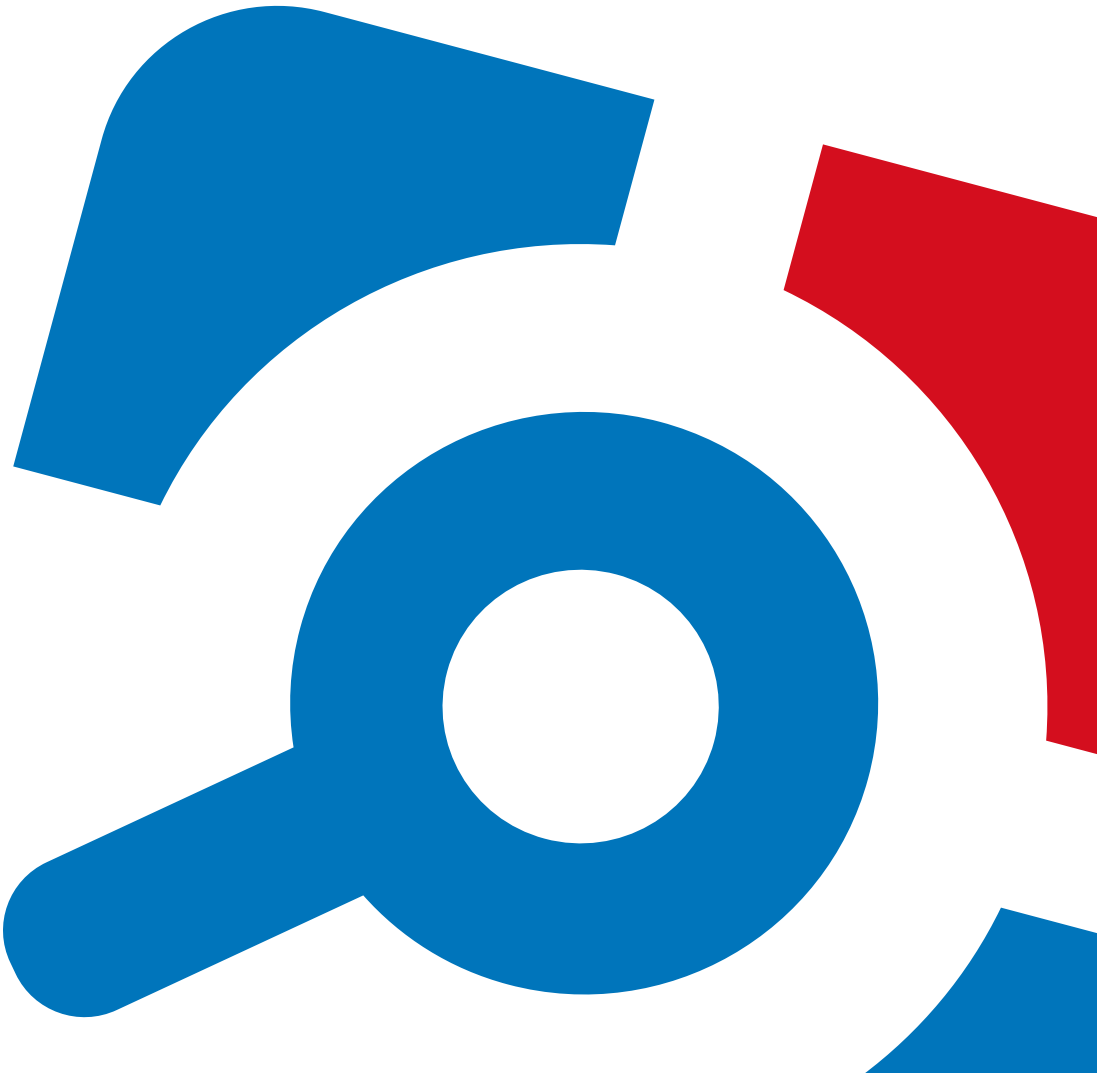
netwrix

Netwrix Auditor for Oracle Database

Quick-Start Guide

Version: 9.7
12/24/2018



Legal Notice

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

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

Disclaimers

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

Table of Contents

1. Introduction

This guide is intended for the first-time users of Netwrix Auditor for Oracle Database. 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 Oracle Database
- Launch data collection
- See how Netwrix Auditor enables complete visibility

NOTE: This guide only covers the basic configuration and usage options for auditing Oracle Database 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 Auditor Installation and Configuration Guide
- Netwrix Auditor Administration Guide
- Netwrix Auditor Intelligence Guide

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, and Windows Server. Empowered with a RESTful API and user activity video recording, 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.

Netwrix Auditor for Oracle Database detects and reports on all changes made to your Oracle Database instance configuration, privileges, and security settings, including database objects and directories, user

accounts, audit policies, sensitive data, and triggers. The product also reports on failed and successful access attempts.

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 Oracle Database:

Data source	Supported Versions
Network Devices	**Cisco devices** • Cisco ASA (Adaptive Security Appliance) 8 and above • Cisco IOS (Internetwork Operating System) 12 and 15 **Syslog devices** • Red Hat Enterprise Linux 7 and 6 • SUSE Linux Enterprise Server 12 • OpenSUSE 42 • Ubuntu 16, 17, 18 NOTE: Red Hat Enterprise Linux 7 and 6, SUSE Linux Enterprise Server 12, openSUSE 42, and Ubuntu (16, 17, 18) are supported out of the box. For other distributions, deployment of rsyslog package may be required. **Fortinet Fortigate** • FortiOS 5, 6
Oracle Database	• Oracle Database 11g

Data source	Supported Versions
	• Oracle Database 12c On-Premise (all editions) • Oracle Database Cloud Service (Enterprise Edition)

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 Oracle Database. Refer to Netwrix Online Helpcenter 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

Hardware component	Starter, evaluation, or small environment
	Recommended 1920 x 1080 or higher

2.2.2. Software Requirements

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

Component	Requirements
Operating system	Windows Server OS: • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 R2 SP1 Windows Desktop OS (64-bit): • Windows 10 • Windows 8.1 • Windows 7 SP1
.NET Framework	• .NET Framework 3.5 SP1. **NOTE:** To audit VMware vSphere 6.7 or 6.5, .NET Framework 4.5 or 4.6 is required.
Installer	• Windows Installer 3.1 and above

2.2.2.1. Additional Components

In order to monitor some data sources, you may be required to install additional software components.

