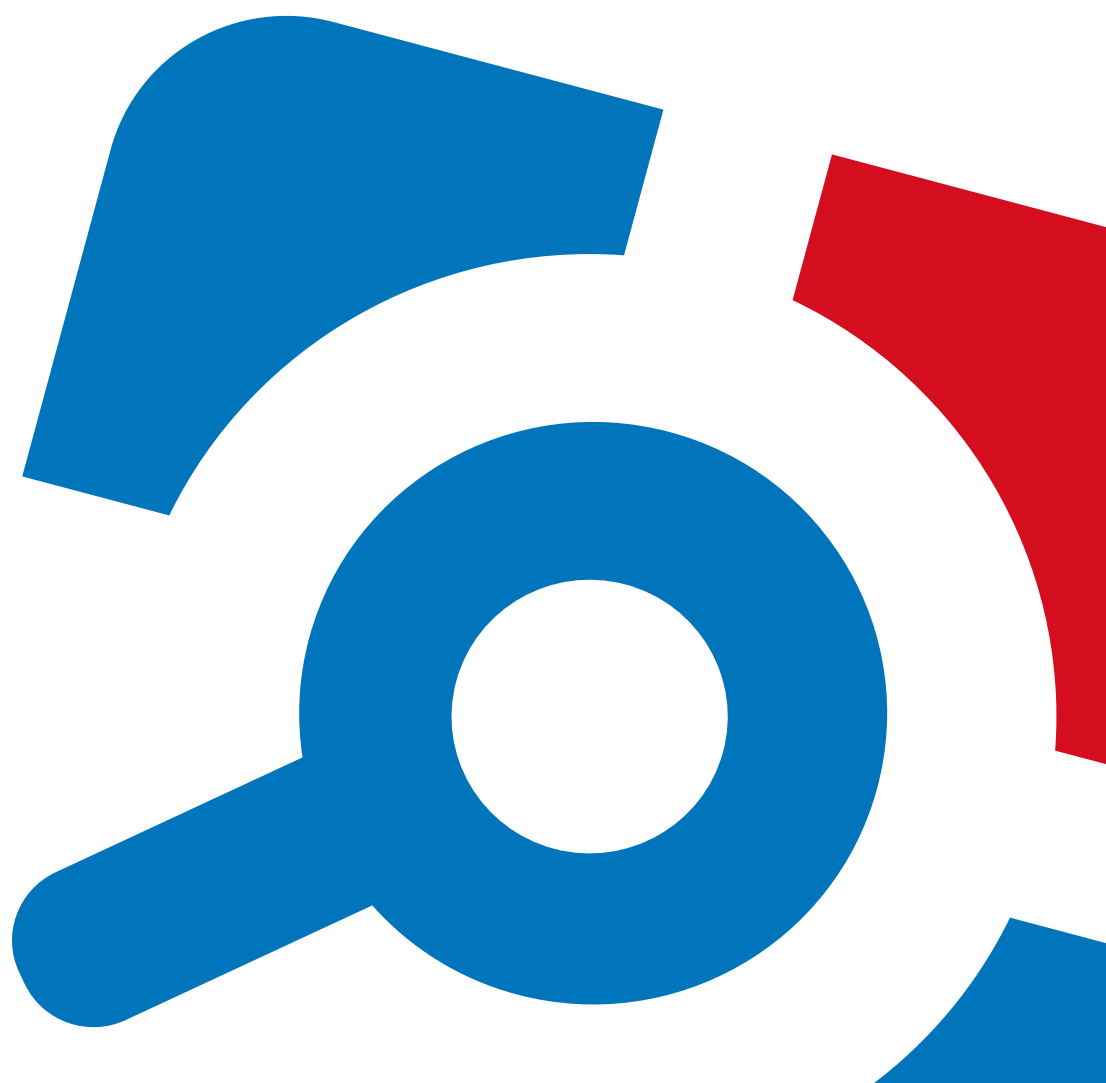


Netwrix Auditor Add-on for SIEM Quick-Start Guide

Version: 9.9
11/27/2020



Legal Notice

The information in this publication is furnished for information use only, and does not constitute a commitment from Netwrix Corporation of any features or functions, as this publication may describe features or functionality not applicable to the product release or version you are using. Netwrix makes no representations or warranties about the Software beyond what is provided in the License Agreement. Netwrix Corporation assumes no responsibility or liability for the accuracy of the information presented, which is subject to change without notice. If you believe there is an error in this publication, please report it to us in writing.

