

Netwrix Auditor for Network Devices Quick-Start Guide

Version: 9.8
5/14/2019



Legal Notice

The information in this publication is furnished for information use only, and does not constitute a commitment from Netwrix Corporation of any features or functions, as this publication may describe features or functionality not applicable to the product release or version you are using. Netwrix makes no representations or warranties about the Software beyond what is provided in the License Agreement. Netwrix Corporation assumes no responsibility or liability for the accuracy of the information presented, which is subject to change without notice. If you believe there is an error in this publication, please report it to us in writing.

Netwrix is a registered trademark of Netwrix Corporation. The Netwrix logo and all other Netwrix product or service names and slogans are registered trademarks or trademarks of Netwrix Corporation. Microsoft, Active Directory, Exchange, Exchange Online, Office 365, SharePoint, SQL Server, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

Disclaimers

This document may contain information regarding the use and installation of non-Netwrix products. Please note that this information is provided as a courtesy to assist you. While Netwrix tries to ensure that this information accurately reflects the information provided by the supplier, please refer to the materials provided with any non-Netwrix product and contact the supplier for confirmation. Netwrix Corporation assumes no responsibility or liability for incorrect or incomplete information provided about non-Netwrix products.

© 2019 Netwrix Corporation.

All rights reserved.

Table of Contents

1. Introduction	5
1.1. Netwrix Auditor Overview	5
2. Prerequisites and System Requirements	6
2.1. Supported Data Sources	6
2.2. Requirements to Install Netwrix Auditor	7
2.2.1. Hardware Requirements	7
2.2.2. Software Requirements	8
3. Review Components Checklist	9
4. Configure Network Devices for Monitoring	10
4.1. Configure Cisco ASA Devices	10
4.2. Configure Cisco IOS	11
4.3. Configure Fortinet FortiGate Devices	11
4.4. Configure PaloAlto Devices	12
4.5. Configure Juniper Devices	13
4.6. Configure SonicWall Devices	14
5. Install the Product	17
6. Monitoring Plans	19
6.1. Create a New Plan	19
6.1.1. New Monitoring Plan	19
6.1.2. Default SQL Server Instance	20
6.1.3. Audit Database	21
6.1.4. Notifications	21
6.1.5. Recipients	22
6.1.6. Monitoring Plan Summary	22
6.2. Add Items for Monitoring	22
6.2.1. Computer	23
6.2.2. IP Range	23
7. Make Test Changes	24

8. See How Netwrix Auditor Enables Complete Visibility	25
8.1. Review an Activity Summary	25
8.2. Review Network Devices Reports	27
8.3. Browse Data with Intelligence Search	29
9. Related Documentation	34
10. Glossary	35
11. Index	36

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 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, 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 you achieve your specific business objectives, refer to [Netwrix Auditor Best Practices Guide](#).

Netwrix Auditor for User Activity collects and reports on user actions performed within a session and can be configured to capture a video of users' activity on the audited computers.

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	<p>Cisco devices</p> <ul style="list-style-type: none"> • Cisco ASA (Adaptive Security Appliance) 8 and above • Cisco IOS (Internetwork Operating System) 12 and 15 <p>Fortinet Fortigate</p> <ul style="list-style-type: none"> • FortiOS 5, 6 <p>SonicWall</p> <ul style="list-style-type: none"> • SonicWall Web Application Firewall 2.0.x.x • SonicWall NSv 6.5.x.x with SonicOS 6.5.x • SonicWall SMA 11.4.x <p>Juniper Networks</p> <ul style="list-style-type: none"> • vSRX with Junos OS 12.1, Junos OS 18.1 • vMX with Junos OS 17.1 <p>Palo Alto</p> <ul style="list-style-type: none"> • 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

Review the hardware requirements for Netwrix Auditor installation.

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.