Data source	Components
• Oracle Database	***On the computer where Netwrix Auditor Server is installed:*** • Microsoft Visual C++ 2010 Redistributable Package—can be installed automatically during the monitoring plan creation. • Oracle Data Provider for .NET and Oracle Instant Client

Data source	Components
	Netwrix recommends downloading the package 64-bit Oracle Data Access Components 12c Release 4 (12.1.0.2.4) for Windows x64 (ODAC121024_x64.zip). Run the setup and select the **Data Provider for .NET** checkbox. Oracle Instant Client will be installed as well. Also, make sure the **Configure ODP.NET and/or Oracle Providers for ASP.Net at machine-wide level** checkbox is selected on the **ODP.NET (Oracle Data Provider)** step.

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
Network and target systems or servers that work as your data sources	Test connectivity to your data source. Make sure you can access it by its NetBIOS and FQDN name from the computer where you intend to install Netwrix Auditor—use the nslookup command-line tool to look up domain names.
SQL Server with Reporting Services (or Advanced Services) 2008 or higher.	Supported SQL Server versions are listed here. Consider maximum database size in different versions. Make your choice based on the size of the environment you are going to monitor, the number of users, and other factors. Remember that maximum database size in Express editions may be insufficient. **NOTE:** Although Netwrix Auditor provides a convenient way to download SQL Server 2014 Express edition right from the product, it is recommended to deploy SQL Server instance in advance. If installed separately, remember to test SQL Server connectivity.

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

3.1. Configure Data Collecting Account

This service account is specified on the monitoring plan creation and is used to collect audit data from the data source items. To ensure successful data collection, Netwrix recommends creating a special service

account in advance. The account must comply with the following requirements depending on the data source.

NOTE: The information in this section is outside the quick-start guide scope and is provided for reference only. See Netwrix Auditor Installation and Configuration Guide for detailed instructions on how to configure your Data Processing Account.

Data source	Rights and permissions
Network Devices	No special configuration required.
Oracle Database	***On the target server:*** • The `CREATE SESSION` system privilege must be granted to an account used to connect to Oracle Database • Depending on your Oracle Database version, the `SELECT` privilege on the following objects must be granted to an account used to connect to Oracle Database: **Oracle Database 11g** • `aud$` • `gv_$xml_audit_trail` • `dba_stmt_audit_opts` • `v_$parameter` • `dba_obj_audit_opts` • `dba_audit_policies` • `dba_audit_mgmt_clean_events` • `gv_$instance` • `fga_log$` **Oracle Database 12c** In addition to the privileges above, add the `SELECT` privilege on the following objects: • `gv_$unified_audit_trail` • `all_unified_audit_actions` • `audit_unified_policies` • `audit_unified_enabled_policies` For Oracle Database 12c Release 2, also grant the `SELECT` privilege on the following object: `audsys.aud$unified` **NOTE:** If you are going to configure Fine Grained Auditing, grant privileges,

Data source	Rights and permissions
	depending on your Oracle Database version, and make sure that you use Oracle Database Enterprise Edition. Alternatively, you can grant the default administrator role to an account.

4. Configure Oracle Database for Monitoring

Before you start monitoring your Oracle Database with Netwrix Auditor, arrange your environment. Depending on your current database version and edition, Oracle provides different types of auditing:

- **Standard Auditing**—For Oracle Database 11g. In Standard Auditing, you use initialization parameters and the `AUDIT` and `NOAUDIT` SQL statements to audit SQL statements, privileges, schema objects, network and multitier activities. See Configure Oracle Database 11g for Auditing for more information.
- **Unified Auditing**—Recommended for Oracle Database 12c. Unified Auditing consolidates all auditing into a single repository and view. This provides a two-fold simplification: audit data can now be found in a single location and all audit data is in a single format. See Configure Oracle Database 12c for Auditing for more information.
- **Fine Grained Auditing**—Available for Oracle Database Enterprise Edition only. Allows auditing of actions associated with columns in application tables along with conditions necessary for an audit record to be generated. It helps focus on security-relevant columns and rows and ignore areas that are less important. See Configure Fine Grained Auditing for more information.

If you are unsure of your audit settings, refer to the following section:

- Verify Your Oracle Database Audit Settings

Also, remember to do the following:

1. Configure Data Collecting Account, as described in Grant Create Session and Select Privileges to Account
2. Configure required protocols and ports, as described in Protocols and Ports Required for Monitoring Oracle Database

4.1. Configure Oracle Database 11g for Auditing

Perform the following steps to configure Standard Auditing on your Oracle Database:

- Select audit trail to store audit records. The following options are available in Oracle Database:

Audit trail	Description
Database audit trail	Set by default.
XML audit trail	Netwrix recommends to store audit records to XML audit trail. In this case, the product will report on actions performed by users with `SYSDBA` and `SYSOPER` privileges. Otherwise, these actions will not be audited.
OS files	Current version of Netwrix Auditor does not support this configuration.

- Enable auditing of selected Oracle Database parameters.

To select audit trail to store audit records

1. On the computer where your database is deployed, run the **sqlplus** tool.
2. Connect to your Oracle Database—use Oracle account with the `SYSDBA` privilege. For example:

   ```
   OracleUser as sysdba
   ```

   Enter your password.
3. Select where to store audit records.