Netwrix is a registered trademark of Netwrix Corporation. The Netwrix logo and all other Netwrix product or service names and slogans are registered trademarks or trademarks of Netwrix Corporation. Microsoft, Active Directory, Exchange, Exchange Online, Office 365, SharePoint, SQL Server, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

Disclaimers

This document may contain information regarding the use and installation of non-Netwrix products. Please note that this information is provided as a courtesy to assist you. While Netwrix tries to ensure that this information accurately reflects the information provided by the supplier, please refer to the materials provided with any non-Netwrix product and contact the supplier for confirmation. Netwrix Corporation assumes no responsibility or liability for incorrect or incomplete information provided about non-Netwrix products.

© 2020 Netwrix Corporation.

All rights reserved.

Table of Contents

1. About This Document	5
2. Solution Overview	6
2.1. How It Works	6
2.1.1. Netwrix Auditor Activity Records to Event Log Add-on	6
2.1.2. Netwrix Auditor Alerts to Event Log Add-on	7
2.2. Compatibility Notice	7
3. Prerequisites	8
3.1. Netwrix Auditor Activity Records to Event Log Add-on	8
3.2. Netwrix Auditor Alerts to Event Log Add-on	9
4. Configuration	10
4.1. Netwrix Auditor Activity Records to Event Log Add-on Settings	10
4.1.1. Connection Parameters	10
4.2. In-Script Parameters	11
4.3. Netwrix Auditor Alerts to Event Log Add-on Settings	13
5. Choose Appropriate Execution Scenario	14
5.1. Netwrix Auditor Activity Records to Event Log Add-on	14
5.2. Netwrix Auditor Alerts to Event Log Add-on	14
6. Exporting Activity Records	16
6.1. Exporting Activity Records Associated with the Alert	16
6.2. Exporting Activity Records in Bulk	16
6.2.1. Applying Filters	17
6.2.2. Automate Add-On Execution	17
7. See Results	19
8. Appendix. Netwrix Auditor Integration Event Log Fields	20

1. About This Document

This guide is intended for the first-time users of Netwrix Auditor Integration API and add-ons. It can be used for evaluation purposes, therefore, it is recommended to read it sequentially, and follow the instructions in the order they are provided. After reading this guide you will be able to:

- Install the add-on
- Configure its parameters
- Use the add-on

NOTE: The add-on works only in combination with Netwrix Auditor so this guide covers a basic procedure for running the add-on and assumes that you have Netwrix Auditor installed and configured in your environment. For installation scenarios, data collection options, as well as detailed information on Integration API, refer to the Online Help Center and product documentation:

- [Netwrix Auditor Online Help Center](#)
- [Netwrix Auditor Installation and Configuration Guide](#)
- [Netwrix Auditor Integration API Guide](#)

2. Solution Overview

Netwrix Auditor Add-on for SIEM helps you to get most from your SIEM investment, in particular, with the following SIEM solutions:

1. Splunk
2. IBM QRadar
3. AlienVault USM
4. Solarwinds Log & Event Manager
5. Intel Security
6. LogRhythm

The add-on works in collaboration with Netwrix Auditor, supplying additional data that augments the data collected by SIEM.

The add-on enriches your SIEM data with actionable context in human-readable format, including the before and after values for every change and data access attempt, both failed and successful. Aggregating data into a single audit trail simplifies analysis, makes your SIEM more cost effective, and helps you keep tabs on your IT infrastructure.

The solution includes two add-ons implemented as PowerShell scripts that facilitate the audit data transition from Netwrix Auditor to SIEM:

- The **Netwrix Auditor Activity Records to Event Log Add-on** allows you to export all audit data collected by Netwrix Auditor - this can be recommended for small-to-medium infrastructures.
- In larger environments and with highly transactional infrastructure, however, it is recommended to use a more intelligent approach to data export. For that, use the **Netwrix Auditor Alerts to Event Log Add-on** that can export only data on critical events and changes that initiate the alert triggering.

