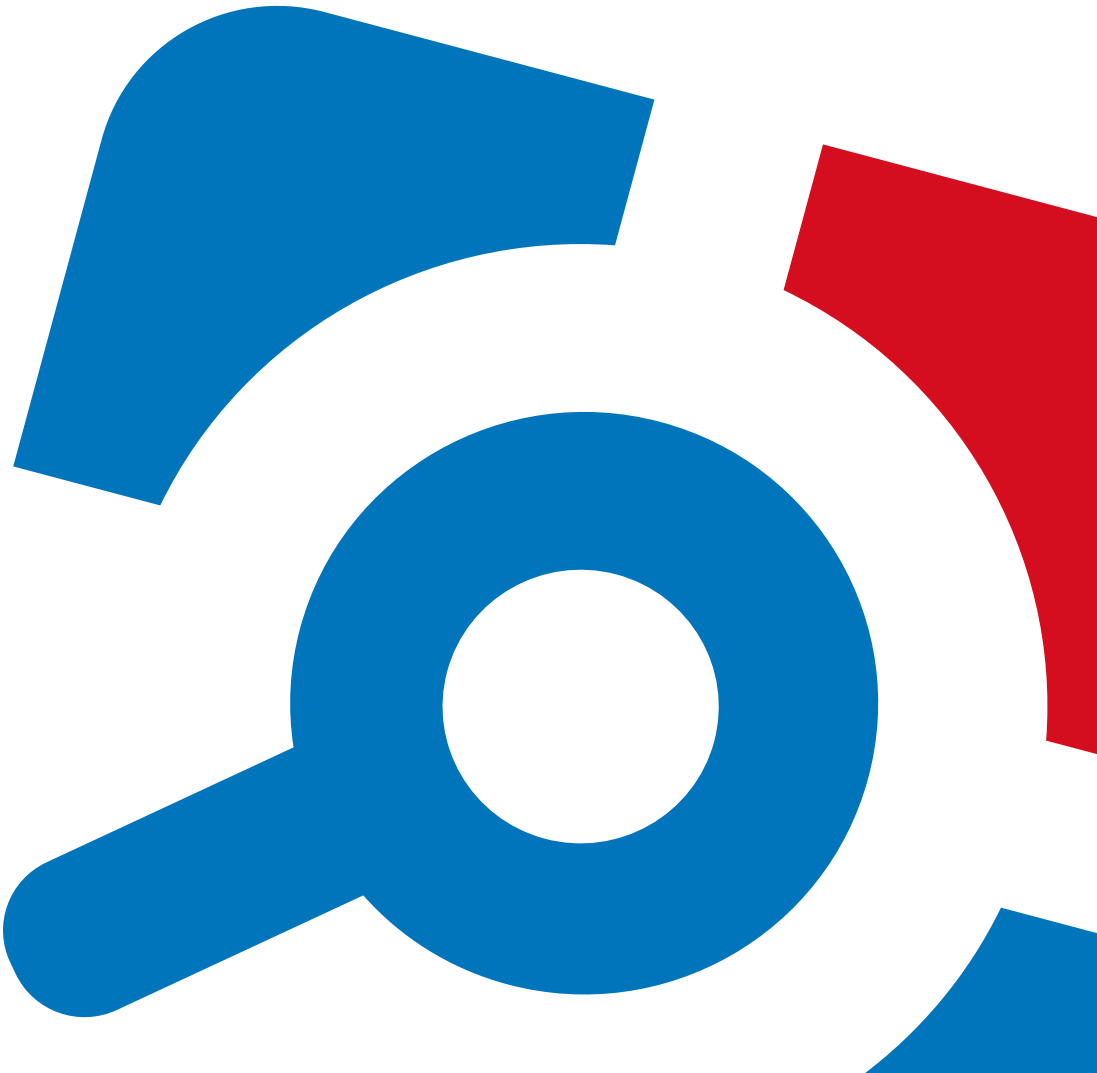
netwrix

Netwrix Auditor for Network Devices

Quick-Start Guide

Version: 9.9
1/21/2020



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.

Table of Contents

1. Introduction

This guide is intended for the first-time users of Netwrix Auditor for Network Devices. 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 and configure Netwrix Auditor
- Create a monitoring plan to start auditing
- Launch data collection
- See how Netwrix Auditor enables complete visibility

NOTE: This guide only covers the basic configuration and usage options for auditing with Netwrix Auditor. For advanced installation scenarios and configuration options, as well as for information on various reporting possibilities and other product features, refer to Netwrix Online Help Center.

1.1. Netwrix Auditor Features and Benefits

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, Active Directory Federation Services, Azure AD, Exchange, Office 365, Windows file servers, EMC storage devices, NetApp filer appliances, Nutanix Files, network devices, SharePoint, Oracle Database, SQL Server, VMware, Windows Server, and User Activity. Empowered with a RESTful API, 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

To learn how Netwrix Auditor can help your achieve your specific business objectives, refer to Netwrix Auditor Best Practices Guide.

2. Prerequisites and System Requirements

This section lists the requirements for the systems that are going to be audited with Netwrix Auditor, and for the computer where the product is going to be installed.

To learn about Netwrix Auditor licenses, refer to the following Netwrix Knowledge Base article: Netwrix Auditor Licensing FAQs. To learn how to install a license, refer to Licenses.

To learn about ports and protocols required for product operation, refer to Protocols and Ports Required for Netwrix Auditor.

To learn about security roles and permissions required for product operation, refer to Configure Netwrix Auditor Service Accounts.

2.1. Supported Data Sources

The table below lists systems that can be monitored with Netwrix Auditor for Network Devices:

Data source	Supported Versions
Network Devices	**Cisco devices** • Cisco ASA (Adaptive Security Appliance) 8 and above • Cisco IOS (Internetwork Operating System) 12 and 15 **Fortinet Fortigate** • FortiOS 5.6 and above **SonicWall** • SonicWall Web Application Firewall 2.0.x.x • SonicWall NSv 6.5.x.x with SonicOS 6.5.x • SonicWall SMA 11.4.x **Juniper Networks** • vSRX with Junos OS 12.1, Junos OS 18.1 • vMX with Junos OS 17.1 **Palo Alto** • Palo Alto with PAN-OS 8.0.0

2.2. Requirements to Install Netwrix Auditor

This section provides the requirements for the computer where Netwrix Auditor is going to be installed. Refer to the following sections for detailed information:

- Hardware Requirements
- Software Requirements

2.2.1. Hardware Requirements

This section provides rough estimations of the resources required for Netwrix Auditor PoC or evaluation deployment. Consider that actual hardware requirements will depend on your monitored infrastructure, the number of users in your environment, and activities that occur in the infrastructure per day.

The metrics provided in this section are valid for clean installation on a server without any additional roles or third part applications installed on it. The use of virtual machine is recommended.

Below you can find rough estimations, calculated for evaluation of Netwrix Auditor for Network Devices. Refer to Netwrix Online Help Center for complete information on the Netwrix Auditor hardware requirements.

You can deploy Netwrix Auditor on a virtual machine running Microsoft Windows guest OS on the corresponding virtualization platform, in particular:

- VMware vSphere
- Microsoft Hyper-V
- Nutanix AHV

Note that Netwrix Auditor supports only Windows OS versions listed in the Software Requirements section.

