Extreme Networks Security WinCollect User Guide

9034872

Published July 2015

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Support

For product support, including documentation, visit: www.extremenetworks.com/documentation/

For information, contact:
Extreme Networks, Inc.
145 Rio Robles
San Jose, California 95134
USA

Table of Contents

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 Extreme SIEM and Extreme Security Log Manager.

Intended audience

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

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. Extreme Networks® systems, products and services are designed to be part of a lawful comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. EXTREME NETWORKS 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.

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

Conventions

This section discusses the conventions used in this guide.

Text Conventions

The following tables list text conventions that are used throughout this guide.

Table 1: Notice Icons

Icon	Notice Type	Alerts you to...
☞	Tip	Helpful tips for using the product.
📝	Note	Important features or instructions.
⚡	Caution	Risk of personal injury, system damage, or loss of data.
⚠	Warning	Risk of severe personal injury.
New	New	This command or section is new for this release.

Table 2: Text Conventions

Convention	Description
`Screen displays`	This typeface indicates command syntax, or represents information as it appears on the screen.
The words enter and type	When you see the word “enter” in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says “type.”
[Key] names	Key names are written with brackets, such as [Return] or [Esc]. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press [Ctrl]+[Alt]+[Del]
Words in italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.

Terminology

When features, functionality, or operation is specific to a switch family, the family name is used. Explanations about features and operations that are the same across all product families simply refer to the product as the "switch."

Providing Feedback to Us

We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team about this document, please contact us using our short online feedback form. You can also email us directly at InternalInfoDev@extremenetworks.com.

Getting Help

If you require assistance, contact Extreme Networks Global Technical Assistance Center using one of the following methods:

Web	www.extremenetworks.com/support
Phone	1-800-872-8440 (toll-free in U.S. and Canada) or 1-603-952-5000 For the Extreme Networks support phone number in your country: www.extremenetworks.com/support/contact
Email	support@extremenetworks.com To expedite your message, enter the product name or model number in the subject line.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number
- A description of the failure
- A description of any action(s) already taken to resolve the problem (for example, changing mode switches or rebooting the unit)
- The serial and revision numbers of all involved Extreme Networks products in the network
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load and frame size at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any previous Return Material Authorization (RMA) numbers

Related Publications

The Extreme Security product documentation listed below can be downloaded from http://documentation.extremenetworks.com.

Extreme Security Analytics Threat Protection

- *Extreme Networks Security API Reference Guide*
- *Extreme Networks Security Application Configuration Guide*
- *Extreme Networks Security Ariel Query Language Guide*
- *Extreme Networks Security DSM Configuration Guide*
- *Extreme Security DSM Configuration Guide Addendum*
- *Extreme Networks Security Hardware Guide*
- *Extreme Networks Security Installation Guide*
- *Extreme Networks Security Juniper NSM Plug-in User Guide*
- *Extreme Networks Security Log Manager Administration Guide*

- *Extreme Networks Security Log Sources User Guide*
- *Extreme Networks Security Managing Log Sources Guide*
- *Extreme Networks Security Offboard Storage Guide*
- *Extreme Security Release Notes*
- *Extreme Networks Security Risk Manager Adapter Configuration Guide*
- *Extreme Networks Security Risk Manager Getting Started Guide*
- *Extreme Networks Security Risk Manager Installation Guide*
- *Extreme Networks Security Risk Manager Migration Guide*
- *Extreme Networks Security Risk Manager User Guide*
- *Extreme Networks Security Troubleshooting System Notifications Guide*
- *Extreme Networks Security Upgrade Guide*
- *Extreme Networks Security Vulnerability Manager Release Notes*
- *Extreme Networks Security Vulnerability Manager User Guide*
- *Extreme Networks Security WinCollect User Guide*
- *Extreme Networks SIEM Administration Guide*
- *Extreme Networks SIEM Getting Started Guide*
- *Extreme Networks SIEM High Availability Guide*
- *Extreme Networks SIEM Troubleshooting Guide*
- *Extreme Networks SIEM Tuning Guide*
- *Extreme Networks SIEM Users Guide*
- *Migrating Extreme Security Log Manager to Extreme SIEM*

Extreme Security Threat Protection

- *Extreme Security Intrusion Prevention System Hardware Replacement Guide*
- *Extreme Security Threat Protection Release Notes*

1 What's new in WinCollect V7.2.2-1

WinCollect V7.2.2-1 includes a simplified installation and upgrade procedure.

Event Rate Tuning Profile

You can select a profile that represents the events per second that the target system collects. For more information see Common WinCollect log source parameters on page 34.

2 WinCollect overview

WinCollect is a scalable Extreme Networks Security Analytics feature that collects Windows™-based events. You 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 *Extreme Networks Security DSM Configuration Guide*.

How does WinCollect Work?

WinCollect is software that collects events from Windows™ systems, and you can use Extreme Security to view these events. WinCollect uses the Windows™ Event Log API to gather events, and then WinCollect sends the events to Extreme Security.

WinCollect managed deployment

A managed WinCollect deployment has a Extreme Security 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 Extreme Security.