2.1. How It Works

2.1.1. Netwrix Auditor Activity Records to Event Log Add-on

On a high level, this add-on works as follows:

1. The add-on connects to the Netwrix Auditor server and retrieves audit data using the Netwrix Auditor Integration API.
2. The add-on processes Netwrix Auditor-compatible data (Activity Records) into log events that work as input for SIEM. Each event contains the user account, action, time, and other details.

3. The add-on creates a special Windows event log named **Netwrix_Auditor_Integration** and stores events there. These events are structured and ready for integration with SIEM.

For more information on the structure of the Activity Record and the capabilities of the Netwrix Auditor Integration API, refer to [Netwrix Auditor Integration API Guide](#) and to [Online Help Center](#).

2.1.2. Netwrix Auditor Alerts to Event Log Add-on

This add-on works as response action to the alert, as follows:

1. The administrator enables and configured response action for selected alert, as described [here](#). Make sure to provide correct path to the script file and to select the Write data to CSV file option.
2. When the alert is triggered, the script starts - it retrieves audit data (activity record fields) from the CSV file and processes it into log events. Each event contains the user account, action, time, and other details.
3. The add-on creates a special Windows event log named **Netwrix_Auditor_Integration** and stores events there. These events are structured and ready for integration with SIEM.

For more information on the alert response actions and CSV file, refer to [Netwrix Auditor Intelligence Guide](#) and to [Online Help Center](#).

2.2. Compatibility Notice

Make sure to check your product version, and then review and update your add-ons and scripts leveraging Netwrix Auditor Integration API. Download the latest add-on version from the Add-on Store.

The solution works with Netwrix Auditor version 9.8 or later.

3. Prerequisites

3.1. Netwrix Auditor Activity Records to Event Log Add-on

On...	Ensure that...
The Netwrix Auditor Server side	<ul style="list-style-type: none"> • Netwrix Auditor version is 9.8 or later. • The Audit Database settings are configured in Netwrix Auditor Server. • The TCP 9699 port (default Netwrix Auditor Integration API port) is open for inbound connections. • The user retrieving data from the Audit Database is granted the Global reviewer role in Netwrix Auditor or is a member of the Netwrix Auditor Client Users group. <p>Alternatively, you can grant the Global administrator role or add the user to the Netwrix Auditor Administrators group. In this case, this user will have the most extended permissions in the product.</p>
The computer where the script will be executed	<ul style="list-style-type: none"> • PowerShell 3.0 or later must be installed. • .NET 4.5 or later must be installed. • Execution policy for powershell scripts is set to <i>"Unrestricted"</i>. Run Windows PowerShell as administrator and execute the following command: <ul style="list-style-type: none"> <code>Set-ExecutionPolicy Unrestricted</code> • The user running the script is granted the write permission on the script folder—the add-on creates a special .bin file with the last exported event. • The user running the script must be a member of the Domain Users group. • At least the first script run should be performed under the account with elevated privileges, as it will be necessary to create event log file and perform other required operations.

3.2. Netwrix Auditor Alerts to Event Log Add-on

On...	Ensure that...
The Netwrix Auditor Server side	<ul style="list-style-type: none"> • Netwrix Auditor version is 9.8 or later. • The alert response action settings in Netwrix Auditor Server are configured as follows: <ul style="list-style-type: none"> • Take action when alert occurs is switched ON • Run field contains the path to Windows PowerShell: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe • With parameters field contains the required parameters, including the path to Netwrix_Auditor_Alerts_to_Event_Log_Add-on.ps1 file. Example: -File C:\Netwrix_Auditor_Add-on_for_SIEM\Netwrix_Auditor_Alerts_to_Event_Log_Add-on.ps1 -NetwrixPathToCsvData <p>NOTE: For details on script parameters, see the section below.</p> <ul style="list-style-type: none"> • Write data to CSV file option is selected • Command line preview looks like this: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -File C:\Netwrix_Auditor_Add-on_for_SIEM\Netwrix_Auditor_Alerts_to_Event_Log_Add-on.ps1 -NetwrixPathToCsvData {CsvFile} • By default, the executable file will be launched under the <i>LocalSystem</i> account. If you want to use another account, make sure it has Log on as batch job privilege on Netwrix Auditor server. <p>NOTE: You may want to perform the test run after configuring the script as the alert response action. If so, consider that current user account (logged on to Netwrix Auditor client) must have local Administrator privileges on Netwrix Auditor server where the executable file is located.</p>

