollect agent files are available for download, the agent downloads and installs updates and restarts required services. No events are lost when you update your WinCollect agent because events are buffered to disk. Event collection forwarding continues when the WinCollect service starts.

**Important:** If you reinstalled QRadar after a previous WinCollect installation, you must delete the ConfigurationServer.PEM file in **Program Files > IBM > WinCollect > config** before WinCollect can function properly.

#### Procedure

1. Download the WinCollect application installation file from the IBM website: (<http://www.ibm.com/support>).
2. Using a program such as WinSCP, copy the installation file to your QRadar system.
3. Log in to QRadar as the root user.
4. For initial installations, create the /media/patch directory. Type the following command:  

```
mkdir /media/patch
```
5. To mount the installation file, type the following command:  

```
mount -t squashfs -o loop Installer_file_name.sfs /media/patch
```

Example:

```
mount -t squashfs -o loop 720_QRadat_wincollectupdate-7.2.0.xxx.sfs /media/patch
```

6. To change to the /media/patch, type the following command:  
`cd /media/patch`
7. To install WinCollect, type the following command and then follow the prompts:  
`./installer`
8. Optional: Verify that WinCollect agents are configured to accept remote updates:
  - a. Log in to QRadar.
  - b. On the navigation menu, click **Data Sources**.
  - c. Click the **WinCollect** icon.
  - d. Click **Agents**.
  - e. Review the **Enabled** column for agents with a **False** value.
  - f. Select the WinCollect agents that have a **False** value in the **Enabled** column.
  - g. Click **Enable/Disable Automatic Updates**.

## Results

WinCollect agents that are enabled for automatic updates are updated and restarted. The amount of time it takes an agent to update depends on the configuration polling interval for the WinCollect agent.

### Related tasks:

“Installing the WinCollect agent on a Windows host” on page 15

Install the WinCollect agent on each Windows host from which you want to collect events in your network. The WinCollect agent can be configured to collect events on local host or from a remote server, or both.

“Installing a WinCollect agent from the command prompt” on page 17

For non-interactive installations, you can install the WinCollect agent from the command prompt. Use silent installation to deploy WinCollect agents simultaneously to multiple remote systems.

---

## Creating an authentication token for WinCollect agents

Third-party or external applications that interact with IBM Security QRadar require an authentication token. Before you install WinCollect agents in your network, you must create an authentication token.

This authentication token is required for every WinCollect agent you install.

The authentication token allows WinCollect agents to exchange data with QRadar appliances. Create one authentication token to be used for all of your WinCollect agents that communicate events with your QRadar host. If the authentication token expires, the WinCollect agent cannot receive log source configuration changes.

### Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click the **Authorized Services** icon.
4. Click **Add Authorized Service**.
5. In the **Manage Authorized Services** window, configure the parameters.

Table 6. Add Authorized Services parameters

Parameter	Description
Service Name	The name can be up to 255 characters in length, for example, WinCollect Agent.
User Role	Administrators can create a user role or assign a default user role to the authorization token. For most configurations, the <b>All</b> user role can be selected. <b>Note:</b> The admin user role provides more privileges, which can create a security concern.
Expiry	Do not set an expiry date for the authentication token.

6. Click **Create Service**.
7. Record the token value.

---

## Installing the WinCollect agent on a Windows host

Install the WinCollect agent on each Windows host from which you want to collect events in your network. The WinCollect agent can be configured to collect events on local host or from a remote server, or both.

### Before you begin

Ensure that the following conditions are met:

- You created an authentication token for the WinCollect agent.  
For more information, see “Creating an authentication token for WinCollect agents” on page 14..
- Your system meets the hardware and software requirements.  
For more information, see “Hardware and software requirements for the WinCollect host” on page 9.
- The required ports are available to WinCollect agents to communicate with QRadar Event Collectors.  
For more information, see “Communication between WinCollect agents and QRadar Event Collector” on page 8.
- If you want to automatically create a log source for this agent, you must know the name of the destination that you want to send your Windows log source to.  
During the installation, you can configure QRadar to automatically create a log source for the WinCollect agent host. You must configure a forwarding destination host for the log source data. For more information, see “Adding a destination” on page 25. The WinCollect agent sends the Windows event logs to the configured destination. The destination can be the console or an Event Collector. To configure automatic log source creation, your QRadar system must be updated to IBM Security QRadar SIEM V7.2.1 software update 1 or later.

### Procedure

1. Download the WinCollect agent setup file from the IBM Support website (<http://www.ibm.com/support>).
2. If the Services window is open on the Windows host, close it to prevent failure of the WinCollect agent installation.

3. Right-click the WinCollect agent installation file and select **Run as administrator**.
4. Follow the prompts in the installation wizard.

**Important:** For stand-alone deployments, you must leave the **Configuration Server (host and port)** field empty.

Table 7. WinCollect installation wizard parameters

Parameter	Description
<b>Host Identifier</b>	<p>Use a unique identifier for each WinCollect agent you install. The name that you type in this field is displayed in the WinCollect agent list of the QRadar Console.</p> <p>The value in the <b>Host Identifier</b> field must match the value in the <b>Host Name</b> field in the WinCollect Agent configuration on the QRadar Console.</p>
<b>Authentication Token</b>	The authentication token that you created in QRadar, for example, af111ff6-4f30-11eb-11fb-1fc117711111.
<b>Configuration Server (host and port)</b>	<p>Required for all installations, except stand-alone mode. Leave blank for stand-alone mode installations.</p> <p>The IP address or host name of your QRadar Console, for example, 100.10.10.1 or myhost</p> <p>This parameter is for the your QRadar Console or Event Collector. To use an Event Collector as your Configuration Server, your QRadar system must be updated to V7.2.1 software update 3 or later.</p>
<b>StatusServer</b>	The address of the appliance to which the status events are sent. If no value is provided, the <b>ConfigurationServer</b> is used. If both values are empty, no status messages are sent.
<b>Enable Automatic Log Source Creation</b>	If this check box is enabled, you must provide information about the log source and the target destination.
<b>Log Source Name</b>	The name can be up to 255 characters in length.
<b>Log Source Identifier</b>	Required if the <b>Enable Automatic Log Source Creation</b> check box is selected. Identifies the remote device that the WinCollect agent polls.
<b>Event Logs</b>	The Windows event logs that you want the log source to collect and send to QRadar.
<b>Target Destination</b>	Required if <b>Automatic Log Source Creation</b> is enabled. The WinCollect destination must be configured in QRadar before you continue entering information in the installation wizard.

Table 7. WinCollect installation wizard parameters (continued)

Parameter	Description
Machine poll interval (msec)	<p>The polling interval that determines the number of milliseconds between queries to the Windows host.</p> <ul style="list-style-type: none"> <li>• Use a polling interval of 3500 when the WinCollect agent collects events from computers that have a low event per second rate, for example, collecting from 50 remote computers that provide 20 events per second or less.</li> <li>• Use a polling interval of 1000 when the WinCollect agent collects events from a few 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.</li> </ul> <p>The minimum polling interval is 250 milliseconds. The default is 3000 milliseconds or 3 seconds.</p>
Minimum number of logs to process per pass	For more information, see IBM Support ( <a href="http://www-01.ibm.com/support/docview.wss?uid=swg21672193">http://www-01.ibm.com/support/docview.wss?uid=swg21672193</a> ).
Maximum number of logs to process per pass	For more information, see IBM Support ( <a href="http://www-01.ibm.com/support/docview.wss?uid=swg21672193">http://www-01.ibm.com/support/docview.wss?uid=swg21672193</a> ).

## Installing a WinCollect agent from the command prompt

For non-interactive installations, you can install the WinCollect agent from the command prompt. Use silent installation to deploy WinCollect agents simultaneously to multiple remote systems.

### About this task

The WinCollect installer uses the following command options:

Table 8. Silent installation options for WinCollect agents

Option	Description
/qn	Runs the WinCollect agent installation in silent mode.
INSTALLDIR	<p>Optional.</p> <p>The name of the installation directory cannot contain spaces. Use quotation marks, " , to enclose the directory, for example, <code>INSTALLDIR="C:\IBM\WinCollect\"</code></p> <p>If you do not use the <code>INSTALLDIR</code> field, WinCollect installs to the default Windows path, such as <code>C:\Program Files\IBM\WinCollect\</code></p>

Table 8. Silent installation options for WinCollect agents (continued)

Option	Description
AUTH_TOKEN=token	Authorizes the WinCollect service, for example, AUTH_TOKEN=af111ff6-4f30-11eb-11fb-1fc1 17711111
HOSTNAME=host name	<p>The Hostname field is used to assign a name to the WinCollect agent. The values that are used in this field can be an identifiable name, hostname, or IP address. In most cases, administrators can use HOSTNAME=%COMPUTERNAME% to auto populate this field.</p> <p><b>Example:</b> HOSTNAME="windows-%computername%"            HOSTNAME=WindowsSrv1            HOSTNAME=%COMPUTERNAME%</p> <p>The IP address or host name of the WinCollect agent host cannot contain the "at" sign, @.</p>
FULLCONSOLEADDRESS=host_address	<p>The IP address or host name of your QRadar appliance that manages the agent. The address must be a QRadar appliance capable of receiving events.</p> <p><b>Example:</b> FULLCONSOLEADDRESS=100.10.10.1            FULLCONSOLEADDRESS=EPqadar.myhost.com</p> <p>For your Windows hosts to communicate with your QRadar Event Collector, all systems in your QRadar deployment must be updated to V7.2.1 Patch 3 or later.</p>
LOG_SOURCE_AUTO_CREATION_ENABLED	<p>If you enable this option, you must configure the log source parameters.</p> <p>QRadar systems must be updated to V7.2.1 Patch 1 or later.</p>
STATUSSERVER	<p>Optional.</p> <p>Specifies the server where the status messages from the agent are sent. The host name or IP address that is specified in this field must be a QRadar appliance capable of receiving events.</p> <p><b>Example:</b>            STATUSSERVER=172.10.10.10            STATUSSERVER=EPqadar.myhost.com</p>
LOG_SOURCE_AUTO_CREATION_PARAMETERS	<p>Ensure that each parameter uses the format: Parameter_Name=value.</p> <p>The parameters are separated with ampersands, &amp;.</p> <p>Your QRadar system must be updated to V7.2.1 Patch 1 or later.</p>



Table 9. Log source creation options.

