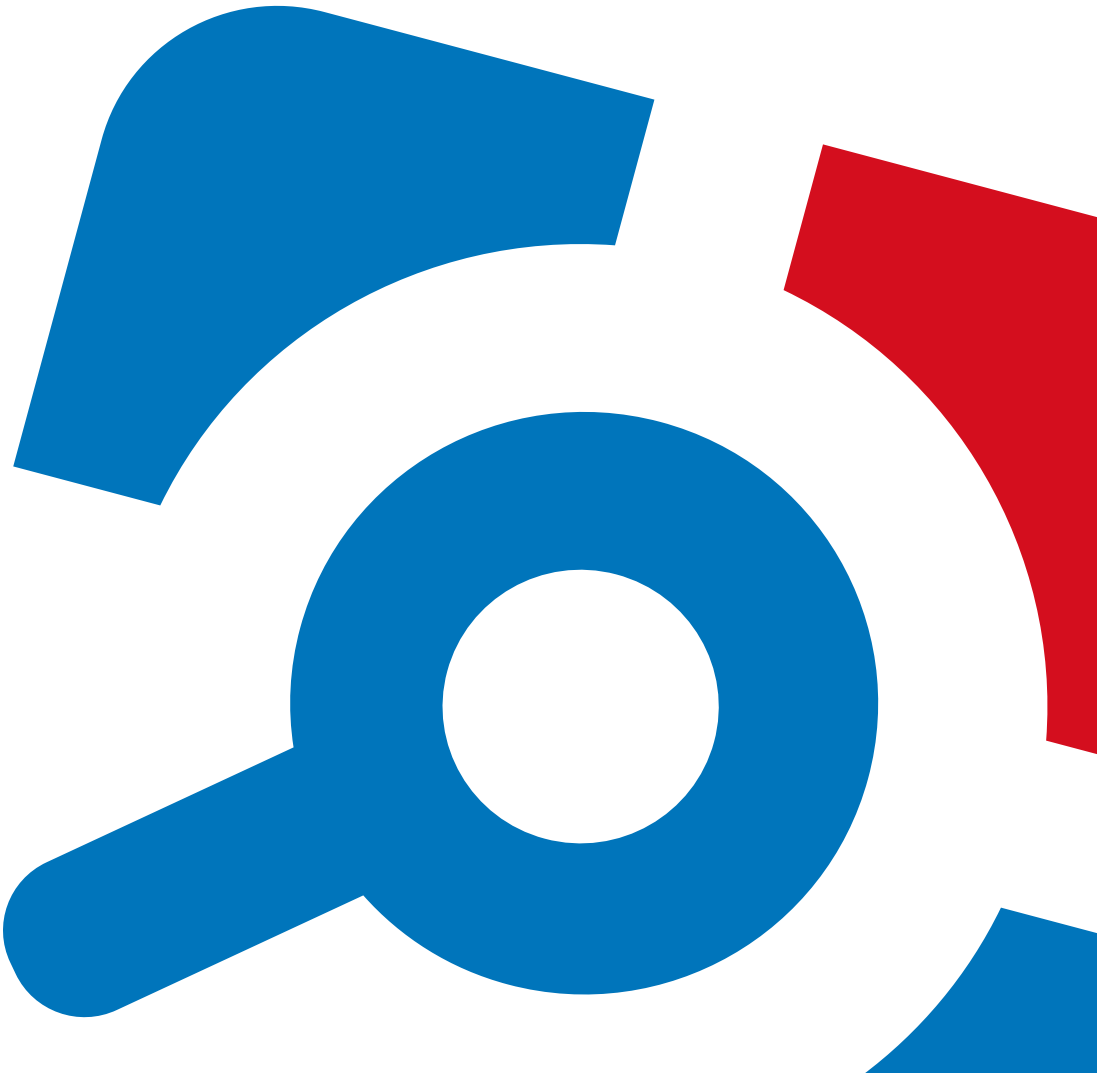
netwrix

Netwrix Auditor Add-on for IBM QRadar

Quick-Start Guide

Version: 9.8
5/14/2019



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.

Table of Contents

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 Event Log Export add-on 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 IBM QRadar.

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.

Implemented as a PowerShell script, this add-on facilitates the audit data transition from Netwrix Auditor to IBM QRadar. All you have to do is provide connection details and schedule the script for execution.

