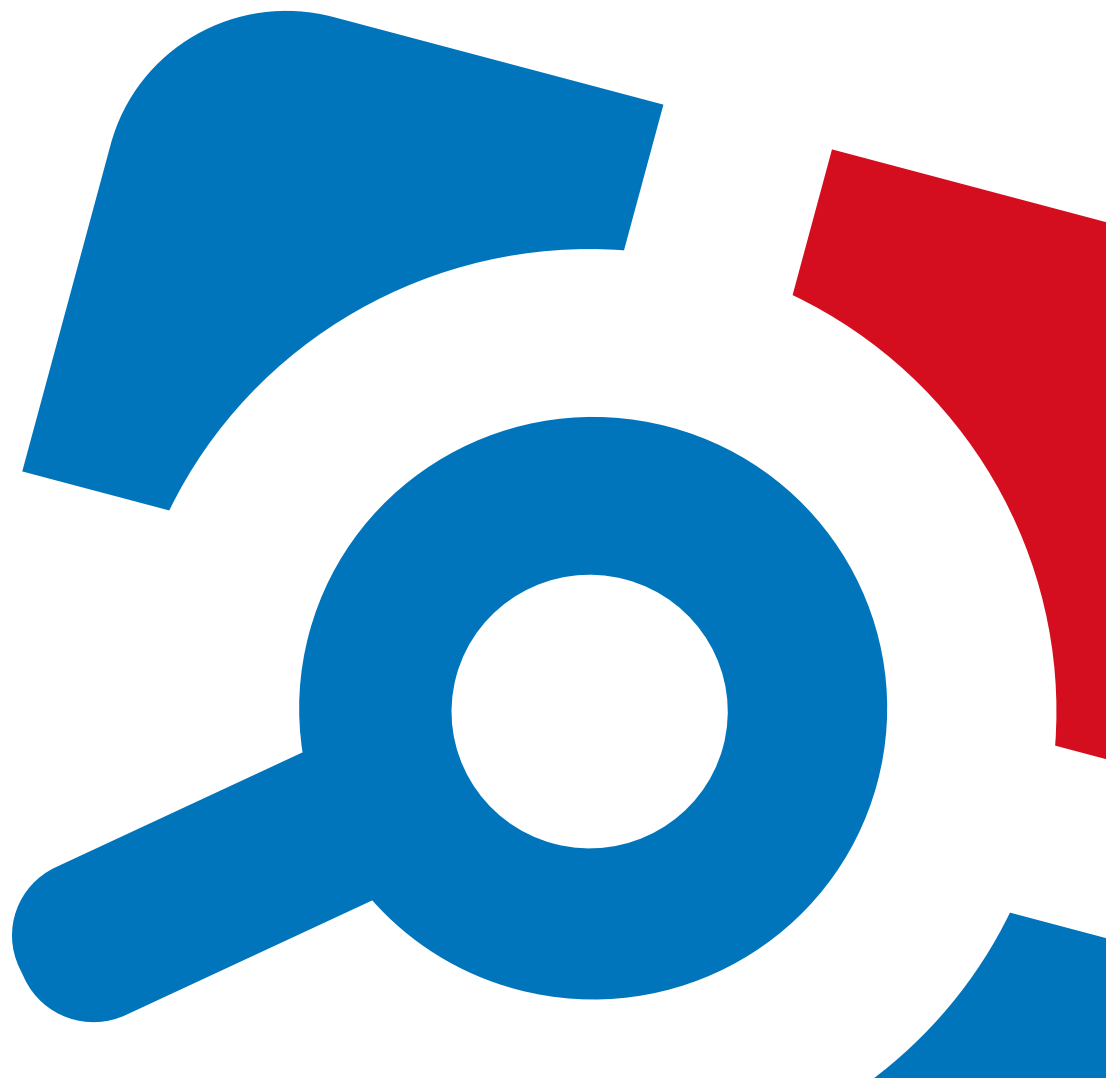


Netwrix Auditor for Network Devices Quick-Start Guide

Version: 10
9/14/2021



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.

© 2021 Netwrix Corporation.

All rights reserved.

Table of Contents

1. Introduction	5
1.1. Netwrix Auditor Features and Benefits	5
2. Prerequisites and System Requirements	6
2.1. Supported Data Sources	6
2.1.1. Considerations for Oracle Database Auditing	8
2.2. Requirements to Install Netwrix Auditor	9
2.2.1. Hardware Requirements	9
2.2.2. Software Requirements	10
2.2.2.1. Using SSRS-based Reports	10
3. Review Components Checklist	12
4. Configure Network Devices for Monitoring	13
4.1. Configure Cisco ASA Devices	13
4.2. Configure Cisco IOS	14
4.3. Configure Cisco Meraki Devices	15
4.4. Configure Fortinet FortiGate Devices	16
4.5. Configure PaloAlto Devices	17
4.6. Configure Juniper Devices	18
4.7. Configure SonicWall Devices	19
4.8. Configure HPE Aruba Devices	22
4.9.	25
4.10. Configure Pulse Secure Devices	25
5. Install the Product	28
6. Monitoring Plans	30
6.1. Using historical data	30
6.2. Create a New Plan	31
6.2.1. Settings for Data Collection	31
6.2.2. Default SQL Server Instance	31
6.2.3. Database Settings	32
6.2.4. SMTP Server Settings	34

6.2.5. Email Notification Recipients	34
6.2.6. Monitoring Plan Summary	34
6.3. Add Items for Monitoring	35
6.3.1. Computer	35
6.3.2. Cisco Meraki	36
6.3.3. Syslog Device	37
6.3.4. IP Range	37
6.4. Launch Data Collection Manually and Update Status	38
7. Make Test Changes	39
8. See How Netwrix Auditor Enables Complete Visibility	40
8.1. Review an Activity Summary	40
8.2. Review Network Devices Reports	42
8.3. Browse Data with Intelligence Search	44
9. Related Documentation	46
10. Glossary	47
11. Index	48

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

This section lists platforms and systems that can be monitored with Netwrix Auditor for Network Devices.