Option	Description/Required Value
Component1.AgentDevice	DeviceWindowsLog
Component1.Action	create
Component1.LogSourceName	Optional. The name that you want to give to this log source.
Component1.LogSourceIdentifier	The IP address or host name of the system that the agent is installed on.
Component1.Destination.Name	The destination name is an alphanumeric value that is used to specify where a WinCollect log source sends event data. This value must be a QRadar appliance capable of receiving event data, such as an Event Processor, Event Collector, or QRadar Console. <b>Important:</b> The destination name must exist in the QRadar user interface before the installation, otherwise the log source configuration parameters are discarded and no log sources are auto created.
Component1.CoalesceEvents	Optional. Increases the event count when the same event occurs multiple times within a short time interval. Coalesced events provide a way to view and determine the frequency with which a single event type occurs on the Log Activity tab. When this option is disabled, events are viewed individually and events are not bundled. New and automatically discovered log sources inherit the value from the System Settings configuration on the Console.
Component1.StoreEventPayload	Optional. Specifies that event payloads are to be stored.
Component1.Encoding	Optional. Use this option to change the default character encoding from UTF-8.
Component1.Log.Application	Required. True or False.  The Windows Application log contains Information, Warning, Error, Success Audit, and Failure Audit events.
Component1.Log.Security	Required. True or False.  The Windows Security log contains events that are defined in the audit policies for the object.
Component1.Log.System	Required. True or False.  The Windows System log contains Security, Application, Setup, System, and Forwarded events.
Component1.Log.DNS+Server	Required. True or False.  The Windows DNS Server log contains DNS events.

Table 9. Log source creation options (continued).

Option	Description/Required Value
Component1.Log.Directory+Service	<p>Required. True or False.</p> <p>The Windows Directory Service log contains events that are written by the active directory.</p>
Component1.Log.File+Replication+Service	<p>Required. True or False.</p> <p>The Windows File Replication Service log contains events about changed files that are replicated on the system.</p>
Component1.MaxLogsToProcessPerPass	<p>Not required.</p> <p>The maximum number of logs (in binary form) that the algorithm attempts to acquire in one pass, if remaining retrievable events exist.</p> <p><b>Example:</b> Component1.MaxLogsToProcessPerPass=400</p> <p><b>Important:</b> Use this parameter to improve performance for event collection, however, this parameter can also increase processor usage. For more information about Tuning, see WinCollect: Tuning older WinCollect Systems (<a href="http://www.ibm.com/support/docview.wss?uid=swg21699327">http://www.ibm.com/support/docview.wss?uid=swg21699327</a>).</p>
Component1.MinLogsToProcessPerPass	<p>Not required.</p> <p>The minimum number of logs (in binary form) that the algorithm attempts to read in one pass, if remaining retrievable events exist.</p> <p><b>Example:</b> Component1.MinLogsToProcessPerPass=200</p> <p><b>Important:</b> You can use this parameter to improve performance for event collection, but this parameter can also increase processor usage. For more information about Tuning, see WinCollect: Tuning older WinCollect Systems (<a href="http://www.ibm.com/support/docview.wss?uid=swg21699327">http://www.ibm.com/support/docview.wss?uid=swg21699327</a>).</p>

## Procedure

1. Download the WinCollect agent setup file from the IBM website ([www.ibm.com/support](http://www.ibm.com/support)).
2. On the Windows host, open a command prompt by using **Run as Administrator**.
3. Ensure that the Services window is closed on the Windows host, otherwise the WinCollect agent installation fails.

**Important:** The destination name that is used during automatic log source creation must exist before the command-line installation runs. Verify the destination name in the QRadar user interface before you start the installation.

4. Type the following command:

```
AGENT-WinCollect-7.2.0.<build>-setup.exe /s /v" /qn  
INSTALLDIR=<"C:\IBM\WinCollect">  
AUTHTOKEN=<token> FULLCONSOLEADDRESS=<host_address>  
HOSTNAME=<hostname> LOG_SOURCE_AUTO_CREATION=<true|false>  
LOG_SOURCE_AUTO_CREATION_PARAMETERS=<"parameters"">
```

The following example shows an installation where the log source is automatically created.

```
C:\>AGENT_x64_WinCollect-7.2.2.1018564-setup.exe /s /v"/qn  
INSTALLDIR="C:\IBM" AUTHTOKEN=111111-aaaa-1111-aaaa-11111111  
FULLCONSOLEADDRESS=qradar.example.com:8413 HOSTNAME=COMPUTER-%COMPUTERNAME%  
LOG_SOURCE_AUTO_CREATION_ENABLED=True LOG_SOURCE_AUTO_CREATION_PARAMETERS="  
"Component1.AgentDevice=DeviceWindowsLog&Component1.Action=create&  
Component1.LogSourceName=%computername%&Component1.LogSourceIdentifier  
=%computername%&Component1.Destination.Name=Local&Component1.CoalesceEvents  
=True&Component1.StoreEventPayload=True&Component1.Encoding=UTF-8&  
Component1.Log.Application=True&Component1.Log.Security=True&  
Component1.Log.System=False&Component1.Log.DNS+Server=False&Component  
1.Log.Directory+Service=False&Component1.Log.File+Replication+Service=False""
```

5. Press Enter.

---

## Uninstalling a WinCollect agent from the command prompt

You can uninstall the WinCollect agent from the command prompt.

### Procedure

1. From the desktop, select **Start > Run**, type cmd, and click **OK**.  
**Attention:** You need to run the command prompt as an administrative user.
2. Type the following command:  

```
msiexec /x{1E933549-2407-4A06-8EC5-83313513AE4B} /norestart /qn
```
3. Press Enter.

---

## Adding multiple destinations to WinCollect agents

In a managed WinCollect deployment, add IBM Security QRadar appliances as destinations for Windows events if a QRadar appliance fails.

### Before you begin

You must create the destinations that you want to add to the WinCollect agent. See “Adding a destination” on page 25.

### About this task

Each destination that you create for a WinCollect agent has its own disk cache for events. If Site A fails and Site B is configured as the Target External Destination, Site B continues to receive events and Site A stores events to disk. If both sites fail, both systems are caching events independently to separate disk queues. As connections return for individual log sources, the agents attempt to balance sending new events and cached events that are queued due to either bursting events, or connection issues.

If your deployment contains many log sources by using multiple destinations, increase the default disk space. Each agent is configured with 6 GB of disk space to cache events. However, if there are 50 log sources or more, each sending to multiple destinations, and a network segment fails, each log source writes two sets of events to the same cache on the Target Internal and the Target External destination. If your deployment contains segments that are unstable or a prone to outages, update the default storage capacity of the agent in the event of a long term outage.

### **Procedure**

1. In QRadar, click the **Admin** tab.
2. On the navigation menu, click **Data Sources**.
3. Click the **WinCollect** icon.
4. Click **Agents** and select the agent that you want to edit.
5. Click **Log Sources**.
6. Select the **Target External Destinations** check box.
7. Select the destinations that you want to add to the agent from the box below the **Target External Destinations** check box.
8. Click **Save**.

---

## Chapter 5. Configuring WinCollect agents after installation

After you install a WinCollect deployment, you manage your deployment by using the IBM Security QRadar.

You can manage your WinCollect agents, destinations, and schedules. You can also manage configuration options for systems with restricted policies.

The WinCollect agent is responsible for communicating with the individual log sources, parsing events, and forwarding the event information to QRadar by using syslog.

After you install the WinCollect agent on your Windows host, wait for QRadar to automatically discover the WinCollect agent. The automatic discovery process typically takes a few minutes to complete.

**Note:** The registration request to the QRadar host might be blocked by firewalls in your network.

---

### Manually adding a WinCollect agent

If you delete your WinCollect agent, you can manually add it back. To reconnect to an existing WinCollect agent, the host name must exactly match the host name that you used before you deleted the agent.

When you delete a WinCollect agent, the IBM Security QRadar Console removes the agent from the agent list and disables all of the log sources that are managed by the deleted WinCollect agent.

WinCollect agents that were previously automatically discovered are not rediscovered in WinCollect. To add a deleted WinCollect agent back to the agent list in the QRadar, you must manually add the deleted agent.

For example, you delete a WinCollect agent that has a host identifier name VM Rack1. You reinstall the agent and use the same host identifier name, VM Rack1. The WinCollect agent does not automatically discover the WinCollect agent.

#### Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **Data Sources**.
3. Click **Agents**.
4. Click **Add**.
5. Configure the parameters.

The following table describes some of the parameters:

Table 10. WinCollect agent parameters

Parameter	Description
<b>Host Name</b>	Depending on the method that you used to install the WinCollect agent on the remote host, the value in the <b>Host Name</b> field must match one of the following values: <ul style="list-style-type: none"> <li>• <b>HOSTNAME</b> field in the WinCollect agent command-line configuration</li> <li>• <b>Host Identifier</b> field in the WinCollect agent installer.</li> </ul>
<b>Description</b>	Optional. If you specified an IP address as the name of the WinCollect agent, add descriptive text to identify the WinCollect agent or the log sources the WinCollect agent is managing.
<b>Automatic Updates Enabled</b>	Controls whether configuration updates are sent to the WinCollect agent.
<b>Heart Beat Interval</b>	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.
<b>Configuration Poll Interval</b>	Defines how often the WinCollect agent polls the IBM Security QRadar Console for updated log source configuration information or agent software updates. The interval ranges from 1 minute to 20 minutes.
<b>Disk Cache Capacity (MB)</b>	Used to buffer events to disk when your event rate exceeds the event throttle or when the WinCollect agent is disconnected from the Console.  6 GB might be required when events are stored on a schedule.
<b>Disk Cache Root Directory</b>	The directory where the WinCollect agent stores cached WinCollect events.

6. Click **Save**.

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

The WinCollect agent is added to the agent list.

**Related tasks:**

“Deleting a WinCollect agent”

When you delete a WinCollect agent, the IBM Security QRadar Console removes the agent from the agent list and disables all of the log sources that are managed by the deleted WinCollect agent.

---

## Deleting a WinCollect agent

When you delete a WinCollect agent, the IBM Security QRadar Console removes the agent from the agent list and disables all of the log sources that are managed by the deleted WinCollect agent.

## Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **Data Sources**.
3. Click the **WinCollect** icon.
4. Select the agents that you want to delete and click **Delete**.
5. Click **Save**.
6. On the **Admin** tab, click **Deploy Changes**.

**Tip:** To delete multiple WinCollect agents, press Ctrl to select multiple agents, and then click **Delete**.

### Related tasks:

“Manually adding a WinCollect agent” on page 23

If you delete your WinCollect agent, you can manually add it back. To reconnect to an existing WinCollect agent, the host name must exactly match the host name that you used before you deleted the agent.

