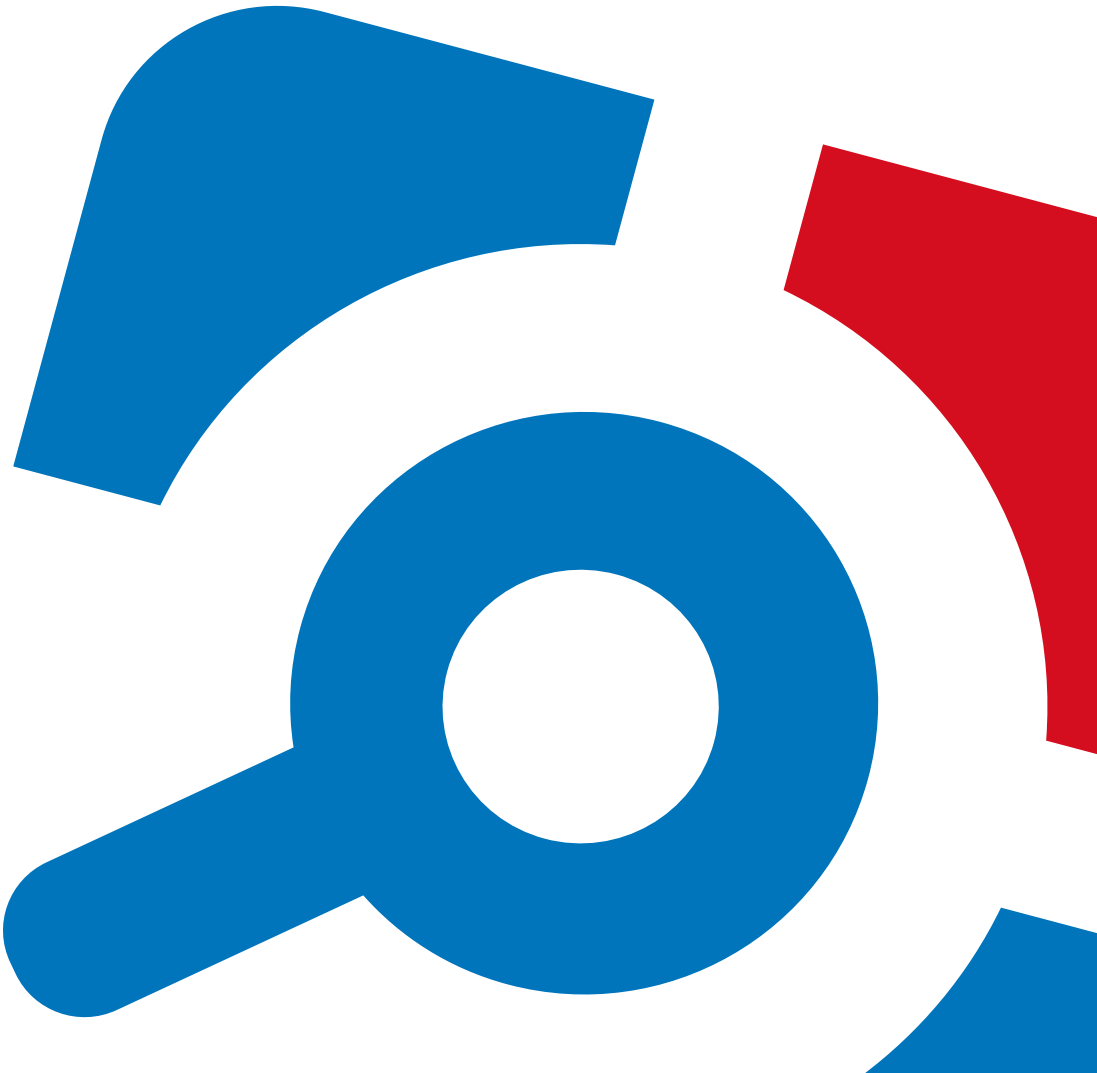
netwrix

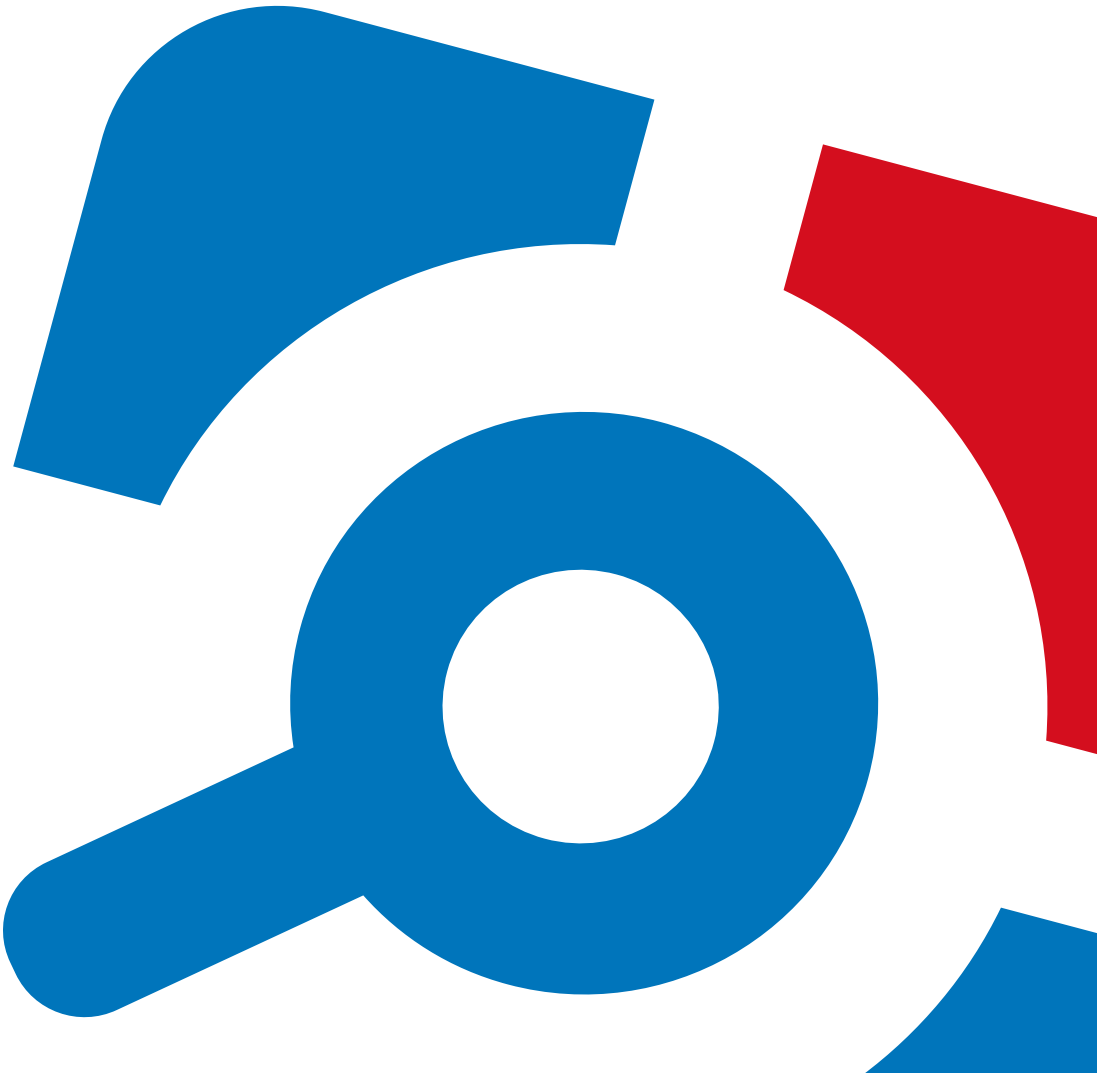
Netwrix Auditor Add-on for CyberArk Privileged Access Security

Quick-Start Guide



netwrix

Version: 9.9
11/14/2019



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 add-on for CyberArk Privileged Access Security (PAS). 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 and configure its parameters
- Execute the add-on
- Review data collection 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 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 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.

CyberArk offers its Privileged Access Security (PAS) solution for managing the privileged accounts and SSH Keys. It enables organizations to manage and monitor all activities associated with the privileged identities, for example, Windows server administrator, root on a UNIX server, etc. A featured set of the Privileged Access Security tools includes, in particular:

- Privileged Session Manager - a tool that enables users to securely connect to remote targets with a standard remote desktop client application, providing isolated sessions.
- Enterprise Password Vault – a tool for storage and centralized management of the privileged accounts; it supports automated changes and logging of the activities associated with all types of privileged passwords and SSH Keys. This tool also includes Central Policy Manager service.