The hardware configuration depends on the size of your monitored environment and the number of activity records processed by the product per day. 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	<p>Windows Server OS:</p> <ul style="list-style-type: none">• Windows Server 2019• Windows Server 2016• Windows Server 2012 R2• Windows Server 2012• Windows Server 2008 R2 SP1 <p>Windows Desktop OS (64-bit):</p> <ul style="list-style-type: none">• Windows 10• Windows 8.1• Windows 7 SP1
.NET Framework	<ul style="list-style-type: none">• .NET Framework 3.5 SP1. <p>NOTE: To audit VMware vSphere 6.7 or 6.5, .NET Framework 4.5 or 4.6 is required.</p>
Installer	<ul style="list-style-type: none">• 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.	<p>Supported SQL Server versions are listed here.</p> <p>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.</p> <p>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.</p> <p>If installed separately, remember to test SQL Server connectivity.</p>
Test account	<p>Netwrix recommends you to create a special account with extensive privileges. This account should have sufficient permissions to:</p> <ul style="list-style-type: none">• Collect audit data. See Configure Data Collecting Account for more information.• Access data stored in the SQL Server instance:<ul style="list-style-type: none">• 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
<ul style="list-style-type: none"> • Log Level • Alert Level • Syslog Level 	Set to "Info".
<ul style="list-style-type: none"> • 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
<ul style="list-style-type: none"> • Log Level • Alert Level • Syslog Level 	Set to "Info".
<ul style="list-style-type: none"> • 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**.

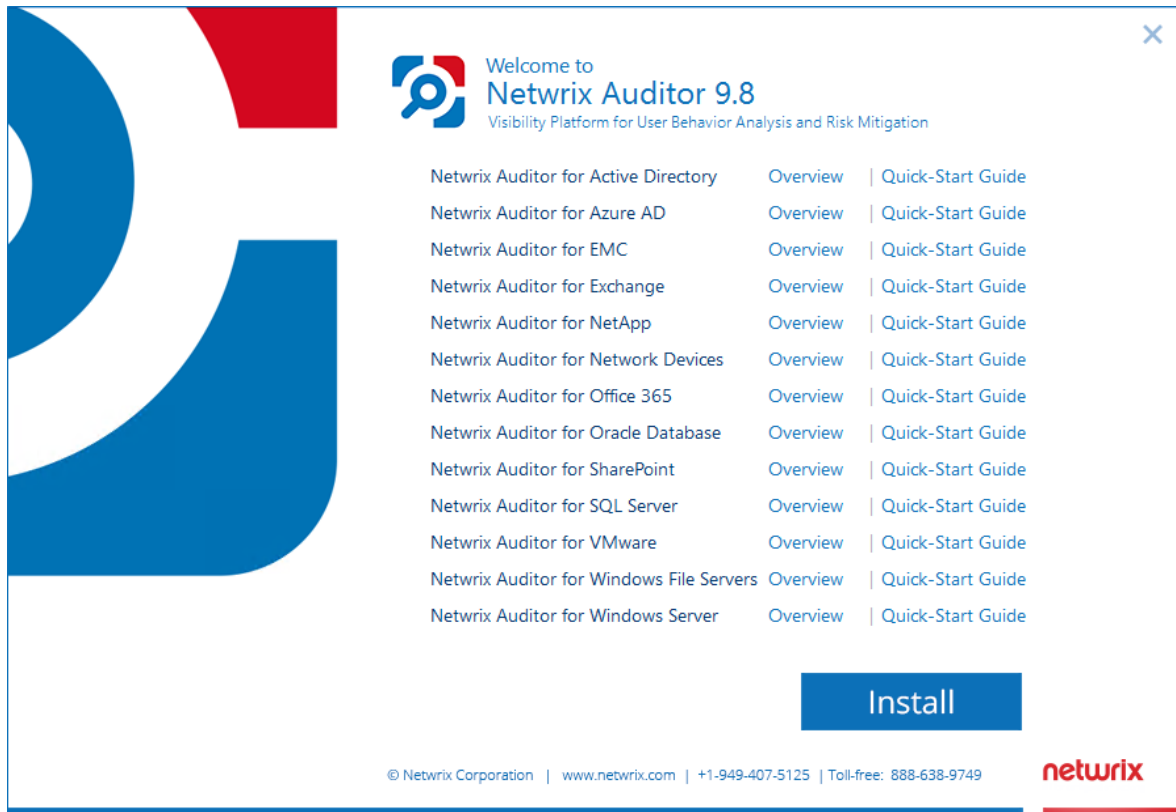
To configure SonicWall NSv series

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 Netrix Auditor

1. Download Netrix Auditor 9.8 from [Netrix website](#).
2. Unpack the installation package. The following window will be displayed on successful operation completion:

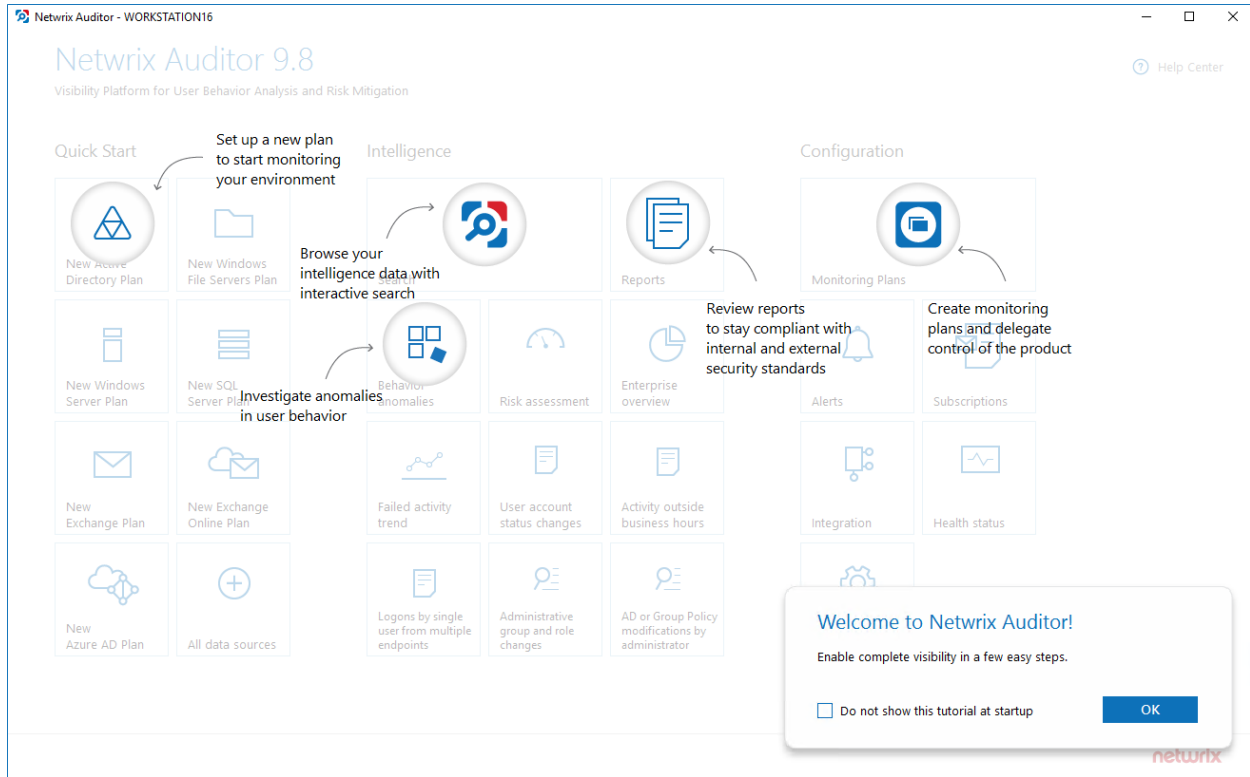


3. Follow the instructions of the setup wizard. When prompted, accept the license agreement.
4. On the **Select Installation Type** step, select **Full installation**.
5. On the **Destination Folder** step, specify the installation folder.
6. On the **Netrix Customer Experience Program** step, you are invited to take part in the Netrix Customer Experience Program. It is optional on your part to help Netrix improve the quality, reliability, and performance of Netrix products and services. If you accept, Netrix 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 Netrix Customer Experience Program later. See [Netrix 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 Netrix 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. Netrix 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 Netrix Auditor page, click the Network Devices tile in the **Quick Start** section.