For more information on the alerts and response actions, see [Online Help Center](#).

4. Configuration

4.1. Netwrix Auditor Activity Records to Event Log Add-on Settings

4.1.1. Connection Parameters

Before running or scheduling the add-on, you must define connection details: Netwrix Auditor Server host, user credentials, etc. Most parameters are optional, the script uses the default values unless parameters are explicitly defined. You can skip or define parameters depending on your execution scenario and security policies. See "Choose Appropriate Execution Scenario" section for more information.

Parameter	Default value	Description
Connection to Netwrix Auditor		
NetwrixAuditorHost	localhost:9699	<p>Assumes that the add-on runs on the computer hosting Netwrix Auditor Server and uses default port 9699.</p> <p>If you want to run the add-on on another machine, provide a name of the computer where Netwrix Auditor Server resides (e.g., 172.28.6.15, EnterpriseNAServer, WKS.enterprise.local).</p> <p>To specify a non-default port, provide a server name followed by the port number (e.g., WKS.enterprise.local:9999).</p>
NetwrixAuditorUserName	Current user credentials	<p>Unless specified, the add-on runs with the current user credentials.</p> <p>If you want the add-on to use another account to connect to Netwrix Auditor Server, specify the account name in the DOMAIN\username format.</p> <p>NOTE: The account must be assigned the Global reviewer role in Netwrix Auditor or be a member of the Netwrix Auditor Client Users group on the computer hosting Netwrix Auditor Server.</p>

Parameter	Default value	Description
NetwrixAuditorPassword	Current user credentials	Unless specified, the script runs with the current user credentials. Provide a different password if necessary.

4.2. In-Script Parameters

You may also need to modify the parameters that define how EventIDs should be generated for exported events, though their default values address most popular usage scenarios. In-script parameters are listed in the table below. To modify them, open the script for edit and enter the values you need.

NOTE: Once set, these parameter values must stay unchanged until the last run of the script — otherwise dynamically calculated EventIDs will be modified and applied incorrectly.

Parameter	Default value	Description
EventID generation		
GenerateEventId	True	<p>Defines whether to generate unique EventIDs. Possible parameter values:</p> <ul style="list-style-type: none"> • True — generate unique EventIDs using Activity Record fields • False — do not generate a unique ID, set EventID=0 for all cases <p>EventID is generated through CRC32 calculation that involves the following Activity Record field values:</p> <ul style="list-style-type: none"> • ObjectType • Action • DataSource (optional, see below for details) <p>NOTE: Only the lowest 16 bits of the calculation result are used.</p> <p>For detailed Activity Record description, refer to Activity Record.</p>
IncludeDataSourceToMakeEventId	True	Defines whether the DataSource field of Activity Record should be used in the EventID calculation. This parameter is

Parameter	Default value	Description
		<p>applied only if GenerateEventId is set to TRUE.</p> <p>NOTE: <i>Object Type - Action</i> pair may be identical for several data sources (e.g., Object='User' and Action='Added'); thus, excluding DataSource from calculation may lead to the same EventID (duplicates). See Exporting Activity Records for details about duplicates.</p>
SetDataSourceAsEventCategory	True	<p>Defines whether to fill in Event Category event field with a numeric value derived from the DataSource field of Activity Record.</p> <p>Possible parameter values:</p> <ul style="list-style-type: none"> • True — generate a numeric value for Event Category using Activity Record field • False — do not generate a numeric value, set Event Category=1 for all cases <p>The Event Category field value is generated through CRC32 calculation that involves the DataSource field of Activity Record.</p> <p>NOTE: Only the lowest 9 bits of the calculation result are used.</p>
SetDataSourceAsEventSource	False	<p>Defines whether to fill in the Event Source event field with the value from the DataSource field of Activity Record.</p> <p>Possible parameter values:</p> <ul style="list-style-type: none"> • True — fill in the Event Source with the value from DataSource field of Activity Record, adding the prefix defined by \$EventSourcePrefix.