Major benefit of the integrated solution implemented with Netwrix Auditor add-on for CyberArk PAS is the increased visibility into actions related to CyberArk tools, in particular:

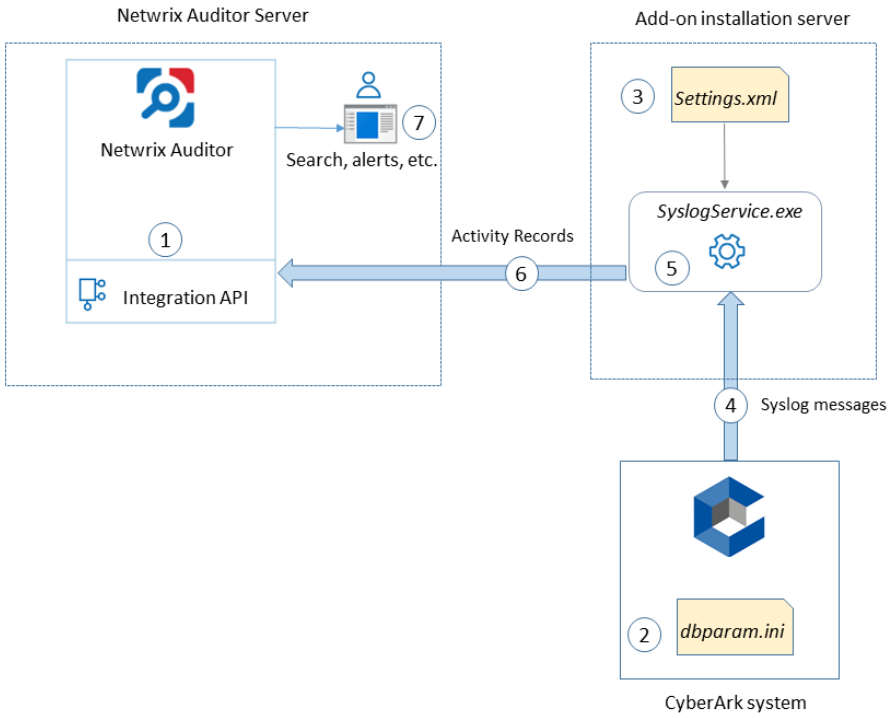
- Visibility into the user account behind the respective isolated session controlled by Privileged Session Manager
- Visibility into the password-related activities, e.g. password retrieval and further actions made to target application or system, and automatic password update for managed accounts in Enterprise Password Vault and Central Policy Manager.

2.1. Compatibility Notice

Netwrix Auditor add-on for CyberArk PAS is compatible with CyberArk Privileged Access Security (PAS) 10.10 and with Netwrix Auditor 9.8 and later.

3. How It Works

The add-on is implemented as a syslog service that collects activity data from CyberArk system (PAS) and sends it to Netwrix Auditor using Netwrix Auditor Integration API.



The add-on operates as a syslog listener for the CyberArk system. On a high level, the solution works as follows:

1. An IT administrator configures Netwrix Auditor Integration API settings to enable data collection and storage to Netwrix database for further reporting, search, etc.

   NOTE: It is recommended to create a dedicated monitoring plan in Netwrix Auditor and add a dedicated item of ***Integration*** type to it — then you will be able to filter data in reports and search results by monitoring plan/item name.

2. On the CyberArk server, the administrator opens the **dbparam.ini** file and specifies the parameters for syslog message forwarding, including add-on installation server settings, the IDs of events to be monitored, etc.

   NOTE: The list of events supported out-of-the box is provided in the Appendix A. Monitored Events.

3. On the add-on installation server, the administrator unpacks the add-on package and runs the **install.cmd** file to deploy and start the main add-on component - syslog service. Then s/he opens the **Settings.xml** configuration file and specifies the necessary parameters for data communication

between the add-on, CyberArk and Netwrix Auditor. After saving configuration settings, the administrator restarts the add-on for changes to take effect.

4. The add-on starts collecting and forwarding activity data: it listens to the specified UDP port and captures designated syslog messages (CyberArk events).
5. The add-on processes these events into Netwrix Auditor-compatible format – activity records. Each activity record contains the *Who-What-When-Where-Action* information (that is, user account, time, action, and other details).
6. Using Netwrix Auditor Integration API, the add-on sends the activity records to Netwrix Auditor Server that writes them to the Audit Database and Long-Term Archive. Data is sent periodically, by default every 5 seconds.