Active Directory domain

[Supported Data Sources](#)

[Supported Data Sources](#)

[Supported Data Sources](#)

[Supported Data Sources](#)

Exchange

[Supported Data Sources](#)

Office 365 and Azure AD

[Supported Data Sources](#)

[Supported Data Sources](#)

[Supported Data Sources](#)

SharePoint

[Supported Data Sources](#)

File storage systems

[Supported Data Sources](#)

[Supported Data Sources](#)

[Supported Data Sources](#)

[Supported Data Sources](#)

Network devices

[Network Devices](#)

Databases

[Supported Data Sources](#)

[Considerations for Oracle Database Auditing](#)

[Supported Data Sources](#)

Windows server

[Supported Data Sources](#)

[Supported Data Sources](#)

[Supported Data Sources](#)

[Supported Data Sources](#)

VMware server

[Supported Data Sources](#)

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 • Cisco Meraki: Netwrix recommends using the latest version of the Meraki Dashboard <p>Fortinet Fortigate</p> <ul style="list-style-type: none"> • FortiOS 5.6 and above <p>SonicWall</p> <ul style="list-style-type: none"> • SonicWall WAF 2.0.0.x / SMA v9.x & v10.x • SonicWall NS 6.5.x.x with SonicOS 6.5.x • SonicWall SMA 12.2 <p>Juniper Networks</p>

Data source	Supported Versions
	<ul style="list-style-type: none">vSRX with Junos OS 12.1, Junos OS 18.1, Junos OS 20.4R2vMX with Junos OS 17.1
	Palo Alto <ul style="list-style-type: none">Palo Alto with PAN-OS 7.0, 8.0, 9.0, 10.0
	Pulse Secure <ul style="list-style-type: none">Pulse Connect Secure 9.1R3 and above
	Aruba <ul style="list-style-type: none">Aruba OS 6.46.4.x – 8.6.0.x (Mobility Master, Mobility Controller)

2.1.1. Considerations for Oracle Database Auditing

Starting with version 9.95, Netwrix Auditor for Oracle Database is focused on versions 12c and above. It means that Oracle Database 11g users will not be able to benefit from latest features and improvements of the product. Oracle Database 11g users should also consider its support expiration dates set by the vendor. So, when planning your Netwrix Auditor deployment, consider the following:

- Several limitations apply to Oracle 11g support in Netwrix Auditor 9.96:
 - Oracle wallets are not supported
 - Lightweight drivers for Oracle Instant Client are not supported
 - Netwrix Auditor client UI does not display any warnings and / or errors regarding to trail audit mode operation
- If you are using Oracle Database 11g and Netwrix Auditor 9.9 (or earlier) and do not plan to upgrade your deployment, you will have all 9.9 capabilities unchanged.
- If you are using Oracle Database 11g and have performed seamless upgrade to Netwrix Auditor 9.96, the audit data collection will operate properly. However, consider [General Considerations and Known Issues](#) and keep in mind Oracle Database 11g support expiration dates.

If you are using Oracle Database 12c or later, make sure you have **Unified auditing** mode enabled. Otherwise, Netwrix Auditor may not operate properly. Refer to [Migrate to Unified Audit](#) for more information.

Check out the following documentation sections:

- [Software Requirements](#)
 - [Configure Oracle Database for Monitoring](#)

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 estimations of the resources required for Netwrix Auditor deployment.

IMPORTANT! 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. It is strongly recommended that you go through the [Deployment Planning](#) section before you start the installation.

Requirements provided in this section apply to a clean installation on a server without any additional roles or third-party applications installed.

Below you can find rough estimations, calculated for evaluation of Netwrix Auditor for Network Devices. Refer to [Netwrix Online Help Center](#) for more 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.

2.2.1.0.1. Scenario 1

Netwrix Auditor and SQL Server instance will be deployed on different servers.

Requirements below apply to Netwrix Auditor server.

Hardware component Evaluation, PoC or starter environment

2.2.1.0.2. Scenario 2

Netwrix Auditor server and SQL Server instance will be deployed on the same machine.

IMPORTANT! In large and extra -large environments, installation of Netwrix Auditor and SQL Server on the same server is not recommended. Instead, deploy an SQL Server instance on a separate server or cluster that meets the requirement in Scenario 1. Refer to related Microsoft guidelines.

Hardware component	Evaluation, PoC or starter environment
Processor	2 cores
RAM	8 GB
Disk space	100 GB—System drive 100 GB—Data drive (Long-Term Archive and SQL Server)

2.2.2. Software Requirements

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

Component	Requirements
Operating system (English-only)	Windows Server OS: <ul style="list-style-type: none"> Windows Server 2019 Windows Server 2016 Windows Server 2012 R2 Windows Server 2012 Windows Desktop OS (64-bit): <ul style="list-style-type: none"> Windows 10 Windows 8.1
.NET Framework	<ul style="list-style-type: none"> .NET Framework 4.5 and above.
Installer	<ul style="list-style-type: none"> Windows Installer 3.1 and above

2.2.2.1. Using SSRS-based Reports

SQL Server Reporting Services are needed for this kind of reports (see [SQL Server Reporting Services](#)). If you plan to export or print such reports, check the requirements below.

Export

To export SSRS-based reports, **Internet Explorer** must be installed on the machine where Netwrix Auditor client runs.

Internet Options must be configured to allow file downloads for the **Local intranet** zone:

1. Select **Internet Options** and click **Security**.
2. Select **Local intranet** zone and click **Custom level**.
3. In the **Settings** list, locate **Downloads >File download** and make sure the **Enabled** option is selected.