Hardware component	Starter, evaluation, or small environment
Processor	2 cores
RAM	4 GB
Disk space	100 GB—System drive 100 GB—Data drive (Long-Term Archive and SQL Server)
Screen resolution	Minimum 1280 x 1024 Recommended 1920 x 1080 or higher

2.2.2. Software Requirements

The table below lists the software requirements for the Netwrix Auditor installation:

Component	Requirements
Operating system	Windows Server OS: • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 Windows Desktop OS (64-bit): • Windows 10 • Windows 8.1
.NET Framework	• .NET Framework 4.5 and above.
Installer	• Windows Installer 3.1 and above

3. Review Components Checklist

To speed up the evaluation process, Netwrix recommends you to ensure that the following services and components are up and running prior to the Netwrix Auditor installation.

Service or component	Recommendations
SQL Server with Reporting Services (or Advanced Services) 2008 or higher.	Supported SQL Server versions are listed here. Consider maximum database size in different versions. Make your choice based on the size of the environment you are going to monitor, the number of users, and other factors. Remember that maximum database size in Express editions may be insufficient. **NOTE:** Although Netwrix Auditor provides a convenient way to download SQL Server 2014 Express edition right from the product, it is recommended to deploy SQL Server instance in advance. If installed separately, remember to test SQL Server connectivity.

Test account	Netwrix recommends you to create a special account with extensive privileges. This account should have sufficient permissions to:
	• Collect audit data. See Configure Data Collecting Account for more information.
	• Access data stored in the SQL Server instance:
	  • The account must be assigned the **Database owner (db_owner)** role and the **dbcreator** server role.
	  • The account must be assigned the **Content Manager** role on the SSRS Home folder.
	• Make test changes in your environment.

4. Configure Network Devices for Monitoring

To configure your network devices for monitoring perform the following procedures, depending on your device:

- Configure Cisco ASA Devices
- Configure Cisco IOS
- Configure Fortinet FortiGate Devices
- Configure PaloAlto Devices
- Configure Juniper Devices
- Configure SonicWall Devices

4.1. Configure Cisco ASA Devices

To configure your Cisco ASA devices, do the following:

1. Navigate to your Cisco ASA device terminal through the SSH/Telnet connection (for example, use PuTTY Telnet client).
2. Access the **global configuration** mode. For example:

   ```
   hostname# configure terminal
   hostname(config)#
   ```

3. Enable logging. For example:

   ```
   hostname(config)# logging enable
   ```

4. Set the IP address of the computer that hosts Netwrix Auditor Server as the `logging host` parameter. And make sure that the UDP port is used for sending syslog messages (e.g., 514 UDP port). For example:

   ```
   hostname(config)# logging host <Netwrix Auditor server IP address>
   ```

   NOTE: Do not select the **EMBLEM format logging** for the syslog server option.

5. Enable the `logging timestamp` option. For example:

   ```
   hostname(config)# logging timestamp
   ```

6. Set the `logging trap` option from 1 to 6 inclusive. For example:

   ```
   hostname(config)# logging trap 5
   ```

4.2. Configure Cisco IOS

To configure your Cisco IOS devices, do the following:

1. Navigate to your Cisco IOS device terminal through the SSH/Telnet connection (for example, use PuTTY Telnet client).
2. Access the **global configuration** mode. For example:

   ```
   Router# configure terminal
   ```

3. Enable time stamps in syslog messages:

   ```
   Router# service timestamps log datetime localtime show-timezone
   ```

4. Set the `logging trap` option from 1 to 6 inclusive. For example:

   ```
   Router# logging trap 5
   ```

5. Set the IP address of the Netwrix Auditor Server as the `logging host` parameter. And make sure that the UDP port is used for sending syslog messages (e.g., 514 UDP port). For example:

   ```
   Router# 192.168.1.5 514
   ```

4.3. Configure Fortinet FortiGate Devices

To configure your Fortinet FortiGate devices, enable logging to multiple Syslog servers and configure FortiOS to send log messages to remote syslog servers in **CEF** format. Do one of the following:

- To configure Fortinet FortiGate devices via Command Line Interface
- To configure Fortinet FortiGate devices through the Fortigate Management Console

To configure Fortinet FortiGate devices via Command Line Interface

1. Log in to the Command Line Interface (CLI).
2. Enter the following commands:

   ```
   config log syslogd setting
   set format cef
   ```

   NOTE: To enable CEF format in some previous FortiOS versions, enter the `set csv disable` command.

   ```
   set csv disable
   set facility <facility_name>
   set port 514
   set reliable disable
   set server <ip_address_of_Receiver>
   ```

```
set status enable
end
```

To configure Fortinet FortiGate devices through the Fortigate Management Console

1. Open **Fortigate Management Console** and navigate to **Log&Report** → **Log Config** → **Log Setting**.
2. Select the **Syslog** checkbox.
3. Expand the **Options** section and complete the following fields:

Option	Description
Name/IP	Enter the address of your Netwrix Auditor Server.
Port	Set to *"514"*.
Level	Select desired logging level.
Facility	Netwrix recommends using default values.
Data format	Select **CEF**. **NOTE:** To enable CEF format in some previous FortiOS versions, unselect the **Enable CSV** checkbox.

4. Click **Apply**.

4.4. Configure PaloAlto Devices

To configure your PaloAlto devices, create a Syslog server profile and assign it to the log settings for each log type.

To configure a Syslog server profile

1. Connect to your PaloAlto device: launch an Internet browser and enter the IP address of the firewall in the URL field (https://<IP address>).
2. In the **Web Interface**, navigate to **Device** → **Server Profiles** → **Syslog**.
3. Click **Add** and specify profile name, for example, *"SyslogProf1"*.
4. Specify syslog server parameters:

Parameter	Description
Name	Specify unique name for a syslog server.
Syslog Server	Provide a server name by entering its FQDN or IPv4 address.
Transport	Select **UDP**.
Port	Provide the name of the UDP port used to listen to network devices (514 port used by default).
Format	Select **IETF**.
Facility	Netwrix recommends using default values.

To configure syslog forwarding

1. In the **Web Interface**, navigate to **Device** → **Log Settings**.
2. For **System**, **Config** and **User-ID** logs, click **Add** and enter unique name of your syslog server.
3. On the **syslog** panel, click **Add** and select the syslog profile you created above.
4. Click **Commit** and review the logs on the syslog server.

4.5. Configure Juniper Devices

To configure you Juniper devices, do the following:

1. Launch the JunOS Command Line Interface (CLI).
2. Execute the following commands:

   ```
   # configure
   # set system syslog host <host address> any info
   ```

   where `<host address>` is the IP address of the computer where Netwrix Auditor Server is installed.

   ```
   # set system syslog host <host address> port <port name>
   ```

   where

   `<host address>` is the IP address of the computer where Netwrix Auditor Server is installed

   AND

   `<port number>` is the name of the UDP port used to listen to network devices (514 port used by default). See Network Devices for more information.

   ```
   # set system syslog time-format <current year>
   ```

```
# commit
```

4.6. Configure SonicWall Devices

To configure your SonicWall devices, do the following, depending on your device type:

- To configure SonicWall Web Application Firewall
- To configure SonicWall SMA
- To configure SonicWall NSv series

To configure SonicWall Web Application Firewall

1. Connect to your SonicWall device. Launch an Internet browser and enter the following in the URL field: *https://<IP address>:84443*, where **IP address** is the IP of the device and **84443** is the default connection port.
2. Log in to the device.
3. In the **Web Interface**, navigate to **Log → Settings** and configure the following:

Parameter	Description
• Log Level • Alert Level • Syslog Level	Set to "Info".
• Enable Audit Log • Send to Syslog Server in Audit Log Settings • Send to Syslog Server in Access Log Settings	Select these checkboxes.
Primary Syslog Server	Enter the address of your Netwrix Auditor Server.
Primary Syslog Server Port	Provide the name of the UDP port used to listen to network devices (514 port used by default).