   NOTE: 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.
7. Users open Netwrix Auditor Client to work with collected data:
   - Search for file changes using certain criteria
   - Export data to PDF or CSV files
   - Save search results as reports
   - Subscribe to search results
   - Configure and receive alerts

3.1. Add-on Delivery Package

Netwrix Auditor add-on for CyberArk PAS delivery package is a ZIP archive that includes the following files:

File name	Description
Install.cmd	Command file that installs and enables Netwrix Auditor add-on for CyberArk service (syslog service).
cyberark-v2.xml	Contains rules for processing CyberArk events. Intended mainly for internal use.
Settings.xml	Contains parameters for the add-on service operation.
SyslogService.exe	Main add-on component, implemented as a Syslog service.
SyslogService.exe.config	Add-on configuration data.
Netwrix_Auditor_Add-on_for_CyberArk_PAS_Quick_Start_Guide.pdf	This document.

File name	Description
Release_Notes.pdf	Release Notes file.

4. Before You Start

4.1. Prerequisites

Before you start working with Netwrix Auditor add-on for CyberArk PAS, check the prerequisites listed in the following table:

Where	Prerequisite to check
The Netwrix Auditor Server side	1. Netwrix Integration API and Audit Database settings are configured in Netwrix Auditor Server settings. See Configure Integration API and Audit Database. 2. The **TCP 9699** port must be open on Windows firewall for inbound connections. 3. User account under which data will be written to the Audit Database requires the **Contributor** role in Netwrix Auditor. See Role-Based Access and Delegation. **NOTE:** Alternatively, you can grant it the **Global administrator** role, or add that account to the **Netwrix Auditor Administrators** group. See Netwrix Auditor Administration Guide for more information.
The machine where Netwrix Auditor add-on for CyberArk PAS will be installed (Netwrix Auditor Server is recommended)	1. The **UDP 514** port must be open on Windows firewall for inbound connections. **NOTE:** If you are using Netwrix Auditor for Network Devices, this port may be already in use, and you should provide another one. Another option is to install the add-on and Netwrix Auditor server on different machines. 2. Any of the following .NET Framework versions must be installed: • 4.6 • 4.5 • 4.0 • 3.5 SP1
CyperArk PAS	Version 10.10.

4.2. Accounts and Rights

By default, the add-on will run under the *Local System* account. So, if the add-on and Netwrix Auditor will be running on different machines, the corresponding computer account will require at least the **Contributor** role in Netwrix Auditor. See Role-Based Access and Delegation for more information.

In case the add-on and Netwrix Auditor are installed on the same server, no special settings are needed.

4.3. Considerations and Limitations

- Netwrix add-on must be deployed in the same subnet as CyberArk PAS and Netwrix Auditor.
- If the monitoring plan name in the <*NetwrixAuditorPlan*> add-on configuration parameter is specified incorrectly, this may lead to temp files generation and, therefore, to inefficient disk space usage.
- If you are using Netwrix Auditor for Network Devices, the 514 UDP port may be already in use, and you should specify another port when configuring the add-on settings (see Deployment Procedure and Appendix B. Add-on Parameters for details). Another option is to install the add-on and Netwrix Auditor server on different machines.

5. Deployment Procedure

5.1. Step 1: Prepare Netwrix Auditor for Data Processing

In Netwrix Auditor client, go to the **Integrations** section and verify Integration API settings:

a. Make sure the **Leverage Integration API** is switched to **ON**.

b. Check the TCP communication port number – default is **9699**.

NOTE: For more information, see Configure Integration API Settings.

By default, activity records are written to ***Netwrix_Auditor_API*** database which is not associated with a specific monitoring plan.

NOTE: Optionally, you can create a dedicated monitoring plan in Netwrix Auditor. In this case, data will be written to a database linked to this plan. Target it at Netwrix API data source and enable for monitoring. Add a dedicated item of ***Integration*** type to the plan for data to be filtered by item name. For more information, see Netwrix Auditor Administration Guide.

In such scenario, you will need to specify this monitoring plan in the *naplan* and *naplanitem* attributes of the *<AcceptList>* → *<Address>* configuration parameters. See Appendix B. Add-on Parameters for details.