Printing

To print SSRS-based reports, SSRS Report Viewer and Netwrix Auditor Client require ActiveX Control to be installed and enabled on the local machine. See this [Knowledge Base article](#) for details.

You can, for example, open any SSRS-based report using Internet Explorer and click **Print**. Internet Explorer will prompt for installation of the additional components it needs for printing. Having them installed, you will be able to print the reports from Netwrix Auditor UI as well.

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 Cisco Meraki Devices](#)
- [Configure Fortinet FortiGate Devices](#)
- [Configure PaloAlto Devices](#)
- [Configure Juniper Devices](#)
- [Configure SonicWall Devices](#)
- [Configure HPE Aruba 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
```

7. Configure the devices to show username for failed logons:

```
hostname(config)# no logging hide username
```

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
```

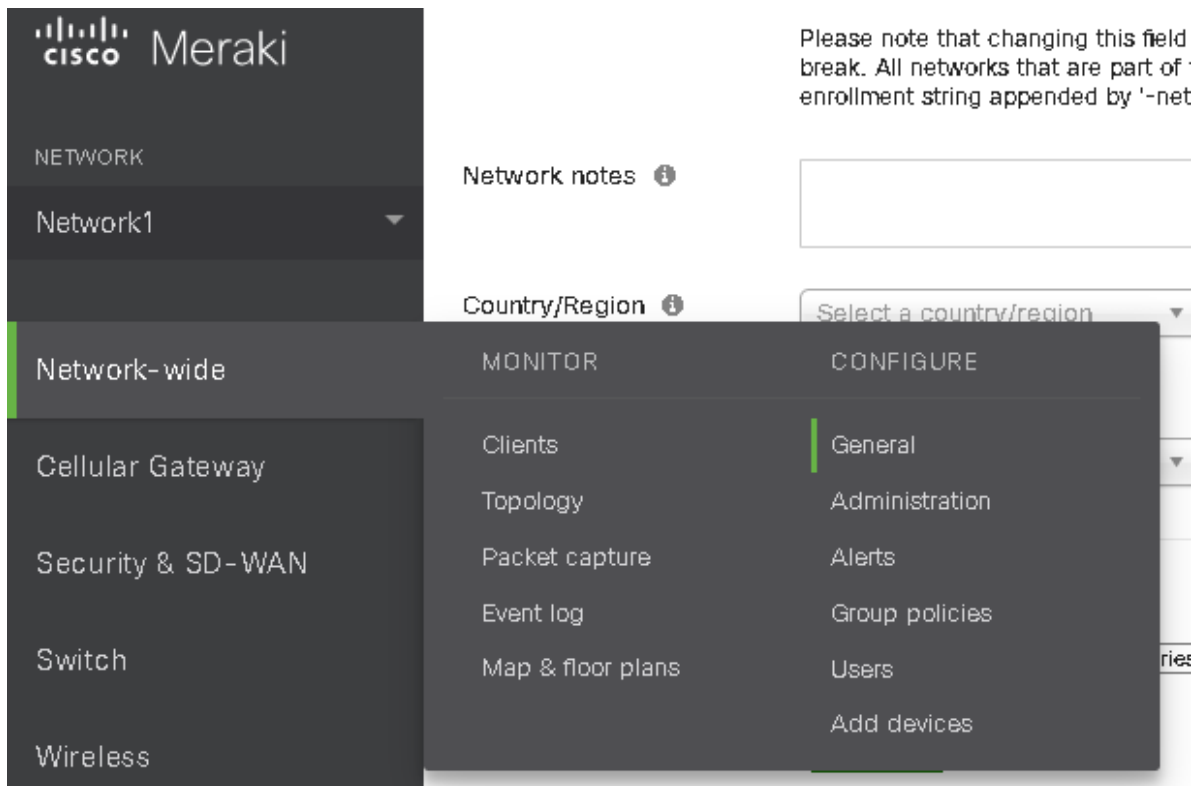
4.3. Configure Cisco Meraki Devices

To configure Cisco Meraki devices, configure the Syslog server for each of your networks.

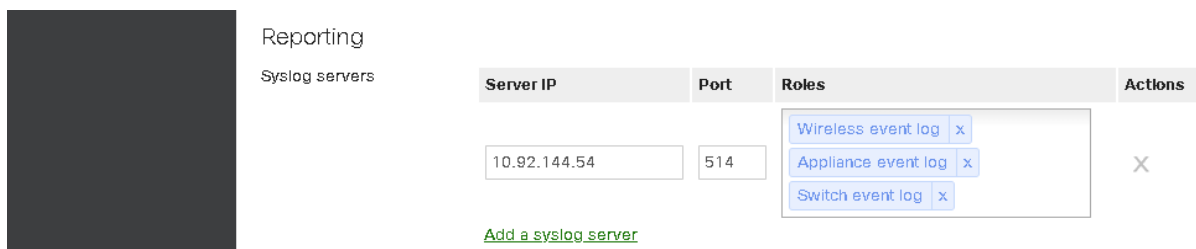
NOTE: Netrix recommends assigning a unique identifier to each Cisco Meraki device; otherwise, the product may count them as a single anonymous device.

To configure the Syslog server, do the following:

1. Sign in to [Cisco Meraki Dashboard](#).
2. Navigate to **Network wide** → **Configure** → **General**.



3. Locate the **Reporting** section and click **Add a syslog server**.



4. In the dialog that opens, complete the following fields:

Option	Description
Server IP	Provide the IP address of the computer that hosts your Netwrix Auditor Server.
Port	Provide the port configured in your monitoring plan for Network Devices (514 by default). See Network Devices for more information.
Roles	Select the following roles: <ul style="list-style-type: none">• Appliance event log• Switch event log• Wireless event log

NOTE: If you need any additional information about the Cisco Meraki devices configuration, refer to Cisco documentation: [Syslog Server Overview and Configuration](#).

4.4. 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**.