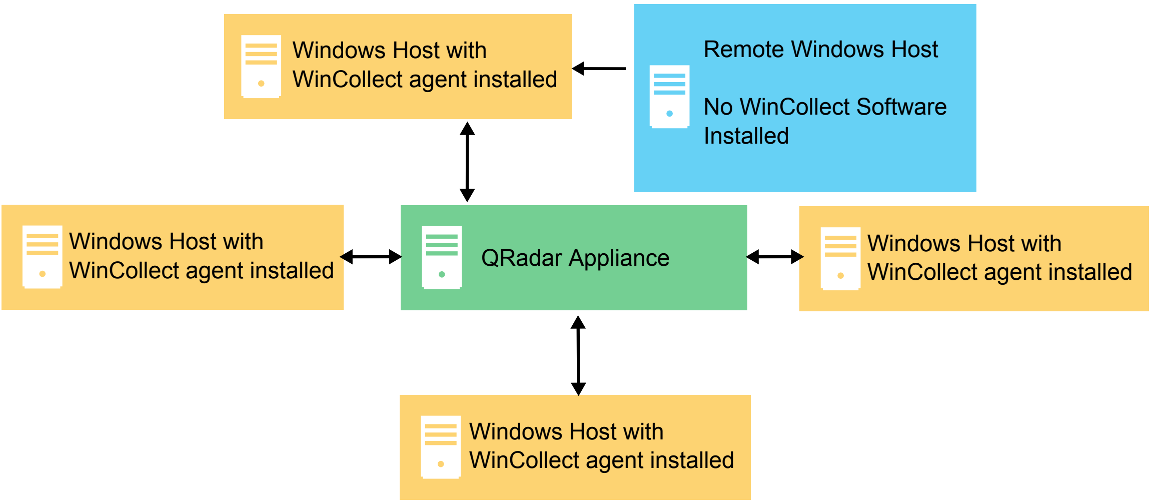
Windows Host with WinCollect agent installed
Remote Windows Host
No WinCollect Software Installed
Windows Host with WinCollect agent installed
QRadar Appliance
Windows Host with WinCollect agent installed
Windows Host with WinCollect agent installed

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 Extreme Security console or a Extreme Security 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 Stand-alone deployments and WinCollect Configuration Console on page 52.

The managed WinCollect deployment has the following capabilities:

- Central management from the Extreme Security 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 Extreme Security. To save time when you configure more than 500 Windows™ hosts, you can use a solution such as Extreme Networks® Endpoint Manager. Automation can help you manage stand-alone instances.

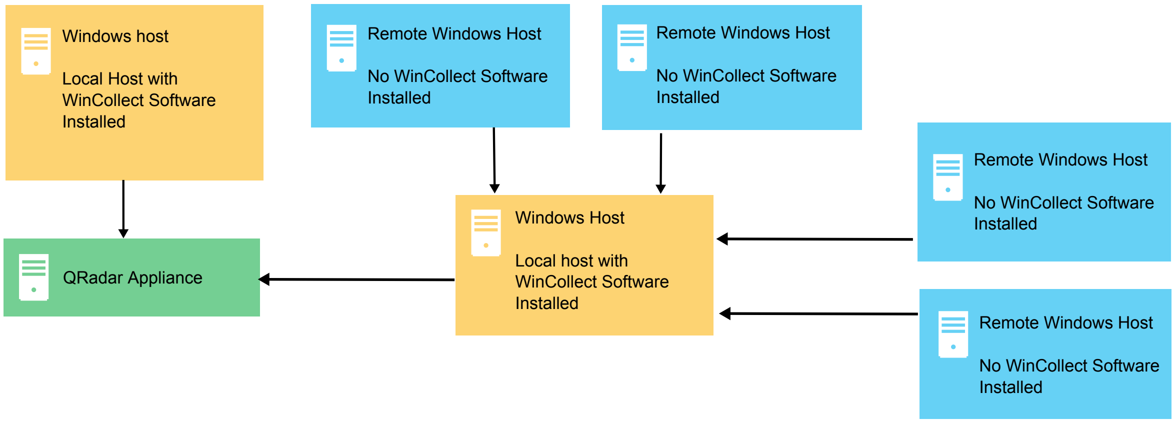
Windows host
Local Host with WinCollect Software Installed
Remote Windows Host
No WinCollect Software Installed
Remote Windows Host
No WinCollect Software Installed
Remote Windows Host
No WinCollect Software Installed
QRadar Appliance
Windows Host
Local host with WinCollect Software Installed
Remote Windows Host
No WinCollect Software Installed

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 Extreme Security.

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 patch 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.

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 Installation prerequisites for WinCollect on page 13.
2. Install the WinCollect application on the Extreme Security console that is used to monitor your Windows™ hosts. For more information, see Installing and upgrading the WinCollect application on Extreme Security appliances on page 18.
3. Create an authentication token so that the Windows™ hosts can send information to Extreme Security. For more information, see Creating an authentication token for WinCollect agents on page 19.
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 20
   - Installing a WinCollect agent from the command prompt on page 22, or
   - Manually adding a WinCollect agent on page 27
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 48.
6. If you want to configure forwarded events, or event subscriptions, see Windows event subscriptions for WinCollect agents on page 32.
7. If you want to tune your WinCollect installation, see the event tuning profile section in Common WinCollect log source parameters on page 34.
8. If you want to set up multiple Extreme Security destinations in case one fails, see Adding multiple destinations to WinCollect agents on page 26.

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 Extreme Security. For more information, see Installing the WinCollect agent on a Windows host on page 20.
2. Install the WinCollect configuration console and, or the WinCollect patch. For more information, see Installing the configuration console and, or the WinCollect patch on page 53 or Silently installing and upgrading WinCollect software on page 54.
3. Configure the destination, or the Extreme Security appliance where the Windows™ hosts send Windows™ events. For more information, see Adding a destination to the WinCollect Configuration Console on page 54.

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 54.
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 55.

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.