5.2. Step 2: Configure Syslog Message Forwarding in CyberArk

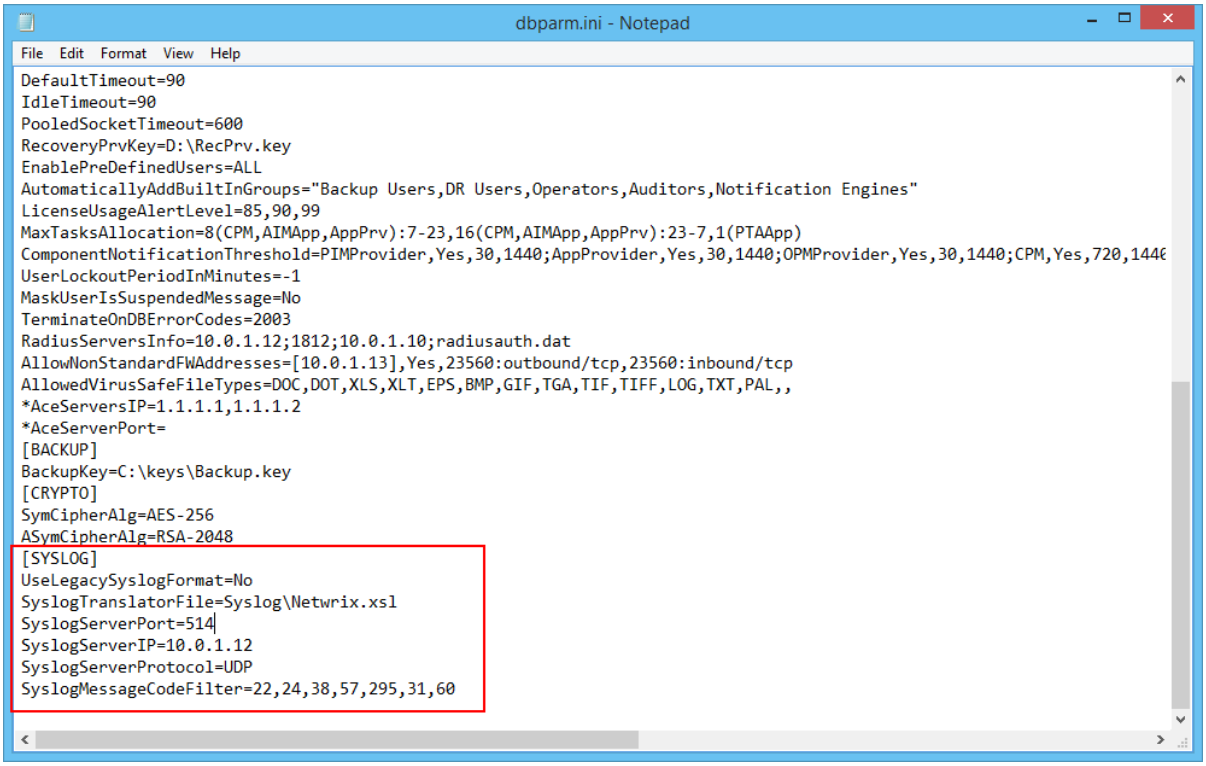
On the CyberArk side, you need to specify the server that will receive Syslog messages from CyberArk, process them and forward to Netwrix Auditor server. This will be the add-on installation server (the machine where *SyslogService.exe* runs).

Do the following:

1. Log in to your CyberArk system.
2. On the CyberArk server, locate the *%Program Files (x86)%\PrivateArk\Server\Conf* folder and open the **dbparam.ini** file for editing.
3. Go to the **[SYSLOG]** section and configure the following parameters:
   - **SyslogTranslatorFile** – relative path to **Netwrix.xsl** file. You will need to create this file manually and copy the content of **SyslogTranslator.sample.xsl** file into it. This sample file is provided by CyberArk. By default, it is located in the *%Program Files (x86)*

%\PrivateArk\Server\Syslog folder.
Place the *Netwrix.xsl* file there, too, so that default relative path should be *\Server\Syslog*.

- **SyslogServerPort** – communication port of the syslog server (i.e. add-on installation server). Default is **514**. Note that if you are using Netwrix Auditor for Network Devices, this port may be already in use, and you should provide another one.
- **SyslogServerIP** - IP address of the add-on installation server.
- **SyslogServerProtocol** – communication protocol for data transfer between CyberArk system and the add-on. Specify **UDP** protocol.
- **SyslogMessageCodeFilter** - IDs of events to forward. The add-on will only collect and process events you specify in this parameter. For the full list of supported events, see Appendix A. Monitored Events. Use comma as a separator.