4.5. 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.

Parameter	Description
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.

4.6. 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
```

4.7. 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 NS 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 NS 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**.

4.8. Configure HPE Aruba Devices

To configure your HPE Aruba devices, enable logging to multiple Syslog servers and configure logging levels. Do one of the following:

- [To configure HPE Aruba devices via Command Line Interface](#)
- [To configure HPE Aruba devices through the Management Console](#)

To configure HPE Aruba devices via Command Line Interface

1. Log in to the Command Line Interface (CLI).
2. Enter the following command to start configuration mode:

```
# configure terminal
```
3. Specify IP address of the computer that hosts your Netwrix Auditor Server to send Syslog messages to:

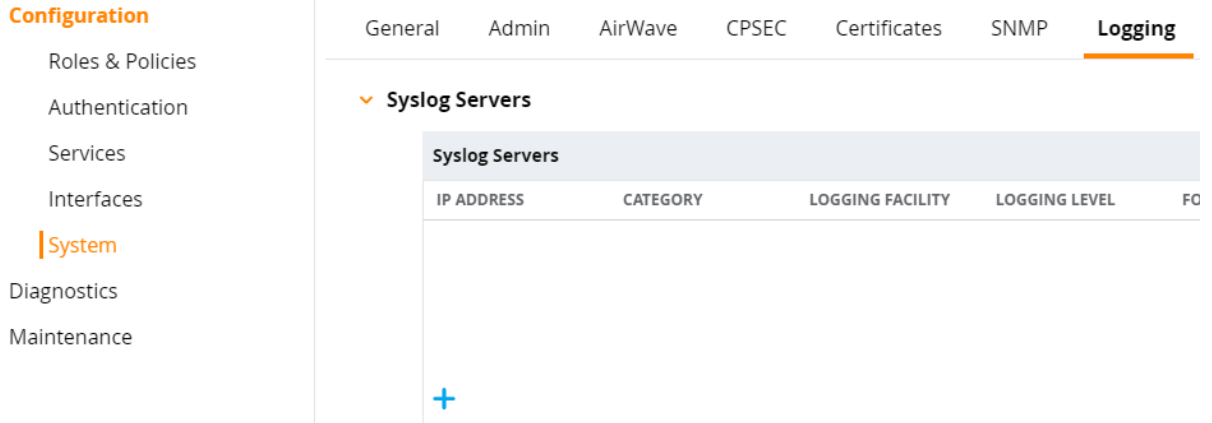
```
# logging <ipaddr> severity information
```
4. Specify event level for the following categories: security, system, user, wireless, network:

```
# logging network level information  
# logging security level information  
# logging system level information  
# logging user level information  
# logging wireless level information
```
5. Apply configuration changes:

```
# write memory
```

To configure HPE Aruba devices through the Management Console

1. Log in to HPE Aruba web interface.
2. Navigate to **Mobility Master** and select a device or a group of devices you want to monitor with Netwrix Auditor.
3. Navigate to **Configuration** → **System** → **Logging** and click + to add a new Syslog Server.




4. In the **Add New Syslog Servers** dialog, complete the following fields:

Option	Description
IP address	Provide the IP address of the new server.
Category	Select None .
Logging facility	Leave empty.
Logging level	Select Informational .
Format	Select None .

5. Click **Submit**. The new server is added to the **Syslog Servers** list.
6. Click **Pending Changes** on the right.
7. In the **Pending Changes for <X> Managed Controller(s)** dialog, select the device you want to apply changes to.
8. Click **Deploy Changes**.
9. If the configuration is correct, you will see the following wizard:

Configuration Deployment Status

Update for 1 Managed Controller(s)			
TARGET	NODEPATH	STATUS	MESSAGE
ArubaMM-VA	Mobility Master		

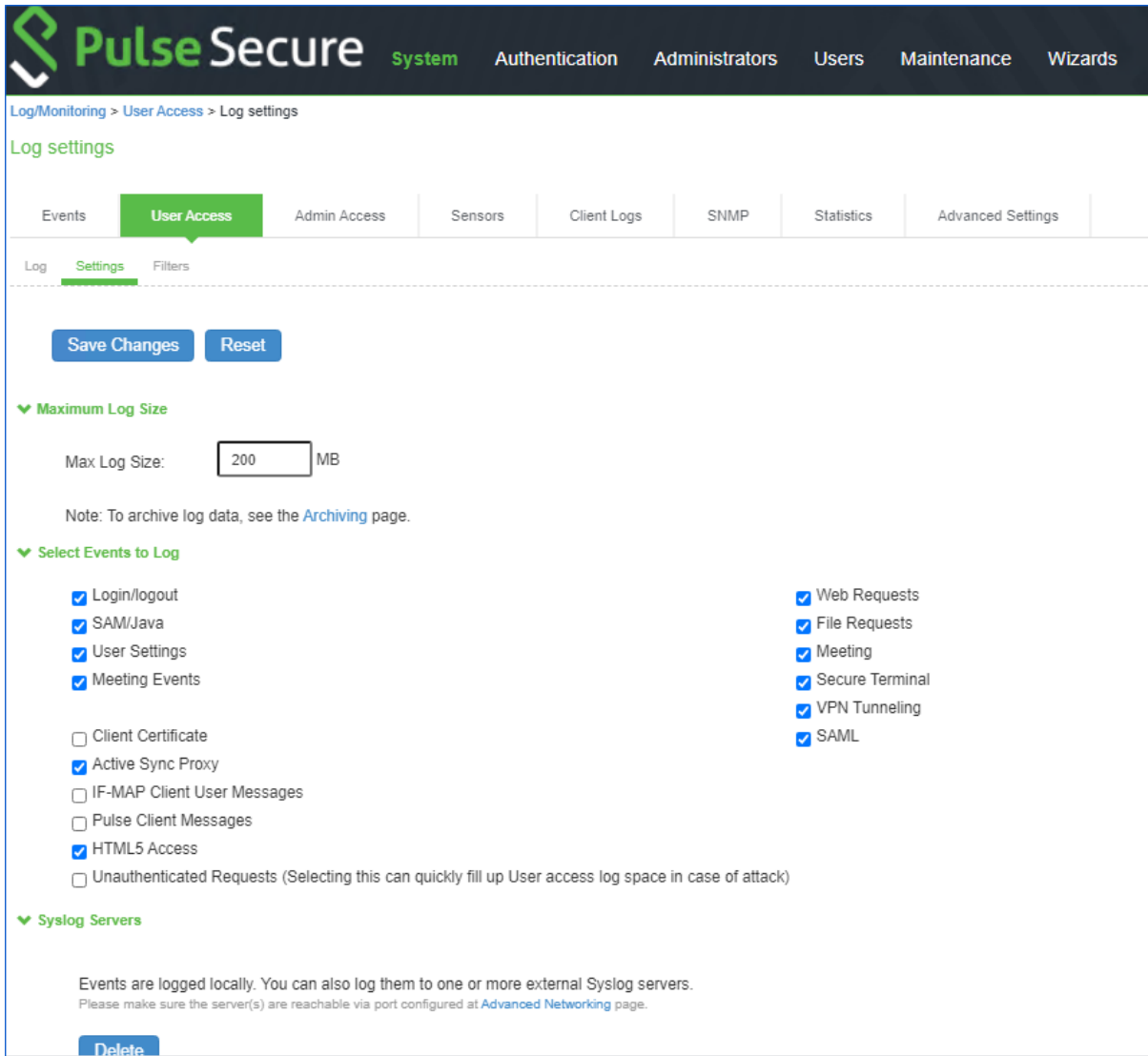
Close

10. Navigate to **Configuration** → **System** → **Logging** and expand the **Logging Levels**.
11. Select the **Informational** value for the following parameters:
 - network
 - system
 - wireless
 - security
12. Deploy pending changes for the logging level: repeat steps 6 - 8.

4.9.

4.10. Configure Pulse Secure Devices

1. Connect to your Pulse Secure device: launch an Internet browser and enter the IP address or device DNS name in the URL field (`https://<IP address / Device DNS name>/admin`).
2. In the **Web Interface**, navigate to **System** → **Log/Monitoring**.
3. Under **Log/Monitoring**, expand the **User Access** link.
4. Locate the **Settings** tab.
5. Under the **Select Events to Log**, select the following (minimal requirement, select other events if needed):
 - Login/Logout
 - VPN Tunneling



6. Under the Syslog Servers, complete the following fields:

Option	Description
Server name/IP	Specify the IP address of the computer where Netrix Auditor Server resides.
Facility	Select desired facility.
Type	Select UDP .
Client Certificate	Use default values.
Filter	Select Standard .

7. Save your changes.

8. Switch to the **Admin Access** tab.

9. Under the **Select Events to Log**, select the following (minimal requirement, select other events if needed):
 - Administrator logins
 - Administrator changes
10. Repeat the step 6 for **Syslog Servers** configuration.
11. Save your changes.
12. Navigate to **System** → **Configuration** → **Advanced Networking**.
13. Expand the **Select the source port to be used for the following features** link.
14. Locate the **Syslog** parameter and set it to *Internal*.

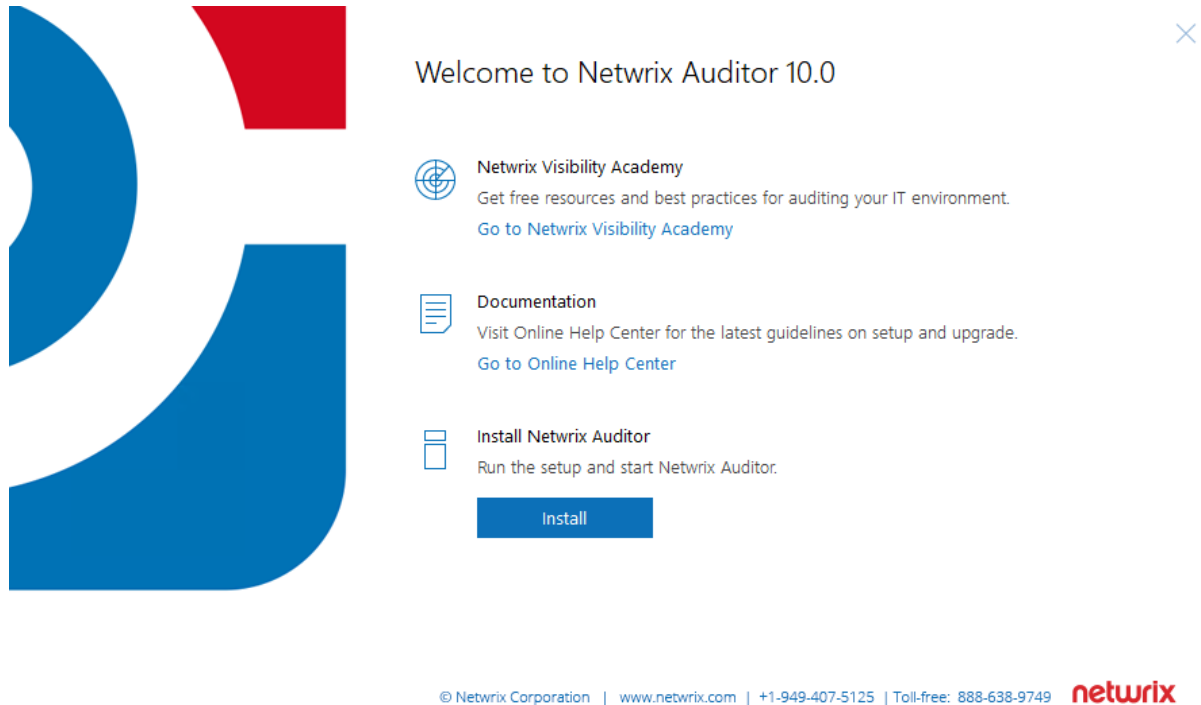
NOTE: Netwrix Auditor must be accessible from the selected network interface

15. Save your changes.
16. Start Netwrix Auditor.
17. Navigate to your monitoring plan for Network Devices.
18. Provide the IP address of the interface you specified on the step 14 as the **Computer** item for your monitoring plan.

5. Install the Product

To install Netwrix Auditor

1. Download Netwrix Auditor 10 from [Netwrix website](#).
2. Unpack the installation package. The following window will be displayed on successful operation completion:

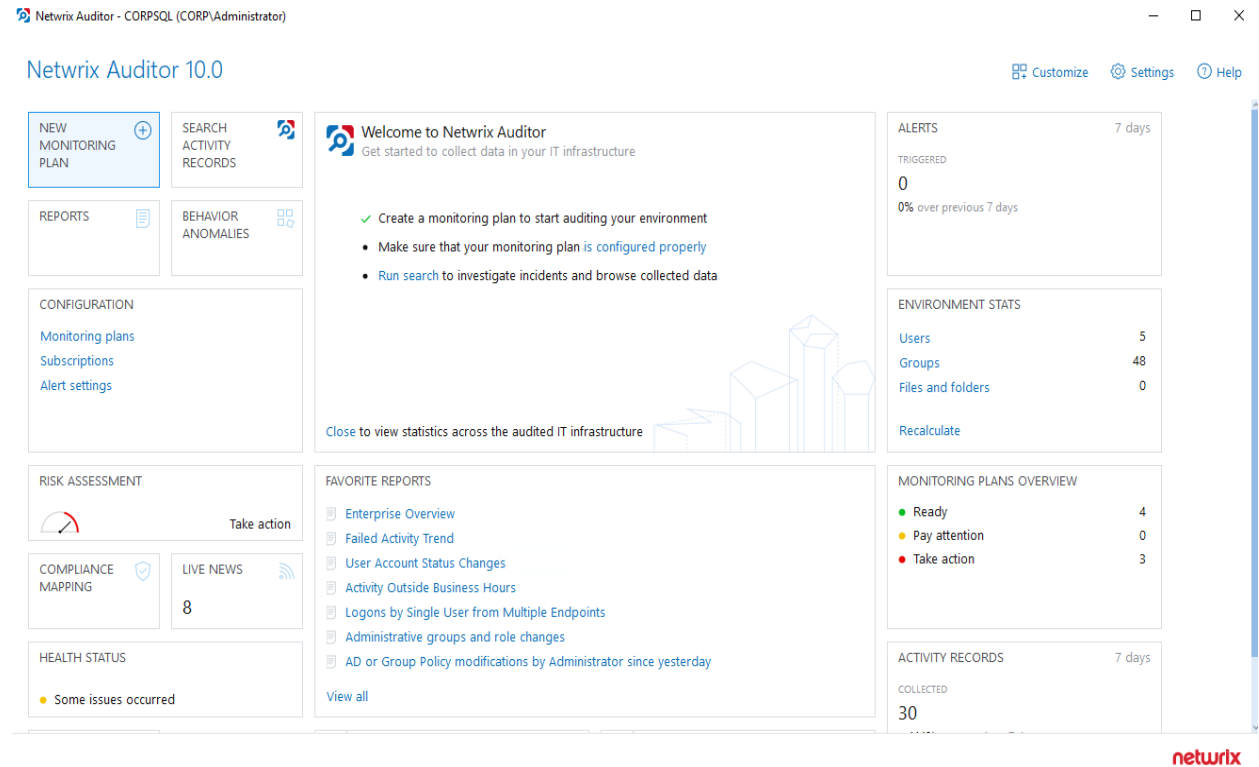


3. Follow the instructions of the setup wizard. When prompted, accept the license agreement.
4. On the **Select Installation Type** step, select **Full installation**.
5. On the **Destination Folder** step, specify the installation folder.