   Review the following for additional information:

To...	Execute the following command...
Store audit records to database audit trail. This is default configuration for Oracle Database. NOTE: If you want to store audit records to database audit trail, do not run this command.	`ALTER SYSTEM SET audit_trail=DB SCOPE=SPFILE;` NOTE: In this case, actions performed by user `SYS` and users connecting with `SYSDBA` and `SYSOPER` privileges will not be audited.

Store audit records to XML audit trail.	`ALTER SYSTEM SET audit_trail=XML SCOPE=SPFILE;`
	
	NOTE: If you want to enable auditing of actions performed by user `SYS` and users connecting with `SYSDBA` and `SYSOPER` privileges, execute the following command:
	`ALTER SYSTEM SET audit_sys_operations=TRUE SCOPE=SPFILE;`

To...	Execute the following command...

Store audit records to XML or database audit trail and keep full text of SQL-specific query in audit records.
 	
NOTE: Only `ALTER` actions will be reported.
	For database audit trail:
	`ALTER SYSTEM SET audit_trail=DB, EXTENDED SCOPE=SPFILE;`
	
	For XML audit trail:
	`ALTER SYSTEM SET audit_trail=XML, EXTENDED SCOPE=SPFILE;`

4. Restart the database:

```
SHUTDOWN IMMEDIATE

STARTUP
```

NOTE: You do not need to restart the database if you changed auditing of objects. You only need to restart the database if you made a universal change, such as turning on or off all auditing. If you use Oracle Real Application Clusters (RAC), see the Starting and Stopping Instances and Oracle RAC Databases section in **Real Application Clusters Administration and Deployment Guide** for more information on restarting your instances.

To enable auditing of Oracle Database changes

1. On the computer where your database is deployed, run the **sqlplus** tool.
2. Connect to your Oracle Database—use Oracle account with the `SYSDBA` privilege. For example:

   ```
   OracleUser as sysdba
   ```

   Enter your password.
3. Enable auditing of selected parameters.

   Review the following for additional information:

To monitor...	Execute the command...

Configuration changes	• For any user:
	`AUDIT ALTER SYSTEM,SYSTEM AUDIT,SESSION,TABLE,USER, VIEW,ROLE,PROCEDURE,TRIGGER,PROFILE,DIRECTORY, MATERIALIZED VIEW,SYSTEM GRANT,NOT EXISTS, ALTER TABLE,GRANT DIRECTORY,GRANT PROCEDURE, GRANT TABLE;`
	
	`AUDIT ALTER DATABASE, FLASHBACK ARCHIVE ADMINISTER;`
	
	• For specific user:
	`AUDIT SYSTEM GRANT, SESSION, TABLE, PROCEDURE BY`

To monitor...	Execute the command...
	`<USER_NAME>;` **NOTE:** You can specify several users separated by commas.
Successful and failed data access and changes	`AUDIT SELECT,INSERT,DELETE,UPDATE,RENAME, FLASHBACK ON <TABLE_NAME>;`

NOTE: After an audit parameter has been enabled or disabled, the product starts collecting data after succeeding logon session.

For additional information on `ALTER SYSTEM` and `AUDIT` parameters, see the following Oracle database administration documents:

- `AUDIT_TRAIL`
- `AUDIT`

Currently, Netwrix Auditor checks audit settings for Standard Auditing when configured to audit specified operations. If any of your current settings conflict with the audit configuration required for Netwrix Auditor, these conflicts will be listed in the **Netwrix Auditor System Health** event log.

4.2. Configure Oracle Database 12c for Auditing

The following auditing modes are available for Oracle Database 12c:

- **Mixed Mode**—Default auditing in a newly installed database. It enables both traditional and the new Unified audit facilities. Netwrix recommends not to use Mixed Mode auditing together with Netwrix Auditor. If you want to leave it as it is, make sure that your audit records are stored to the XML audit trail, otherwise Netwrix Auditor will not be able to collect changes made with `SYSDBA` or `SYSOPER` privilege.

  NOTE: The product does not log any errors on these events to the **Netwrix Auditor System Health** log.

- **Unified Auditing**—Recommended. See the following Oracle technical article for detailed instructions on how to enable Unified Auditing: Enabling Unified Auditing.

  Perform the following steps to configure Unified Auditing on your Oracle Database:

  - Create and enable an audit policy to audit specific parameters across your Oracle Database.

    NOTE: After an audit policy has been enabled or disabled, the product starts collecting data after succeeding logon session.

  - If needed, create and enable specific audit policies to audit successful data access and changes, user actions, component actions, etc.

To configure Oracle Database 12c Unified Auditing

1. On the computer where your database is deployed, run the **sqlplus** tool.
2. Connect to your Oracle Database—use Oracle account with the `SYSDBA` privilege. For example:

   ```
   OracleUser as sysdba
   ```

   Enter your password.

3. Create and enable audit policies. Review the following for additional information:

To monitor...	Execute the command...
Configuration changes	• Create an audit policy (e.g., `nwx_actions_pol`) for any user: `CREATE AUDIT POLICY nwx_actions_pol ACTIONS CREATE TABLE,DROP TABLE,ALTER TABLE,GRANT,REVOKE, CREATE VIEW,DROP VIEW,CREATE PROCEDURE, ALTER PROCEDURE,RENAME,AUDIT,NOAUDIT, ALTER DATABASE,ALTER USER,ALTER SYSTEM, CREATE USER,CREATE ROLE,SET ROLE,DROP USER, DROP ROLE,CREATE TRIGGER,ALTER TRIGGER, DROP TRIGGER,CREATE PROFILE,DROP PROFILE, ALTER PROFILE,DROP PROCEDURE, CREATE MATERIALIZED VIEW,DROP MATERIALIZED VIEW, ALTER ROLE,TRUNCATE TABLE,CREATE FUNCTION, ALTER FUNCTION,DROP FUNCTION,CREATE PACKAGE, ALTER PACKAGE,DROP PACKAGE,CREATE PACKAGE BODY, ALTER PACKAGE BODY,DROP PACKAGE BODY,LOGON,LOGOFF, CREATE DIRECTORY,DROP DIRECTORY,CREATE JAVA, ALTER JAVA,DROP JAVA,PURGE TABLE, CREATE PLUGGABLE DATABASE,ALTER PLUGGABLE DATABASE, DROP PLUGGABLE DATABASE,CREATE AUDIT POLICY, ALTER AUDIT POLICY,DROP AUDIT POLICY, CREATE FLASHBACK ARCHIVE,ALTER FLASHBACK ARCHIVE, DROP FLASHBACK ARCHIVE;` • Enable the audit policy: `AUDIT POLICY nwx_actions_pol;`

