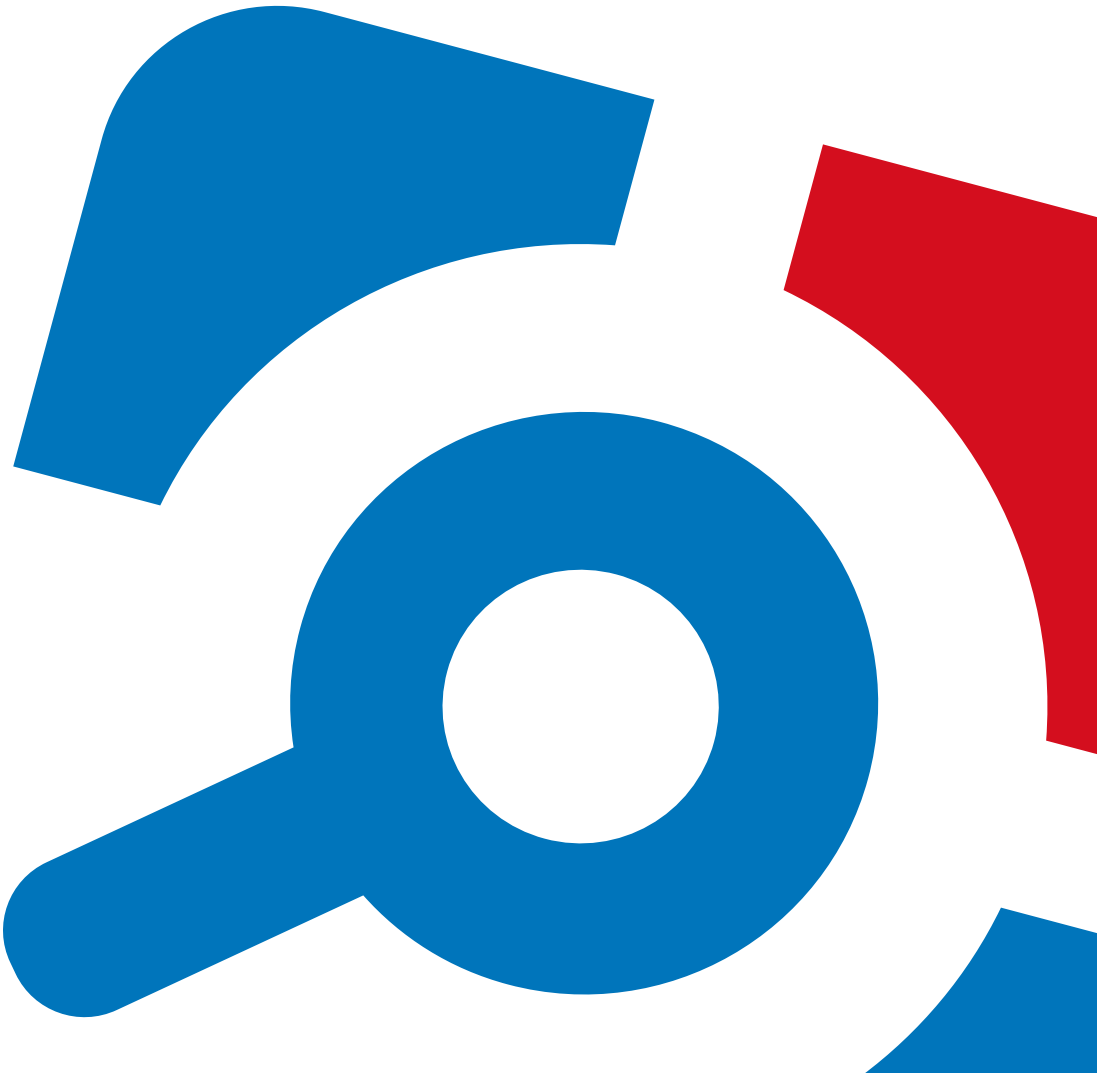
netwrix

Netwrix Auditor

HP ArcSight Add-on Quick-Start Guide

Version: 8.0
6/3/2016



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 4
1.1. Netwrix Auditor Overview 4
1.2. How It Works 6
2. Netwrix Auditor Integration API Overview 9
3. HP ArcSight Add-on 10
3.1. Prerequisites 10
3.2. Security 10
3.3. Run the Script 10
3.4. See Results 12

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:

- Run the integration script
- Review results

NOTE: This guide only covers the basic procedure for running add-ons and assumes that Netwrix Auditor has been already deployed in your network and collects audit data. For installation scenarios, data collection options, as well as for detailed information on Integration API, refer to:

- Netwrix Auditor Installation and Configuration Guide
- Netwrix Auditor Administrator's Guide
- Netwrix Auditor Integration API Guide

1.1. Netwrix Auditor Overview

Netwrix Auditor is an IT auditing platform that delivers complete visibility into changes and data access in hybrid cloud IT environments by providing actionable audit data about *who* changed *what*, *when* and *where* each change was made, and *who* has access to *what*. Netwrix Auditor helps organizations prevent security breaches caused by insider attacks, pass compliance audits with far less effort and expense, and keep tabs on what privileged users are doing in the environment.

