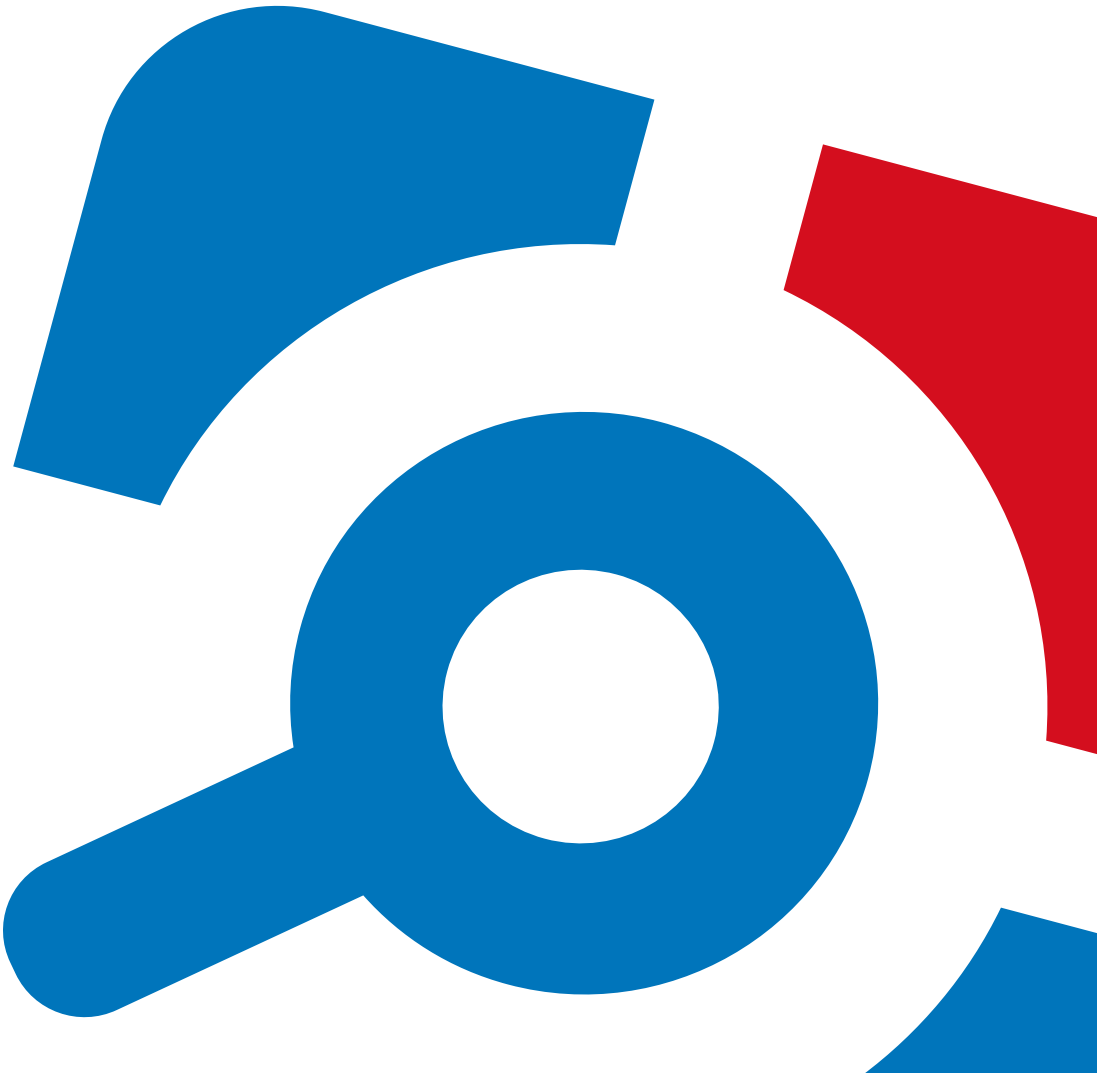
netwrix

Netwrix Auditor
CEF Export Add-on
Quick-Start Guide

Version: 9.6
5/8/2018



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. Introduction

This guide is intended for the first-time users of Netwrix Auditor Integration API 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:

- Define add-on parameters
- Execute the add-on
- Review results

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:

- Netwrix Auditor Installation and Configuration Guide
- Netwrix Auditor Administration Guide
- Netwrix Auditor Integration API Overview

1.1. Netwrix Auditor Overview

Netwrix Auditor is a visibility platform for user behavior analysis and risk mitigation that enables control over changes, configurations and access in hybrid IT environments to protect data regardless of its location. The platform provides security analytics to detect anomalies in user behavior and investigate threat patterns before a data breach occurs.