Data access and changes (successful and failed)	• Create the audit policy (e.g., `nwx_actions_obj_pol`):
	`CREATE AUDIT POLICY nwx_actions_obj_pol ACTIONS DELETE on hr.employees, INSERT on hr.employees, UPDATE on hr.employees, SELECT on hr.employees, FLASHBACK on hr.employees CONTAINER = CURRENT;`
	• Enable the audit policy (e.g., `nwx_actions_obj_pol`):
	`AUDIT POLICY nwx_actions_obj_pol;`

Component actions: `Oracle Data Pump`, `Oracle Recovery Manager`, and `Oracle SQL*Loader`	• Create the audit policies (e.g., `nwx_sqlloader_dp_pol`, etc.):
	NOTE: No special configuration required to audit RMAN events.
	`CREATE AUDIT POLICY nwx_datapump_expimp_pol ACTIONS COMPONENT=DATAPUMP ALL;`
	`CREATE AUDIT POLICY nwx_sqlloader_dp_pol ACTIONS COMPONENT=DIRECT_LOAD LOAD;`

To monitor...	Execute the command...

Direct Path Load	• Enable these policies:
	`AUDIT POLICY nwx_datapump_expimp_pol;`
	`AUDIT POLICY nwx_sqlloader_dp_pol;`

For additional information on `CREATE AUDIT POLICY` and `AUDIT POLICY` parameters, see the following Oracle Database administration documents:

- `CREATE AUDIT POLICY`
- `AUDIT POLICY`

Currently, Netwrix Auditor checks audit settings for Unified Auditing when accomptability is enabled for `ACTIONS`. If any of your current settings conflict with the audit configuration required for Netwrix Auditor, these conflicts will be listed in the **Netwrix Auditor System Health** event log.

4.3. Configure Fine Grained Auditing

When configuring Fine Grained Auditing, you need to create an audit policy with required parameters set. The procedure below contains instructions on how to create, disable and delete such audit policies.

NOTE: Fine Grained audit policies can be configured for Oracle Database Enterprise Edition only. Keep in mind that if you have Fine Grained policies configured, you will receive a permanent error in the **Netwrix Auditor System Health** log because Netwrix Auditor cannot detect it. Use Unified and Standard audit policies to keep track of data changes.

To configure Fine Grained Auditing

Below is an example of Fine Grained audit policy that enables auditing of audit statements `(INSERT, UPDATE, DELETE,` and `SELECT)` on table `hr.emp` to audit any query that accesses the `salary` column of the employee records that belong to `sales` department. Review the following for additional information:

To...	Execute the following command...
To create audit policy	`EXEC DBMS_FGA.ADD_POLICY(object_schema => 'hr', object_name => 'emp', policy_name => 'chk_hr_emp', audit_condition => 'dept = ''SALES'' ', audit_column => 'salary', statement_types => 'INSERT,UPDATE,DELETE,SELECT');`
To disable audit policy	`EXEC DBMS_FGA.DISABLE_POLICY(object_schema => 'hr', object_name =>'emp', policy_name => 'chk_hr_emp');`
To delete audit policy	`EXEC DBMS_FGA.DROP_POLICY(object_schema => 'hr', object_name =>'emp', policy_name => 'chk_hr_emp');`

NOTE: Refer to Oracle documentation for additional information on Fine Grained Auditing.

4.4. Verify Your Oracle Database Audit Settings

You can verify your Oracle Database audit settings manually. Do one of the following, depending on your Oracle Database version and edition.

Oracle Database version/edition	Command

Oracle Database 11g (Standard Auditing)	`SELECT audit_option, success, failure FROM dba_stmt_audit_opts;`
	
	NOTE: To review your initialization parameters, execute the following command:
	`SHOW PARAMETERS audit%r;`

Oracle Database 12c (Unified Auditing)	`select USER_NAME, ENABLED_OPT, SUCCESS, FAILURE from AUDIT_UNIFIED_ENABLED_POLICIES;`
Oracle Database Enterprise Edition (Fine Grained Auditing)	`SELECT POLICY_NAME, ENABLED from DBA_AUDIT_POLICIES;`

NOTE: If you want to clean your audit settings periodically, refer to the following Oracle Help Center article for more information: Database PL/SQL Packages and Types Reference.

5. 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 Linux-based Systems
- Configure Fortinet FortiGate Devices

5.1. 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
   ```

5.2. 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 audited Cisco ASA device 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
   ```

5.3. Configure Linux-based Systems

Configure your systems, depending on your Linux distribution. Review the following for additional information:

- To configure Red Hat Enterprise Linux system
- To configure other Linux-based systems

To configure Red Hat Enterprise Linux system

1. Open the **/etc/rsyslog.conf** file.
2. Add the following line:

   ```
   *.* @name:port;RSYSLOG_SyslogProtocol23Format
   ```

   Where `name` is a FQDN, NetBIOS name or IP address of the computer where Netwrix Auditor Server is installed and `port` is a listened port.

   For example: `*.* @172.28.18.25:514;RSYSLOG_SyslogProtocol23Format`
3. Launch the **RHEL** console and execute the following command: `service rsyslog restart`.

To configure other Linux-based systems

1. Open the **/etc/rsyslog.d/50-default.conf** file.
2. Add the following line:

   ```
   *.* @name:port;RSYSLOG_SyslogProtocol23Format
   ```

   Where `name` is a FQDN, NetBIOS name or IP address of the computer where Netwrix Auditor Server is installed and `port` is a listened port.