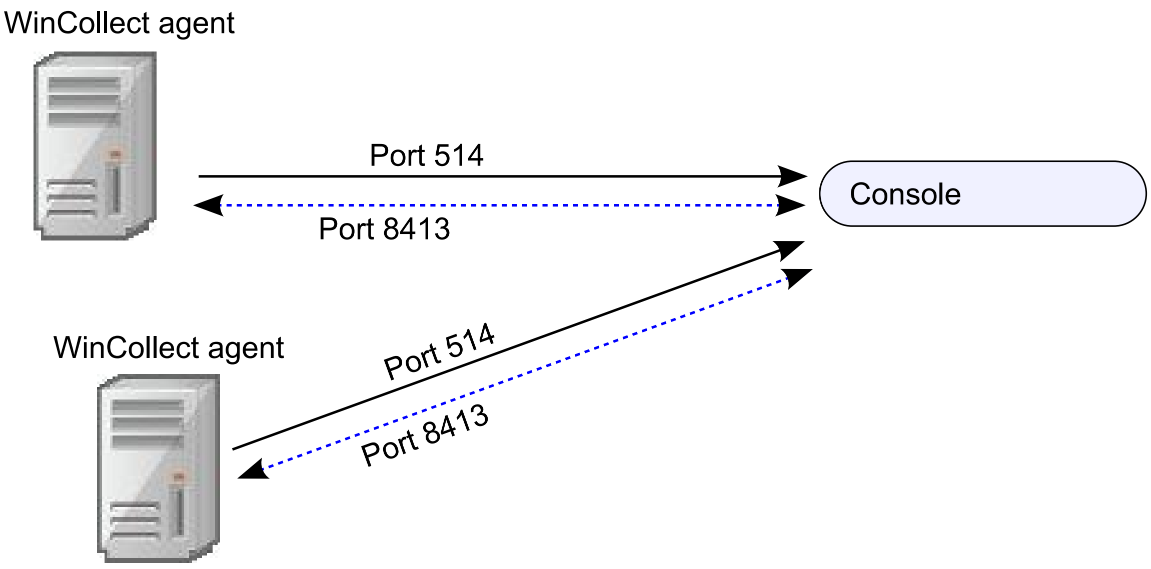

Figure 3: Local collection for WinCollect agents

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.

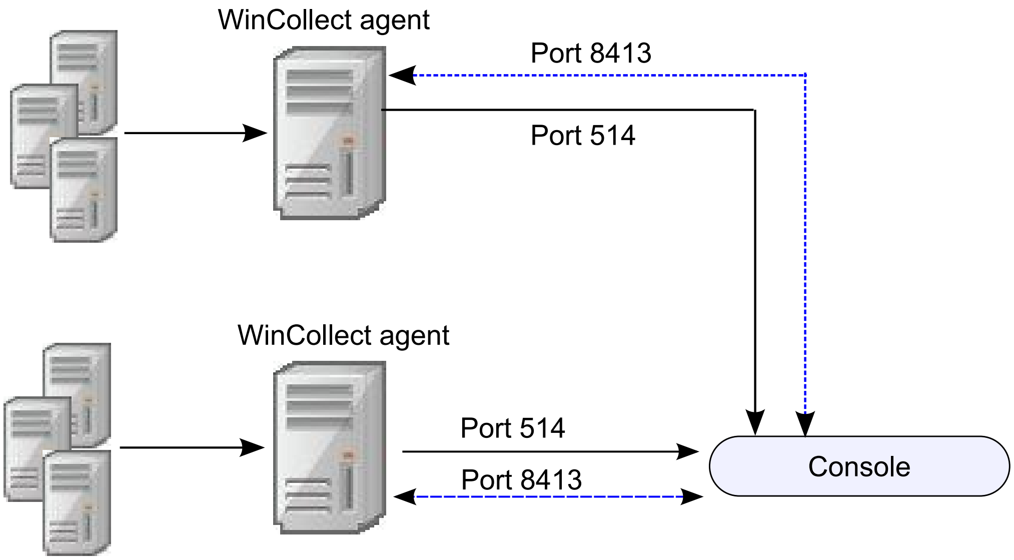

Figure 4: Remote collection for WinCollect agents

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 Event Collector

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

WinCollect agent communication to Extreme Security Console and Event Collectors

All WinCollect agents communicate with the Extreme Security Console and Event Collectors to forward events to Extreme Security and request updated information. You must ensure firewalls that are between the Extreme Security 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 Extreme Security. 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 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 3: 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 example Windows™ XP. For more information, see your Windows™ documentation.

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 4: Hardware requirements for WinCollect

Requirement	Description
Memory	8 GB 2 GB reserved for the WinCollect agent
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 5: Software requirements

Requirement	Description
Operating system	Windows™ Server 2003 (most recent) Windows™ Server 2008 (most recent) Windows™ Server 2012 (most recent) Windows™ 7 (most recent) Windows™ 8 (most recent) Windows™ Vista (most recent) Windows™ XP (most recent)
Distribution	One WinCollect agent for each host.
Required user role permissions for installation	Administrator Administrative permissions are not required for remote collection.

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 6: 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.

Prerequisites for upgrading WinCollect agents

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

WinCollect and Extreme Security software versions

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

- If you are running Extreme Security Analytics V7.1 (MR2), ensure that WinCollect agent 7.1.0-QRADAR-AGENT-WINCOLLECT-7.1-613263 is installed.
- If you are running Extreme Security V7.2.0 or later, ensure that WinCollect agent 7.2.0-QRADAR-AGENT-WINCOLLECT-7.2-613265 is installed.

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 Extreme Security, select Help > About
2. Select the Additional Release Information link.