On a high level, the 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 IBM QRadar. 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 IBM QRadar.

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. 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 in the Add-on Store. For more information about schema updates, refer to Netwrix Auditor Integration API.

The add-on works with Netwrix Auditor version 9.7 or later. Please note that starting with version 9.8, Netwrix provides a universal add-on for all SIEM solutions listed above.

3. Prerequisites

Before running Netwrix Auditor Add-on for IBM QRadar, ensure that all the necessary components and policies are configured as follows:

On...	Ensure that...
The Netwrix Auditor Server side	• Netwrix Auditor version is **9.7** 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. 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.
The computer where the script will be executed	• PowerShell **3.0** or later must be installed. • .NET **4.5** or later must be installed. • Execution policy for powershell scripts is set to *"Unrestricted"*. Run **Windows PowerShell** as administrator and execute the following command: `Set-ExecutionPolicy Unrestricted` • 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.

4. Configure Add-On Parameters

4.1. 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	Assumes that the add-on runs on the computer hosting Netwrix Auditor Server and uses default port 9699. 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). To specify a non-default port, provide a server name followed by the port number (e.g., WKS.enterprise.local:9999).
NetwrixAuditorUserName	Current user credentials	Unless specified, the add-on runs with the current user credentials. 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. 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.
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	Defines whether to generated unique EventIDs. Possible parameter values: • **True** — generate unique EventIDs using Activity Record fields • **False** — do not generate a unique ID, set EventID=0 for all cases EventID is generated through CRC32 calculation that involves the following Activity Record field values: • ObjectType • Action • DataSource (optional, see below for details) NOTE: Only the lowest 16 bits of the calculation result are used. For detailed Activity Record description, refer to Activity Record.
IncludeDataSourceToMakeEventId	True	Defines whether the DataSource field of Activity Record should be used in the EventID calculation. This parameter is applied only if **GenerateEventId** is set to TRUE. NOTE: *Object Type - Action* pair may be identical for several data sources (e.g., Object='User' and Action='Added'); thus, excluding

Parameter	Default value	Description
		DataSource from calculation may lead to the same EventID (duplicates). See Run the Add-On with PowerShell for details about duplicates.
SetDataSourceAsEventCategory	True	Defines whether to fill in Event Category event field with a numeric value derived from the DataSource field of Activity Record. Possible parameter values: • **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 The Event Category field value is generated through CRC32 calculation that involves the DataSource field of Activity Record. NOTE: Only the lowest 9 bits of the calculation result are used.
SetDataSourceAsEventSource	False	Defines whether to fill in the Event Source event field with the value from the DataSource field of Activity Record. Possible parameter values: • **True** — fill in the Event Source with the value from DataSource field of Activity Record, adding the prefix defined by **$EventSourcePrefix**. Default prefix is *NA*, for example:*NA Windows Server* • **False** — set Event Source to *Netwrix_Auditor_Integration_API* for all cases NOTE: If the script cannot fill in the Event

Parameter	Default value	Description
		Source for some DataSource, the default value *Netwrix_Auditor_Integration_API* will be used. 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.

5. Choose Appropriate Execution Scenario

Netwrix Auditor Add-on for IBM QRadar runs 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.	`C:\Add-ons\Netwrix_Auditor_Add-on_for_IBM_QRadar.ps1`
The add-on runs on the Netwrix Auditor Server with explicitly defined credentials. Activity Records are exported to a local event log.	`C:\Add-ons\Netwrix_Auditor_Add-on_for_IBM_QRadar.ps1 -NetwrixAuditorUserName enterprise\NAuser -NetwrixAuditorPassword NetwrixIsCool`
The add-on exports Activity Records from a remote Netwrix Auditor Server using current user credentials and writes data to a local event log.	`C:\Add-ons\Netwrix_Auditor_Add-on_for_IBM_QRadar.ps1-NetwrixAuditorHost 172.28.6.15`
The add-on exports Activity Records from a remote Netwrix Auditor Server using explicitly defined credentials and writes data to a local event log.	`C:\Add-ons\Netwrix_Auditor_Add-on_for_IBM_QRadar.ps1-NetwrixAuditorHost 172.28.6.15 -NetwrixAuditorUserName enterprise\NAuser -NetwrixAuditorPassword NetwrixIsCool`

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.