For example: `*.* @172.28.18.25:514;RSYSLOG_SyslogProtocol23Format`

3. Launch the **UBUNTU** console and execute the following command: `service rsyslog restart`.

5.4. 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:

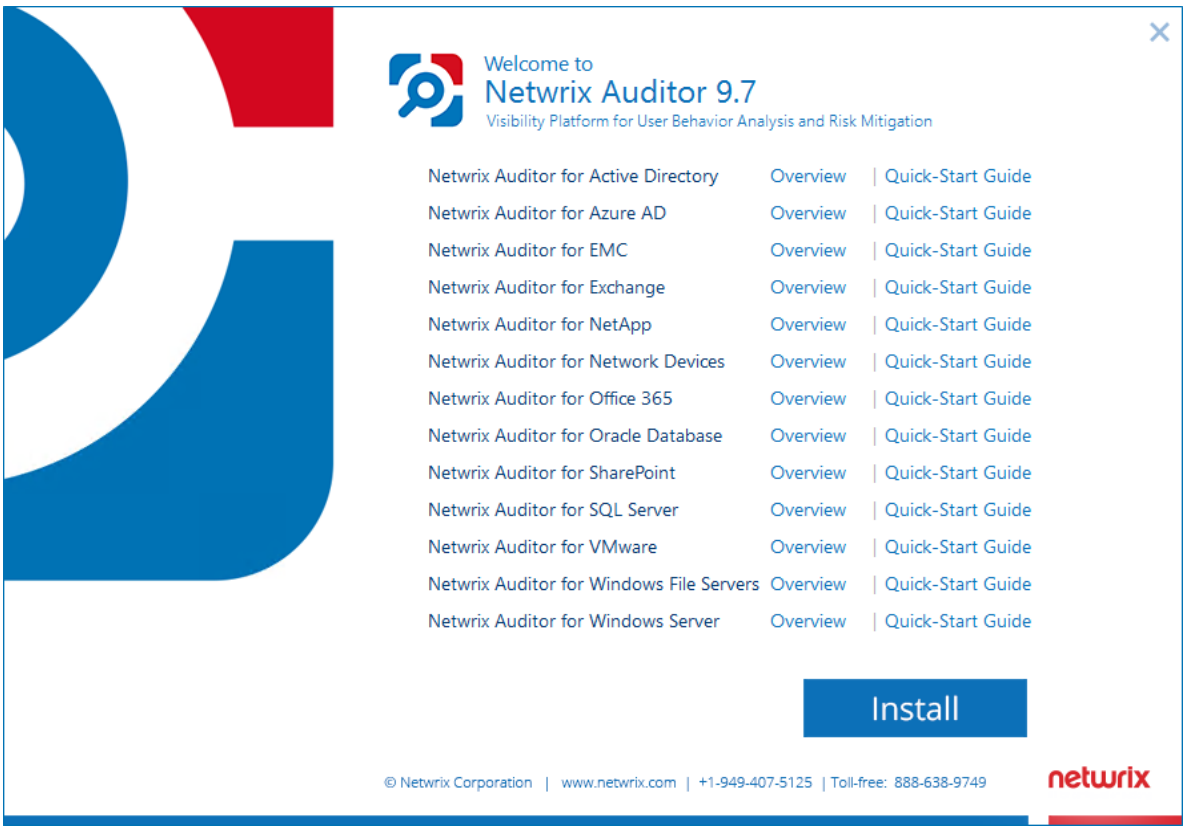
Option	Description
Name/IP	Enter the hostname or IP address of the Receiver.
Port	Set to *"514"*.
Level	Select desired logging level.
Facility	Netwrix recommends using default values.
Data format	Select **CEF**. NOTE: To enable CEF format in some previous FortiOS versions, unselect the **Enable CSV**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

4. Click **Apply**.

6. Install the Product

To install Netwrix Auditor

1. Download Netwrix Auditor 9.7 from Netwrix website.
2. Unpack the installation package. The following window will be displayed on successful operation completion:

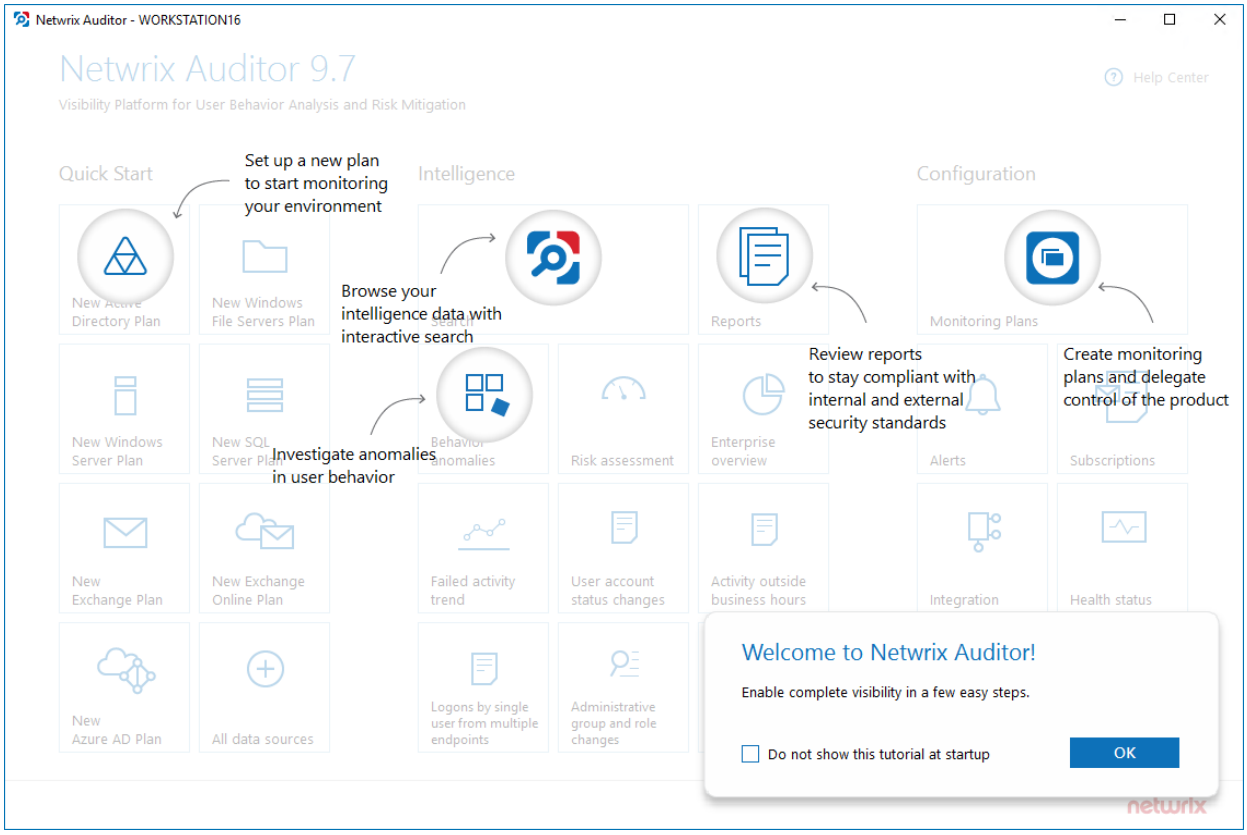


3. Follow the instructions of the setup wizard. When prompted, accept the license agreement.
4. On the **Select Installation Type** step, select **Full installation**.
5. On the **Destination Folder** step, specify the installation folder.
6. On the **Netwrix Customer Experience Program** step, you are 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.



7. Monitoring Plans

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

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

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

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

7.1. Create a New Plan

On the main Netwrix Auditor page, click the **All data sources**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:

- Choose a data source for monitoring
- 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

7.1.1. New Monitoring Plan (Data Source)

Specify the **Oracle Database** tile.

7.1.2. New Monitoring Plan

Option	Description
Specify the account for	Provide a user name and a password for the account that Netwrix Auditor

Option	Description
collecting data	will use to collect data. By default, the user name is prepopulated with your account name. Make sure the account has sufficient permissions to collect data. For a full list 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.

7.1.3. 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: • 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.

7.1.4. 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.

7.1.5. 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.
Sender address	Enter the address that will appear in the **From** field. NOTE: It is recommended to click **Send Test Email**. 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 authentication	Select this checkbox if the implicit SSL mode is used, which means that an SSL connection is established before any meaningful data is sent.
Enforce certificate validation to ensure security	Select this checkbox if you want to verify security certificate on every email transmission.

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

7.1.7. 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.

Oracle Database data source requires additional system components and updates to be installed on your computer. If you have not installed them before, Netwrix Auditor will inform you and prompt you to check data source prerequisites instead of adding an item. Review required components on the **Oracle Database** data source page, deploy them, and then click **Save&Close**. You will see your newly created plan; click **Add item** under your **Oracle Database** data source.

NOTE: Netwrix Auditor for Oracle Database incompatible with Oracle Data Access Components for .Net Framework 4.0 and above. Check that the .Net Framework 3.5 feature is enabled prior to downloading prerequisites.

7.2. 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.

7.2.1. Oracle Database Instance

Complete the following fields:

Option	Description
Specify Oracle Database instance	Provide connection details in the following format: *host:port/service_name*. Make sure audit settings are configured for your Oracle Database instance.
Specify the account for collecting data	Select the account that will be used to collect data for this item.

8. 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.

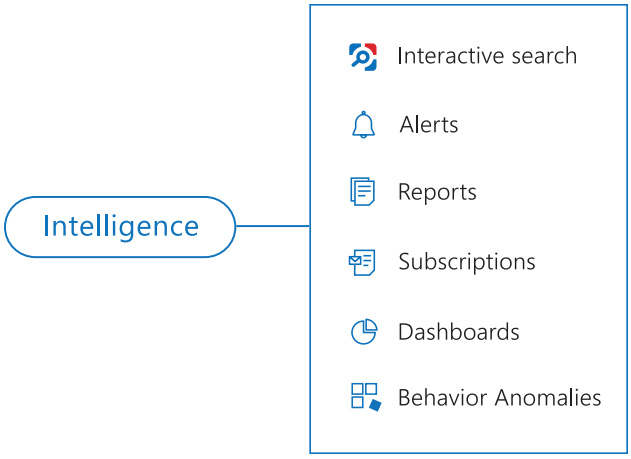
For example, make the following test changes:

- Create a new user
- Create a new role
- 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.

9. 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
- Review Oracle Database Overview
- Review the All Oracle Database Activity by User Report
- Browse Data with Intelligence Search