The wizard that appears will help you set up a new plan in a few easy steps:

- 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. New Monitoring Plan

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

New Monitoring Plan

Specify the account for collecting data

User name:

Password:

Note: Make sure the account has sufficient permissions to access and collect data from your data sources. [Learn more...](#)

Specify data collection settings

Enable network traffic compression

Adjust audit settings automatically

Note: Netwrix Auditor will continually enforce the relevant audit policies in your environment. [Learn more...](#)

Collect data for state-in-time reports

Option	Description
Specify the account for collecting data	<p>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.</p> <p>Make sure the account has sufficient permissions to collect data. For a full list 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.</p>

6.1.2. Default SQL Server Instance

To provide search, alerting, and report capabilities, Netwrix Auditor has to store security intelligence data in the Audit Database hosted on a SQL Server instance. Make sure the **Disable security intelligence and make data available only in activity summaries** checkbox is cleared.

Specify one of the following options:

- **Install a new instance of Microsoft SQL Server Express automatically**—Select if you want Netwrix Auditor to download and configure SQL Server 2014 Express with Advanced Services.

- **Use an existing SQL Server instance**—Select to continue using an installed SQL Server instance. Netwrix Auditor detects local SQL Server instance automatically and prepopulates the fields. 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: <ul style="list-style-type: none"> • Windows authentication • SQL Server authentication
User name	Specify the account to be used to connect to the SQL Server instance. NOTE: This account must be granted the database owner (db_owner) role and the dbcreator server role. See Configure Audit Database Account for more information.
Password	Enter a password.

6.1.3. Audit Database

Specify a database name to store security intelligence data for your monitoring plan, or disable this functionality. 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.

Netwrix Auditor will create a database on the SQL Server instance you specify.

6.1.4. Notifications

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 detects SMTP settings; however, for your first plan you should provide them manually. Complete the following fields:

Option	Description
SMTP server	Enter your SMTP server address. It can be your company's Exchange server or any public mail server (e.g., Gmail, Yahoo).
Port number	Specify your SMTP server port number.

Option	Description
Sender address	Enter the address that will appear in the From field. NOTE: It is recommended to click <input type="checkbox"/> . The system will send a test message to the specified email address and inform you if any problems are detected.
SMTP authentication	Select this checkbox if your mail server requires the SMTP authentication.
User name	Enter a user name for the SMTP authentication.
Password	Enter a password for the SMTP authentication.
Use Secure Sockets Layer encrypted connection (SSL)	Select this checkbox if your SMTP server requires SSL to be enabled.
Use implicit SSL	Select this checkbox if the implicit SSL mode is used, which means that an SSL connection is established before any meaningful data is sent.

6.1.5. Recipients

Specify who will receive daily activity summaries that list changes that occurred for a given time period. 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

Your plan is almost complete. Provide a name and description for your monitoring plan. Make sure the **Add item now** checkbox is selected. In this case, on the next step, you will be prompted to add an item for monitoring.

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.

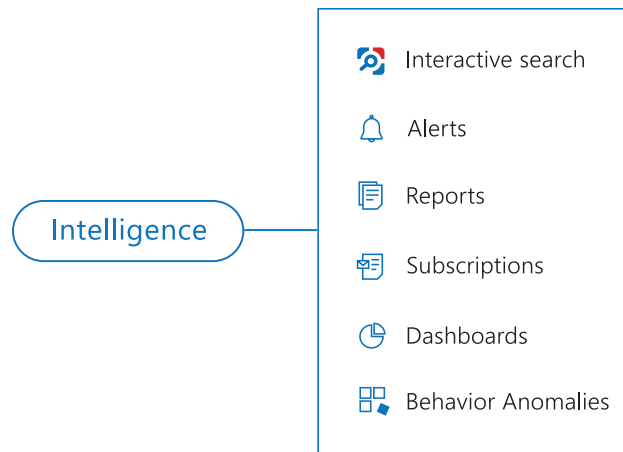
For example, make the following test changes:

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

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.