You can also use ssh to log in to the Extreme Security Console, and run the following command:

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

Checking minimum WinCollect versions before upgrade installations

Before you install the new WinCollect agent, open the WinCollect pane in the Admin tab, and ensure that all WinCollect agents are listed as version 7.1.2.

If you installed AGENT-WINCOLLECT-7.1-613263 or AGENT-WINCOLLECT-7.2-613265, but one or more agents are still listed as version 7.1.1, ensure that you wait for the V7.1.2 update to be replicated to the agents. The time that you wait depends on what you previously configured for the Configuration Poll Interval in the WinCollect Agent Configuration pane.

4 WinCollect installations

To install WinCollect, you must download and install a WinCollect agent on your Extreme Security 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 Extreme Security appliances

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

When you upgrade a WinCollect application file, the Extreme Security host automatically updates all WinCollect agents that are enabled to receive automatic updates from the Console. WinCollect agents request updated configurations from the Extreme Security 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 Extreme Security after a previous WinCollect installation, you must delete the ConfigurationServer.PEM file in Program Files > IBM > WinCollect > config before WinCollect can function properly.

1 Download the WinCollect application installation file from Customer Support (www.extremenetworks.com/support/).
2 Using a program such as WinSCP, copy the installation file to your Extreme Security system.
3 Log in to Extreme Security 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_QRadar_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: If you are performing a WinCollect upgrade, push the upgrade to the managed WinCollect Agent hosts. Complete the following steps:

a Log in to Extreme Security.

b On the navigation menu, click Data Sources.

c Click the WinCollect icon.

d Click Agents.

e Select the WinCollect application that you want to update in your deployment.

f If the application is disabled, click Enable/Disable Automatic Updates.

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 Links

Installing the WinCollect agent on a Windows host on page 20

Installing a WinCollect agent from the command prompt on page 22

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 Extreme Security Analytics 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 Extreme Security appliances. Create one authentication token to be used for all of your WinCollect agents that communicate events with your Extreme Security host. If the authentication token expires, the WinCollect agent cannot receive log source configuration changes.

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 7: 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 **All** user role can be selected. Note The admin user role provides more privileges, which can create a security concern.

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.

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 19.

  .
- Your system meets the hardware and software requirements.

  For more information, see Hardware and software requirements for the WinCollect host on page 15.
- The required ports are available to WinCollect agents to communicate with Extreme Security Event Collectors.

  For more information, see Communication between WinCollect agents and Event Collector on page 14.
- 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 Extreme Security 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 29. 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 Extreme Security system must be updated to Extreme SIEM V7.2.1 Patch 1 or later.

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 Console (host and port)** field empty.

Table 8: WinCollect installation wizard parameters

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

Table 8: WinCollect installation wizard parameters (continued)

Parameter	Description
Machine poll interval (msec)	The polling interval that determines the number of milliseconds between queries to the Windows™ host. • 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. • 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. The minimum polling interval is 100 milliseconds (.1 seconds). The default is 3000 milliseconds or 3 seconds.
Minimum number of logs to process per pass	For more information, see IBM® Support (http://www-01.ibm.com/support/docview.wss?uid=swg21672193)..
Maximum number of logs to process per pass	For more information, see IBM® Support (http://www-01.ibm.com/support/docview.wss?uid=swg21672193)..

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.

The WinCollect installer uses the following command options:

Table 9: Silent installation options for WinCollect agents

Option	Description
`/qn`	Runs the WinCollect agent installation in silent mode.
`INSTALLDIR`	The name of the installation directory cannot contain spaces. Use quotation marks, ", to enclose the directory, for example, `INSTALLDIR=“C:\IBM\WinCollect\”`
`AUTHTOKEN=token`	Authorizes the WinCollect service, for example, `AUTH_TOKEN=af111ff6-4f30-11eb-11fb-1fc1 17711111`
`HOSTNAME=host name`	The IP address or host name of the WinCollect agent host cannot contain the "at" sign, @. The value in the HOSTNAME field must match the value in the Host Name field in the WinCollect Agent configuration on the Extreme Security Console.
`FULLCONSOLEADDRESS=host_address`	The IP address or host name of your Extreme Security Console or Event Collector, for example, FULLCONSOLEADDRESS=100.10.10.1. For your Windows™ hosts to communicate with your Extreme Security Event Collector, all systems in your Extreme Security deployment must be updated to V7.2.1 Patch 3 or later.

Table 9: Silent installation options for WinCollect agents (continued)

Option	Description
LOG_SOURCE_AUTO_CREATION	If you enable this option, you must configure the log source parameters. Extreme Security systems must be updated to V7.2.1 Patch 1 or later.
STATUSSERVER	Optional. Specifies the server where the status messages from the agent are sent. Example STATUSSERVER="100.10.10.255" STATUSSERVER="%COMPUTERNAME%"
LOG_SOURCE_AUTO_CREATION_ PARAMETERS	Ensure that each parameter uses the format: `Parameter_Name=value`. The parameters are separated with ampersands, &. Your Extreme Security system must be updated to V7.2.1 Patch 1 or later.

Table 10: 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 name of the Extreme Security Event Collector that polls the remote log source. Use this parameter in a distributed deployment to improve Extreme Security Console system performance by moving the polling task to an Event Collector. Use this option only if the **Component1.Destination.Id** option is not set.
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.