Parameter	Default value	Description
		<p>Default prefix is <i>NA</i>, for example:<i>NA Windows Server</i></p> <ul style="list-style-type: none"> • False — set Event Source to <i>Netwrix_Auditor_Integration_API</i> for all cases <p>NOTE: If the script cannot fill in the Event Source for some DataSource, the default value <i>Netwrix_Auditor_Integration_API</i> will be used.</p> <p>If the event source for particular DataSource does not exist in the Netwrix_Auditor_Integration event log, elevated privileges are required for add-on execution.</p>

4.3. Netwrix Auditor Alerts to Event Log Add-on Settings

This add-on requires you to specify the following parameter:

Parameter	Description	Example
NetwrixPathToCsvData	Specify path to the auxiliary CSV file storing the data of activity records associated with the alert.	%ProgramData%\Netwrix Auditor\ AuditCore\AuditArchive\ AlertsToolLauncher\ Csv\file.csv

5. Choose Appropriate Execution Scenario

5.1. Netwrix Auditor Activity Records to Event Log Add-on

This add-on can run on any computer in your environment. For example, you can run the add-on on the computer where Netwrix Auditor is installed, or on a remote server. Depending on the execution scenario you choose, you have to define a different set of parameters. See "Configure Add-on Parameters" section for more information.

Netwrix suggests the following execution scenarios:

Scenario	Example
The add-on runs on the Netwrix Auditor Server with the current user credentials. Activity Records are exported to a local event log.	<code>C:\Add-ons\Netwrix_Auditor_Activity_Records_to_Event_Log_Add-on.ps1</code>
The add-on runs on the Netwrix Auditor Server with explicitly defined credentials. Activity Records are exported to a local event log.	<code>C:\Add-ons\Netwrix_Auditor_Activity_Records_to_Event_Log_Add-on.ps1 - NetwrixAuditorUserName enterprise\NAuser - NetwrixAuditorPassword NetwrixIsCool</code>
The add-on exports Activity Records from a remote Netwrix Auditor Server using current user credentials and writes data to a local event log.	<code>C:\Add-ons\Netwrix_Auditor_Activity_Records_to_Event_Log_Add-on.ps1- NetwrixAuditorHost 172.28.6.15</code>
The add-on exports Activity Records from a remote Netwrix Auditor Server using explicitly defined credentials and writes data to a local event log.	<code>C:\Add-ons\Netwrix_Auditor_Activity_Records_to_Event_Log_Add-on.ps1 - NetwrixAuditorHost 172.28.6.15 - NetwrixAuditorUserName enterprise\NAuser - NetwrixAuditorPassword NetwrixIsCool</code>

For security reasons, Netwrix recommends running the script with current user credentials (skipping user credentials). Create a special user account with permissions to both Netwrix Auditor data and event log and use it for running the script.

5.2. Netwrix Auditor Alerts to Event Log Add-on

The script will be executed on Netwrix Auditor server.

By default, Netwrix Auditor uses the *Local/System* account to run PowerShell scripts. If you want to use another account, in the alert settings go to **Response Action**, select the **Use custom credentials** checkbox and specify user name and password. Make sure this account has **Log on as batch job** privilege.

6. Exporting Activity Records

6.1. Exporting Activity Records Associated with the Alert

To export only important audit data, that is, the Activity Records that led to the alert triggering, configure the alert response action, providing path to `Netwrix_Auditor_Alerts_to_Event_Log_Add-on.ps1`. See [Prerequisites](#) for details.

6.2. Exporting Activity Records in Bulk

As said, Netwrix recommends exporting the most important data, using the script described above. However, if you need to export all Activity Records in bulk, follow the recommendations below.