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

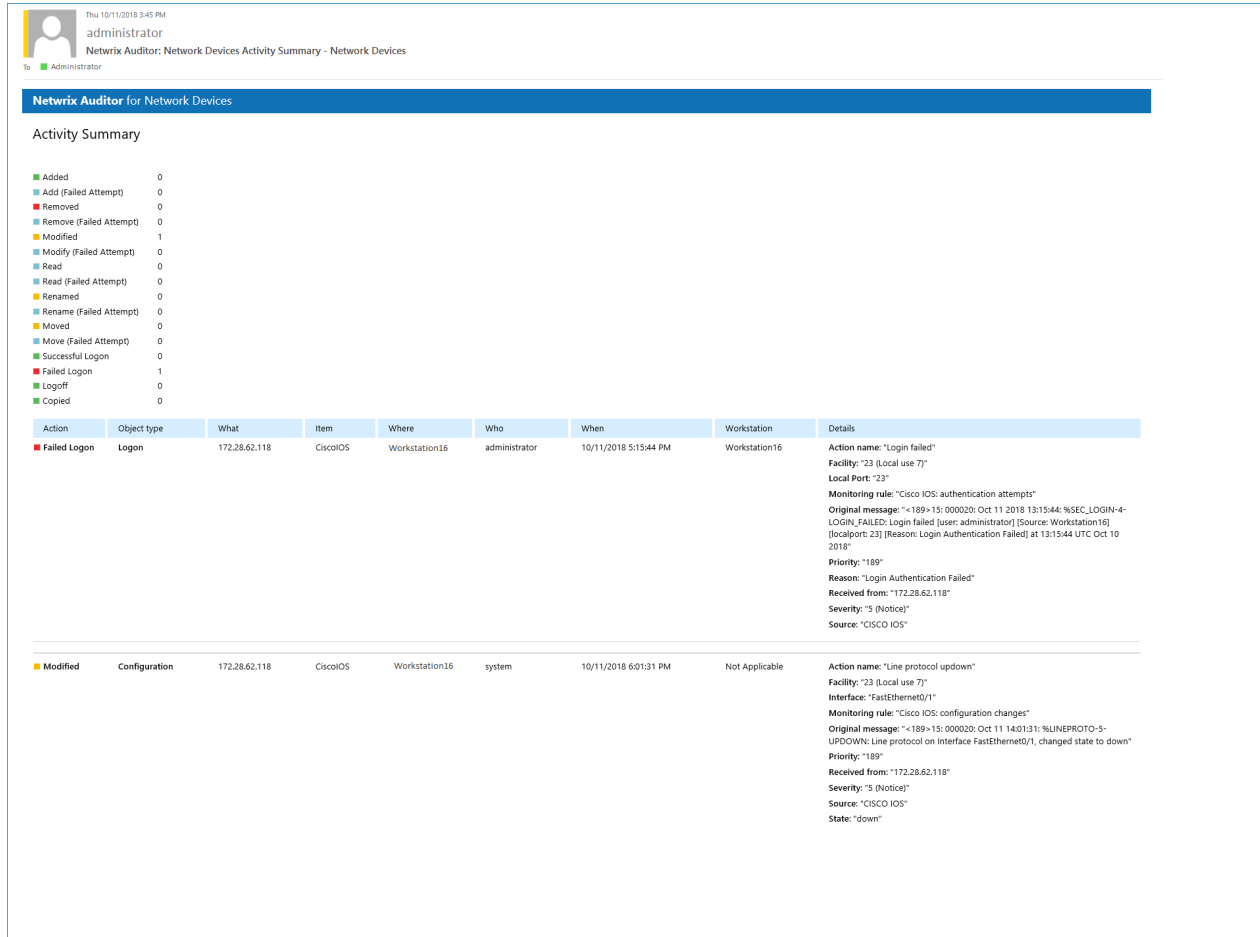
1. Navigate to **Monitoring Plans** and select your plan in the list.
2. Click **Edit**.
3. In the your monitoring plan settings, click **Update** in the right pane.
4. Check your mailbox for an email notification and make sure that the data collection has completed successfully.