6. On the **Netwrix Customer Experience Program** step, you are 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. Review the following for more information about the product navigation: [First Launch](#).



6. Monitoring Plans

To start auditing your environment and analyzing user behavior with Netwrix Auditor, create a monitoring plan.

A monitoring plan defines data collection, notification, and storage settings.

To start collecting data, and add items to its scope.

So, to collect data from your environment, you need to do the following:

1. Specify a data source and create a monitoring plan with a wizard. See [Create a New Plan](#) for more information.
2. Add items to be monitored. An item is a specific object you want to audit. As soon as the item is added, to the monitoring plan, Netwrix Auditor starts collecting data from it. See [Add Items for Monitoring](#) for more information.

6.1. Using historical data

For many data sources, you can instruct Netwrix Auditor to collect state-in-time data along with event data. For that, Netwrix Auditor uses state-in-time snapshots of the relevant system (for example, see [Data Collection from VMware Servers](#)).

To keep users up-to-date on actual system state, Netwrix Auditor updates the latest snapshot on the regular basis. Thus, only the latest snapshot is available for ongoing reporting in Netwrix Auditor.

However, you may need to generate reports based on the historical data. For that, you must import the historical snapshots to the database.

NOTE: To import snapshots, you must be assigned the *Global administrator* or the *Global reviewer* role. See [Assign Roles](#) for more information.

To import historical snapshots:

1. Select the monitoring plan you need.
2. Select the required data source and click **Edit data source** on the right to open its properties.
3. Click **General** on the left.
4. In the **Manage historical snapshots** section, click **Manage**.
5. In the **Manage Snapshots** window, select the snapshots that you want to import — use the arrows to move the selected snapshots to the **Snapshots available for reporting** list. When finished, click **OK**.

6.2. Create a New Plan

On the main Netrix 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

6.2.1. Settings for Data Collection

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.

Option	Description
Specify the account for collecting data	<p>Provide a user name and a password for the account that Netrix 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 Data Collecting Account. Netrix recommends creating a special service account with extended permissions.</p> <p>NOTE: If you want to audit network devices or Azure AD/Office 365 infrastructure, you can use any account here.</p>

6.2.2. Default SQL Server Instance

To provide searching, alerting and reporting capabilities, Netrix 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 Netrix Auditor databases. To read more, refer to [SQL Server and Audit Database](#).

NOTE: Alternatively, you can instruct Netrix 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: <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. <p>NOTE: This account must be granted the database owner (db_owner) role and the dbcreator server role.</p>
Password	Enter a password.

IMPORTANT! If you want to use Group Managed Service Account (gMSA) to access the SQL Server instance hosting the database, consider that in this case Netwrix Auditor will not be able to generate SSRS-based reports (due to [Microsoft limitations](#)).