4. Save the **dbparam.ini** file.

5.3. Step 3: Download the Add-On

1. Download the distribution package **Netwrix_Auditor_Add-on_for_CyberArk_PAS.zip**.
2. Unpack it to a folder on the computer where you plan to deploy the add-on.

NOTE: It is recommended to deploy the add-on on Netwrix Auditor server.

5.4. Step 4: Install the Add-on

Run the **Install.cmd** file from the add-on folder.

This command installs the add-on and configures a Windows firewall inbound connection rule to allow connections via default UDP port **514**.

NOTE: If you plan to change this port, then remember to do it in the following files:

- **Install.cmd** (otherwise, you will have to open the necessary port on Windows firewall manually)
- **Settings.xml** — modify *<ListenUdpPort>* if neecessary

5.5. Step 5: Configure Add-on Parameters

1. Open the add-on folder and edit the **Settings.xml** file to configure the following add-on parameters:

    a. *<Address>* - defines the IP addresses of possible syslog events sources. The add-on will only collect and process events from these sources. Enter the IP address of your CyberArk server.

    b. *<ListenUdpPort>* – listening port for the incoming syslog messages (events). Default UDP port is **514**.

    c. *<NetwrixAuditorEndpoint>* – Netwrix Auditor server name (or IP address) and port number followed by endpoint. For example:

    ```
    https://localhost:9699/netwrix/api/v1/activity_records
    ```

    here:

    - `localhost` - stands for local Netwrix Auditor server
    - `9699` - port for communication between the add-on and Netwrix Auditor via Netwrix Integration API
    - `netwrix/api/v1/activity_records` - Netwrix Integration API endpoint

2. Save the **Settings.xml** file.
3. Restarts the add-on service (*SyslogService.exe*) for changes to take effect.

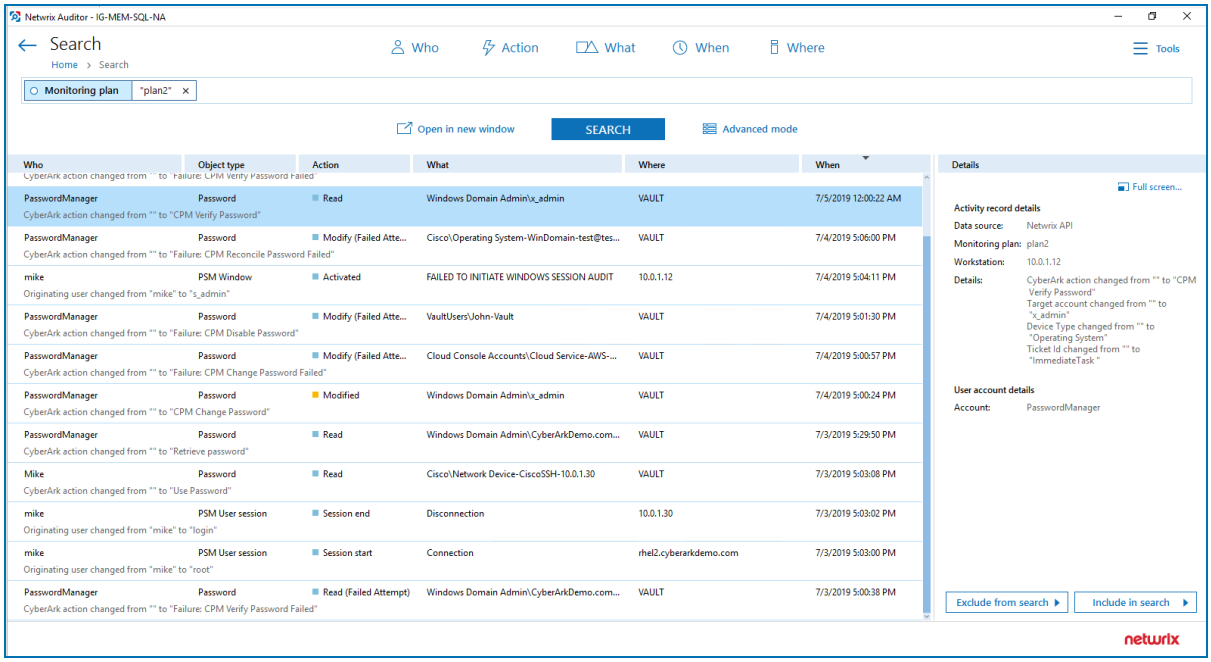
If you later need to modify parameters in the **Settings.xml** file, remember to save the changes and then restart the add-on service (*SyslogService.exe*).