Netwrix Auditor enables auditing of the broadest variety of IT systems, including Active Directory, Exchange, file servers, SharePoint, SQL Server, VMware and Windows Server. It also supports monitoring of privileged user activity in all other systems, even if they do not produce any logs, by enabling video recording of user screen activity and later search and replay. More than 160,000 IT departments worldwide rely on Netwrix Auditor to secure IT infrastructure, prove compliance and increase operational efficiency. The product has earned over 70 awards from leading industry publications, including SC Magazine, Windows IT Pro, Redmond Magazine and WindowSecurity.com.

Major benefits:

- **Change auditing and alerting:** Netwrix Auditor detects all configuration, content and security changes across your entire IT infrastructure. Reports and real-time alerts include the critical who, what, when and where details, including before and after values, enabling quick and effective response.

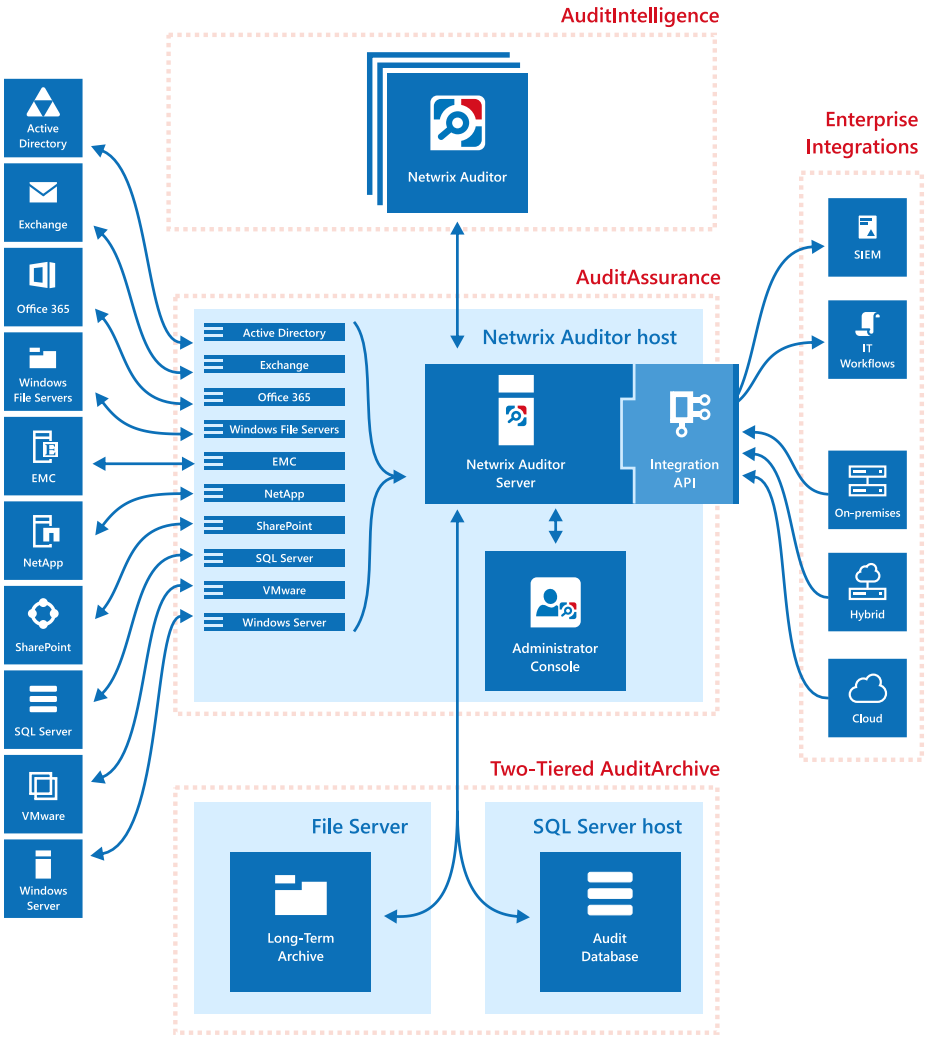
- **AuditIntelligence interactive search:** Netwrix Auditor enables you to easily search through audit data and fine-tune sorting and filtering criteria so you can quickly hone in on exactly the information you need.
- **Configuration assessment:** State-in-time™ reports show configuration settings at any point in time, such as group membership or password policy settings as they were configured a year ago.
- **Access auditing:** Monitoring of and reporting on successful and failed access to systems and data helps keep sensitive data safe.
- **Predefined reports and diagrams:** Netwrix Auditor includes more than 150 predefined reports and diagrams. Reports can be exported to a range of formats, including PDF and XLS, and stakeholders can subscribe to reports to stay informed automatically by email.
- **AuditArchive™:** Netwrix Auditor's scalable two-tiered storage system (file-based + SQL database) holds consolidated audit data for more than 10 years.
- **Unified platform:** Many vendors require multiple standalone tools that are hard to integrate, but Netwrix Auditor is a unified platform that can audit the entire IT infrastructure.