---

## WinCollect destinations

WinCollect destinations define the parameters for how the WinCollect agent forwards events to the Event Collector or IBM Security QRadar Console.

### Adding a destination

To assign where WinCollect agents in your deployment forward their events, you can create destinations for your WinCollect deployment.

#### Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **Data Sources**.
3. Click the **WinCollect** icon.
4. Click **Destinations** and then click **Add**.
5. Configure the parameters.

The following table describes some of the parameters

*Table 11. Destination parameters*

Parameter	Description
<b>Port</b>	IBM Security QRadar receives events from WinCollect agents on either UDP or TCP port 514.
<b>Throttle (events per second)</b>	Defines a limit to the number of events that the WinCollect agent can send each second.
<b>Queue High Water Mark (bytes)</b> <b>Important:</b> The destination name is used during automatic log source creation and must exist before the command-line installation runs. Verify the destination name in QRadar before starting the installation.	Defines an upper limit to the size of the event queue.  If the high water mark limit is reached, the WinCollect agent attempts to prioritize events to reduce the number of queued events.

Table 11. Destination parameters (continued)

Parameter	Description
<b>Queue Low Water Mark (bytes)</b> <b>Important:</b> Do not change the default values unless QRadar support recommends the change.	Defines a lower limit to the size of the event queue.  If the queue changes from a high water mark to a level that is at or below the low water mark limit, the event prioritization returns to normal.
<b>Storage Interval (seconds)</b> <b>Important:</b> Do not change the default values unless QRadar support recommends the change. <b>Important:</b> Do not change the default values unless QRadar support recommends the change.	Defines an interval before the WinCollect agent writes events to disk or memory.
<b>Processing Period (microseconds)</b> <b>Important:</b> Do not change the default values unless QRadar support recommends the change.	Defines the frequency with which the WinCollect agent evaluates the events in the forward queue and the events in the on disk queue. Used to optimize event processing.
<b>Schedule Mode</b>	If you select the <b>Forward Events</b> option, the WinCollect agent forwards events within a user-defined schedule. When the events are not being forwarded, they are stored until the schedule runs again.  If you select the <b>Store Events</b> option, the WinCollect agent stores events to disk only within a user-defined schedule and then forwards events to the destination as specified.

6. Click **Save**.

## Deleting a destination from WinCollect

If you delete a destination, the event forwarding parameters are removed from the WinCollect agent.

Destinations are a global parameter. If you delete a destination when log sources are assigned to the destination, the WinCollect agent cannot forward events. Event collection is stopped for a log source when an existing destination is deleted. Events on disk that were not processed are discarded when the destination is deleted.

### Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **Data Sources**.
3. Click the **WinCollect** icon.
4. Click **Destinations**.
5. Select the destination that you want to delete and click **Delete**.



## Scheduling event forwarding and event storage for WinCollect agent

Use a schedule to manage when WinCollect agents forward or store events to disk in your deployment.

Schedules are not required. If a schedule does not exist, the WinCollect agent automatically forwards events and stores them only when network limitations cause delays.

You can create schedules for your WinCollect deployment to assign when the WinCollect agents in your deployment forward their events. Events that are unable to be sent during the schedule are automatically queued for the next available interval.

### Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **Data Sources**.
3. Click the **WinCollect** icon.
4. Click **Schedules**.
5. Click **Add** and then click **Next**.
6. Configure the parameters, and select a check box for each day of the week that you want included in the schedule.
7. Click **Next**.
8. To add a destination to the schedule, from the **Available Destinations** list, select a destination and click the selection symbol, >.
9. Click **Next** and then click **Finish**.

---

## Configuration options for systems with restricted policies for domain controller credentials

Users with appropriate remote access permissions might be able to collect events from remote systems without using domain administrator credentials. Depending on what information you collect, the user might need extra permissions. To collect Security event logs remotely, for example, the user that is configured in the QRadar log source must have remote access to the Security event log from the server where the Agent is installed.

### Restriction:

For remote collection, the WinCollect user must work with their Windows administrator to ensure access to the following items:

- Security, system, and application event logs
- The remote registry
- Any directories that contain .dll or .exe files that contain message string information

With certain combinations of Windows operating system and group policies in place, alternative configurations might not be possible.

Remote collection inside or across a Windows domain might require domain administrator credentials to ensure that events can be collected. If your corporate

policies restrict the use of domain administrator credentials, you might be required to complete more configuration steps for your WinCollect deployment.

When WinCollect agents collect events from the local host, the event collection service uses the Local System account credentials to collect and forward events. Local collection requires that you install a WinCollect agent on a host where local collection occurs.

## Local installations with no remote polling

Install WinCollect locally on each host that you cannot remotely poll. After you install WinCollect, IBM Security QRadar automatically discovers the agent and you can create a WinCollect log source.

You can specify to use the local system by selecting the Local System check box in the log source configuration.

Local installations are suitable for domain controllers where the large event per second (EPS) rates can limit the ability to remotely poll for events from these systems. A local installation of a WinCollect agent provides scalability for busy systems that send bursts of events when user activity is at peak levels.

## Configuring access to the registry for remote polling

Before a WinCollect log source can remotely poll for events, you must configure a local policy for your Windows-based systems.

When a local policy is configured on each remote system, a single WinCollect agent uses the Windows Event Log API to read the remote registry and retrieve event logs. The Windows Event Log API does not require domain administrator credentials. However, the event API method does require an account that has access to the remote registry and to the security event log.

By using this collection method, the log source can remotely read the full event log. However, the method requires WinCollect to parse the retrieved event log information from the remote host against cached message content. WinCollect uses version information from the remote operating system to ensure that the message content is correctly parsed before it forwards the event to IBM Security QRadar.

### Procedure

1. Log on to the Windows computer that you want to remotely poll for events.
2. Select **Start > StartPrograms > Administrative Tools** and then click **Local Security Policy**.
3. From the navigation menu, select **Local Policies > User Rights Assignment**.
4. Right-click **Manage auditing and security log > Properties**.
5. From the **Local Security Setting** tab, click **Add User or Group** to add your WinCollect user to the local security policy.
6. Log out of the Windows host and try to poll the remote host for Windows-based events that belong to your WinCollect log source.

If you cannot collect events for the WinCollect log source, verify that your group policy does not override your local policy. You can also verify that the local firewall settings on the Windows host allow remote event log management.

## Windows event subscriptions for WinCollect agents

To provide events to a single WinCollect agent, you can use Windows event subscriptions to forward events. With event subscriptions configured, numerous Windows hosts can forward their events to IBM Security QRadar without administrator credentials.

### Forwarded events

The events that are collected are defined by the configuration of the event subscription on the remote host that sends the events. WinCollect forwards all of the events that are sent by the subscription configuration, regardless of what event log check boxes are selected for the log source.

Windows event subscriptions, or forwarded events, are not considered local or remote, but are event listeners. The WinCollect **Forwarded Events** check box enables the WinCollect log source to identify Windows event subscriptions. The WinCollect agent displays only a single log source in the user interface, but this log source is listening and processing events for potentially hundreds of event subscriptions. One log source in the agent list is for all event subscriptions. The agent recognizes the event from the subscription, processes the content, and then sends the syslog event to QRadar.

Forwarded events are displayed as *Windows Auth @ IP address* in the **Log Activity** tab. Conversely, locally or remotely collected events appear as *Windows Auth @ IP address* or *hostname*. When WinCollect processes a locally or remotely collected event, WinCollect includes an extra syslog header that identifies the event as a WinCollect event. Because the forwarded event is a pass-through or listener, the extra header is not included, and forwarded events appear like standard and don't include the WinCollect identifier.

**Important:** WinCollect collects only those forwarded events that appear in the Windows Event Viewer.

### Domain controllers

If you have domain controllers, consider installing local WinCollect agents on the servers. Due to the potential number of generated events, use a local log source with the agent installed on the domain controller.

### Supported software environments

Event subscriptions apply only to WinCollect agents and hosts that are configured on the following Windows operating systems:

- Windows 8 (most recent)
- Windows 7 (most recent)
- Windows Server 2008 (most recent)
- Windows Server 2012 (most recent)
- Windows Vista (most recent)

**Important:** WinCollect is not supported on versions of Windows that have been moved to End Of Life by Microsoft. After software is beyond the Extended Support End Date the product might still function as expected, however, IBM will not make code or vulnerability fixes to resolve WinCollect issues for older operating systems. For example, Microsoft Windows Server 2003 R2 and Microsoft Windows XP are operating systems that are beyond the 'Extended Support End Date'. Any questions about this announcement can be discussed in the IBM Security QRadar Collecting Windows Events (WMI/ALE/WinCollect) forum. For

more information, see <https://support.microsoft.com/en-us/lifecycle/search> (<https://support.microsoft.com/en-us/lifecycle/search>).

For more information about event subscriptions, see your Microsoft documentation or the Microsoft technical website (<http://technet.microsoft.com/en-us/library/cc749183.aspx>).

## Troubleshooting event collection

Microsoft event subscriptions don't have an alert mechanism exists to indicate when an event source stopped sending. If a subscription fails between the two Windows systems, the subscription appears active, but the service that is responsible for the subscription can be in an error state. With WinCollect, the remotely polled or local log sources can time out when events are not received within 720 minutes (12 hours).

## Using Microsoft event subscriptions

To use event subscriptions, you must complete these tasks:

### Before you begin

WinCollect supports event subscriptions with the following parameters:

- **Forwarded Events** selected in the **Destination log** list.
- `RenderedText` for the content format.
- `en_US` for the locale.

### Procedure

1. Configure event subscriptions on your Windows hosts.
2. Configure a log source on the WinCollect agent that receives the events.  
You must select the **Local System** check box and **Forwarded Events** check box for the WinCollect log source.

---

## WinCollect logs

WinCollect logs provide information about your deployment. Logs provide valuable information for troubleshooting issues.

### WinCollect log overview

WinCollect generates log event extended format (LEEF), or syslog messages in the **Status Server** field during installation and configuration. These log messages report on the status of the WinCollect service, authorization token, and configuration, and more.

#### Example:

The following example displays a LEEF message that alerts administrators that the WinCollect agent is generating more events than the log source is tuned for.

```
<13>Sep 22
09:07:56 IPADDRESS LEEF:1.0|IBM|WinCollect|7.2|3|src=MyHost.example.com
dst=10.10.10.10
sev=4 log=Device.WindowsLog.EventLog.MyHost.example.com.System.Read
msg=Reopening event log
due to falling too far behind (approx 165 logs skipped). Incoming
EPS r.avg/max =
150.50/200.00. Approx EPS possible with current tuning = 40.00
```

For more information, see Log Source Event Rates and Tuning Profiles (<http://www.ibm.com/support/docview.wss?uid=swg21672193>).