6. Working with Collected Data

To leverage data collected with the add-on, you can do the following in Netwrix Auditor:

- Search for required data. For that, start Netwrix Auditor client and navigate to **Search**. After specifying the criteria you need, click **Search**. You will get a list of activity records with detailed information on who did what in the reported time period.

NOTE: You can apply a filter to narrow down your search results to the **Netwrix API** data source only.



- Also, you can click **Tools** in the upper-right corner and select the command you need. For example:
  - If you want to periodically receive the report on the results of search with the specified criteria, click **Subscribe**. Then specify how you want the report to be delivered – as an email or as a file stored to the file share.
  - To create an alert on the specific occurrences, click **Create alert**.
  - To export filtered data to PDF or CSV, click **Export data**.
- You can also configure and receive alerts on the events you are interested in.

See for more information, see Netwrix Auditor User Guide and Online Help Center.

7. Maintenance and Troubleshooting

Netwrix Auditor add-on for CyberArk PAS operations are logged into the **SyslogService.txt** file. This file is located in the same folder as **SyslogService.exe.**

To change the add-on logging level, use the **LogLevel** parameter in the **Settings.xml** file.

- It is recommended that before the first run you set this parameter to `debug`. This will facilitate operations tracking and possible problem solving.
- After that it is strongly recommended to re-set this parameter to `error` to prevent the uncontrolled log growth.

If you cannot see collected data in Netwrix Auditor, check the following:

1. In Netwrix Auditor settings, go to the **Integrations** section and make sure the **Leverage Integration API** is switched to **ON**. Check the communication port number – default is **9699**.
2. If you configured a dedicated monitoring plan, make sure data source monitoring is enabled.
3. Verify the parameters you provided in **Settings.xml** and **dbparam.ini**.

8. Appendix A. Monitored Events

Netwrix Auditor add-on for CyberArk PAS supports monitoring of the following syslog events from CyberArk PAS:

Event ID	Description
22	Password verification by Central Policy Manager (success)
24	Password stored in EPV changed by Central Policy Manager (success)
31	Password reconciliation by Central Policy Manager (success)
38	Password verification by Central Policy Manager (failure)
57	Password stored in Enterprise Password Vault changed by Central Policy Manager (failure)
60	Password reconciliation by Central Policy Manager (failure)
130	Password stored in Enterprise Password Vault disabled by Central Policy Manager
295	User retrieved a password stored in Enterprise Password Vault
300	User session started in Privileged Session Manager
302	User session ended in Privileged Session Manager
308	User used a password stored in Enterprise Password Vault
411	A window was activated by user in Privileged Session Manager

9. Appendix B. Add-on Parameters

To configure the add-on parameters, you need to edit the **Settings.xml** file in the add-on folder. You must define connection details: Netwrix Auditor Server host, endpoint, etc.

Most parameters are optional; you can skip or define parameters depending on your execution scenario and security policies.

The service uses the default values unless parameters are explicitly defined (*<parameter>***value***</parameter>*).

Parameters in **Settings.xml** can be grouped as follows:

- **General parameters** that affect add- on execution. They are listed in the table below.
- Settings for a certain event source (within the *Source* section) that can override general settings.
- **Internal parameters** that should not be modified in most cases. They are listed in the Appendix C. Add-on Internal Parameters.

Parameter	Default value	Description
	General parameters	
ListenUdpPort	514	Specify UDP port for listening to the incoming syslog events.
NetwrixAuditorEndpoint	https://localhost:9699/netwrix/api/v1/activity_records	Netwrix Auditor Server IP address and port number followed by endpoint for posting Activity Records. 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).