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



The example Activity Summary 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:

The screenshot shows the Netrix Auditor search interface. The search criteria are: Data source: "Network Devices", Action: "Failed Logon", Object type: "Session". The search results table shows one entry for user 'administrator' performing a 'Failed Logon' action on '10/10/2018 5:15...' at 'Workstation16'. The details pane on the right provides comprehensive information about the event, including the action name 'Login failed', source 'CISCO IOS', and a detailed log message: 'Oct 10 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'.

Who	Object type	Action	What	Where	When
administrator	Logon	Failed Logon	172.28.62.118	Workstation16	10/10/2018 5:15:...

Configuration changes on network devices:

The screenshot shows the Netrix Auditor search interface with search criteria: Data source: "Network Devices", Action: "Modified", Object type: "Configuration". The search results table shows one entry for user 'system' performing a 'Modified' action on '10/11/2018 6:01:31...' at 'Workstation16'. The details pane on the right provides information about the configuration change, including the action name 'Line protocol updown', source 'CISCO IOS', and a detailed log message: 'Oct 11 14:01:31: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down'. The user account details section shows the account is 'system'.

Who	Object type	Action	What	Where	When
system	Configuration	Modified	172.28.62.118	Workstation16	10/11/2018 6:01:31...

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.

For example, consider adding these filters:

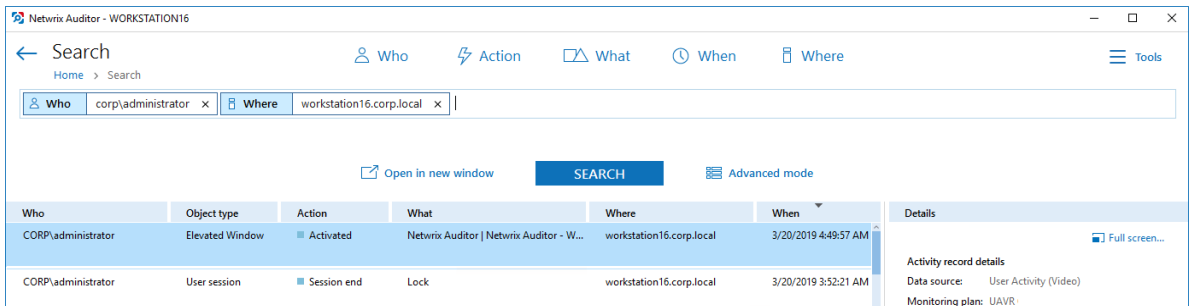
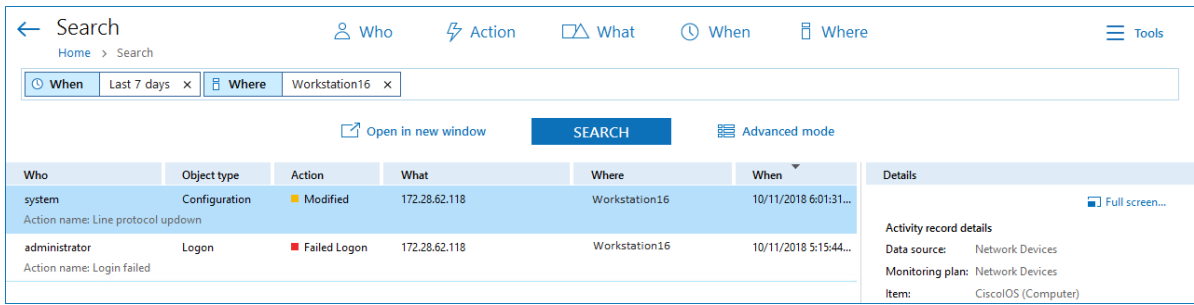
Filter	Value
	Specify your server.
WHERE	
	Specify a timeframe.
WHEN	

NOTE: Refer to [Netwrix Online Helpcenter](#) for detailed instructions on how to apply filters and change match types.