4. Click **Accept**.
5. Navigate to **Log → Categories**.
6. Select the following checkboxes:

- **Authentication**
- **Authorization & Access**
- **System**
- **Web Application Firewall**
- **Geo IP & Botnet Filter In Log Categories (Standard)**

7. Click **Accept**.

To configure SonicWall SMA

1. Connect to your SonicWall device. Launch an Internet browser and enter the following in the URL field: *https://<IP address>:8443*, where **IP address** is the IP of the device and **8443** is the default connection port.
2. Log in to the device.
3. In the **Web Interface**, navigate **Log** → **Settings** and configure the following:

Parameter	Description
• Log Level • Alert Level • Syslog Level	Set to "Info".
• Enable Audit Log • Send to Syslog Server in Audit Log Settings • Send to Syslog Server in Access Log Settings	Select these checkboxes.
Primary Syslog Server	Enter the address of your Netwrix Auditor Server.
Primary Syslog Server Port	Provide the name of the UDP port used to listen to network devices (514 port used by default).

4. Click **Accept**.
5. Navigate to **Log** → **Categories**.
6. Select the following checkboxes:
   - **Authentication**
   - **Authorization & Access**
   - **System**

- **Web Application Firewall**
- **Geo IP & Botnet Filter In Log Categories (Standard)**

7. Click **Accept**.

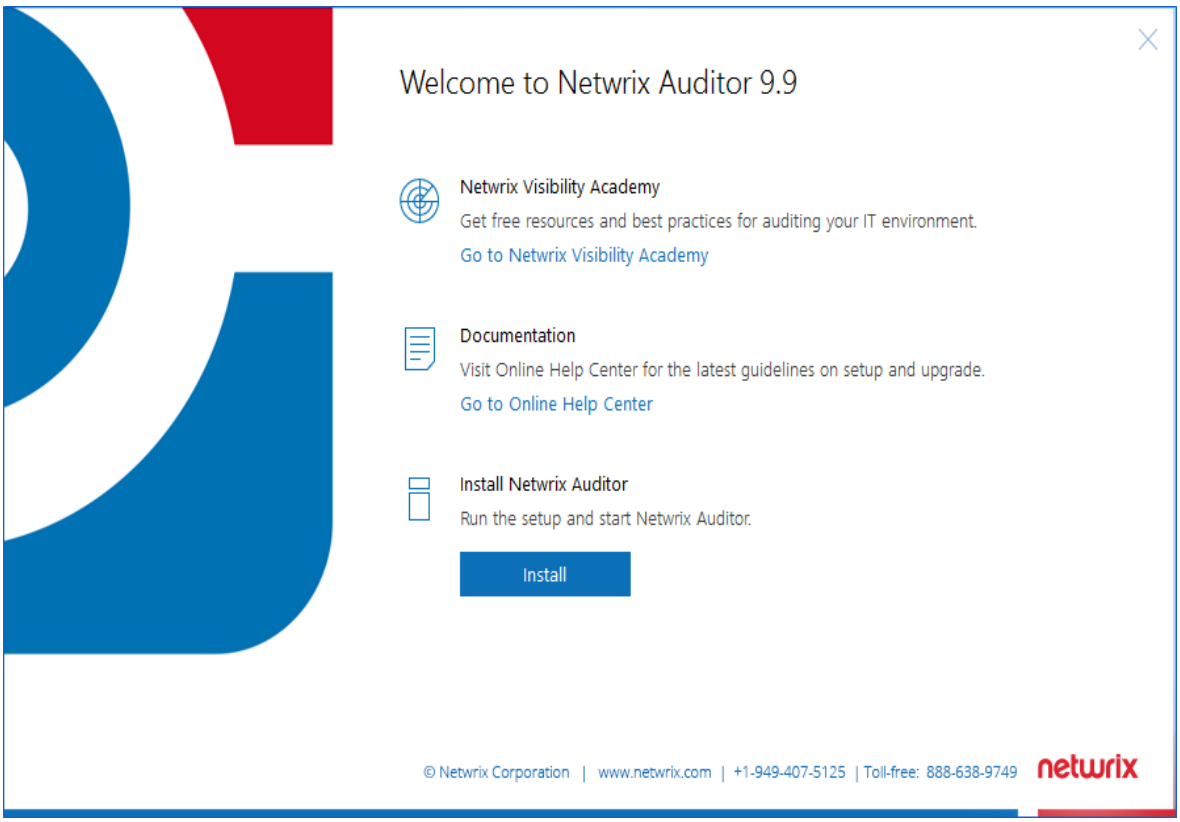
To configure SonicWall NSv series

1. Connect to your SonicWall device. Launch an Internet browser and enter the following in the URL field: *https://<IP address>:443*, where **IP address** is the IP of the device and **443** is the default connection port.
2. Log in to the device.
3. In the **Web Interface**, navigate to **Manage** → **Log Settings** → **Base Setup**.
4. Select all checkboxes in the **Syslog** column.
5. Click **Accept**.
6. Navigate to **Manage** → **Log Settings** → **Syslog**.
7. Set the **Syslog Format** to **Default**.
8. Click **Add**.
9. In the dialog appears, select **Create new address object** option in the **Name or IP Address** combo box.
10. Provide name and IP address of the new object.
11. Click **OK**.
12. In the **Add Syslog Server** dialog, find the IP address you specified on the step 10 in the **Name or IP Address** list.
13. Click **OK**.
14. Click **Save**.

5. Install the Product

To install Netwrix Auditor

1. Download Netwrix Auditor 9.9 from Netwrix website.
2. Unpack the installation package. The following window will be displayed on successful operation completion:

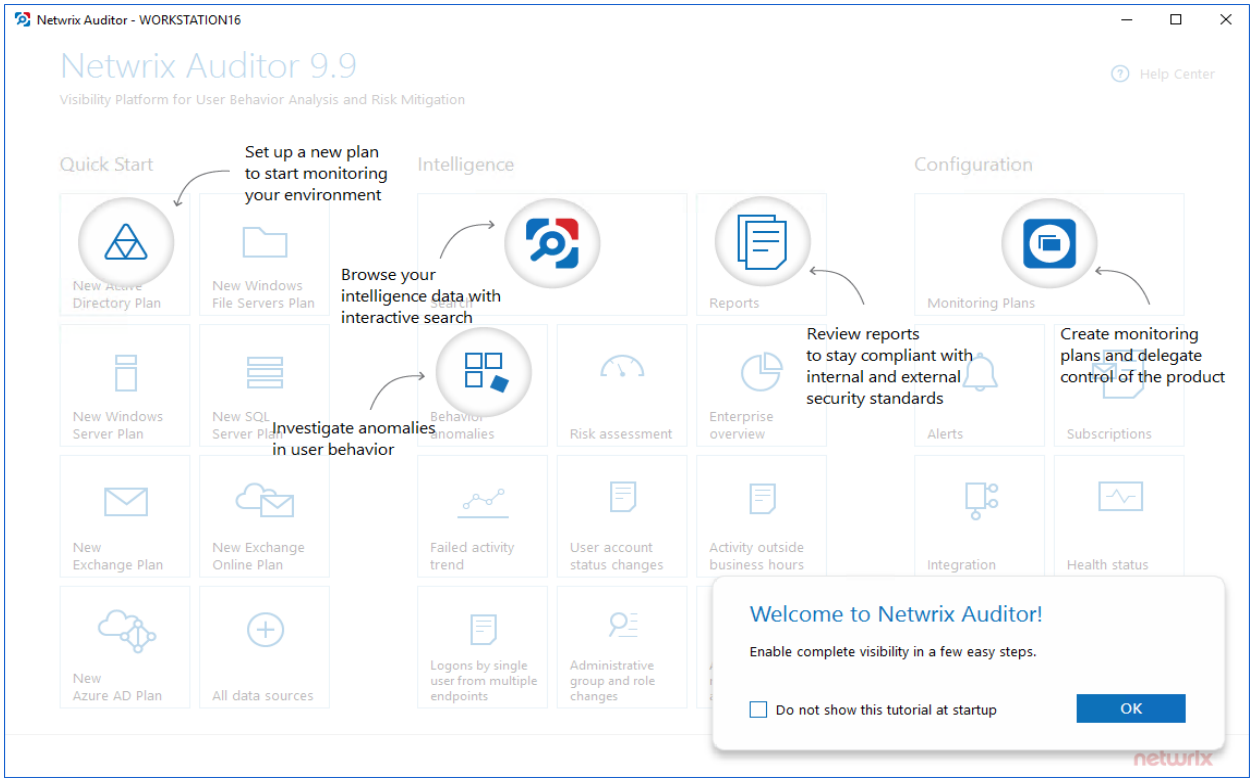


3. Follow the instructions of the setup wizard. When prompted, accept the license agreement.
4. On the **Select Installation Type** step, select **Full installation**.
5. On the **Destination Folder** step, specify the installation folder.
6. On the **Netwrix Customer Experience Program** step, you are invited to take part in the Netwrix Customer Experience Program. It is optional on your part to help Netwrix improve the quality, reliability, and performance of Netwrix products and services. If you accept, Netwrix collects statistical information on how the Licensee uses the product in accordance with applicable law. Select **Skip** if you do not want to participate in the program.

   NOTE: You can always opt-out of the Netwrix Customer Experience Program later.See Netwrix Online Helpcenter for instructions on how to cancel participation in the program.

7. Click **Install**.

After a successful installation, Netwrix Auditor shortcut will be added to the **Start** menu/screen and the product will start.



6. Monitoring Plans

To start auditing your environment and analyzing user behavior with Netwrix Auditor, create a monitoring plan. All your monitoring plans are listed in the **Monitoring Plans** section.

A monitoring plan defines your data sources and general data collection, notification, and storage settings. To start collecting data, choose a data source, such as , and add items to its scope. Item is a specific object you want to audit. All data sources and items in your plan share common settings so that you can supervise and manage several data collections as one.

On a high level, you should perform the following steps to start monitoring your environment:

1. Specify a data source and create a monitoring plan with a wizard. See Create a New Plan for more information.
2. Add items for monitoring. Netwrix Auditor does not collect data until you specify an item. See Add Items for Monitoring for more information.

6.1. Create a New Plan

On the main Netwrix Auditor page, click the **All data sources** and select **Network Devices** tile in the **Quick Start** section.

Then follow the steps of the Monitoring Plan Wizard:

- Specify an account for collecting data
- Specify default SQL Server instance and configure the Audit Database to store your data
- Configure notification settings
- Specify the recipients who will receive daily activity summaries
- Specify a plan name

6.1.1. Settings for Data Collection

At this step of the wizard, specify the account that Netwrix Auditor will use to access the data source, and general settings for data collection.

Option	Description
Specify the account for collecting data	Provide a user name and a password for the account that Netwrix Auditor will use to collect data. By default, the user name is prepopulated with your account name. Make sure the account has sufficient permissions to collect data. For a full list

Option	Description
	of the rights and permissions, and instructions on how to configure them, refer to Configure Data Collecting Account. Netwrix recommends creating a special service account with extended permissions.

6.1.2. Default SQL Server Instance

To provide searching, alerting and reporting capabilities, Netwrix Auditor needs an SQL Server where audit data will be stored in the databases. To store data from the data sources included in the monitoring plan, the wizard creates an Audit Database for each plan. At this step, you should specify the default SQL Server instance that will host Netwrix Auditor databases. To read more, refer to SQL Server and Audit Database.

NOTE: Alternatively, you can instruct Netwrix Auditor not to store data to the databases but only to the repository (Long-Term Archive) – in this scenario, you will only be able to receive activity summaries. Reporting and alerting capabilities will not be provided.

NOTE: Make sure the **Disable security intelligence and make data available only in activity summaries** checkbox is cleared.

Select one of the following options:

- **Install a new instance of Microsoft SQL Server Express automatically** — this option is available at the first run of the wizard. It allows you to deploy SQL Server 2016 SP2 Express with Advanced Services on the local machine. This SQL Server will be used as default host for Netwrix Auditor databases.
- **Use an existing SQL Server instance** — select this option to use an existing SQL Server instance.

  NOTE: Local SQL Server instance is detected automatically, and input fields are pre-populated with its settings.

  Complete the following fields:

Option	Description
SQL Server instance	Specify the name of the SQL Server instance to store audit data.
Authentication	Select the authentication type you want to use to connect to the SQL Server instance: • Windows authentication • SQL Server authentication
User name	Specify the account to be used to connect to the SQL Server instance.

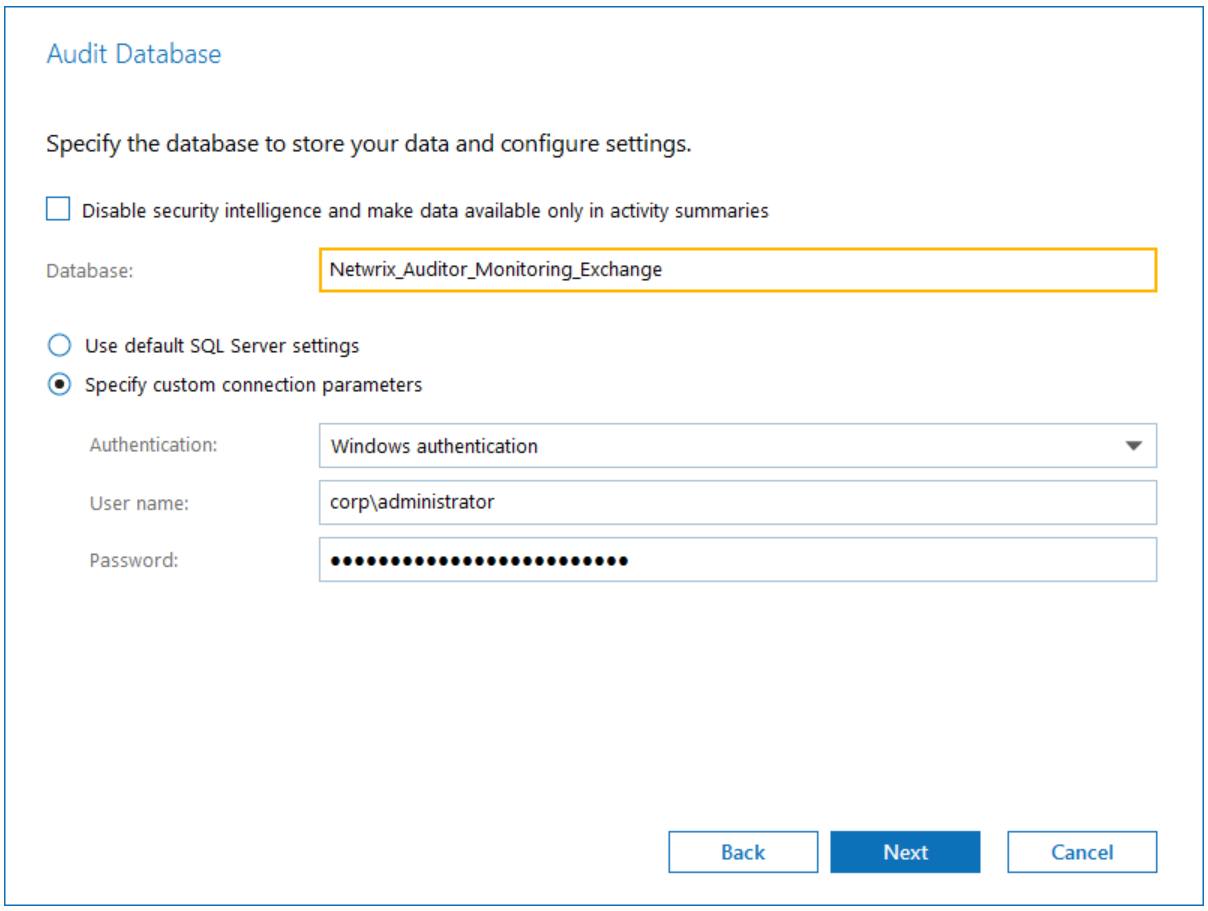
Option	Description
	NOTE: This account must be granted the **database owner (db_owner)** role and the **dbcreator** server role.
Password	Enter a password.