Application	Features
Netwrix Auditor for Active Directory	Netwrix Auditor for Active Directory detects and reports on all changes made to the managed Active Directory domain, including AD objects, Group Policy configuration, directory partitions, and more. It makes daily snapshots of the managed domain structure that can be used to assess its state at present or at any moment in the past. The product provides logon activity summary, reports on interactive and non-interactive logons including failed logon attempts. Also, Netwrix Auditor for Active Directory helps detect and manage inactive users and expiring passwords. In addition, Netwrix Auditor for Active Directory provides a built–in Active Directory Object Restore tool that allows reverting unwanted changes to AD objects down to their attribute level.
Netwrix Auditor for Exchange	Netwrix Auditor for Exchange detects and reports on all changes made to Microsoft Exchange configuration and permissions. In addition, it tracks mailbox access events in the managed Exchange organization, and notifies the users whose mailboxes have been accessed by non–owners.
Netwrix Auditor for Office 365	Netwrix Auditor for Office 365 detects and reports on all changes made to Microsoft Exchange Online configuration and permissions. In addition, it tracks mailbox access events in the managed Exchange Online organization, and notifies the users whose mailboxes have been accessed by non–owners.

Application	Features
Netwrix Auditor for Windows File Servers	Netwrix Auditor for Windows File Servers detects and reports on all changes made to Windows–based file servers, including modifications of files, folders, shares and permissions, as well as failed and successful access attempts.
Netwrix Auditor for EMC	Netwrix Auditor for EMC detects and reports on all changes made to EMC Celerra, VNX/VNXe and Isilon storages, including modifications of files, folders, shares and permissions, as well as failed and successful access attempts.
Netwrix Auditor for NetApp	Netwrix Auditor for NetApp detects and reports on all changes made to NetApp Filer appliances both in cluster- and 7-modes, including modifications of files, folders, shares and permissions, as well as failed and successful access attempts.
Netwrix Auditor for SharePoint	Netwrix Auditor for SharePoint detects and reports on read access and changes made to SharePoint farms, servers and sites, including modifications of content, security settings and permissions.
Netwrix Auditor for SQL Server	Netwrix Auditor for SQL Server detects and reports on all changes to SQL Server configuration and database content.
Netwrix Auditor for VMware	Netwrix Auditor for VMware detects and reports on all changes made to ESX servers, folders, clusters, resource pools, virtual machines and their virtual hardware configuration.
Netwrix Auditor for Windows Server	Netwrix Auditor for Windows Server detects and reports on all changes made to Windows–based server configuration, including hardware devices, drivers, software, services, applications, networking settings, registry settings, DNS, and more. It also provides automatic consolidation and archiving of event logs data. Netwrix Auditor collects Windows event logs and syslog events from multiple computers across the network, stores them centrally in a compressed format, and enables convenient analysis of event log data. In addition, Netwrix Auditor for Windows Server can be configured to capture a video of users' activity on the audited computers.

1.2. How It Works

The image below provides overview of Netwrix Auditor architecture and gives a brief description of product components and incorporated technologies.



The **AuditIntelligence** technology is a brand new way of dealing with audit data, investigating incidents and enabling complete visibility across the entire IT infrastructure. **AuditIntelligence** is brought by the **Netwrix Auditor** client that provides easy access to audit data for IT managers, business analysts and other relevant employees via a straightforward and user-friendly interface. The **Netwrix Auditor** client allows generating reports, searching and browsing your audit data. You can install as many **Netwrix Auditor** clients as needed on workstations in your network, so that your authorized team members can benefit from using audit data collected by a single **Netwrix Auditor Server** to investigate issues and keep track of changes.