Parameter	Default value	Description
		NOTE: Do not modify the endpoint part (/netwrix/api ....)
NetwrixAuditor CertificateThumbprint	NOCHECK	Netwrix Auditor Certificate Thumbprint Property. Possible values: • `Empty`—Check Netwrix Auditor certificate via Windows Certificate Store. • `AB:BB:CC.`—Check Netwrix Auditor Server certificate thumbprint identifier. • `NOCHECK`—Do not check Netwrix Auditor certificate. Make sure to select this parameter if you plan to specify servers by their IP.
NetwrixAuditorPlan	—	Unless specified, data is written to **Netwrix_ Auditor_ API** database and is not associated with a specific monitoring plan. Specify a name of associated monitoring plan in Netwrix Auditor. In this case, data will be written to a database linked to this plan. **NOTE:** If you select a plan name in the add-on, make sure a dedicated plan is created in Netwrix Auditor, the **Netwrix API** data source is added to the plan and enabled for monitoring. Otherwise, the add-on will not be able to write data to the Audit Database.
NetwrixAuditorPlanItem	—	Unless specified, data is not associated with a specific

Parameter	Default value	Description
		monitoring plan and thus cannot be filtered by item name. Specify an item name here. **NOTE:** Make sure to create a dedicated item in Netwrix Auditor in advance.
EventStorePath	—	Select where to store temporary files of syslog messages before the add-on sends them to Netwrix Auditor Server. **NOTE:** Netwrix recommends to store these files in the same directory with the add-on (SyslogService.exe).
LogLevel	warning	Specify logging level: • none • info • warning (used by default) • error • debug
WriteCriticalIssues ToEventLog	0	Instructs the add-on to write important events (like service start or critical issue) not only to its own log but also to Netwrix event log. • 1=yes • 0=no (default)
Parameters within SourceList		
You can specify parsing rules for each specific event source and define parameters to override general settings, such as time zone, default plan name, etc.		
NetwrixAuditorPlan	—	When specified, overrides the general settings.
NetwrixAuditorPlanItem	—	When specified, overrides the

Parameter	Default value	Description
		general settings.
AppNameRegExp	—	Custom regular expression pattern that will be used to retrieve the application name from your syslog messages. The add-on will match the application name and the files with syslog parsing rules to be applied. **NOTE:** The pattern you provide here must match the application name in your custom rule file. Unless specified, RFC 3164/5424 format is used.
AppNameGroupID	—	Define application name value by Group ID only if messages are not formatted in accordance with RFC 3164/5424. Otherwise, leave the default value.
RuleFileList PathFile	cyberark-v2.xml	Specify paths to XML file(s) with regular expression parsing rules. You can create a custom file or use rules provided out of the box. Currently, the **cyberark- v2.xml** rule file is shipped with this add-on. You can specify several rule files. The service will check if the AppName parameter in the first rule file matches the AppNameRegExp and AppNameGroupID regular expression in this file. If not, the service will proceed to the next rule file.
AcceptList Address	—	Specify a list of IP addresses of syslog events sources. The service will collect and process events

Parameter	Default value	Description
		from these sources only. **NOTE:** Events collected from any other source will be ignored. The *Address* parameter may be followed by optional attributes that override parameters specified above: • *naplan*—A name of associated monitoring plan • *naplanitem*—A name of associated item For example: `<Address naplan="NFSmonitoring" naplanitem="NFS">172.28.3.15 </Address>`

NOTE: Remember to save **Settings.xml** after editing is complete.

After you modify parameters in the **Settings.xml** file, remember to save the changes and then restart the add-on main service (*SyslogService.exe*) for them to take effect.

10. Appendix C. Add-on Internal Parameters

Internal parameters listed in the table below are intended for performance tuning. In most cases the default values should be used.

Parameter	Default value	Description
EventsFromMemoryFirst	1	Instructs the add-on to save events to temporary storage only if there is no free space in queues: • 1=yes • 0=no
ConcurrentSend	-1	Specifies the number of threads for concurrent forwarding of events to Netwrix Auditor. Default value is -1 (switch off concurrent forwarding).
SenderSleepTime	30	Specifies the retry interval in seconds to send messages to Netwrix Auditor (30 - 3600 seconds).
TaskLimit	8	Specifies the number of threads and queues for concurrent handling of events.
QueueSizeLimit	100	Specifies the maximum number of events to keep in queue before saving to temporary storage or sending to Netwrix API.
QueueTimeLimit	5	Specifies the length of timeout before events from queue (not full) are saved to temporary storage or sent to Netwrix API: • From 5 to 300 – timeout in seconds. • -1 – disable timeout.