6.1.3. Database Settings

At this step, you need to specify a database where Netwrix Auditor will store data collected from the data sources included in this monitoring plan.

NOTE: It is strongly recommended to target each monitoring plan at a separate database.

Make sure the **Disable security intelligence and make data available only in activity summaries** checkbox is cleared and **Use default SQL Server settings** is checked.



Configure the following:

Setting	Description
Disable security intelligence ...	Only select this option if you do not want your data to be stored in the database. In this case, you will only be able to receive activity summaries. Reporting and alerting capabilities will not be provided. To store data to the database, leave this check box cleared.
Database	Default database name is *Netwrix_Auditor_<monitoring_plan_name>*. It is recommended that you enter a meaningful name for the database here. It may include the data source type (e.g. *Exchange_Audit_Data* or *OracleSrv02_Audit_Data*), or so. If you decided to use the existing SQL Server instance instead of dedicated, you may want to use *Netwrix_Auditor* prefix to distinguish Netwrix Auditor databases from others.
Use default SQL Server settings	Select this option if you want Netwrix Auditor to connect to the SQL Server instance using the default settings you specified Default SQL Server Instance .
Specify custom connection parameters	Select this option to use custom credentials when connecting to SQL Server. Specify authentication method and the account that Netwrix Auditor will use. Make sure this account has sufficient rights to connect to SQL Server and work with the databases. See Configure Audit Database Account for details.

Netwrix Auditor will connect to the default SQL Server instance and create a database with the specified name on it.

NOTE: Global settings that apply to all databases with audit data (including retention period and SSRS server used for reporting) are available on the **Audit Database** page of Netwrix Auditor settings. See Audit Database for details.

6.1.4. SMTP Server Settings

When you create the first monitoring plan, you are prompted to specify the email settings that will be used for activity and health summaries, reports and alerts delivery. For the monitoring plans that follow, Netwrix

Auditor will automatically detect SMTP settings; however, for your first plan you should provide them manually. See this section for details.

6.1.5. Email Notification Recipients

Specify who will receive daily emails: Activity Summary Email on changes in the monitored infrastructure, and Health Summary Email on Netwrix Auditor operations and health.

Click **Add Recipient** and enter your email.

NOTE: It is recommended to click . The system will send a test message to the specified email address and inform you if any problems are detected.

6.1.6. Monitoring Plan Summary

At this step of the wizard, to provide a meaningful name and optional description for your monitoring plan.

To start collecting data, you should specify the objects (items) that belong to the target data source and should be processed according to the settings of this monitoring plan. For example, for Exchange data source the item will be your Exchange server, for Windows Server data source - computer, IP range or AD container, and so on. To add items right after finishing the monitoring plan wizard, select the **Add item now** checkbox. See Add Items for Monitoring for details.

6.2. Add Items for Monitoring

Once you completed monitoring plan wizard and specified data sources, add items for monitoring.

Each data source has a dedicated item type. Netwrix Auditor automatically suggests item types associated with your data source.

6.2.1. Computer

Complete the following fields:

Option	Description
Specify a computer	Provide a server name by entering its FQDN, NETBIOS or IPv4 address. You can click **Browse** to select a computer from the list of computers in your network.
Specify the account for collecting data	Select the account that will be used to collect data for this item.

6.2.2. IP Range

NOTE: For evaluation purposes, Netwrix recommends selecting **Computer** as an item for a monitoring plan. Once the product is configured to collect data from the specified items, audit settings (including Core and Compression services installation) will be applied to all computers within AD Container or IP Range.

Complete the following fields:

Option	Description
Specify IP range	Specify an IP range for the audited computers. To exclude computers from within the specified range, click **Exclude**. Enter the IP subrange you want to exclude, and click **Add**.
Specify the account for collecting data	Select the account that will be used to collect data for this item.

7. Make Test Changes

Now that the product has collected a snapshot of the data source's current configuration state, you can make test changes to see how they will be reported by Netwrix Auditor.

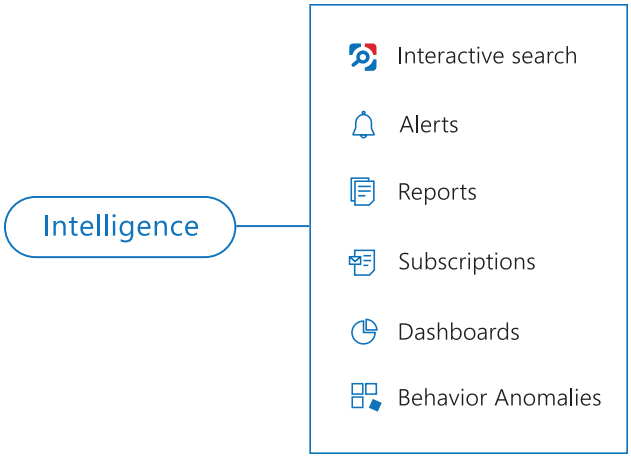
NOTE: Before making any test changes to your environment, ensure that you have the sufficient rights, and that the changes conform to your security policy.

For example, make the following test changes:

- Perform failed logon attempt to a network device
- Modify your network device configuration

8. See How Netwrix Auditor Enables Complete Visibility

After you have made test changes to your environment, you can see how Netwrix Auditor brings security intelligence into your IT infrastructure and enables complete visibility. Take a closer look at the **Intelligence** section. It contains everything you need to enable complete visibility in your environment.



This chapter explains how to review your test changes with some of the Intelligence options and Activity Summary. Review the following for additional information:

- Review an Activity Summary
- Review Network Devices Reports
- Browse Data with Intelligence Search

In order not to wait for a scheduled Activity Summary generation, force data collection and email delivery.