AuditAssurance is a technology that consolidates audit data from multiple independent sources (event logs, configuration snapshots, change history records, etc.). This allows detecting *who* changed *what*, *where* and *when* each change was made, and *who* has access to *what* even if one or several sources of information do not contain all of the required data, for example because it was deleted, overwritten, and so on.

AuditAssurance is provided by **Netwrix Auditor Server** and **Integration API**. **Netwrix Auditor Server** is a core part of **Netwrix Auditor** that collects, transfers and processes audit data. It contains several internal components responsible for gathering audit data from audited systems. **Netwrix Auditor Server** is managed with **Netwrix Auditor Administrator Console**, an interface for IT administrators designed to

configure IT infrastructure for auditing, define auditing scope, specify data collection, Audit Database and SMTP settings. **Netwrix Auditor Administrator Console** does not provide access to audit data. **Integration API** is a RESTful API that leverages audit data with custom on-premises or cloud data sources even if they are not supported as audited systems yet. API enables integration with third-party SIEM solutions by importing and exporting data to and from Netwrix Auditor.

Netwrix Auditor Server and **Integration API** interact with the **Two-Tiered AuditArchive** that is a scalable repository used for storing audit data collected by Netwrix Auditor and imported from other data sources and IT systems using **Integration API**. The **Two-Tiered AuditArchive** includes:

- The file-based **Long-Term Archive**
- The SQL-based short-term **Audit Database**

2. Netwrix Auditor Integration API Overview

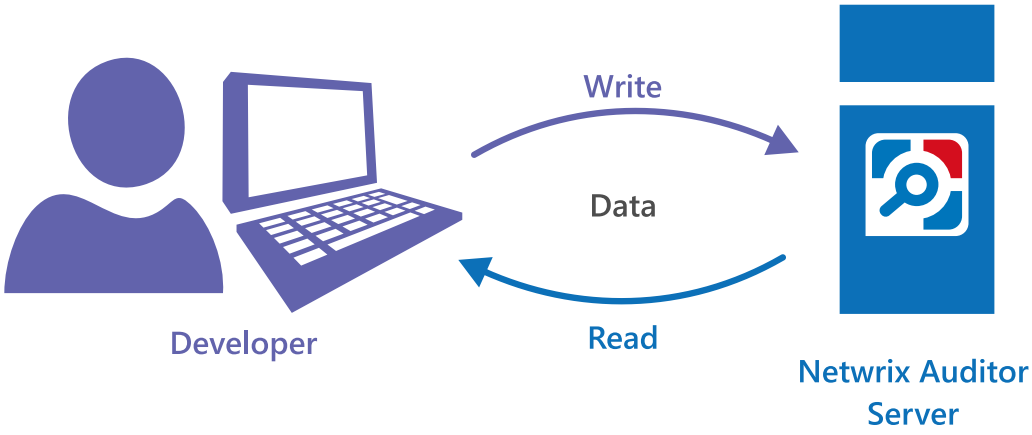
Netwrix Auditor Integration API—endless integration, auditing and reporting capabilities.

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**: Centralize auditing and reporting by feeding Netwrix Auditor with audit data from any existing on-premises or cloud applications. All of your audit data will be centrally stored and ready for reporting.
- **Data out**: Get the most from your SIEM investment by feeding more granular audit data into your HP Arcsight, Splunk, IBM QRadar or other solution, thus increasing the signal-to-noise ratio. Moreover, you can also feed the granular audit data from Netwrix Auditor into critical IT processes, such as change management or ticketing, to further automate and streamline operations.

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 located on Netwrix Auditor Server and access audit data from remote computers. Also, Netwrix prepares 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.

3. HP ArcSight Add-on

This powershell script exports Activity Records from the Audit Database to HP ArcSight in its native CEF format. Use this script to integrate Netwrix Auditor and ArcSight and extend auditing possibilities.

Download the script at: Netwrix Auditor Add-on Store.

3.1. Prerequisites

Before running this script, ensure:

- On Netwrix Auditor side:
  - The Audit Database is configured and contains audit data.
  - Execution policy for powershell scripts is set to *"Unrestricted"*. Run **Windows PowerShell** as administrator and execute the following command:

    ```
    Set-ExecutionPolicy Unrestricted
    ```
- On HP ArcSight side:
  - The TCP-receiver is configured.

3.2. Security

Netwrix Auditor Integration API uses HTTPS with an automatically generated certificate for running requests to its endpoints. By default, add-ons are configured to accept all certificates that is appropriate for evaluation purposes and allows running the script without adjusting.