Table 10: Log source creation options (continued)

Option	Description/Required Value
`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.
`Component1.Log.Directory+Service`	Required. True or False. The Windows™ Directory Service log contains events that are written by the active directory.
`Component1.Log.File+Replication +Service`	Required. True or False. The Windows™ File Replication Service log contains events about changed files that are replicated on the system.
`Component1.MaxLogsToProcessPerPass`	Not required. The maximum number of logs (in binary form) that the algorithm attempts to acquire in one pass, if there are remaining events to be retrieved Example `Component1.MaxLogsToProcessPerPass=400` . Important You can use this parameter to improve performance for event collection, however, this parameter can also increase processor usage. Contact Customer Support before you attempt to tune individual agents.
`Component1.MinLogsToProcessPerPass`	Not required. The minimum number of logs (in binary form) that the algorithm attempts to read in one pass, if there are remaining retrievable events. Example `Component1.MinLogsToProcessPerPass=200` Important You can use this parameter to improve performance for event collection, but this parameter can also increase processor usage. Contact Customer Support before you attempt to tune individual agents.

1 Download the WinCollect agent setup file from Customer Support (www.extremenetworks.com/support/).

2. From the desktop, select **Start** > **Run**, type **cmd**, and click **OK**.
3. Ensure that the **Services** window is closed on the Windows™ host, otherwise the WinCollect agent installation fails.
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.

```
AGENT-WinCollect-<version>-setup.exe /s /v"/qn INSTALLDIR="C:\IBM
\WinCollect"
AUTHTOKEN=eb59386c-e098-49b8-ba40-6fb46bfe7d1
FULLCONSOLEADDRESS=100.10.10.1:8413 HOSTNAME=my_host
LOG_SOURCE_AUTO_CREATION_ENABLED=True
LOG_SOURCE_AUTO_CREATION_PARAMETERS=
""Component1.AgentDevice=
DeviceWindowsLog&Component1.Action=create&Component1.LogSourceName=
LSN2&Component1.LogSourceIdentifier=
100.10.12.1>&Component1.Destination.Name=Dest1&Component1.CoalesceEvents=
True&Component1.StoreEventPayload=True&Component1.
Encoding=UTF-8&Component1.Log.Application=True&Component1.Log.Security=
True&Component1.Log.System=True&Component1.Log.DNS+Server=
False&Component1.Log.Directory+Service=
False&Component1.Log.File+Replication+Service=False"""
```

   The following example shows an installation where automatic log creation is not used:

```
AGENT-WinCollect-<version>-setup.exe /s /v"/qn
INSTALLDIR="C:\IBM\WinCollect" AUTHTOKEN=eb59386c-e098-49b8-
ba40-6fb46bfe7d1
FULLCONSOLEADDRESS=100.10.10.1 HOSTNAME=my_host
```

5. Press Enter.

Uninstalling a WinCollect agent from the command prompt

You can uninstall the WinCollect agent from the command prompt.

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 Extreme Networks Security Analytics appliances as destinations for Windows™ events if a Extreme Security appliance fails.

You must create the destinations that you want to add to the WinCollect agent. See Adding a destination on page 29.

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.

1. In Extreme Security, 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.

5 Configuring WinCollect agents after installation

After you install a WinCollect deployment, you manage your deployment by using the Extreme Security Analytics.

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 Extreme Security by using syslog.

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

Note
The registration request to the Extreme Security 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 Extreme Security Analytics 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 Extreme Security, you must manually add the deleted agent.

For example, you delete a WinCollect agent that has a host identifier name VMRack1. You reinstall the agent and use the same host identifier name, VMRack1. The WinCollect agent does not automatically discover the WinCollect agent.

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 11: WinCollect agent parameters

Parameter	Description
Host Name	Depending on the method that you used to install the WinCollect agent on the remote host, the value in the Host Name field must match one of the following values: • HOSTNAME field in the WinCollect agent command-line configuration • Host Identifier field in the WinCollect agent installer.
Description	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.
Automatic Updates Enabled	Controls whether configuration updates are sent to the WinCollect agent.
Heart Beat Interval	This option defines how often the WinCollect agent communicates its status to the Extreme Security Console. The interval ranges from 0 seconds (Off) to 20 minutes.
Configuration Poll Interval	Defines how often the WinCollect agent polls the Extreme Security Console for updated log source configuration information or agent software updates. The interval ranges from 1 minute to 20 minutes.
Disk Cache Capacity (MB)	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.
Disk Cache Root Directory	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 Links

Deleting a WinCollect agent on page 28

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

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 Links

Manually adding a WinCollect agent on page 27

WinCollect destinations

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

Adding a destination

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

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 12: Destination parameters

Parameter	Description
Port	Extreme Security Analytics receives events from WinCollect agents on either UDP or TCP port 514.
Throttle (events per second)	Defines a limit to the number of events that the WinCollect agent can send each second.
Queue High Water Mark (bytes)	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.
Queue Low Water Mark (bytes)	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.
Storage Interval (seconds)	Defines an interval before the WinCollect agent writes events to disk or memory.

Table 12: Destination parameters (continued)

Parameter	Description
Processing Period (microseconds)	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.
Schedule Mode	If you select the Forward Events 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 Store Events 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.

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.

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 Extreme Security 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, Extreme Security Analytics 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 Extreme Security Analytics.

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 Extreme Security Analytics without administrator credentials.

If you have multiple Windows™ hosts that are sending an average of 5 EPS, and a 20 EPS peak, you can send many subscriptions to your agent. Ensure that you have an adequate buffer for event peaks.

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 Extreme Security.

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.

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.

You can use Windows™ event subscriptions with domain controllers, however, if advanced security auditing options are enabled, you can generate more events faster than the system can send them. 5,000 EPS is the theoretical limit. With a local WinCollect agent, the events are cached to the 6 GB of default disk space. This caching provides an extra layer of protection for systems that produce a high EPS rate. The disk space can manage event spikes which are common in domain controllers.