6. Run the Add-On with PowerShell

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_Add-on_for_IBM_QRadar.ps1 -
NetwrixAuditorHost 172.28.6.15
```

   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.

6.0.1. 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.

6.1. Automate Add-On Execution

To ensure you feed the most recent data to your SIEM solution, Netwrix recommends scheduling a daily task for running the 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 Auditor Add-on for IBM QRadar. 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 *"Start a program"*.
Program/script	Input *"Powershell.exe"*.
Add arguments (optional)	Add a path to the add-on in double quotes and specify add-on parameters. For example: `-file "C:\Add-ons\Netwrix_Auditor_Add-on_for_IBM_QRadar.ps1" -NetwrixAuditorHost 172.28.6.15`

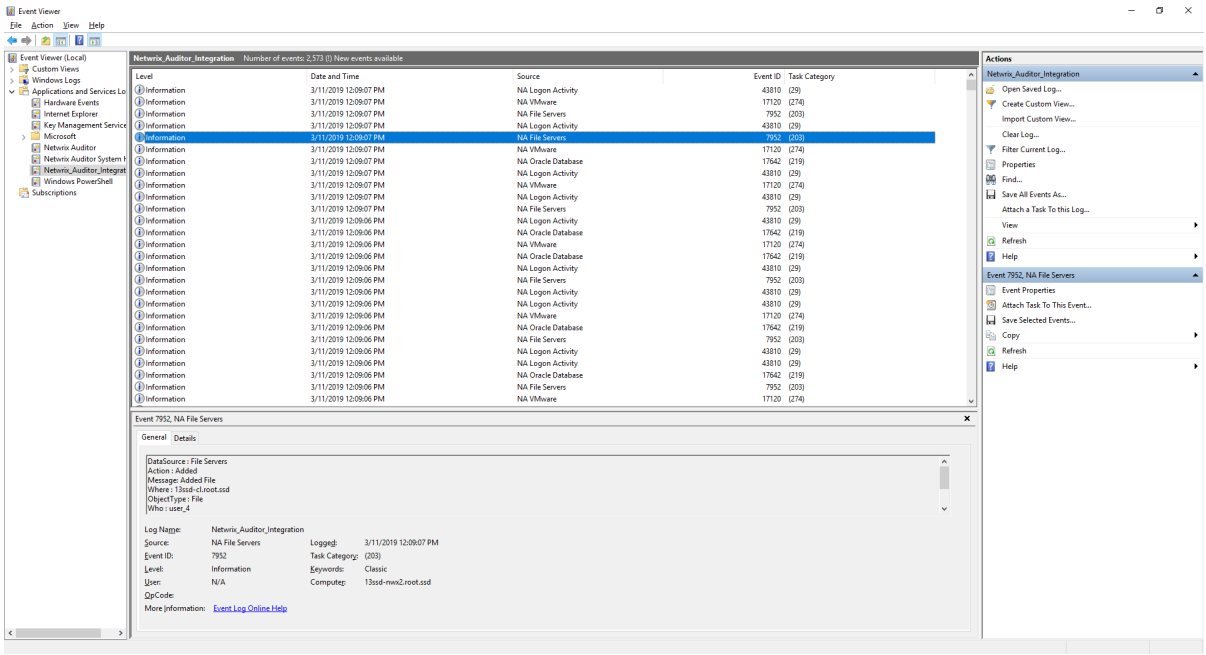
6. Save the task.

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 → Netwrix_Auditor_Integration** log.
3. Review events.

Now you can augment IBM QRadar with data collected by Netwrix 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 *{Data Source Name}*** -OR- **Netwrix _Auditor_Integration_API**	Depending on *SetDataSourceAsEventSource* in-script parameter. See Configure Add-On Parameters
EventID	***{Calculated by add-on}*** -OR- **0**	Depending on *GenerateEventId* in-script parameter (calculation result also depends on *IncludeDataSourceToMakeEventId* parameter — if *GenerateEventId* = *True*). See Configure Add-On Parameters
Task Category	***{DataSource ID}*** -OR- **1**	Depending on *SetDataSourceAsEventCategory* in-script parameter. See Configure Add-On Parameters

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.