Netwrix Auditor includes applications for Active Directory, Azure AD, Exchange, Office 365, Windows file servers, EMC storage devices, NetApp filer appliances, SharePoint, Oracle Database, SQL Server, VMware, and Windows Server. Empowered with a RESTful API and user activity video recording, the platform delivers visibility and control across all of your on-premises or cloud-based IT systems in a unified way.

Major benefits:

- Detect insider threats—on premises and in the cloud
- Pass compliance audits with less effort and expense
- Increase productivity of IT security and operations teams

2. Netwrix Auditor CEF Export Add-on Overview

Netwrix Auditor CEF Export Add-on allows exporting audit data into Common Event Format (CEF)-formatted log. CEF is a unified standard for log management introduced by HP ArcSight. This standard is designed to simplify integration between SIEM solutions and third-party auditing software.

The Netwrix Auditor CEF Export Add-on works in collaboration with Netwrix Auditor, supplying additional data that augments the data collected by your 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.

Implemented as a PowerShell script, this add-on facilitates the audit data transition from Netwrix Auditor to SIEM solutions that use CEF as input data. 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 CEF-formatted log that works as input for SIEM solutions such as HPE ArcSight. Each event contains the user account, action, time, and other details.
3. The add-on saves CEF file in a designated folder, from where it can be acquired by your SIEM solution.

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 Overview.

2.1. Compatibility Notice

In Netwrix Auditor 9.0, Netwrix has updated API schemas. The scripts and add-ons designed for Netwrix Auditor 8.0 – 8.5 might become inoperable in Netwrix Auditor 9.6, while new add-ons designed for 9.0 and 9.6 cannot run at Netwrix Auditor 8.0 – 8.5.

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.

3. Use the Add-On

3.1. Prerequisites

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

On...	Ensure that...
The Netwrix Auditor Server side	• 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	• 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 have the **write** permission on the folder where the CEF file will be stored.

3.2. Define Parameters for Add-On

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 for more information.

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.

Parameter	Default value	Description
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.
OutputFolder	—	Provide a path to the folder to store CEF log files. NOTE: This is a mandatory parameter.

3.3. Choose Appropriate Execution Scenario

Netwrix Auditor CEF Export Add-on 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 Netwrix Auditor CEF Export Add-on Overview 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 folder.	`C:\Add-ons\Netwrix_Auditor_CEF_Export_Add-on.ps1 -OutputFolder C:\CEF_Export`
The add-on runs on the Netwrix Auditor Server with explicitly defined credentials. Activity Records are exported to a local folder.	`C:\Add-ons\Netwrix_Auditor_CEF_Export_Add-on.ps1 -OutputFolder C:\CEF_Export -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 folder.	`C:\Add-ons\Netwrix_Auditor_CEF_Export_Add-on.ps1 -OutputFolder C:\CEF_Export -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 folder.	`C:\Add-ons\Netwrix_Auditor_CEF_Export_Add-on.ps1 -OutputFolder C:\CEF_Export -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 destination folder and use it for running the script.

3.4. Run the Add-On with PowerShell

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_CEF_Export_Add-on.ps1 -OutputFolder
C:\CEF_Export -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 AuditorAudit Database execution may take a while. Ensure the script execution completed successfully. The CEF log file will be created in the destination folder. Note that details (or 'msg' in CEF terms) exceeding 16000 symbols are trimmed.

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.

3.5. Automate Add-On Execution

To ensure you feed the most recent data to your SIEM solution that uses CEF as input data, 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 CEF Export Add-on. 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 CEF file. 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_CEF_Export_Add-on.ps1" -OutputFolder C:\CEF_Export -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**.

3.6. See Results

1. Navigate to the destination folder and open a CEF log file.
2. Review audit data exported from the Netwrix Auditor Audit Database. For example, review this CEF-formatted string:

```
CEF:0|Netwrix|Active Directory|1.0|Added|Added
user|0|shost=enterprisedc.enterprise.local cat=user
suser=enterprise\\administrator
filePath=\\local\\enterprise\\users\\newuser start=Mar 28 2017 14:01:48
```

Now you can feed your SIEM solutions with data collected by Netwrix Auditor.