To launch data collection manually

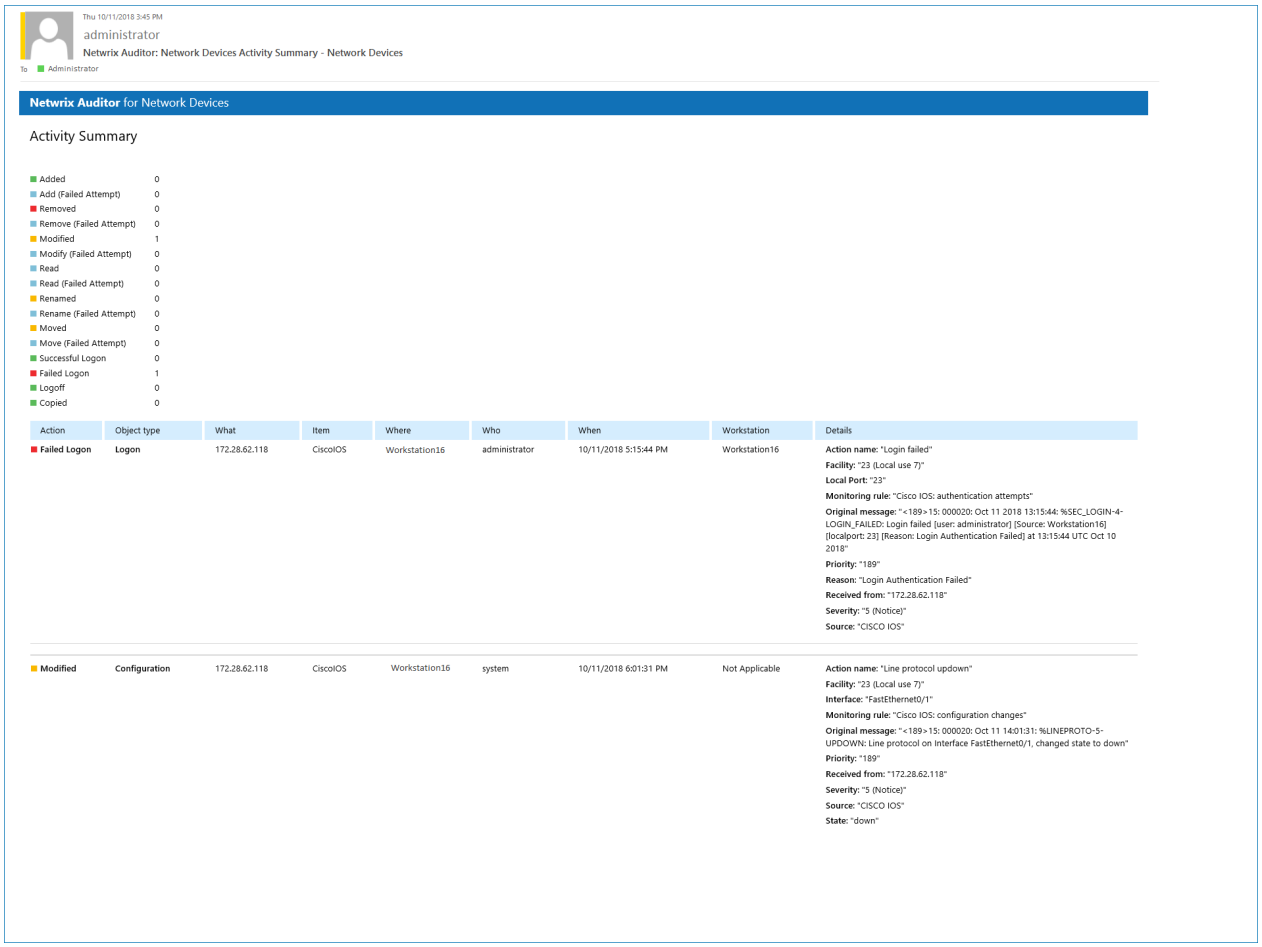
1. Navigate to **Monitoring Plans** and select your plan in the list.
2. Click **Edit**.
3. In the your monitoring plan settings, click **Update** in the right pane.
4. Check your mailbox for an email notification and make sure that the data collection has completed successfully.

8.1. Review an Activity Summary

Activity Summary email is generated automatically by Netwrix Auditor and lists all changes that occurred since the last Activity Summary delivery. By default, an Activity Summary is generated daily at 3:00 AM and

delivered to the specified recipients. You can also launch data collection and Activity Summary generation manually.

After the data collection has completed, check your mailbox for an Activity Summary and see how your test changes are reported



Thu 10/11/2018 3:45 PM
administrator
Netwrix Auditor: Network Devices Activity Summary - Network Devices
To Administrator

Netwrix Auditor for Network Devices

Activity Summary

Added	0
Add (Failed Attempt)	0
Removed	0
Remove (Failed Attempt)	0
Modified	1
Modify (Failed Attempt)	0
Read	0
Read (Failed Attempt)	0
Renamed	0
Rename (Failed Attempt)	0
Moved	0
Move (Failed Attempt)	0
Successful Logon	0
Failed Logon	1
Logoff	0
Copied	0

Action	Object type	What	Item	Where	Who	When	Workstation	Details
Failed Logon	**Logon**	172.28.62.118	CiscoIOS	Workstation16	administrator	10/11/2018 5:15:44 PM	Workstation16	**Action name:** "Login failed" **Facility:** "23 (Local use 7)" **Local Port:** "23" **Monitoring rule:** "Cisco IOS: authentication attempts" **Original message:** "<189>15: 000020: Oct 11 2018 13:15:44: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: administrator] [Source: Workstation16] [localport: 23] [Reason: Login Authentication Failed] at 13:15:44 UTC Oct 10 2018" **Priority:** "189" **Reason:** "Login Authentication Failed" **Received from:** "172.28.62.118" **Severity:** "5 (Notice)" **Source:** "CISCO IOS"
Modified	**Configuration**	172.28.62.118	CiscoIOS	Workstation16	system	10/11/2018 6:01:31 PM	Not Applicable	**Action name:** "Line protocol updown" **Facility:** "23 (Local use 7)" **Interface:** "FastEthernet0/1" **Monitoring rule:** "Cisco IOS: configuration changes" **Original message:** "<189>15: 000020: Oct 11 14:01:31: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down" **Priority:** "189" **Received from:** "172.28.62.118" **Severity:** "5 (Notice)" **Source:** "CISCO IOS" **State:** "down"

The example Activity Summar provide the following information:

Column	Description
Action	Shows the type of action that was performed on the object.
Object Type	Shows the type of the object.
What	Shows the name of the changed object or its path.
Item	Shows the item associated with the selected monitoring plan.
Where	Shows the name of the server where the change occurred.
Who	Shows the name of the account under which the change was made.

Column	Description
When	Shows the exact time when the change occurred.
Workstation	Shows the of the computer where the user was logged on when the change was made.
Details	Shows the before and after values of the modified object, object attributes, etc.

8.2. Review Network Devices Reports

The Netwrix Auditor client provides a variety of predefined reports that aggregate data from the entire audited IT infrastructure or individual data sources.