You search for syslog messages by using the IP address of the WinCollect agent. QRadar tracks information from the audit log to determine when log sources are created, when searches are run, and so on.

## WinCollect log types

The default log directory is C:\Program Files\IBM\WinCollect\logs\.

WinCollect log types are described in the following table.

*Table 12. WinCollect log types*

Subfolder	Description
WinCollect_System.log	Captures system information, such as the operating system that the agent is installed on, RAM and CPU information from the operating system, service start-up information, and WinCollect version information.
WinCollect_Code.log	Captures information for spillover and cache messages, file reader messages, authorization token messages, IP address or host name information for the local host, issues with destinations, log source auto-creation, stand-alone mode messages, and thread or process start-up and shutdown messages. Use this log to investigate the WinCollect configuration. This log does not provide information about event collection.
WinCollect_Device.log	Used to log messages when WinCollect collects events, the protocols that run event log collection. The following issues are logged in the WinCollect_Device.log:  Loading Plug-in  Connection issues  Permission or Authentication  Windows error codes (hex value codes provided by the operating system, such as 0x000005 access denied)  File path or location  Event log is overdue to be polled  Event log transactions  RPC is unavailable (unable to find the location that you specified)  Reopening due to falling too far behind (tuning messages)

## Disk space management for log files

New installations of WinCollect 7.2.3 manage disk space for logs by generating a ".1" version when the log size exceeds 20 MB. After a ".5" version is created, WinCollect deletes the oldest version of the log.

WinCollect also manages disk space by archiving checkpoint folders. When QRadar updates WinCollect with new code, the checkpoint folders store a backup of the replaced code. WinCollect archives the oldest patch checkpoint folder after 10 are created. WinCollect creates an archive folder that contains a list of files in the patch checkpoint folder, and a compressed file of the AgentConfig.xml file. WinCollect then deletes the patch checkpoint folder that it archived.

If you upgraded to WinCollect 7.2.3 from a previous version, you must configure the log rollover feature on WinCollect agents. For more information, see Configure log rollover (<http://www.ibm.com/support/docview.wss?uid=swg21975273>).

---

## Chapter 6. Log sources for WinCollect agents

A single WinCollect agent can manage and forward events from the local system or remotely poll a number of Windows-based log sources and operating systems for their events.

Log sources that communicate through a WinCollect agent can be added individually. If the log sources contain similar configurations, you can simultaneously add multiple, or bulk add log sources. A change to an individually added log source updates only the individual log source. A change that is made to a group of log sources updates all of the log sources in the log source group.

**Important:** If your deployment has user accounts on different domains with the same user name, ensure that you configure domain information when you create the WinCollect log source.

---

### Common WinCollect log source parameters

Common parameters are used when you configure a log source for a WinCollect agent or a WinCollect plug-in. Each WinCollect plug-in also has a unique set of configuration options.

*Table 13. Common WinCollect log source parameters*

Parameter	Description
<b>Log Source Identifier</b>	The IP address or host name 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.  Used to poll events from remote sources
<b>Local System</b>	Disables remote collection of events for the log source.  The log source uses local system credentials to collect and forward events to the QRadar.
<b>Domain</b>	Optional  The domain that includes the Windows-based log source.  The following examples use the correct syntax: LAB1, server1.mydomain.com The following syntax is incorrect: syntax:\\mydomain.com
<b>DNS Domain Name</b>	Optional  Identifies the DNS Domain.

Table 13. Common WinCollect log source parameters (continued)

Parameter	Description
<p><b>Event Rate Tuning Profile</b></p>	<p>Select the profile from the drop-down list that represents the target system. For the default polling interval of 3000 ms, the approximate Events per second (EPS) rates attainable are as follows:</p> <p><b>Default (Endpoint):</b> 33-50 Events per second (EPS)</p> <p><b>Typical Server:</b> 166-250 EPS</p> <p><b>High Event Rate Server:</b> 416-625 EPS</p> <p>For a polling interval of 1000 ms the approximate EPS rates are as follows:</p> <p><b>Default (Endpoint):</b> 100-150 Events per second (EPS)</p> <p><b>Typical Server:</b> 500-750 EPS</p> <p><b>High Event Rate Server:</b> 1250-1875 EPS</p> <p>For more information about tuning WinCollect, see IBM Support (<a href="http://www.ibm.com/support/docview.wss?uid=swg21672193">http://www.ibm.com/support/docview.wss?uid=swg21672193</a>).</p>
<p><b>Polling Interval (MS)</b></p>	<p>The interval, in milliseconds, between times when WinCollect polls for new events.</p>
<p><b>Application or Service Log Type</b></p>	<p>Optional.</p> <p>Used for XPath queries.</p> <p>Provides a specialized XPath query for products that write their events as part of the Windows application log. Therefore, you can separate Windows events from events that are classified to a log source for another product.</p>



Table 13. Common WinCollect log source parameters (continued)

Parameter	Description
<b>Log Filter Type</b>	<p>Configures the WinCollect agent to ignore specific events from the Windows event log.</p> <p>You can also configure WinCollect agents to ignore events globally by ID code or log source.</p> <p>Exclusion filters for events are available for the following log source types: Security, System, Application, DNS Server, File Replication Service, and Directory Service</p> <p>Global exclusions use the <b>EventIDCode</b> field from the event payload. To determine the values that are excluded, source and ID exclusions use the <b>Source=</b> field and the <b>EventIDCode=</b> field of the Windows event payload. Separate multiple sources by using a semi-colon.</p> <p><b>Example:</b> Exclusion filters can use commas and hyphens to filter single EventIDs or ranges, such as 4609, 4616, 6400-6405.</p> <p>For more information about filtering, see WinCollect Event Filtering (<a href="http://www.ibm.com/support/docview.wss?uid=swg21672656">http://www.ibm.com/support/docview.wss?uid=swg21672656</a>).</p>
<b>Forwarded Events</b>	<p>Enables QRadar to collect events that are forwarded from remote Windows event sources that use subscriptions.</p> <p>Forward events that use event subscriptions are automatically discovered by the WinCollect agent and forwarded as if they are a syslog event source.</p> <p>When you configure event forwarding from your Windows system, enable event pre-rendering.</p>
<b>Event Types</b>	<p>At least one event type must be selected.</p>
<b>Enable Active Directory Lookups</b>	<p>If the WinCollect agent is in the same domain as the domain controller that is responsible for the Active Directory lookup, you can select this check and leave the override domain and DNS parameters blank.</p> <p><b>Important:</b> You must enter values for the <b>Domain Controller Name Lookup</b> and <b>DNS Domain Name Lookup</b> parameters.</p>
<b>Override Domain Controller Name</b>	<p>Required when the domain controller that is responsible for Active Directory lookup is outside of the domain of the WinCollect agent.</p> <p>The IP address or host name of the domain controller that is responsible for the Active Directory lookup.</p>

Table 13. Common WinCollect log source parameters (continued)

Parameter	Description
<b>Override DNS Domain Name</b>	The fully qualified domain name of the DNS server that is responsible for the Active Directory lookup, for example, wincollect.com
<b>Remote Machine Poll Interval (ms)</b>	<p>The number of milliseconds between queries that poll remote Windows hosts for new events. The higher the expected event rate, the more frequently the WinCollect agent needs to poll remote hosts for events.</p> <p>Use 7500 when the WinCollect agent collects events from many remote computers that have a low event per second rate, for example, 100 remote computers that provide 10 events per second or less.</p> <p>Use 3500 when the WinCollect agent collects events from many remote computers that have a low event per second rate, for example, 50 remote computers that provide 20 events per second or less.</p> <p>Use 1000 when the WinCollect agent collects events from a few remote computers that have a high event per second rate, for example, 10 remote computers that provide 100 events per second or less.</p> <p>For more information, see Log Source Event Rates and Tuning Profiles (<a href="http://www.ibm.com/support/docview.wss?uid=swg21672193">http://www.ibm.com/support/docview.wss?uid=swg21672193</a>).</p>
<b>XPath Query</b>	<p>Structured XML expressions that you can use to retrieve customized events from the Windows security event log.</p> <p>If you specify an XPath query to filter events, the check boxes that you selected from the <b>Standard Log Type</b> or <b>Event Type</b> are ignored. The events that QRadar collects use the contents of the XPath Query.</p> <p>To collect information by using an XPath Query, you might be required to enable <b>Remote Event Log Management</b> on Windows 2008.</p>
<b>Credibility</b>	<p>Indicates the integrity of an event or offense as determined by the credibility value from the source devices.</p> <p>Credibility increases if multiple sources report the same event.</p>
<b>Target Internal Destination</b>	Managed hosts with an event processor component in the QRadar Deployment Editor can be the target of an internal destination.

Table 13. Common WinCollect log source parameters (continued)

Parameter	Description
<b>Target External Destination</b>	Forwards your events to one or more external destinations that you configured in your destination list.
<b>Coalescing Events</b>	<p>Enables the log source to coalesce (bundle) events.</p> <p>By default, automatically discovered log sources inherit the value of the <b>Coalescing Events</b> list from the <b>System Settings</b> properties in QRadar. However, when you create or edit a log source, you can select the <b>Coalescing Events</b> check box to coalesce events for an individual log source.</p>
<b>Store Event Payload</b>	<p>Enables the log source to store event payload information.</p> <p>By default, automatically discovered log sources inherit the value of the Store Event Payload list from the <b>System Settings</b> properties in QRadar. However, when you create or edit a log source, you can select the <b>Store Event Payload</b> check box to retain the event payload for an individual log source.</p>

## Adding a log source to a WinCollect agent

When you add a new log source to a WinCollect agent or edit the parameters of a log source, the WinCollect service is restarted. The events are cached while the WinCollect service restarts on the agent.

### Before you begin

If you want to configure a log source that uses a WinCollect plug-in, you must read the requirements and perform the necessary steps to prepare the third-party device. For more information, see WinCollect plug-in requirements.

### Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **Data Sources**.
3. Click the **WinCollect** icon.
4. Click **Agents**.
5. Select the WinCollect agent, and click **Log Sources** and then click **Add**.
6. Choose one of the following options:
  - For a WinCollect log source, select **Microsoft Windows Security Event Log** from the **Log Source Type** list and then select WinCollect from the **Protocol Configuration** list.
  - Select a WinCollect plug-in option from the **Log Source Type** list, and then configure the plug-in specific parameters. For information about these parameters, see the configuration options for log sources that use WinCollect plug-ins.
7. Configure the generic log source parameters.