Nonetheless, Netwrix recommends changing the accept-all-certificates behavior by commenting out a corresponding string in the script (starts with `$WebRequest.ServerCertificate`). With enabled certificate validation, the first option is to continue using a Netwrix-generated certificate. The **Netwrix Integration API** certificate is created automatically along with Netwrix Auditor installation and is located in the **Personal** store. In this case, enable trust on the computer where you are going to run the script. The other option is to assign a new certificate acquired from any reliable source.

See Netwrix Auditor Integration API Guide for detailed instructions on how to assign a new certificate and enable trust on remote computers.

3.3. Run the Script

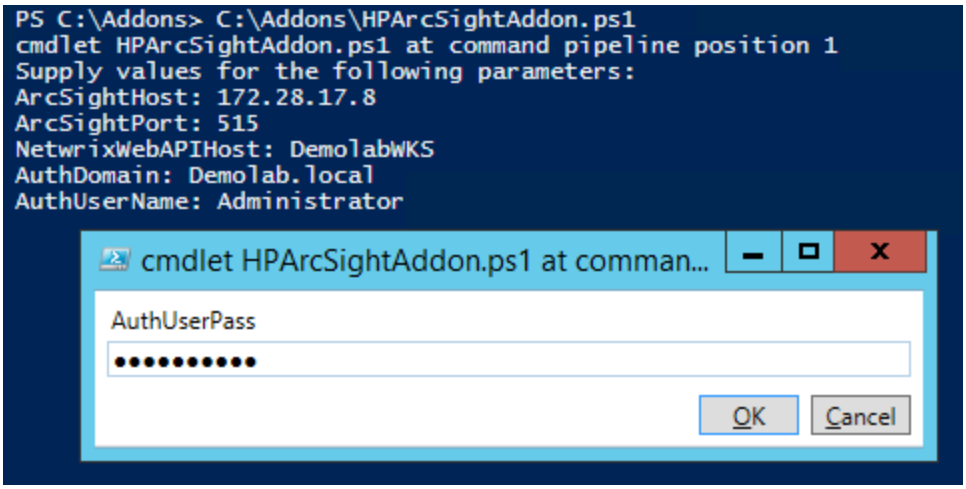
1. Right-click a script and select **Edit**. **Windows PowerShell ISE** will start.
2. Review the script.

- Update port number if you do not use a default 9699 port (`$NetwrixWebAPIPort='9699'`).
- Comment out the string `$WebRequest.ServerCertificateValidationCallback = { HttpsValidationCallback }` by appending the **#** sign if you want to disable accepting all certificates and enable certificate validation.

NOTE: Save the script after updating.

3. Click (**Run Script**).
4. During the script execution, you will be prompted to provide the following details:

Input parameter	Description
ArcSightHost	Provide a name of the computer where HP ArcSight resides (e.g., 172.28.6.15, ArcSightSRV, ArcSightSRV.enterprise.local).
ArcSightPort	Provide a port configured for communication on HP ArcSight server.
NetwrixWebAPIHost	Provide a name of the computer where Netwrix Auditor Server resides (e.g., 172.28.6.15, EnterpriseWKS, WKS.enterprise.local). **NOTE:** Given certificate validation is enabled, provide the computer name as it appears in certificate properties.
AuthDomain	Provide a domain name.
AuthUserName	Specify an account to retrieve data. **NOTE:** The account must be a member of the **Netwrix Auditor Client Users** group on the computer that hosts Netwrix Auditor Server.
AuthUserPass	Provide a password.



5. Wait for the script to execute. Depending on the Audit Database size it may take a while. Ensure the script execution completed successfully.

3.4. See Results

1. Log on to your HP ArcSight Logger web interface.
2. On the **Summary** page, select the **Event Summary by Receiver** diagram and click the **TCP Receiver** segment (Activity Records are imported through TCP Receiver).
3. On the **Analyze** page that opens, review the search field. Ensure your computer is listed as TCP Receiver (e.g., "172.28.10.136 [TCP Receiver]"). If you imported Activity Records from more than one computer, add all of them in the search field.

   NOTE: You might want to modify time range and the fields shown.

4. Review imported Activity Records.

	Time (Event Time)	Device	Logger	deviceVendor	deviceProduct	deviceVersion	deviceEventClassId	name
1	2016/04/06 12:26:14 EDT	172.28.10.136 [TCP Receiver]	Local	Netwrix	Active Directory	1.0	Added	Added group
2	2016/04/06 12:26:14 EDT	172.28.10.136 [TCP Receiver]	Local	Netwrix	Active Directory	1.0	Added	Added user