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)

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).

Process for using Microsoft™ event subscriptions

To use event subscriptions, you must complete these tasks:

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.

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.

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
Log Source Identifier	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
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 Extreme Security.
Domain	Optional The domain that includes the Windows™-based log source. The following examples use the correct syntax: `LAB1`, `server1.mydomain.com` The following example uses incorrect `syntax:\\mydomain.com`

Table 13: Common WinCollect log source parameters (continued)

Parameter	Description
Event Rate Tuning Profile	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: Default (Endpoint): 33-50 Events per second (EPS) Typical Server: 166-250 EPS High Event Rate Server: 416-625 EPS For a polling interval of 1000 ms the approximate EPS rates are as follows: Default (Endpoint): 100-150 Events per second (EPS) Typical Server: 500-750 EPS High Event Rate Server: 1250-1875 EPS For more information about tuning WinCollect, contact Customer Support (www.extremenetworks.com/support/).
Polling Interval (MS)	The interval, in milliseconds, between times when WinCollect polls for new events.
Application or Service Log Type	Optional. Used for XPath queries. 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.
Log Filter Type	Configures the WinCollect agent to ignore specific events from the Windows™ event log. You can also configure WinCollect agents to ignore events globally by ID code or log source. Exclusion filters for events are available for the following log source types: Security, System, Application, DNS Server, File Replication Service, Directory Service Global exclusions use the EventIDCode field from the event payload. To determine the values that are excluded, source and ID exclusions use the `Source=` field and the `EventIDCode=` field of the Windows™ event payload. Separate multiple sources by using a semi-colon.
Forwarded Events	Enables Extreme Security to collect events that are forwarded from remote Windows™ event sources that use subscriptions. Forward events that use event subscriptions are automatically discovered by the WinCollect agent and forwarded as if they are a syslog event source. When you configure event forwarding from your Windows™ system, enable event pre-rendering.
Event Types	At least one event type must be selected.
Enable Active Directory Lookups	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.
Override Domain Controller Name	Required when the domain controller that is responsible for Active Directory lookup is outside of the domain of the WinCollect agent. The IP address or host name of the domain controller that is responsible for the Active Directory lookup.
Override DNS Domain Name	The fully qualified domain name of the DNS server that is responsible for the Active Directory lookup, for example, `wincollect.com`

Table 13: Common WinCollect log source parameters (continued)

Parameter	Description
Remote Machine Poll Interval (ms)	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. 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. 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. 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.
XPath Query	Structured XML expressions that you can use to retrieve customized events from the Windows™ security event log. If you specify an XPath query to filter events, the check boxes that you selected from the Standard Log Type or Event Type are ignored. The events that Extreme Security collects use the contents of the XPath Query. To collect information by using an XPath Query, you might be required to enable Remote Event Log Management on Windows™ 2008. Microsoft™ Server 2003 does not support XPath Queries for events.
Credibility	Indicates the integrity of an event or offense as determined by the credibility value from the source devices. Credibility increases if multiple sources report the same event.
Target Internal Destination	Managed hosts with an event processor component in the Extreme Security Deployment Editor can be the target of an internal destination.
Target External Destination	Forwards your events to one or more external destinations that you configured in your destination list.
Coalescing Events	Enables the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the Coalescing Events list from the System Settings properties in Extreme Security. However, when you create or edit a log source, you can select the Coalescing Events check box to coalesce events for an individual log source.
Store Event Payload	Enables the log source to store event payload information. By default, automatically discovered log sources inherit the value of the Store Event Payload list from the System Settings properties in Extreme Security. However, when you create or edit a log source, you can select the Store Event Payload check box to retain the event payload for an individual log source.

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.

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.

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

Use the reference information to 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.

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

Table 14: Microsoft™ DHCP protocol parameters

Parameter	Description
Log Source Type	Microsoft DHCP
Protocol Configuration	WinCollect Microsoft DHCP
Local System	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 Extreme Security
Folder Path	For a local directory path, use the `c:\WINDOWS\system32\dhcp`directory. For a remote directory path, use the `\\DHCP IP address\c$\Windows\System32\dhcp` directory.
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 **Folder Path** field.

Related Links

Common WinCollect log source parameters on page 34
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 File Forwarder log source.

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

Table 15: File Forwarder protocol parameters

Parameter	Description
Log Source Type	Universal DSM
Protocol Configuration	WinCollect File Forwarder
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 Extreme Security Analytics.
Root Directory	The location of the log files to forward to Extreme Security. 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, for example, `\\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 Folder Path field.
Monitoring Algorithm	The Continuous Monitoring option is intended for files systems that append data to log files. The File Drop 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 Notification-based (local) option uses the Windows™ file system notifications to detect changes to your event log. The Polling-based (remote) 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.
File Reader Type	If you choose the Text (file held open) option, the system that generates your event log continually leaves the file open to append events to the end of the file. If you choose the Text (file open when reading) 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. If you select the Memory Mapped Text (local only) 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.

Related Links

Common WinCollect log source parameters on page 34

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.

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

Table 16: Microsoft™ IAS protocol parameters

Parameter	Description
Log Source Type	Microsoft IAS Server
Protocol Configuration	WinCollect Microsoft IAS / NPS
Local System	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 Extreme Security
Folder Path	For a local directory path, use the`%WINDIR%\System32\Logfiles`directory. For a remote directory path, use the `\\<IASIP>\c$\Windows\System32\Logfiles` directory.
File Monitor Policy	The Notification-based (local) option uses the Windows™ file system notifications to detect changes to your event log. The Polling-based (remote) 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.
Polling Interval	The amount of time between queries to the root log directory for new events.