8. Click **Save**.
9. On the **Admin** tab, click **Deploy Changes**.

---

## Microsoft DHCP log source configuration options

Configure the WinCollect plug-in for Microsoft DHCP.

**Restriction:** The WinCollect agent must be in the same time zone as the remote DHCP server that it is configured to poll.

*Table 14. Microsoft DHCP protocol parameters*

Parameter	Description
Log Source Type	Microsoft DHCP
Protocol Configuration	WinCollect Microsoft DHCP
Local System	The WinCollect agent must be installed on the Microsoft DHCP Server.  The log source uses local system credentials to collect and forward events to the QRadar

*Table 15. Default root log directory paths for Microsoft DHCP events.*

The DHCP event logs that are monitored by WinCollect are defined by the directory path that you specify in your WinCollect DHCP log source.

Collection type	Root log directory
Local	c:\WINDOWS\system32\dhcp
Remote	\\DHCP IP address\c\$\Windows\System32\dhcp

*Table 16. Example log format for Microsoft DHCP events.*

WinCollect evaluates the root log directory folder to automatically collect new DHCP events that are written to the event log. DHCP event logs start with DHCP, contain a three-character day of the week abbreviation, and end with a .log file extension. Any DHCP log files that are in the root log directory and match either an IPv4 or IPv6 DHCP log format are monitored for new events by the WinCollect agent.

Log type	Example of log file format
IPv4	DhcpSrvLog-Mon.log
IPv6	DhcpV6SrvLog-Wed.log

**Related reference:**

“Common WinCollect log source parameters” on page 33  
Common parameters are used when you configure a log source for a WinCollect agent or a WinCollect plug-in. Each WinCollect plug-in also has a unique set of configuration options.

## File Forwarder log source configuration options

Use the reference information to configure the WinCollect plug-in for the File Forwarder log source.

You must also configure parameters that are not specific to this plug-in.

Table 17. File Forwarder protocol parameters

Parameter	Description
Log Source Type	Universal DSM
Protocol Configuration	Select <b>Universal DSM</b> .
Local System	Disables remote collection of events for the log source. The log source uses local system credentials to collect and forward events to the IBM Security QRadar.
Root Directory	The location of the log files to forward to QRadar.  If the WinCollect agent remotely polls for the file, the root log directory must specify both the server and the folder location for the log files. <b>Example:</b> \\server\sharedfolder\remotelogs\.
File Pattern	The regular expression (regex) required to filter the file names. All files that match the pattern are included in the processing. The default file pattern is .* and matches all files in the Root Directory.
Monitoring Algorithm	The <b>Continuous Monitoring</b> option is intended for files systems that append data to log files.  The <b>File Drop</b> option is used for the log files in the root log directory that are read one time, and then ignored in the future.
File Monitor Type	The <b>Notification-based (local)</b> option uses the Windows file system notifications to detect changes to your event log.  The <b>Polling-based (remote)</b> option monitors changes to remote files and directories. The agent polls the remote event log and compares the file to the last polling interval. If the event log contains new events, the event log is retrieved.

Table 17. File Forwarder protocol parameters (continued)

Parameter	Description
<b>File Reader Type</b>	<p>If you choose the <b>Text (file held open)</b> option, the system that generates your event log continually leaves the file open to append events to the end of the file.</p> <p>If you choose the <b>Text (file open when reading)</b> option, the system that generates your event log opens the event log from the last known position, and then writes events and closes the event log.</p> <p>If you select the <b>Memory Mapped Text (local only)</b> option, only when advised by IBM Professional Services. This option is used when the system that generates your event log polls the end of the event log for changes. This option requires the Local System check box to be selected.</p>

**Related reference:**

“Common WinCollect log source parameters” on page 33

Common parameters are used when you configure a log source for a WinCollect agent or a WinCollect plug-in. Each WinCollect plug-in also has a unique set of configuration options.

## Microsoft IAS log source configuration options

Use the reference information to configure the WinCollect plug-in for Microsoft IAS.

### Supported versions of Microsoft IAS in WinCollect

The Microsoft IAS plug-in for WinCollect supports the following software versions:

- Windows 2008 operating systems with Microsoft Network Policy Server 2008 enabled
- Windows 2012 operating systems with Microsoft Network Policy Server 2012 enabled

### Supported Microsoft IAS or NPS server log formats

Microsoft IAS and NPS installations write RADIUS and authentication events to a common log directory.

To collect these events with WinCollect, you must configure your Microsoft IAS or Microsoft NPS to write an event log file to a directory. WinCollect does not support events that are logged to a Microsoft SQL Server.

WinCollect supports the following event log formats:

- Data Transformation Service (DTS)
- Open Database Connectivity (ODBC)
- Internet Authentication Service (IAS)

## Microsoft IAS directory structure for event collection

The event logs that are monitored by WinCollect are defined by the configuration of the root directory in your log source.

When you specify a root log directory, you must point the WinCollect agent to the folder that contains your Microsoft ISA or NPS events. The root log directory does not recursively search sub-directories for event files.

To increase performance, you can create a sub folder to contain your IAS and NPS event logs. For example, \Windows\System32\Logfiles\NPS. When you create a specific event folder, the agent does not have to evaluate many files to locate your event logs.

If your system generates large amounts of IAS or NPS events, you can configure your Windows system to create a new event log at daily intervals. This action ensures that agents do not have to search large logs for new events.

Table 18. Event log default directory structure for Microsoft IAS

Event version	Root Log Directory
Microsoft Windows 2008 and Windows 2008R2	\Windows\System32\Logfiles\
Microsoft Windows 2012	\Windows\System32\Logfiles\

## Microsoft IAS protocol parameters

Table 19. Microsoft IAS protocol parameters

Parameter	Description
<b>Log Source Type</b>	<b>Microsoft IAS Server</b>
<b>Protocol Configuration</b>	<b>WinCollect Microsoft IAS / NPS</b>
<b>Local System</b>	To collect local events, the WinCollect agent must be installed on the same host as your Microsoft DHCP Server.  The log source uses local system credentials to collect and forward events to the QRadar
<b>Folder Path</b>	For a local directory path, use the %WINDIR%\System32\Logfiles directory.  For a remote directory path, use the \\<IASIP>\c\$\Windows\System32\Logfiles directory.
<b>File Monitor Policy</b>	The <b>Notification-based (local)</b> option uses the Windows file system notifications to detect changes to your event log.  The <b>Polling-based (remote)</b> option monitors changes to remote files and directories. The agent polls the remote event log and compares the file to the last polling interval. If the event log contains new events, the event log is retrieved.
<b>Polling Interval</b>	The amount of time between queries to the root log directory for new events.

**Related reference:**

“Common WinCollect log source parameters” on page 33

Common parameters are used when you configure a log source for a WinCollect agent or a WinCollect plug-in. Each WinCollect plug-in also has a unique set of configuration options.

---

## Microsoft IIS protocol configuration options

You can configure a log source to use the Microsoft IIS protocol. This protocol supports a single point of collection for W3C format log files that are on a Microsoft IIS web server.

### Overview for the WinCollect Microsoft IIS plug-in

To collect Microsoft IIS events, a WinCollect agent must be installed on your Microsoft Server. Remote polling for Microsoft IIS events is not supported by the WinCollect Microsoft IIS plug-in.

Microsoft Internet Information Services (IIS) includes a range of administrative features for managing websites. You can monitor attempts to access your websites to determine whether attempts were made to read or write to your files. You can create a single Microsoft IIS log source to record events from your entire website directory or individual websites.

The Microsoft IIS device plug-in can read and forward events for the following logs:

- Website (W3C) logs
- File Transfer Protocol (FTP) logs
- Simple Mail Transfer Protocol (SMTP) logs
- Network News Transfer Protocol (NNTP) logs

The WinCollect IIS plug-in can monitor W3C, IIS, and NCSA formatted event logs. However, the IIS and NCSA event formats do not contain as much event information in their event payloads as the W3C event format. To collect the maximum information available, you can configure your Microsoft IIS Server to write events in W3C format. WinCollect can collect both ASCII and UTF-8 encoded event log files.

**Restriction:** The Microsoft authentication protocol NTLMv2 is not supported by the Microsoft IIS protocol.

### Supported versions of Microsoft IIS

The Microsoft IIS plug-in for WinCollect supports the following Microsoft IIS software versions:

- Microsoft IIS Server 6.0
- Microsoft IIS Server 7.0
- Microsoft IIS Server 7.5
- Microsoft IIS Server 8.0

### Microsoft IIS protocol parameters



Table 20. Microsoft IIS protocol parameters

Parameter	Description
Protocol Configuration	Select <b>Microsoft IIS</b> .
File Pattern	The regular expression (regex) that identifies the event logs.
Root Directory	The directory path to your Microsoft IIS log files. <ul style="list-style-type: none"> <li>• For Microsoft IIS 6.0 (individual site), use %SystemRoot%\LogFiles\site name</li> <li>• For Microsoft 7.0-8.0 (full site), use %SystemDrive%\inetpub\logs\LogFiles</li> <li>• For Microsoft IIS 7.0-8.0 (individual site), use %SystemDrive%\inetpub\logs\LogFiles\site name</li> </ul>
Protocol Logs	The items that you want to collect from Microsoft IIS.
Log Source Identifier	The IP address or host name of your Microsoft IIS Server.  The log source identifier must be unique for the log source type.
Root Directory	The directory path to your Microsoft IIS log files.
Polling Interval	The polling interval, which is the amount of time between queries to the root log directory for new events.  The default polling interval is 5000 milliseconds.
FTP	Collects File Transfer Protocol (FTP) events from Microsoft IIS.
NNTP/News	Collects Network News Transfer Protocol (NNTP) events from Microsoft IIS.
SMTP/Mail	Collects Simple Mail Transfer Protocol (SMTP) events from Microsoft IIS.
W3C	Collects website (W3C) events from Microsoft IIS.
WinCollect Agent	Manages the WinCollect agent log source.

---

## Microsoft ISA log configuration options

Use the reference information to configure the WinCollect plug-in for Microsoft ISA.

### Supported versions of Microsoft ISA

The Microsoft ISA plug-in for WinCollect supports the following software versions:

- Microsoft ISA Server 2004
- Microsoft ISA Server 2006
- Microsoft Forefront Threat Management Gateway 2010

### Supported Microsoft ISA or TMG server log formats

Microsoft ISA and Forefront Threat Management Gateway installations create individual firewall and web proxy event logs in a common log directory. To collect these events with WinCollect, you must configure your Microsoft ISA or Microsoft TMG to write event logs to a log directory. Events that log to a Microsoft SQL database are not supported by WinCollect.