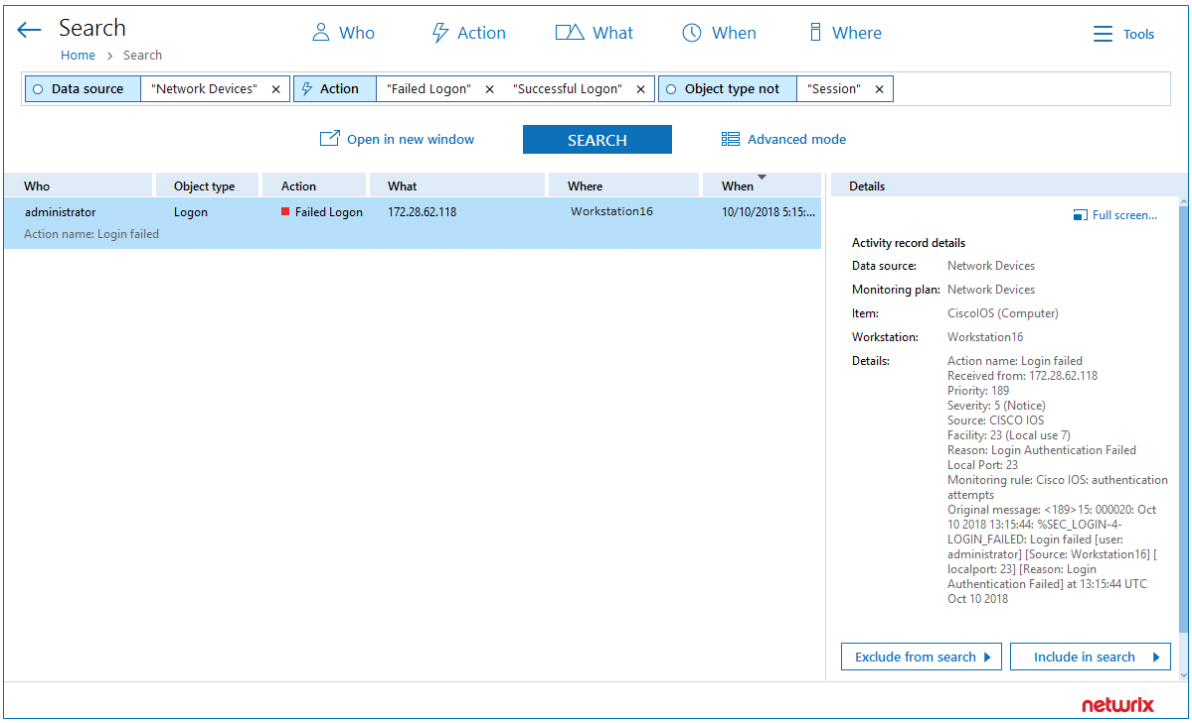
Change and activity reports can be found under the **Reports → Predefined → Network Devices** and provide a narrower insight into what is going on in the audited infrastructure and help you stay compliant with various standards and regulations (FISMA, HIPAA, PCI, SOX, etc.).

After collecting initial data, making test changes to your environment and running data collection again, you can take advantage of the reports functionality.

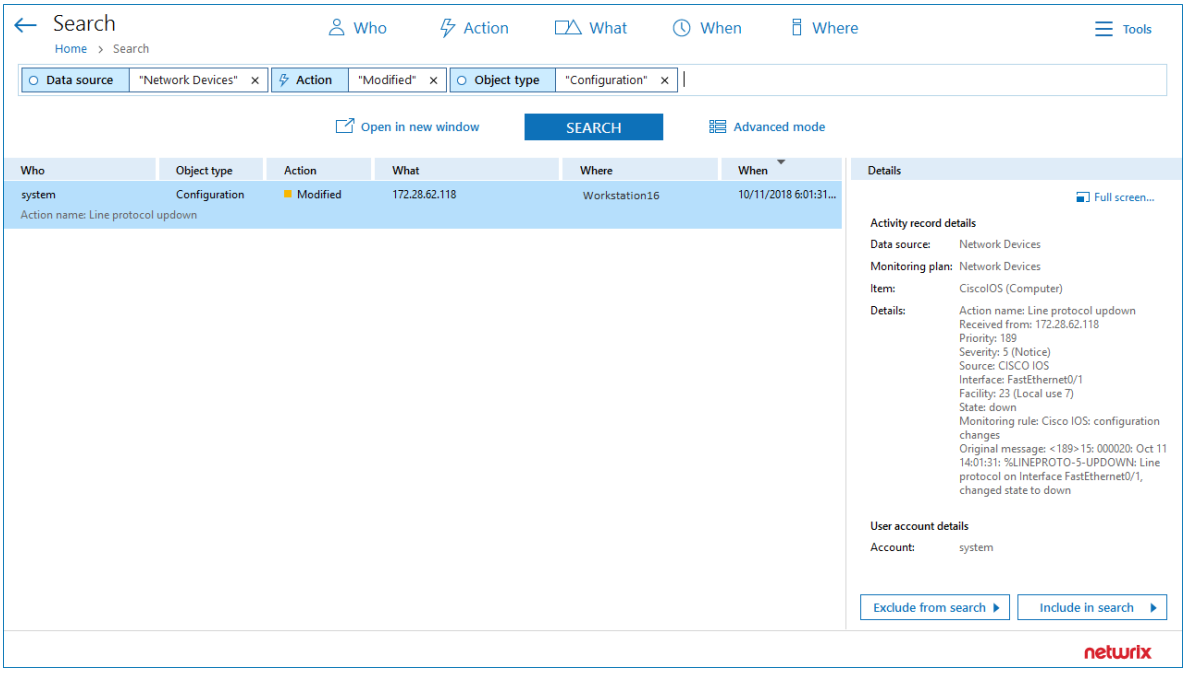
To see how your changes are listed in the report

1. On the main Netwrix Auditor page, navigate to **Reports → Predefined → Network Devices**.
2. Select the **Logons to network devices** and/or **Configuration changes on network devices** reports.
3. Click **View** to open the report.

   Logons to network devices:



Configuration changes on network devices:



These reports based on **Interactive search** engine. See Browse Data with Intelligence Search for more information.

8.3. Browse Data with Intelligence Search

Netwrix Auditor delivers complete visibility into your IT infrastructure. Its convenient interactive search interface enables you to investigate incidents and browse data collected across the entire IT infrastructure. When running a search, you are not limited to a certain data source, change type, or object name. You can create flexible searches that provide you with precise results on *who* changed *what*, and *when* and *where* each change was made.

After collecting initial data, making test changes to your environment and running data collection again, you can review changes in details with Intelligence search.

To browse your audit data and see you test changes

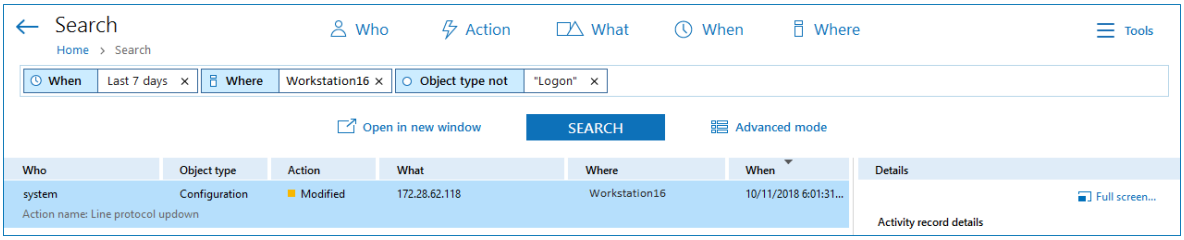
1. On the main Netwrix Auditor page, navigate to **Intelligence → Search**.
2. Add search filters to your search by clicking on a corresponding icon and providing a value. By default, all entries that contain this filter value are shown. For an exact match, use quotation marks.