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

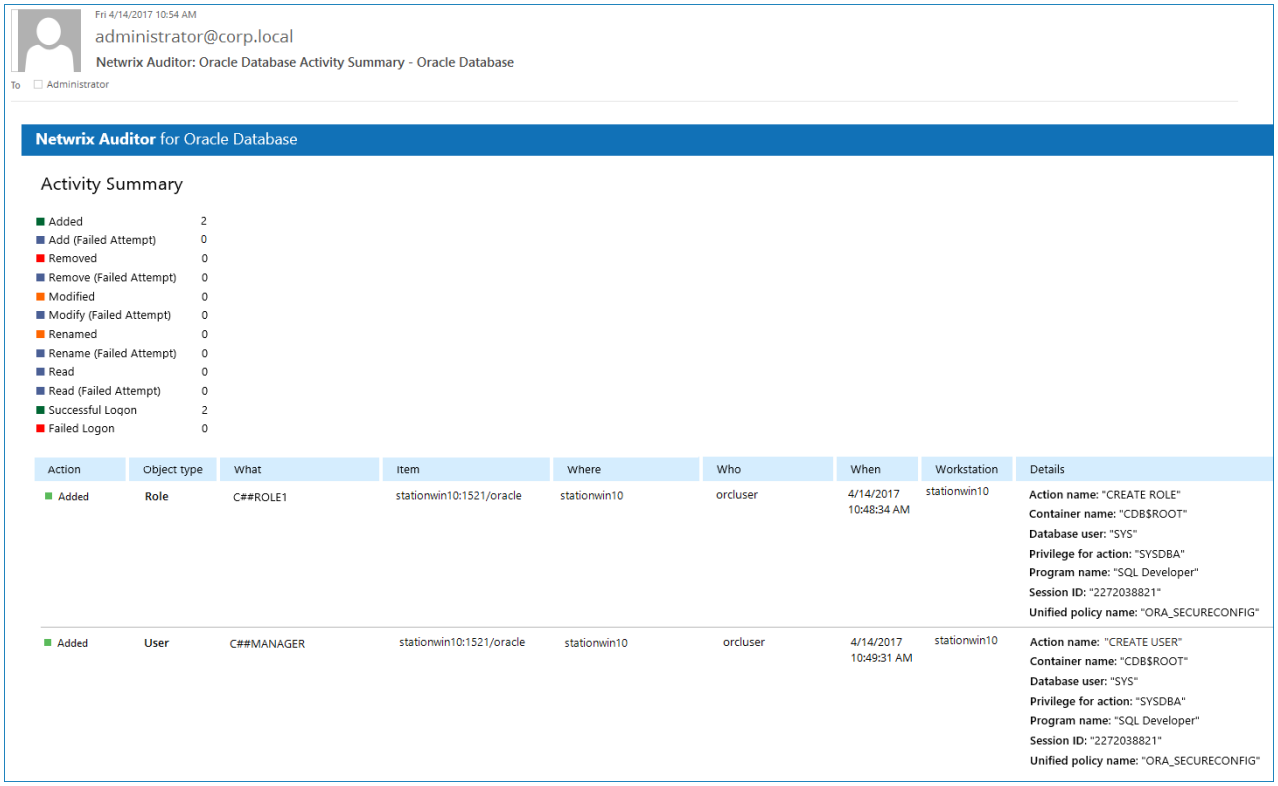
To launch data collection manually

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.

9.1. 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:



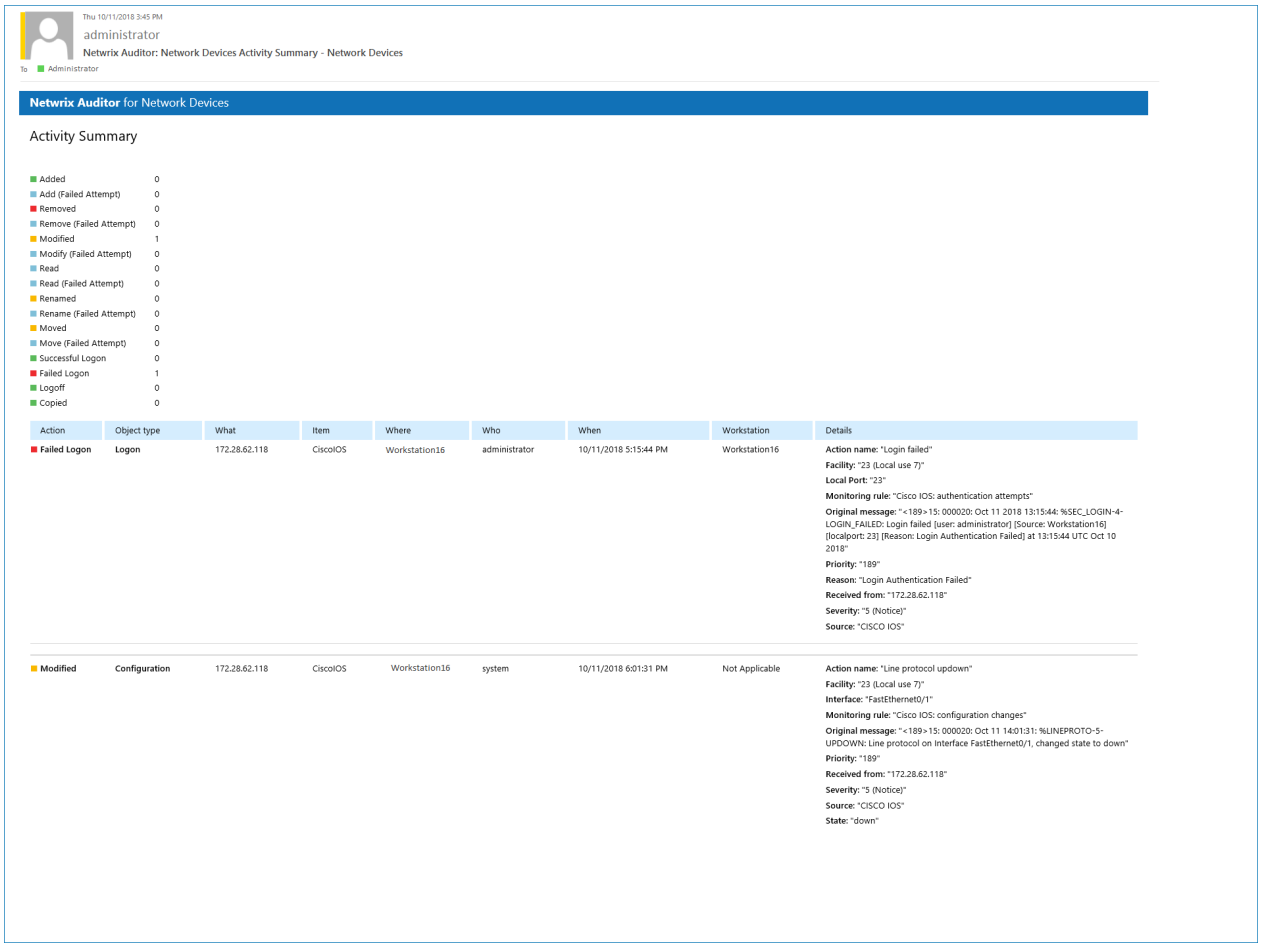
Fri 4/14/2017 10:54 AM
administrator@corp.local
Netwrix Auditor: Oracle Database Activity Summary - Oracle Database
To Administrator