WinCollect supports the following event log formats:

- Web proxy logs in WC3 format (w3c\_web)
- Microsoft firewall service logs in WC3 format (w3c\_fws)
- Web Proxy logs in IIS format (iis\_web)
- Microsoft firewall service logs in IIS format (iis\_fws)

The W3C event format is the preferred event log format. The W3C format contains a standard heading with the version information and all of the fields that are expected in the event payload. The W3C event format for the firewall service log and the web proxy log can be customized to include or exclude fields from the event logs.

Most administrators can use the default W3C format fields. If the W3C format is customized, the following fields are required to properly categorize events:

Table 21. W3C format required fields

Required field	Description
Client IP (c-ip)	Source IP address.
Action	Action that is taken by the firewall.
Destination IP (r-ip)	Destination IP address.
Protocol (cs-protocol)	Application protocol name, for example, HTTP or FTP.
Client user name (cs-username)	User account that made the data request of the firewall service.
Client user name (username)	User account that made the data request of the web proxy service.

## Microsoft ISA directory structure for event collection

The event logs that are monitored by WinCollect are defined by the configuration of the root directory in your log source.

When you specify a root log directory, WinCollect evaluates the directory folder and recursively searches the subfolders of the root log directory to determine when new events are written to the event log. By default, the WinCollect ISA plug-in polls the root log directory for updated event logs every 5 seconds.

Table 22. Event log default directory structure for Microsoft ISA

Version	Root Log Directory
Microsoft ISA 2004	<Program Files>\MicrosoftISAServer\ISALogs\
Microsoft ISA 2006	%systemroot%\LogFiles\IAS\
Microsoft Threat Management Gateway	<Program Files>\<Forefront Directory>\ISALogs\

## WinCollect Microsoft ISA protocol parameters

Table 23. WinCollect Microsoft ISA protocol parameters

Parameter	Description
Log Source Type	Microsoft ISA
Protocol Configuration	WinCollect Microsoft ISA / Forefront TMG

Table 23. WinCollect Microsoft ISA protocol parameters (continued)

Parameter	Description
<b>Local System</b>	To collect local events, the WinCollect agent must be installed on the same host as your Microsoft ISA or Forefront TMG server. The log source uses local system credentials to collect and forward events to the IBM Security QRadar.
<b>Root Directory</b>	<p>When you specify a remote file path, use a dollar sign, \$, instead of a colon, :, to represent your drive name.</p> <p>Microsoft ISA 2004</p> <ul style="list-style-type: none"> <li>For a local directory path, use &lt;Program Files&gt;\MicrosoftISAServer\ISALogs\</li> <li>For a remote directory path, use \&lt;ISA server IP&gt;\&lt;Program Files&gt;\MicrosoftISAServer\ISALogs\</li> </ul> <p>Microsoft ISA 2006</p> <ul style="list-style-type: none"> <li>For a local directory path, use %systemroot%\LogFiles\ISA\</li> <li>For a remote directory path, use \&lt;ISA server IP&gt;%systemroot%\LogFiles\ISA\</li> </ul> <p>Microsoft Threat Management Gateway</p> <ul style="list-style-type: none"> <li>For a local directory path, use &lt;Program Files&gt;\&lt;Forefront Directory&gt;\ISALogs\</li> <li>For a remote directory path, use \&lt;ISA server IP&gt;\&lt;Program Files&gt;\&lt;Forefront Directory&gt;\ISALogs\</li> </ul>
<b>File Pattern</b>	The regular expression (regex) required to filter the file names. All files that match the pattern are included in the processing. The default file pattern is .* and matches all files in the <b>Folder Path</b> field.
<b>File Monitor Policy</b>	<p>The <b>Notification-based (local)</b> option uses the Windows file system notifications to detect changes to your event log.</p> <p>The <b>Polling-based (remote)</b> option monitors changes to remote files and directories. The agent polls the remote event log and compares the file to the last polling interval. If the event log contains new events, the event log is retrieved.</p>
<b>Polling Interval</b>	The amount of time between queries to the root log directory for new events.

**Related reference:**

“Common WinCollect log source parameters” on page 33

Common parameters are used when you configure a log source for a WinCollect agent or a WinCollect plug-in. Each WinCollect plug-in also has a unique set of configuration options.

---

## Juniper Steel-Belted Radius log source configuration options

Use the reference information to configure the WinCollect plug-in for Juniper Steel-Belted Radius.

Table 24. WinCollect Juniper Steel-Belted Radius protocol parameters

Parameter	Description
Log Source Type	Juniper Steel-Belted Radius
Protocol Configuration	WinCollect SBR
Local System	To collect local events, the WinCollect agent must be installed on the same host as the Juniper Steel-Belted Radius server. The log source uses local system credentials to collect and forward events to the IBM Security QRadar.
Root Directory	The directory that contains the files that you want to monitor. Due to the restrictions in the distributed system, the QRadar user interface does not verify the path to the root directory. Ensure that you enter a valid local Windows path.
File Monitor Policy	<p>The <b>Notification-based (local)</b> option uses the Windows file system notifications to detect changes to your event log.</p> <p>The <b>Polling-based (remote)</b> option monitors changes to remote files and directories. The agent polls the remote event log and compares the file to the last polling interval. If the event log contains new events, the event log is retrieved.</p>
Polling Interval	The amount of time between queries to the root log directory for new events.

---

## Microsoft SQL Server log source configuration options

Use the reference information to configure the WinCollect plug-in for Microsoft SQL Server.

### Overview for the WinCollect Microsoft SQL plug-in

The error log is a standard text file that contains SQL Server information and error messages. WinCollect monitors the SQL error log for new events and forwards the event to IBM Security QRadar. The error log can provide meaningful information to assist you in troubleshooting issues or alerting you to potential or existing problems. The error log output includes the time and date the message was logged, the source of the message, and the description of the message. If an error occurs, the log contains the error message number and a description. Microsoft SQL Servers retain backups of the last six error log files.

WinCollect can collect SQL error log events. To collect Microsoft SQL Server audit and authentication events, you can configure the Microsoft SQL Server DSM. For more information, see the *IBM Security QRadar DSM Configuration Guide*.

WinCollect agents support local collection and remote polling for Microsoft SQL Server installations. To remotely poll for Microsoft SQL Server events, you must provide administrator credentials or domain administrator credentials. If your network policy restricts the use of administrator credentials, you can install a WinCollect agent on the same host as your Microsoft SQL Server. Local installations of WinCollect do not require special credentials to forward SQL events to QRadar.

The SQL event logs that are monitored by WinCollect are defined by the directory path that you specify in your WinCollect SQL log source. The following table provides you with the default directory paths for the Root Log Directory field in your log source.

*Table 25. Default root log directory paths Microsoft SQL events*

Microsoft SQL version	Collection type	Root log directory
2000	Local	C:\Program Files\Microsoft SQL Server\Mssql\Log
2000	Remote	\\SQL IP address\c\$\Program Files\Microsoft SQL Server\Mssql\Log
2005	Local	c:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\LOG\
2005	Remote	\\SQL IP address\c\$\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\LOG\
2008	Local	C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Log\
2008	Remote	\\SQL IP address\c\$\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Log\
2008R2	Local	C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\Log
2008R2	Remote	\\SQL IP address\c\$\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\Log

Log files that do not match the SQL event log format are not parsed or forwarded to QRadar.

## Supported versions of Microsoft SQL

The Microsoft SQL plug-in for WinCollect supports the following Microsoft SQL software versions:

- Microsoft SQL Server 2000
- Microsoft SQL Server 2005
- Microsoft SQL Server 2008
- Microsoft SQL Server 2008R2
- Microsoft SQL Server 2012
- Microsoft SQL Server 2014

*Table 26. Microsoft SQL Server protocol parameters*

Parameter	Description
Log Source Type	Microsoft SQL
Protocol Configuration	WinCollect Microsoft SQL

Table 26. Microsoft SQL Server protocol parameters (continued)

Parameter	Description
<b>Root Directory</b>	<p>Microsoft SQL 2000</p> <ul style="list-style-type: none"> <li>• For a local directory path, use C:\Program Files\Microsoft SQL Server\Mssql\Log</li> <li>• For a remote directory path, use \\SQL IP address\c\$\Program Files\Microsoft SQL Server\Mssql\Log</li> </ul> <p>Microsoft SQL 2005</p> <ul style="list-style-type: none"> <li>• For a local directory path, use c:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\LOG\</li> <li>• For a remote directory path, use \\SQL IP address\c\$\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\LOG\</li> </ul> <p>Microsoft SQL 2008</p> <ul style="list-style-type: none"> <li>• For a local directory path, use C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Log\</li> <li>• For a remote directory path, use \\SQL IP address\c\$\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Log\</li> </ul> <p>Microsoft SQL 2008R2</p> <ul style="list-style-type: none"> <li>• For a local directory path, use C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\Log</li> <li>• For a remote directory path, use \\SQL IP address\c\$\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\Log</li> </ul>
<b>File Monitor Policy</b>	<p>The <b>Notification-based (local)</b> option uses the Windows file system notifications to detect changes to your event log.</p> <p>The <b>Polling-based (remote)</b> option monitors changes to remote files and directories. The agent polls the remote event log and compares the file to the last polling interval. If the event log contains new events, the event log is retrieved.</p>

**Related reference:**

“Common WinCollect log source parameters” on page 33

Common parameters are used when you configure a log source for a WinCollect agent or a WinCollect plug-in. Each WinCollect plug-in also has a unique set of configuration options.

---

## NetApp Data ONTAP configuration options

Use this reference information to configure the WinCollect plug-in for NetApp ONTAP.

*Table 27. WinCollect NetApp Data ONTAP protocol parameters.*

Parameter	Description
Log Source Type	NetApp Data ONTAP
Protocol Configuration	WinCollect NetApp Data ONTAP
User Name	The account name that is used to log in to the Windows domain or system.
Domain	The network domain to which the user name belongs.
Target Directory	The network path to the directory where you want to monitor files.  <b>Attention:</b> Due to the restrictions in the distributed system, this path is not verified by the QRadar user interface. Ensure that you type a valid Windows UNC path that is shared by the NetApp appliance.
Polling Interval	The interval, in milliseconds, at which the remote directory is checked for new event log files. Even though the remote device does not generate new files on a period of less than 60 seconds, the optimal polling interval is less than 60 seconds. This practice ensures the collection of files that might be when WinCollect is restarted.
WinCollect Agent	The WinCollect Agent that you want to use to collect NetApp Data ONTAP events.