   Filters are used to narrow your search results. To create a unique set of filters, you can:

   - Add different filters to your search. Search results will be sorted by all selected filters since they work as a logical conjunction (e.g., **Who***: Administrator* AND **Action***: Added*).
   - Specify several values in the same filter to search for any of them (e.g., **Action***: Modified* OR **Action***: Removed*). To do this, select a filter again and specify a new value.

   NOTE: Refer to Netwrix Online Helpcenter for detailed instructions on how to apply filters and change match types
3. Click **Search**.
4. Now, you can narrow your search and modify it right from the search results pane. Click any entry that contains excess data, select **Exclude from search** in the **Details** section and specify a filter, e.g., **Object type:** *Logon* to leave information on network device configuration changes only.

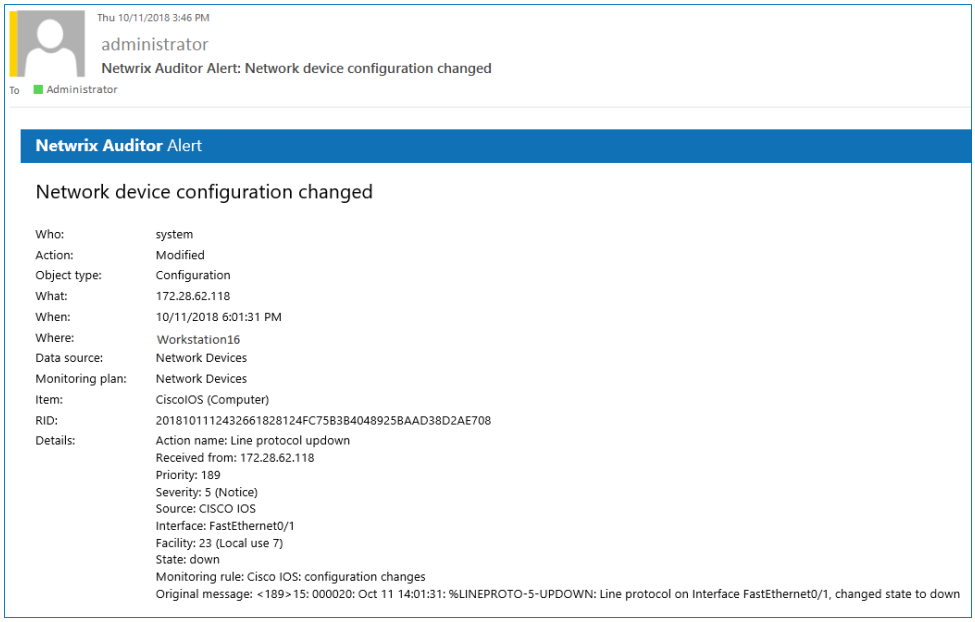
   Your **Search** field will be updated, the **Object type not** filter will be added. Make sure to click **Search** again to update your search results.



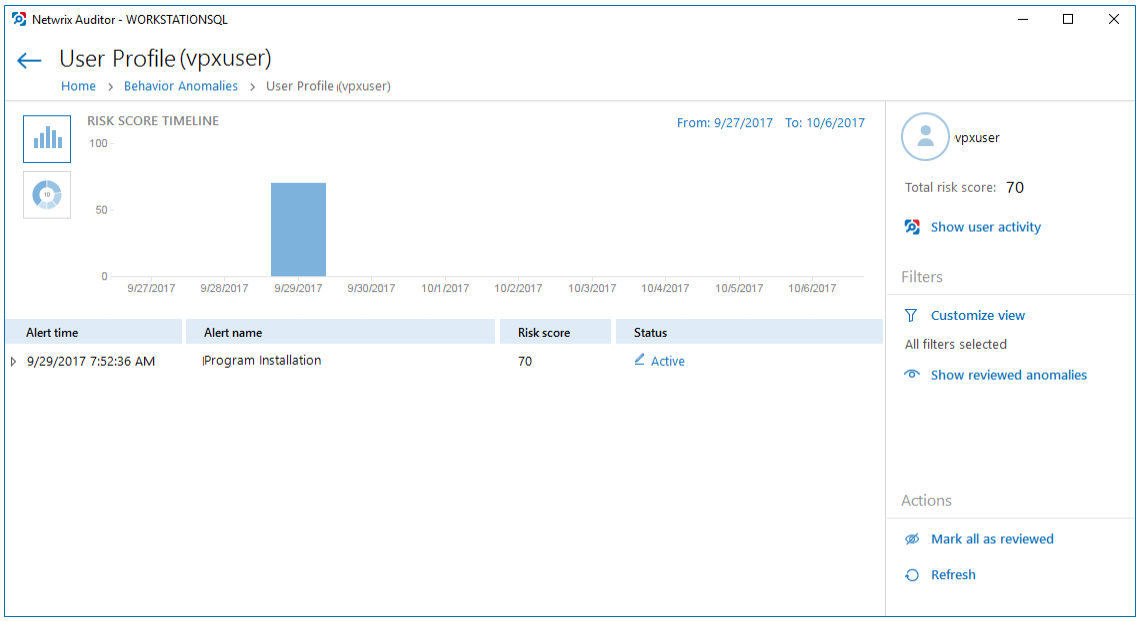
5. Having reviewed your search results, navigate to **Tools**.
   - Click **Save as report** to save the selected set of filters. This search will be added to the **Custom** section inside **Reports**, so that you will be able to access it instantly. Refer to Custom Search-Based Reports for detailed instructions on how to create saved searches.

- Click **Create alert** to get instant email or SMS notifications on suspicious activity that matches your current search criteria. You only need to specify a name for a new alert, add recipient and assign a risk score. The selected set of search criteria will be associated with the new alert automatically. Refer to Alerts for detailed instructions on how to create and configure alerts.

  Try making more similar test changes to provoke an alert. For example:



Once you have received the alert, click the **Behavior Anomalies** tile on the main Netwrix Auditor page to see how the product identifies potentially harmful users and displays their risk scores. Drill-down to user profile to review anomalies and mitigate risks. Refer to Netwrix Online Helpcenter for more information on behavior anomalies and risk scores.



9. Related Documentation

The table below lists all documents available to support Netwrix Auditor for Network Devices:

Document	Description
Netwrix Auditor Online Help Center	Gathers information about Netwrix Auditor from multiple sources and stores it in one place, so you can easily search and access any data you need for your business. Read on for details about the product configuration and administration, its security intelligence features, such as interactive search and alerts, and Integration API capabilities.
Netwrix Auditor Installation and Configuration Guide	Provides detailed instructions on how to install Netwrix Auditor, and explains how to configure your environment for auditing.
Netwrix Auditor Administration Guide	Provides step-by-step instructions on how to configure and use the product.
Netwrix Auditor Intelligence Guide	Provides detailed instructions on how to enable complete visibility with Netwrix Auditor interactive search, report, and alert functionality.
Netwrix Auditor Integration API Guide	Provides step-by-step instructions on how to leverage Netwrix Auditor audit data with on-premises and cloud auditing solutions using RESTful API.
Netwrix Auditor Release Notes	Lists the known issues that customers may experience with Netwrix Auditor 9.9, and suggests workarounds for these issues.

10. Glossary

M

My Term
: My definition

11. Index