6.2.3. 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.

Audit Database

Specify the database to store your data and configure settings.

Disable security intelligence and make data available only in activity summaries

Database:

Use default SQL Server settings

Specify custom connection parameters

Authentication:

User name:

Password:

Configure the following:

Setting	Description
<p>Disable security intelligence ...</p>	<p>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.</p> <p>To store data to the database, leave this check box cleared.</p>
<p>Database</p>	<p>Default database name is <i>Netwrix_Auditor_<monitoring_plan_name></i>.</p> <p>It is recommended that you enter a meaningful name for the database here. It may include the data source type (e.g. <i>Exchange_Audit_Data</i> or <i>OracleSrv02_Audit_Data</i>), or so.</p> <p>If you decided to use the existing SQL Server instance instead of dedicated, you may want to use <i>Netwrix_Auditor</i> prefix to distinguish Netwrix Auditor databases</p>

Setting	Description
	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.

6.2.4. 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.

6.2.5. 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 **Test**. The system will send a test message to the specified email address and inform you if any problems are detected.

6.2.6. 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.

6.3. 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.

6.3.1. Computer

Complete the following fields:

Option	Description
General	
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.

6.3.2. Cisco Meraki

Complete the following fields:

Option	Description
User name	Provide the name of the service account configured to access Cisco Meraki Dashboard. For more information on how to configure the account, refer to .
Password	Provide the password for this account.

NOTE: Accounts with multi-factor authentication are not supported. Netwrix recommends creating a special cloud account to access your data securely.

6.3.3. Syslog Device

Complete the following fields:

Option	Description
General	
Specify syslog host or network source	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Host or network source name — 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. • 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 port and protocol for incoming connections	Use Port and Protocol to provide the port required for incoming connections (default is UDP port 514).

Devices

Configure monitoring rules for required network devices:

- Cisco (ASA, IOS, Meraki)
- Fortinet (FortiGate FortiOS)
- Juniper (Junos OS)
- Palo Alto (PAN-OS)
- Sonic Wall (NS, SMA, WAF)
- HPE (ArubaOS)

6.3.4. 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
General	
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.

6.4. Launch Data Collection Manually and Update Status

If you do not want to wait until a scheduled data collection, you can launch it manually.

NOTE: Not applicable to Netwrix Auditor for User Activity. For this data source, the product sends real-time data about sessions and activity.

Along with data collection, the following actions will be performed:

- An Activity Summary email will be generated and sent to the specified recipients. It will list all changes that occurred since the last scheduled or on-demand Activity Summary delivery.
- Changes that occurred between data collections will be written to the Long-Term Archive and the Audit Database, and become available in the Netwrix Auditor client.
- A state-in-time data will be updated.