Related Links

Common WinCollect log source parameters on page 34

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.

To read the log files, folder paths that contain an administrative share (C$), require NetBIOS privileges on the administrative share (C$). Local or domain administrators have sufficient privileges to access log files on administrative shares.

Fields for the Microsoft™ IIS protocol that support file paths allow administrators to define a drive letter with the path information. For example, the field can contain the `c$/LogFiles/` directory for an administrative share, or the `LogFiles/`directory for a public share folder path, but cannot contain the `c:/LogFiles` directory.

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

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

Table 17: Microsoft™ IIS protocol parameters

Parameter	Description
Protocol Configuration	Microsoft IIS
File Pattern	The regular expression (regex) that identifies the event logs.
Root Directory	The directory path to your Microsoft™ IIS log files. • For Microsoft™ IIS 6.0 (full site), use %SystemRoot%\LogFiles • For Microsoft™ IIS 6.0 (individual site), use %SystemRoot%\LogFiles \site name • For Microsoft™ 7.0-8.0 (full site), use %SystemDrive%\inetpub\logs \LogFiles • For Microsoft™ IIS 7.0-8.0 (individual site), use %SystemDrive%\inetpub \logs\LogFiles\site name
Protocol Logs	The items that you want to collect from Microsoft™ IIS.

Microsoft™ ISA log configuration options

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

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

Table 18: WinCollect Microsoft™ DHCP protocol parameters

Parameter	Description
Log Source Type	Microsoft ISA
Protocol Configuration	WinCollect Microsoft ISA / Forefront TMG
Local System	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 Extreme Security Analytics.

Table 18: WinCollect Microsoft™ DHCP protocol parameters (continued)

Parameter	Description
Root Directory	When you specify a remote file path, use a dollar sign, $, instead of a colon, :, to represent your drive name. Microsoft™ ISA 2004 • For a local directory path, use `<`*`Program Files`*`>\MicrosoftISAServer\ISALogs\` • For a remote directory path, use \\<*`ISA server IP`*>\\<*`Program Files`*>\MicrosoftISAServer\ISALogs\\ Microsoft™ ISA 2006 • For a local directory path, use `%systemroot%\LogFiles\ISA\` • For a remote directory path, use `\<`*`ISA server IP`*`>\%systemroot%\LogFiles\ISA\` Microsoft™ Threat Management Gateway • For a local directory path, use <*`Program Files`*>\\<*`Forefront Directory`*>\ISALogs\\ • For a remote directory path, use \\\\<*`ISA server IP`*>\\<*`Program Files`*>\\<*`Forefront Directory`*>\ISALogs\\
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 Folder Path field.
File Monitor Policy	The Notification-based (local) option uses the Windows™ file system notifications to detect changes to your event log. The Polling-based (remote) 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.
Polling Interval	The amount of time between queries to the root log directory for new events.

Related Links

Common WinCollect log source parameters on page 34

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.

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

Table 19: WinCollect Juniper Steel-Belted Radius protocol parameters

Parameter	Description
Log Source Type	Juniper Steel-Belted Radius
Protocol Configuration	WinCollect SBR

Table 19: WinCollect Juniper Steel-Belted Radius protocol parameters (continued)

Parameter	Description
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 Extreme Security Analytics.
Root Directory	The directory that contains the files that you want to monitor. Due to the restrictions in the distributed system, the Extreme Security user interface does not verify the path to the root directory. Ensure that you enter a valid local Windows™ path.
File Monitor Policy	The Notification-based (local) option uses the Windows™ file system notifications to detect changes to your event log. The Polling-based (remote) 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.
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.

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

Table 20: Microsoft™ SQL Server protocol parameters

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

Table 20: Microsoft™ SQL Server protocol parameters (continued)

Parameter	Description
Root Directory	Microsoft™ SQL 2000 • For a local directory path, use `C:\Program Files\Microsoft SQL Server\Mssql\Log` • For a remote directory path, use `\\SQL IP address\c$\Program Files\Microsoft SQL Server\Mssql\Log` Microsoft™ SQL 2005 • For a local directory path, use `c:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\LOG\` • For a remote directory path, use `\\SQL IP address\c$\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\LOG\` Microsoft™ SQL 2008 • For a local directory path, use `C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Log\` • For a remote directory path, use `\\SQL IP address\c$\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Log\` Microsoft™ SQL 2008R2 • For a local directory path, use `C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\Log` • For a remote directory path, use `\\SQL IP address\c$\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\Log`
File Monitor Policy	The Notification-based (local) option uses the Windows™ file system notifications to detect changes to your event log. The Polling-based (remote) 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.

Related Links

Common WinCollect log source parameters on page 34

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.

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

Table 21: 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.

Table 21: WinCollect NetApp Data ONTAP protocol parameters (continued)

Parameter	Description
Domain	The network domain to which the user name belongs.
Target Directory	The network path to the directory where you want to monitor files. Attention Due to the restrictions in the distributed system, this path is not verified by the Extreme Security 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.
Target Internal Destination	The Extreme Security Event Collector that you want to use.
Target External Destinations	To enable the use of an external event collector, select the check box and then select an external destination.

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 22: Microsoft™ SQL Server protocol parameters

Parameter	Description
Log Source Type	Microsoft Windows Security Event Log
Protocol Configuration	WinCollect
Standard Log Types	Clear all of the log type check boxes. The XPath query defines the log types for the log source.
Forwarded Events	Clear this check box.
Event Types	Clear this check box. The XPath query defines the log types for the log source.
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 Remote Event Log Management option on Windows™ 2008. Note Microsoft™ Server 2003 does not support XPath Queries for events.