---

## XPath log source configuration options

Use the reference information to create a log source that includes the XPath query from the Event Viewer

You must also configure parameters that are not specific to this plug-in.

*Table 28. XPath protocol parameters*

Parameter	Description/Action
Log Source Type	Microsoft Windows Security Event Log
Protocol Configuration	Select WinCollect .
Standard Log Types	Ensure that none of the log type check boxes are selected.  The XPath query defines the log types for the log source.
Forwarded Events	Do not select this check box.
Event Types	Do not select <b>Event Type</b> check boxes. The XPath query defines the log types for the log source.

Table 28. XPath protocol parameters (continued)

Parameter	Description/Action
WinCollect Agent	The WinCollect agent that manages this log source.
XPath Query	The XPath query that you defined in Microsoft Event Viewer.  To collect information by using an XPath query, you might be required to enable the <b>Remote Event Log Management</b> option on Windows 2008.

**Related reference:**

“Common WinCollect log source parameters” on page 33

Common parameters are used when you configure a log source for a WinCollect agent or a WinCollect plug-in. Each WinCollect plug-in also has a unique set of configuration options.

## XPath queries

An XPath query is a log source parameter that filters specific events when the query communicates with a Windows 2008 event log.

XPath queries use XML notation and are available in QRadar when you retrieve events by using the WinCollect protocol. The most common method of creating an XPath query is to use Microsoft Event Viewer to create a custom view. The custom view that you create for specific events in Event Viewer can generate XPath notations. You can then copy this generated XPath notation in your XPath query to filter your incoming log source events for specific event data.

**Note:** To manually create your own XPath queries, you must be proficient with XPath 1.0 and XPath queries

### Enabling remote log management on Windows 7

You can enable remote log management only when your log source is configured to remotely poll other Windows operating systems. You can enable remote log management on Windows 7 for XPath queries.

You can enable remote log management on Windows 7 for XPath queries.

#### Procedure

1. On your desktop, select **Start > Control Panel**.
2. Click the **System and Security** icon.
3. Click **Allow a program through Windows Firewall**.
4. If prompted, click **Continue**.
5. Click **Change Settings**.
6. From the Allowed programs and features pane, select **Remote Event Log Management**.

Depending on your network, you might need to correct or select more network types.

7. Click **OK**.



## Enabling remote log management on Windows 2008

You can enable remote log management only when your log source is configured to remotely poll other Windows operating systems. You can enable remote log management on Windows Server 2008 for XPath queries.

You can enable remote log management on Windows Server 2008 for XPath queries.

### Procedure

1. On your desktop, select **Start > Control Panel**.
2. Click the **Security** icon.
3. Click **Allow a program through Windows Firewall**.
4. If prompted, click **Continue**.
5. From the **Exceptions** tab, select **Remote Event Log Management** and click **OK**.

## Enabling remote log management on Windows 2008R2

You can enable remote log management only when your log source is configured to remotely poll other Windows operating systems. You can enable remote log management on Windows 2008R2 for XPath queries.

You can enable remote log management on Windows 2008R2 for XPath queries.

### Procedure

1. On your desktop, select **Start > Control Panel**.
2. Click the **Window Firewall** icon.
3. Click **Allow a program through Windows Firewall**.
4. If prompted, click **Continue**.
5. Click **Change Settings**.
6. From the Allowed programs and features pane, select **Remote Event Log Management** check box.

Depending on your network, you might need to correct or select more network types.

7. Click **OK**.

## Creating a custom view

Use the Microsoft Event Viewer to create custom views, which can filter events for severity, source, category, keywords, or specific users.

WinCollect supports up to 10 selected event logs in the XPath query. Event IDs that are suppressed do not contribute towards the limit.

WinCollect log sources can use XPath filters to capture specific events from your logs. To create the XML markup for your XPath Query parameter, you must create a custom view. You must log in as an administrator to use Microsoft Event Viewer.

XPath queries that use the WinCollect protocol the TimeCreated notation do not support filtering of events by a time range. Filtering events by a time range can lead to errors in collecting events.

### Procedure

1. On your desktop, select **Start > Run**.
2. Type the following command:

Eventvwr.msc

3. Click **OK**.
4. If you are prompted, type the administrator password and press Enter.
5. Click **Action > Create Custom View**.  
When you create a custom view, do not select a time range from the **Logged** list. The **Logged** list includes the **TimeCreated** element, which is not supported in XPath queries for the WinCollect protocol.
6. In **Event Level**, select the check boxes for the severity of events that you want to include in your custom view.
7. Select an event source.
8. Type the event IDs to filter from the event or log source.  
Use commas to separate IDs. The following list contains an individual ID and a range: 4133, 4511-4522
9. From the **Task Category** list, select the categories to filter from the event or log source.
10. From the **Keywords** list, select the keywords to filter from the event or log source.
11. Type the user name to filter from the event or log source.
12. Type the computer or computers to filter from the event or log source.
13. Click the **XML tab**.
14. Copy and paste the XML to the **XPath Query** field of your WinCollect log source configuration

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

## What to do next

Configure a log source with the XPath query. For more information, see “XPath log source configuration options” on page 49.

## XPath query examples

Use XPath examples for monitoring events and retrieving logon credentials, as a reference when you create XPath queries.

For more information about XPath queries, see your Microsoft documentation.

### Example: Monitoring events for a specific user

In this example, the query retrieves events from all Windows event logs for the guest user.

**Important:** XPath queries cannot filter Windows Forwarded Events.

```
<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>

</Query>
</QueryList>.

```

### Example: Credential logon for Windows 2008

In this example, the query retrieves specific event IDs from the security log for Information-level events that are associated with the account authentication in Windows 2008.

```

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

```

Table 29. Event IDs used in credential logon 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.