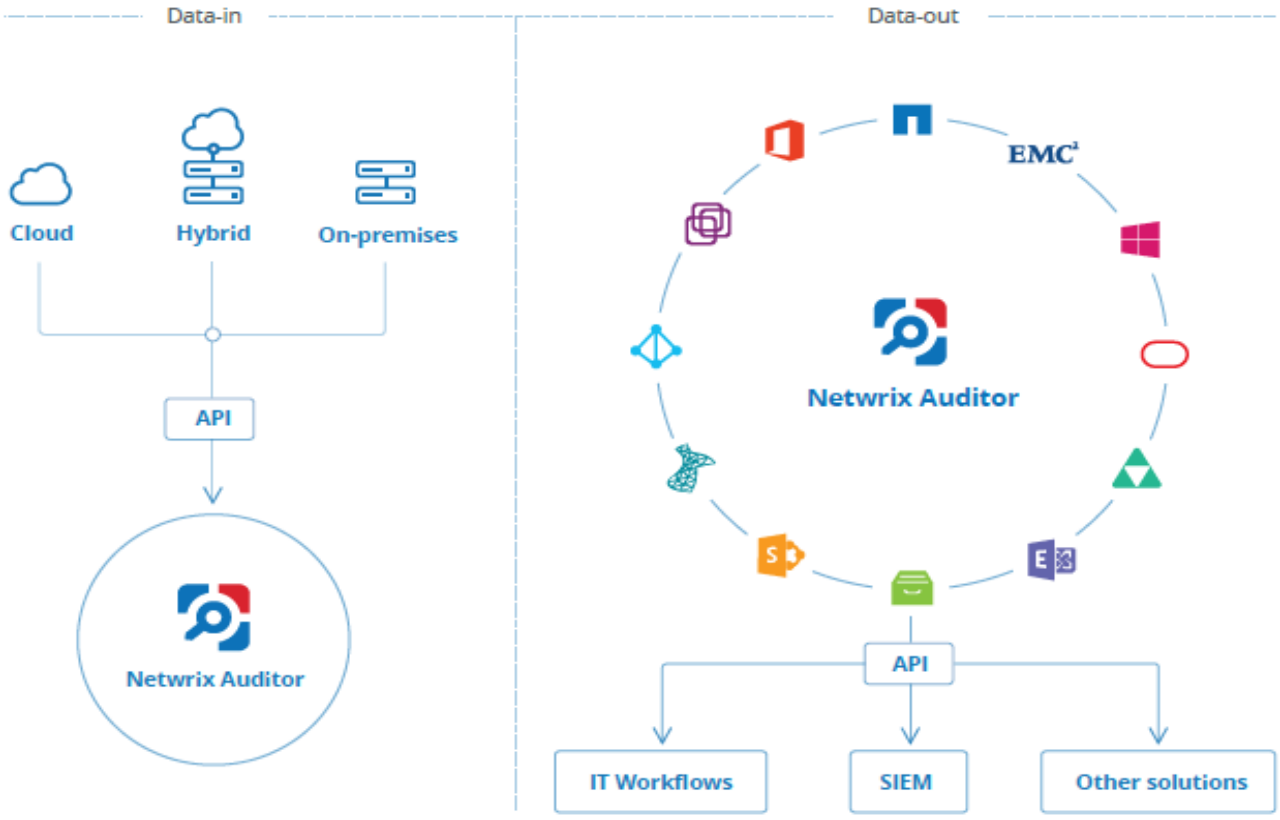
4. Netwrix Auditor Integration API Overview

Netwrix Auditor CEF Export Add-on leverages Netwrix Auditor Integration API. Although you can always use the add-on as is, but Netwrix encourages customers to create their own integration add-ons. The add-ons created based on Netwrix Auditor Integration API capabilities are easily tailored to your specific environment and business requirements.

Netwrix Auditor Integration API—endless integration, auditing and reporting capabilities.

The Netwrix Auditor Integration API provides access to audit data collected by Netwrix Auditor through REST API endpoints. According to the RESTful model, each operation is associated with a URL. Integration API provides the following capabilities:

- **Data in**: Solidify security and meet regulatory compliance standards by enabling visibility into what is going on in any third-party application.
- **Data out**: Further automate your business processes, IT security and operations workflows by enriching third-party solutions with actionable audit data.



Netwrix Auditor Integration API operates with XML- and JSON-formatted Activity Records—minimal chunks of audit data containing information on *who* changed *what*, *when* and *where* this change was made. XML format is set as default.

With Integration API you can write Activity Records to the SQL Server-based Audit Database and access audit data from remote computers. Also, Netwrix prepares add-ons—sample scripts—to help you integrate your SIEM solutions with Netwrix Auditor.

Netwrix does not limit you with applications that can be used with Integration API. You can write RESTful requests using any tool or application you prefer—cURL, Telerik Fiddler, various Google Chrome or Mozilla FireFox plug-ins, etc.

See Netwrix Auditor Integration API Guide for more information.