To launch data collection manually

1. Navigate to **All monitoring plans** → your monitoring plan, select **Edit**.
2. In the right pane, click **Update**.

NOTE: Depending on the size of the monitored environment and the number of changes, data collection may take a while.

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.

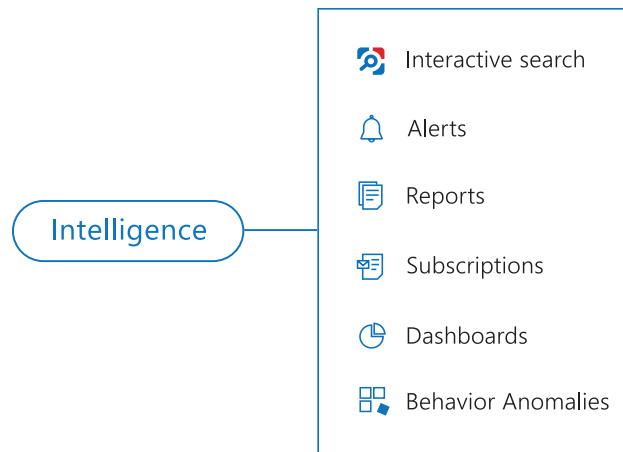
NOTE: Before making any test changes to your environment, ensure that you have the sufficient rights, and that the changes conform to your security policy.

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

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 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: not "Session". The search results table shows one entry:

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

The details pane on the right shows the following information:

- Activity record details:**
 - Data source: Network Devices
 - Monitoring plan: Network Devices
 - Item: CiscoIOS (Computer)
 - Workstation: Workstation16
- Details:**
 - Action name: Login failed
 - Received from: 172.28.62.118
 - Priority: 189
 - Severity: 5 (Notice)
 - Source: CISCO IOS
 - Facility: 23 (Local use 7)
 - Reason: Login Authentication Failed
 - Local Port: 23
 - Monitoring rule: Cisco IOS: authentication attempts
 - Original message: <189>15: 000020: 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

Configuration changes on network devices:

The screenshot shows the Netrix Auditor search interface. The search criteria are: Data source: "Network Devices", Action: "Modified", Object type: "Configuration". The search results table shows one entry:

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

The details pane on the right shows the following information:

- Activity record details:**
 - Data source: Network Devices
 - Monitoring plan: Network Devices
 - Item: CiscoIOS (Computer)
- Details:**
 - Action name: Line protocol updown
 - Received from: 172.28.62.118
 - Priority: 189
 - Severity: 5 (Notice)
 - Source: CISCO IOS
 - Interface: FastEthernet0/1
 - Facility: 23 (Local use 7)
 - State: down
 - 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
- User account details:**
 - Account: system

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.

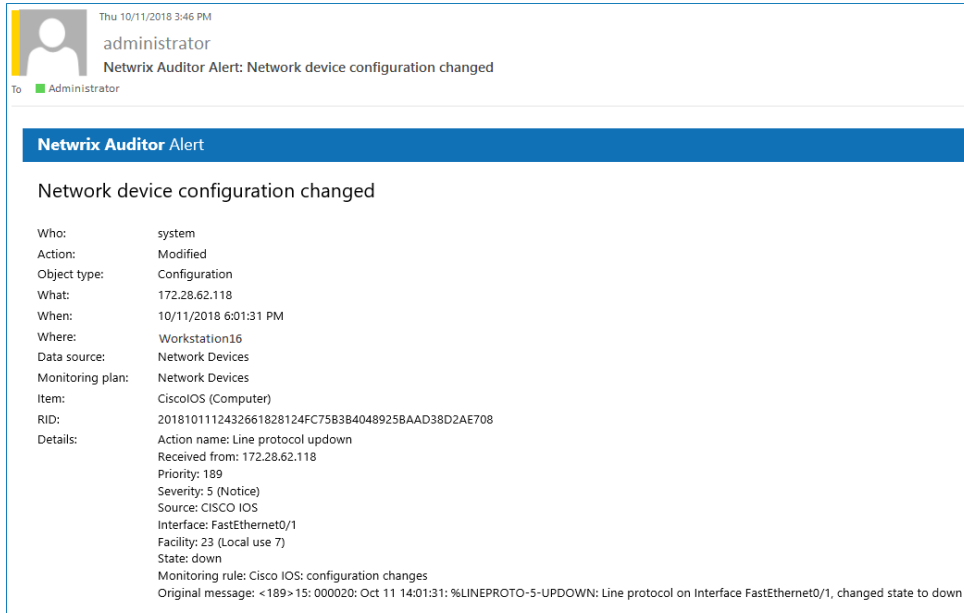
Your **Search** field will be updated, the **Object type not** filter will be added. Make sure to click **Search** again to update your search results.

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

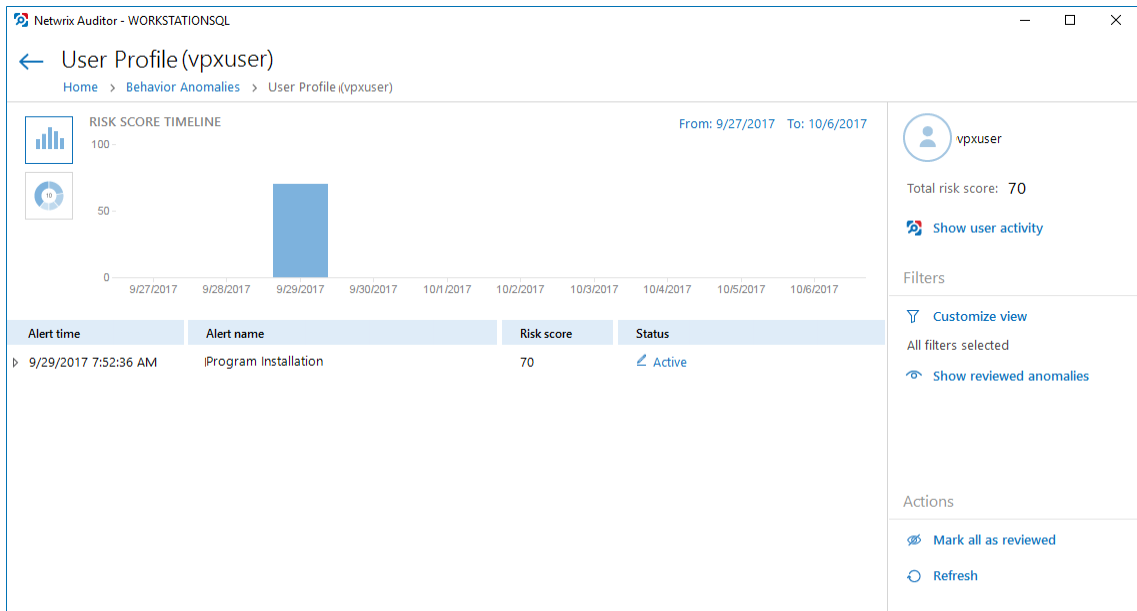
5. Having reviewed your search results, navigate to **Tools**.
 - Click **Save as report** to save the selected set of filters. This search will be added to the **Custom** section inside **Reports**, so that you will be able to access it instantly. Refer to [Custom Search-Based Reports](#) for detailed 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 Netrix 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 [Netrix 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 10, and suggests workarounds for these issues.

10. Glossary

M

My Term

My definition

11. Index

	A
Activity Summary	40
	C
Checklist	12
Configure audit	
NDA	13
	D
Data Collection	
Launch data collection manually	38, 40
Data sources	6
	E
Environment	6
	I
Install	
Netwrix Auditor	6, 28
System requirements	6
Items	35
Computer	35
IP Range	37
	M
Make Changes	39
Monitoring plan	
Add item	35
New	31
Overview	30
	N
NDA	13

	O
Overview 5	
	R
Related Documentation 46	
	S
System requirements 6, 9	
Hardware requirements 9	
Software requirements 10	
	U
Update status 38	