### Example: Retrieving events based on user

In this example, the query examines event IDs to retrieve specific events for a user account that 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 >= 4722
and EventID <= 4726) or (EventID >= 4741 and EventID
<= 4743) )]]</Select>
</Query>
</QueryList>

```

Table 30. Event IDs used in database example.

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

Table 30. Event IDs used in database example (continued).

ID	Description
4743	A user account was deleted.

---

## Bulk log sources for remote event collection

Bulk log sources are designed for systems that have multiple log sources with the same protocol configuration.

### Procedure

1. Create a destination for Windows events on each IBM Security QRadar appliance that you want to use for Windows event collection. See “Adding a destination” on page 25.

**Important:** It is helpful to provide a destination name that includes the IP address, such as "Agent1\_1.2.3.4". If you have to edit the log source and change a destination in the future, you can determine the IP address for the destination. Also, set the throttle value to 5000 EPS, which is the max EPS rate for a WinCollect agent.

2. Create bulk log sources. See “Adding log sources in bulk for remote collection.”
3. Wait for the configurations to be pushed to the remote agents.
4. Verify in the **Log Activity** tab that events being received.

## Adding log sources in bulk for remote collection

You can add multiple log sources at one time in bulk to IBM Security QRadar. The log sources must share a common configuration protocol and be associated with the same WinCollect agent.

You can upload a text file that contains a list of IP addresses or host names, run a query against a domain controller to get a list of hosts, or manually enter a list of IP addresses or host names by typing them in one at a time.

Depending on the number of WinCollect log sources that you add at one time, it can take time for the WinCollect agent to access and collect all Windows events from the log source list.

### Before you begin

Ensure that you created destinations so that WinCollect agents can send Windows events to QRadar appliances. Ensure that you created one destination for each QRadar Event Collector 16xx or 18xx appliance.

Plan your bulk collection strategy with the WinCollect Event Log Report tool. For more information, see GitHub (<https://github.com/ibm-security-intelligence/wincollect>).

### About this task

You can have a maximum of 500 log sources for each managed WinCollect agent. You must also remain under 5,000 EPS for local collection and 2,500 EPS for remote polling on the WinCollect Agent. You can review the Event Viewer on the Windows systems to determine how many EPS are generated in each hour. Divide

that value by 3600 seconds to get the EPS rate. This calculation helps you to plan how many agents you need to install. Alternately, look at events over a 24-hour period to see how busy each Windows server is. This helps determine how to tune agents and avoid minimum and maximum EPS rates that you see only when reviewing hour-by-hour.

## Procedure

1. On the **Admin** tab navigation menu, click **Data Sources**, and then click the **WinCollect** icon.
2. Select the WinCollect agent that you want to assign log sources to, and click **Log Sources**.
3. Click **Bulk Actions > Bulk Add**.
4. Provide a name for the bulk log source. To make it easy to locate, specify the name as the WinCollect agent that does remote collection.
5. From the **Log Source Type list** box, select **Microsoft Windows Security Event Log**.
6. From the **Protocol Configuration list** box, select **WinCollect**.
7. Use the tuning value specified by the WinCollect Event Log Report tool to tune your log sources appropriately.
8. Select all of the **Standard Log Types** check boxes. The WinCollect agent reads and forwards these remote logs to QRadar.

**Important:** Do not select **Forwarded Events** the check box. Forwarded events is a special use case. Selecting this option will not add multiple log sources correctly.

9. Select all of the **Event Types** check boxes.
10. Select the **Enable Active Directory Lookups** check box. This option identifies user names in Windows events that appear as a hexadecimal and resolves them to human readable user names.
11. From the **WinCollect Agent** list, select the Windows host that manages the log source.
12. From the **Target Internal Destination** list, select the QRadar appliance that receives and processes the Windows events.
13. Add the IP addresses for the Windows operating systems that you want to remotely poll for events.

You can upload a text file that contains a list of IP addresses or host names, run a query against a domain controller to get a list of hosts, or manually enter a list of IP addresses or host names by typing them in one at a time.

Depending on the number of WinCollect log sources that you add at one time, it can take time for the WinCollect agent to access and collect all Windows events from the log source list.

14. Click **Save** and then click **Continue**.

## What to do next

Wait for the configurations to be pushed to the remote agents. Verify in the **Log Activity** tab that events are received.

### Related tasks:

“Adding a log source to a WinCollect agent” on page 37

When you add a new log source to a WinCollect agent or edit the parameters of a log source, the WinCollect service is restarted. The events are cached while the

WinCollect service restarts on the agent.

---

## Chapter 7. Stand-alone deployments and WinCollect Configuration Console

A stand-alone deployment is a Windows host in unmanaged mode with WinCollect software installed. The Windows host can either gather information from itself, the local host, and, or remote Windows hosts. Remote hosts don't have the WinCollect software installed. The Windows host with WinCollect software installed polls the remote hosts, and then sends event information to IBM Security QRadar.

---

### WinCollect Configuration Console overview

In stand-alone deployments, which are also called unmanaged deployments, use the WinCollect Configuration Console to manage your WinCollect deployment. Use the WinCollect Configuration Console to add devices that you want WinCollect to collect agents from, and add the IBM Security QRadar destination where you want to send events.

**Prerequisites:** Before you can install the WinCollect Configuration Console, you must do the following:

- Install the WinCollect agent in stand-alone mode. For more information, see “Installing the WinCollect agent on a Windows host” on page 15.
- Install .net framework version 3.5
- Install Microsoft Management Console (MMC) 3.0 and later.

The following table describes the WinCollect Configuration Console.

Table 31. WinCollect Configuration Console window

Sections	Description
<b>Global Configuration</b>	The <b>Global Configuration</b> parameter allows you to view, add and update information about the system where WinCollect data is stored.
	<b>Disk Manager</b> - the path to the WinCollect Data, which is used to buffer events to disk when the event rate exceeds the event throttle.
	<b>Capacity</b> is the maximum capacity allowed for the contents of the Data Folder. WinCollect does not write to this folder after the maximum capacity is reached.
	<b>Installation Information</b> - displays information about the WinCollect agent installation.
	<b>Application Identifier</b> - the header of the payload messages sent to the status server. <b>Status Server</b> - where the WinCollect Agent status events, such as heart beat messages and any warnings or errors generated by the WinCollect Agent, are sent.
<b>Security Manager</b> - centralized credentials, used to collect events from remote devices.	
<b>Destinations</b>	The <b>Destinations</b> parameter defines where WinCollect device data is sent.
	<b>Syslog TCP</b> or <b>Syslog UDP</b> destinations, with the following parameters:  <b>Name</b> <b>Hostname</b> <b>Port</b> <b>Throttle (events per second)</b>  You can expand a destination to view all devices that are assigned to the destination.
<b>Devices</b>	The <b>Device</b> parameter contains available device types. Under each device types, you can view or update multiple device parameters.

## Installing the configuration console

Download and install the WinCollect configuration console to manage your stand-alone deployment. You can choose an option to install just the WinCollect patch, if you are deploying WinCollect on a large number of Windows hosts that do not require the configuration console.



## Before you begin

- Uninstall any versions of WinCollect configuration console. For more information, see “Uninstalling a WinCollect agent from the command prompt” on page 21.
- The existing WinCollect agent must be in stand-alone mode before you can install the configuration console. For more information about WinCollect agent installations, see “Installing a WinCollect agent from the command prompt” on page 17.
- .NET framework 3.5 features are required. For information about how to verify .NET installations, see [www.ibm.com/support \(https://www.ibm.com/support/docview.wss?uid=swg21701063\)](http://www.ibm.com/support/docview.wss?uid=swg21701063).
- Microsoft Management Console (MMC) 3.0 and later is required.
- The WinCollect Stand-alone patch installer supports the following Windows software versions:
  - Windows Server 2008 (most recent)
  - Windows Server 2012 (most recent)
  - Windows 7 (most recent)
  - Windows 8 (most recent)
  - Windows Vista (most recent)

**Important:** WinCollect is not supported on versions of Windows that have been moved to End Of Life by Microsoft. After software is beyond the Extended Support End Date the product might still function as expected, however, IBM will not make code or vulnerability fixes to resolve WinCollect issues for older operating systems. For example, Microsoft Windows Server 2003 R2 and Microsoft Windows XP are operating systems that are beyond the 'Extended Support End Date'. Any questions about this announcement can be discussed in the IBM Security QRadar Collecting Windows Events (WMI/ALE/WinCollect) forum. For more information, see <https://support.microsoft.com/en-us/lifecycle/search> (<https://support.microsoft.com/en-us/lifecycle/search>).

## Procedure

1. Download the patch software from IBM Support ([www.ibm.com/support/fixcentral](http://www.ibm.com/support/fixcentral)). onto the Windows host where you want to install the configuration console.
2. Open the executable file on your system.
3. Follow the steps in the installation wizard. You can select an option to install both the WinCollect configuration console, and the WinCollect patch, or just the patch.

---

## Silently installing, upgrading, and uninstalling WinCollect software

Enter a command to complete all installation and upgrading tasks for the WinCollect stand alone patch, and the WinCollect Configuration Console, rather than using the installation wizard. You can also upgrade WinCollect agents with the patch installer only.

## Procedure

1. Download the patch software from IBM Support ([www.ibm.com/support/fixcentral](http://www.ibm.com/support/fixcentral)).
2. Install or upgrade both the WinCollect stand alone patch and the WinCollect Configuration Console by using the following commands:

```
<setup.exe> /s /v" /qn"
```

3. Change the installation directory of the WinCollect Configuration Console by using the following command:

```
<setup.exe> /s /v" /qn ADDLOCAL=ALL INSTALLDIR=<PATH>"
```

4. Install or upgrade only the WinCollect stand-alone patch by using the following command:

```
<setup.exe> /s /v" /qn ADDLOCAL=WinCollect_StandAlone_Patch"
```

5. If you want to uninstall the WinCollect Configuration Console, use the following command:

```
<setup.exe> /s /x /v" /qn"
```

For more information about stand-alone installs, see IBM Support ([www.ibm.com/support/docview.wss?uid=swg21698381](http://www.ibm.com/support/docview.wss?uid=swg21698381)).

---

## Creating a WinCollect credential

Create a credential that contains login information. WinCollect uses the credential information to log into devices and collect logs.

### Procedure

1. Expand the **Global Configuration** parameter and right-click **Security Manager**.
2. Select **Add New Credential**.
3. In the **New Credential Name** box, add a name for the new credential and click **OK**.
4. Click the new credential under **Security Manager** to open the **Basic Configurations** window for the credential.
5. Enter the required properties for the new credential.
6. Click **Deploy Changes** under **Actions**.

---

## Adding a destination to the WinCollect Configuration Console

Add an IBM Security QRadar instance as a destination for WinCollect data.

### Procedure

1. In the WinCollect Configuration Console, expand the **Destinations** parameter.
2. Right-click the **Syslog TCP** or **Syslog UDP** parameter, depending upon which destination type you want to add, and click **Add New Destination**.
3. In the **New Destination Name** box, add a name for the destination. Click **OK**.

**Important:** It is helpful to provide a destination name that includes the IP address, such as "Agent1\_1.2.3.4". If you have to edit the log source and change a destination in the future, you can determine the IP address for the destination.

4. Expand **Syslog TCP** or **Syslog UDP**, and select the destination that you added to view the **Properties** window.
5. Define the **Name**, **Hostname**, **Port**, and **Throttle** for the new destination.
6. Click **Deploy Changes** under **Actions**.

---

## Adding a device to the WinCollect Configuration Console

Add the devices that WinCollect monitors to the WinCollect Configuration Console.

## Procedure

1. Under **Devices**, right-click the device type that matches the device you want to add and select **Add New Device**.
2. In the **Add New Device** box, enter a name for the destination device.
3. In the **Basic Configurations** window, complete the parameters for the new destination device.
4. Click **Deploy Changes** under **Actions**.

---

## Sending encrypted events to QRadar

Configure a log source in stand-alone deployments of WinCollect to send encrypted events to IBM Security QRadar with TLS syslog. TLS Syslog is not supported in managed WinCollect deployments.

### Before you begin

In QRadar, configure a Universal DSM that uses the TLS Syslog protocol. For more information, see the *IBM Security QRadar Log Sources User Guide*.

The uDSM opens a port and provides the certificate that is necessary for communicating by using TLS. If you delete the uDSM, TLS communication stops.

### Procedure

1. Use SSH to log in to QRadar as the root user.
2. Copy the certificate, including -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- from `/opt/qradar/conf/trusted_certificates/syslog-tls.cert` to a temporary location. You will paste this certificate into the WinCollect Configuration Console.
3. In the WinCollect Configuration Console, expand **Destinations**, and click **Add Destination**.
4. In the **New Destination Name** box, add a name for the destination and then click **OK**.
5. Select the new destination and enter the IP address of the target QRadar appliance in the **Hostname** field.
6. Type 6514 in the **Port** field.
7. Type the events per second (EPS) rate for your deployment in the **Throttle** field.
8. Paste the certificate that you copied from QRadar into the **Certificate** field.
9. Click **Deploy Changes** under **Actions**.

---

## Collecting local Windows logs

This use case scenario describes the settings required to collect logs from the host where the WinCollect Configuration Console is installed, and send them to IBM Security QRadar.

### Procedure

1. Install the WinCollect Configuration Console on the host on which that you want to collect windows logs. Download the patch from IBM Support ([www.ibm.com/support/fixcentral](http://www.ibm.com/support/fixcentral)).

2. Create a destination for the QRadar instance where you want to send WinCollect information. See “Adding a destination to the WinCollect Configuration Console” on page 60.
3. Configure the local Microsoft event log device that is monitored. See “Adding a device to the WinCollect Configuration Console” on page 60.

**Important:** In the **Device Address** field, type the IP address or hostname of the local Windows system that you want to poll for events.

4. Click **Deploy Changes** under **Actions**.

---

## Collecting remote Windows logs

This use case scenario describes the settings that are required in the WinCollect Configuration Console to collect windows logs from hosts that do not have WinCollect software installed, and send the logs to IBM Security QRadar.

### Procedure

1. Install the WinCollect Configuration Console on the windows machine that collects the log information. Download the patch from IBM Support ([www.ibm.com/support/fixcentral](http://www.ibm.com/support/fixcentral)).
2. Create a credential to use when you log in to remote hosts. See “Creating a WinCollect credential” on page 60.
3. Create the QRadar destination where Windows events are sent. See “Adding a destination to the WinCollect Configuration Console” on page 60.
4. Configure the devices that are monitored. See “Adding a device to the WinCollect Configuration Console” on page 60.

**Important:** In the **Device Address** field, type the IP address or hostname of the remote Windows system that you want to poll for events.

5. Click **Deploy Changes** under **Actions**.

---

## 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](http://ibm.com)<sup>®</sup> are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (<sup>®</sup> or <sup>™</sup>), these symbols

indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at Copyright and trademark information ([www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml)).

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.



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

Other company, product, and service names may be trademarks or service marks of others.

---

## Privacy policy considerations

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

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

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

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









Printed in USA