First, provide a path to your add-on followed by script parameters with their values. Each parameter is preceded with a dash; a space separates a parameter name from its value. You can skip some parameters—the script uses a default value unless a parameter is explicitly defined. If necessary, modify the parameters as required.

To run the script with PowerShell

1. On computer where you want to execute the add-on, start **Windows PowerShell**.
2. Type a path to the add-on. Or simply drag and drop the add-on file in the console window.
3. Add script parameters. The console will look similar to the following:

```
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.
PS C:\Users\AddOnUser> C:\Add-ons\Netwrix_Auditor_Activity_Records_to_Event_Log_Add-on.ps1.ps1
```

NOTE: If the script path contains spaces (e.g., `C:\Netwrix Add-ons\`), embrace it in double quotes and insert the ampersand (&) symbol in front (e.g., `& "C:\Netwrix Add-ons\"`).

4. Hit **Enter**.

Depending on the number of Activity Records stored in Netwrix Auditor Audit Database execution may take a while. Ensure the script execution completed successfully. The **Netwrix Auditor Integration** event log will be created and filled with events.

By default, the **Netwrix Auditor Integration** event log size is set to *1GB*, and retention is set to *"Overwrite events as needed"*. For details on event record fields, please refer to the Appendix.

NOTE: Event records with more than 30,000 characters length will be trimmed.

At the end of each run, the script creates the `Netwrix_Auditor_Event_Log_Export_Add-on_EventIDs.txt` file. It defines mapping between the Activity Records and related Event IDs .

You can use this file to track possible duplicates of Event IDs created at each script execution. Duplicates, if any, are written to the `Netwrix_Auditor_Event_Log_Export_Add-on_EventIDsDuplicates.txt` file.

Similarly, the add-on also creates the `Netwrix_Auditor_Event_Log_Export_Add-on_CategoriesIDs.txt` file that defines mapping between the Data Source and related Category ID.

6.2.1. Applying Filters

Every time you run the script, Netwrix Auditor makes a timestamp. The next time you run the script, it will start retrieving new Activity Records. Consider the following:

- By default, the add-on does not apply any filters when exporting Activity Records. If you are running the add-on for the first time (there is no timestamp yet) with no filters, it will export Activity Records for the last month only. This helps to optimize solution performance during the first run. At the end of the first run, the timestamp will be created, and the next run will start export from that timestamp.
- However, if you have specified a time period for Activity Records to be exported, then this filter will be applied at the add-on first run and the runs that follow.

6.2.2. Automate Add-On Execution

To ensure you feed the most recent data to your SIEM solution, you can schedule a daily task for running the Netwrix Auditor Activity Records to Event Log add-on.

To create a scheduled task

1. On the computer where you want to execute the add-on, navigate to **Task Scheduler**.
2. Select **Create Task**.
3. On the **General** tab, specify a task name, e.g., Netwrix AuditorAdd-on for SIEM. Make sure the account that runs the task has all necessary rights and permissions.
4. On the **Triggers** tab, click **New** and define the schedule. This option controls how often audit data is exported from Netwrix Auditor and saved to event log. Netwrix recommends scheduling a daily task.
5. On the **Actions** tab, click **New** and specify action details. Review the following for additional information:

Option	Value
Action	Set to <i>"Start a program"</i> .
Program/script	Input <i>"Powershell.exe"</i> .

Option	Value
Add arguments (optional)	Add a path to the add-on in double quotes and specify add-on parameters. For example: <pre>-file "C:\Add-ons\Netwrix_Auditor_Audit_Records_to_Event_Log_Add-on.ps1"</pre>