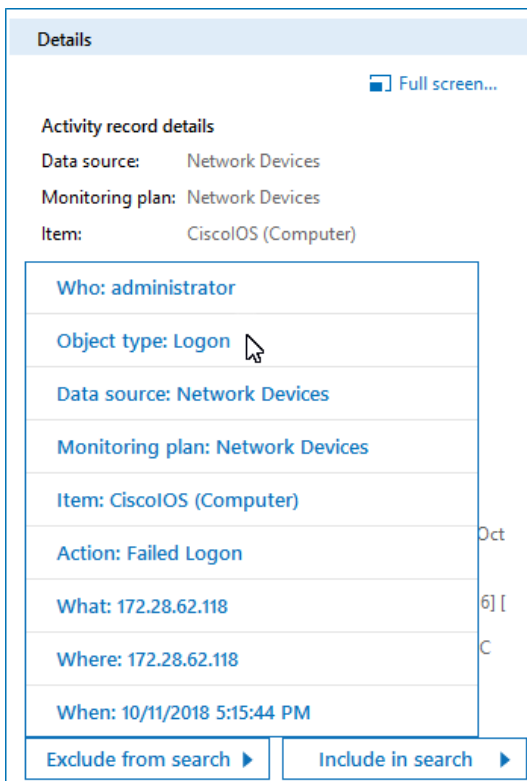
As a result, you will see the following filters in the **Search** field:



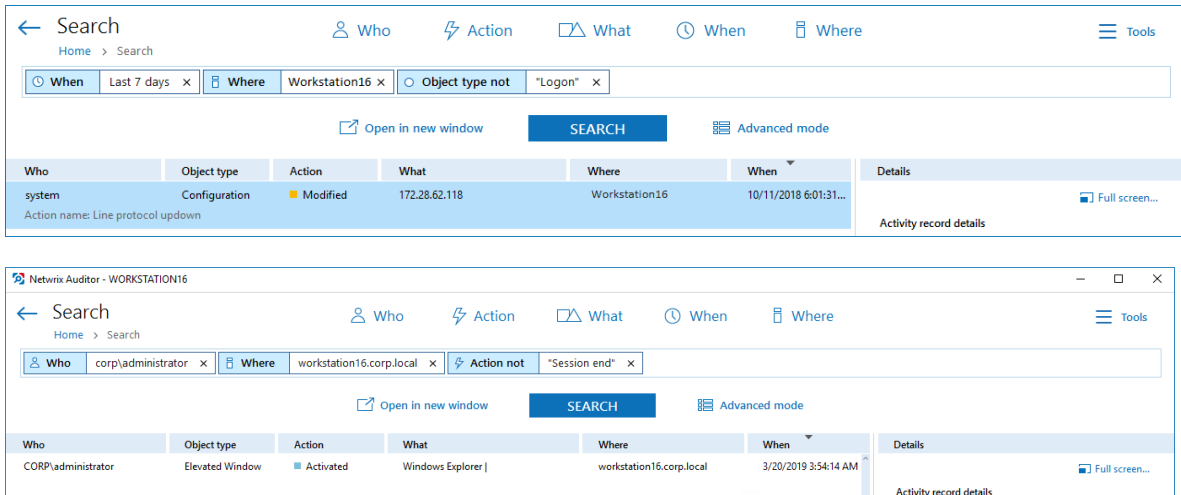
3. Click Search.



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.