Related Links

Common WinCollect log source parameters on page 34

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 Extreme Security 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

Enables 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.

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

Enables 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.

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

Enables 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.

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.

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 Extreme Networks Security Analytics. Check boxes that you select from the **Standard Log Type** or **Event Type** are ignored by the log source configuration.

Configure a log source with the XPath query. For more information, see XPath log source configuration options on page 44.

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.

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

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 &gt;= 4776 and EventID <= 4777) )]]</Select>
```

```
</Query>
</QueryList>
```

Table 23: 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 &gt;= 4722
and EventID <= 4726) or (EventID &gt;= 4741 and EventID
<= 4743) )]]</Select>
</Query>
</QueryList>
```

Table 24: 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.
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.

1 Create a destination for Windows™ events on each Extreme Networks Security Analytics appliance that you want to use for Windows™ event collection. See Adding a destination on page 29.

> 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 on page 49.

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 Extreme Networks Security Analytics. 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.

Ensure that you created destinations so that WinCollect agents can send Windows™ events to Extreme Security appliances. Ensure that you created one destination for each Extreme Security Event Collector 16xx or 18xx appliance.
You can have a maximum of 500 log sources for each managed WinCollect agent. You must also remain under 5,000 EPS 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.

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 Tune the WinCollect Agent by using the **Event Rate Tuning Profile** list.

- **Default (Endpoint)**: 33-50 Events per second (EPS)
- **Typical Server**: 166-250 EPS
- **High Event Rate Server**: 416-625 EPS

8 Adjust the Polling Interval option to increase or decrease the EPS rate. The maximum is 5,000 EPS for a single WinCollect agent.

Table 25: Default (Endpoint) polling intervals

Polling interval	Min EPS	Max EPS
3000	40	60
2500	48	72
2000	60	90
1500	80	120
1250	96	144
1000	120	180
750	160	240
500	240	360

Table 26: Typical Server polling intervals

Polling interval	Min EPS	Max EPS
3000	200	300
2500	240	360
2000	300	450
1500	400	600
1250	480	720
1000	600	900
750	800	1200
500	1200	1800

Table 27: High Event Rate Server Polling intervals

Polling interval	Min EPS	Max EPS
3000	500	750
2500	600	900
2000	750	1125
1500	1000	1500
1250	1200	1800
1000	1500	2250
750	2000	3000

Important

To prevent stability issues with WinCollect, do not set a polling interval under 350 milliseconds.

9 Select all of the **Standard Log Types** check boxes. The WinCollect agent reads and forwards these remote logs to Extreme Security.

> 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.

10 Select all of the **Event Types** check boxes.

11 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.

12 From the **WinCollect Agent** list, select the Windows™ host that manages the log source.

13 From the **Target Internal Destination** list, select the Extreme Security appliance that receives and processes the Windows™ events.

14 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.

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

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

Related Links

Adding a log source to a WinCollect agent on page 36

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.

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 Extreme Networks Security Analytics.

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 Extreme Networks Security Analytics destination where you want to send events.

Prerequisites

Before you can install the WinCollect Collect 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 20.
- Install .net framework version 3.5
- Install Microsoft™ Management Console (MMC) 3.0 and later.

The following table describes the WinCollect Configuration Console.

Table 28: WinCollect Configuration Console window

Sections	Description
Global Configuration	The Global Configuration parameter allows you to view, add and update information about the system where WinCollect data is stored.
	Disk Manager - the path to the WinCollect Data, which is used to buffer events to disk when the event rate exceeds the event throttle. Capacity 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.
	Installation Information - displays information about the WinCollect agent installation. Application Identifier - the header of the payload messages sent to the status server. Status Server - where the WinCollect Agent status events, such as heart beat messages and any warnings or errors generated by the WinCollect Agent, are sent.
	Security Manager - centralized credentials, used to collect events from remote devices.
Destinations	The Destinations parameter defines where WinCollect device data is sent.
	Syslog TCP or Syslog UDP destinations, with the following parameters: Name Hostname Port Throttle (events per second) You can expand a destination to view all devices that are assigned to the destination.
Devices	The Device parameter contains available device types. Under each device types, you can view or update multiple device parameters.

Installing the configuration console and, or the WinCollect patch

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.

1. Download the patch software from Customer Support (www.extremenetworks.com/support/).
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 and upgrading 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.

1. Download the patch software from Customer Support (www.extremenetworks.com/support/).
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. Uninstall the WinCollect Configuration Console by using 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).

Creating a WinCollect credential

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

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 Extreme Networks Security Analytics instance as a destination for WinCollect data.

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.

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**.

Use Case: 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 Extreme Networks Security Analytics.

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).

2 Create a destination for the Extreme Security instance where you want to send WinCollect information. See Adding a destination to the WinCollect Configuration Console on page 54.

3 Configure the local Microsoft™ event log device that is monitored. See Adding a device to the WinCollect Configuration Console on page 55.

> 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**.

Use Case: 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 Extreme Networks Security Analytics.

1 Install the WinCollect Configuration Console on the windows machine that collects the log information. Download the patch from Customer Support (www.extremenetworks.com/support/).

2 Create a credential to use when you log in to remote hosts. See Creating a WinCollect credential on page 54.

3. Create the Extreme Security destination where Windows™ events are sent. See Adding a destination to the WinCollect Configuration Console on page 54.
4. Configure the devices that are monitored. See Adding a device to the WinCollect Configuration Console on page 55.

   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**.