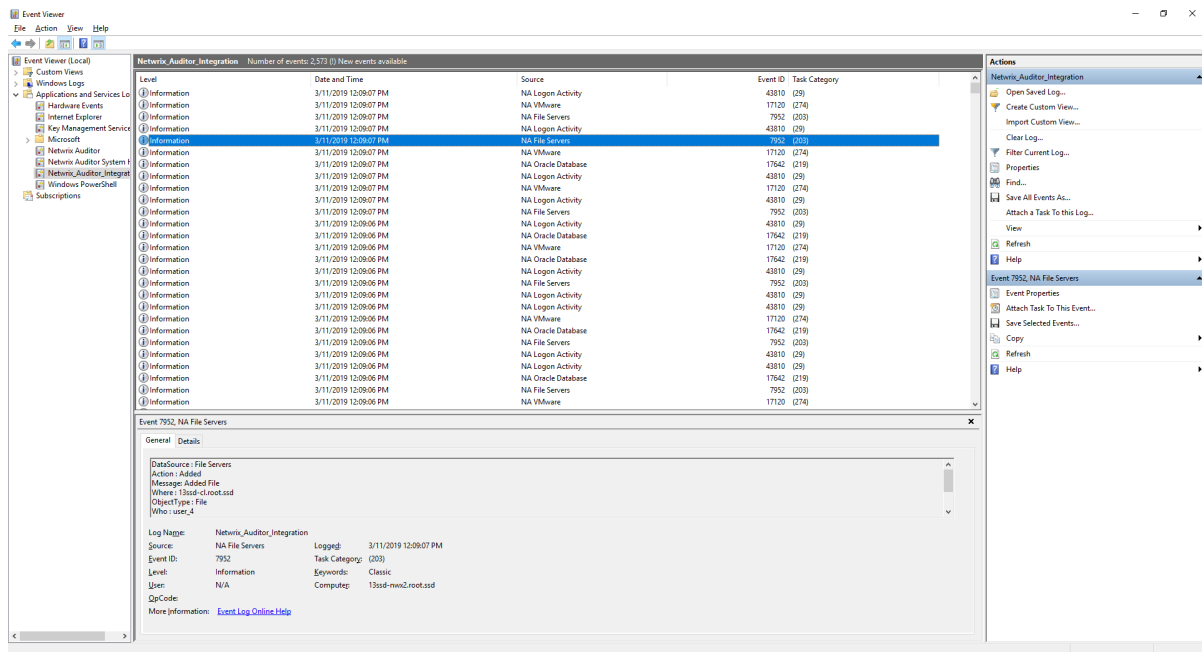
6. Save the task.

After creating a task, wait for the next scheduled run or navigate to **Task Scheduler** and run the task manually. To do this, right-click a task and click **Run**.

7. See Results

1. On the computer where you executed the add-on, navigate to **Start** → **All Programs** → **Event Viewer**.
2. In the Event Viewer dialog, navigate to **Event Viewer (local)** → **Applications and Services Logs** → **Netrix_Auditor_Integration** log.
3. Review events.

Now you can augment SIEM with data collected by Netrix Auditor.



8. Appendix. Netwrix Auditor Integration Event Log Fields

This section describes how the add-on fills in the **Netwrix Auditor Integration** event log fields with data retrieved from Netwrix Auditor Activity Record.

NOTE: The Activity Record structure is described in the [Activity Record Reference](#) section.

Event log field name	Filled in with value	Details
Source	NA <i>{Data Source Name}</i> -OR- Netwrix_Auditor_Integration_API	Depending on <i>SetDataSourceAsEventSource</i> in-script parameter. See Configuration
EventID	<i>{Calculated by add-on}</i> -OR- 0	Depending on <i>GenerateEventId</i> in-script parameter (calculation result also depends on <i>IncludeDataSourceToMakeEventId</i> parameter — if <i>GenerateEventId = True</i>). See Configuration
Task Category	<i>{DataSource ID}</i> -OR- 1	Depending on <i>SetDataSourceAsEventCategory</i> in-script parameter. See Configuration

EventData is filled in with data from the Activity Record fields as follows:

Entry in EventData	Activity Record field
DataSource	{DataSource}
Action	{Action}
Message	{Action ObjectType}
Where	{Where}
ObjectType	{ObjectType}

Entry in EventData	Activity Record field
Who	{Who}
What	{What}
When	{When}
Workstation	{Workstation}
Details	{Details}

NOTE: Details are filled in only if this Activity Record field is not empty.