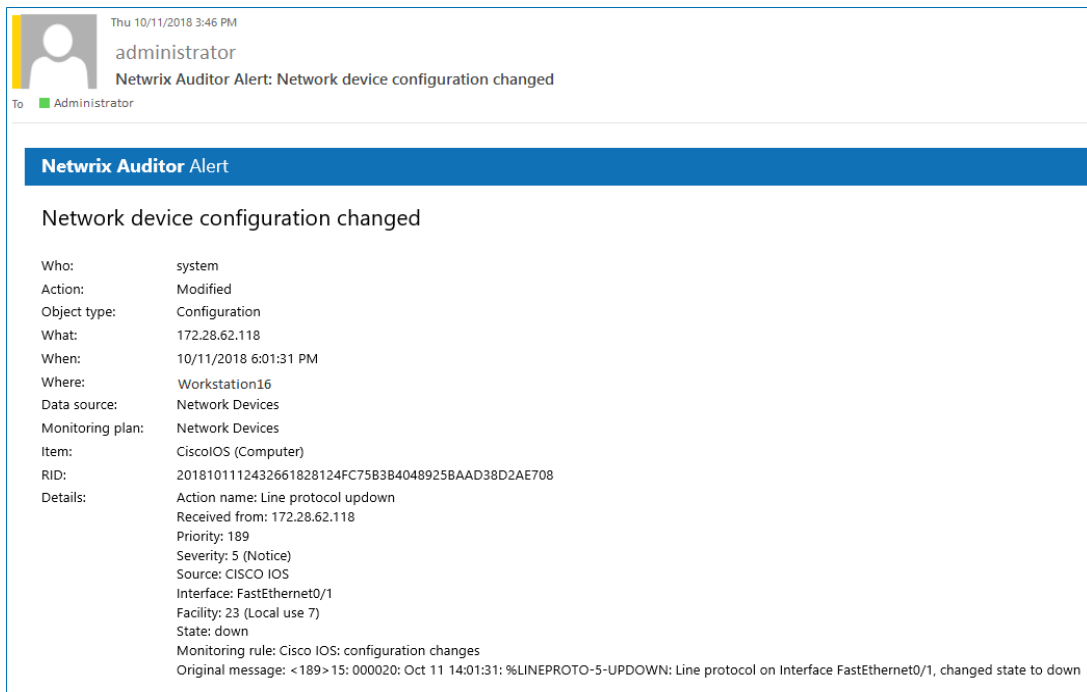
Your **Search** field will be updated, the **Object type not** filter will be added. Make sure to click **Search** again to update your search results.




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:






Wed 3/20/2019 4:48 PM

Administrator

Netwrix Auditor Alert: Elevated Windows

To  Administrator

Netwrix Auditor Alert

Elevated Windows

Who:	CORP\administrator
Action:	Activated
Object type:	Elevated Window
What:	Windows Shell Experience Host Jump List for Skype
When:	3/20/2019 6:46:36 AM
Where:	workstation16.corp.local
Workstation:	workstation16.corp.local
MAC:	
Data source:	User Activity (Video)
Monitoring plan:	UAVR
Item:	172.28.6.31 (Computer)
RID:	2019032013480413961400F6FFC85423AB0943129BCBFFF4

This message was sent by Netwrix Auditor from **Workstation16.corp.local**.
www.netwrix.com

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.

The screenshot displays the 'User Profile (CORP\administrator)' page in Netrix Auditor. The page is divided into several sections:

- Header:** Shows the user profile name 'CORP\administrator' and the total risk score of 70.
- RISK SCORE TIMELINE:** A bar chart showing the risk score over time from 9/27/2017 to 10/6/2017. A single bar on 9/29/2017 indicates a risk score of 70.
- Alerts Table:** A table with columns for Alert time, Alert name, Risk score, and Status. One alert is listed: 'New Users' on 9/29/2017 at 7:52:36 AM, with a risk score of 70 and a status of 'Active'.
- Filters and Actions:** A sidebar on the right contains options to 'Show user activity', 'Customize view', 'Show reviewed anomalies', 'Mark all as reviewed', and 'Refresh'.

Alert time	Alert name	Risk score	Status
9/29/2017 7:52:36 AM	New Users	70	Active

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 9.8, and suggests workarounds for these issues.

10. Glossary

M

My Term

My definition

11. Index

	A
Activity Summary 25	
	C
Checklist 9	
Configure audit	
NDA 10	
	D
Data Collection	
Launch data collection manually 25	
Data sources 6	
	E
Environment 6	
	I
Install	
Netwrix Auditor 6, 17	
System requirements 6	
Items 22	
Computer 23	
IP Range 23	
	M
Make Changes 24	
Monitoring plan	
Add item 22	
New 19	
Overview 19	
	N
NDA 10	

O

Overview 5

R

Related Documentation 34

S

System requirements 6-7

 Hardware requirements 7

 Software requirements 8