Netwrix Auditor for Oracle Database

Activity Summary

Added	2
Add (Failed Attempt)	0
Removed	0
Remove (Failed Attempt)	0
Modified	0
Modify (Failed Attempt)	0
Renamed	0
Rename (Failed Attempt)	0
Read	0
Read (Failed Attempt)	0
Successful Logon	2
Failed Logon	0

Action	Object type	What	Item	Where	Who	When	Workstation	Details
Added	Role	C##ROLE1	stationwin10:1521/oracle	stationwin10	orcluser	4/14/2017 10:48:34 AM	stationwin10	**Action name:** "CREATE ROLE" **Container name:** "CDB$ROOT" **Database user:** "SYS" **Privilege for action:** "SYSDBA" **Program name:** "SQL Developer" **Session ID:** "2272038821" **Unified policy name:** "ORA_SECURECONFIG"
Added	User	C##MANAGER	stationwin10:1521/oracle	stationwin10	orcluser	4/14/2017 10:49:31 AM	stationwin10	**Action name:** "CREATE USER" **Container name:** "CDB$ROOT" **Database user:** "SYS" **Privilege for action:** "SYSDBA" **Program name:** "SQL Developer" **Session ID:** "2272038821" **Unified policy name:** "ORA_SECURECONFIG"



Thu 10/11/2018 3:45 PM

administrator

Netwrix Auditor: Network Devices Activity Summary - Network Devices

To Administrator

Netwrix Auditor for Network Devices

Activity Summary

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

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

The example Activity Summary provides 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 Oracle Database instance where the change occurred.
Who	Shows the name of the account under which the change was made.
When	Shows the exact time when the change occurred.
Workstation	Shows the name 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.

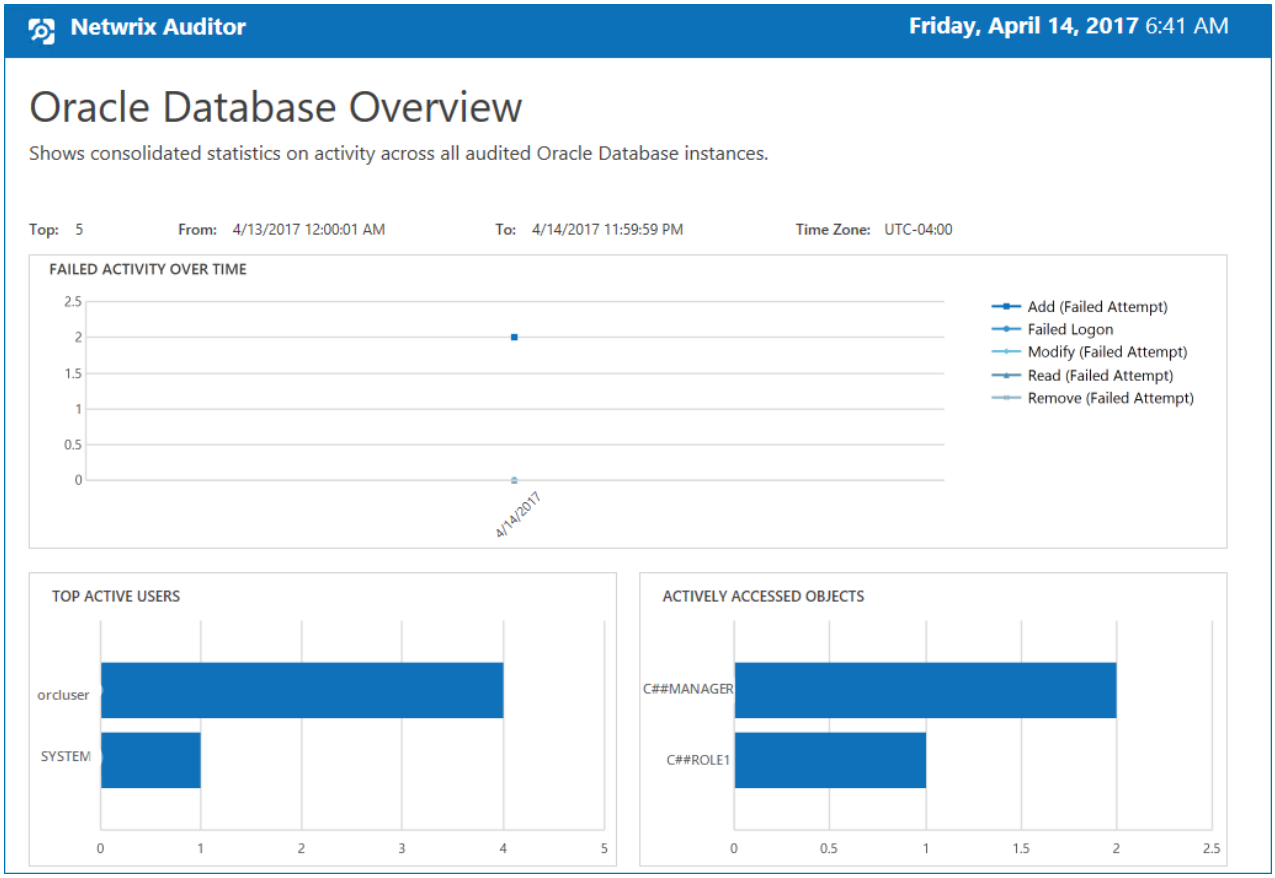
9.2. Review Oracle Database Overview

Enterprise diagram provides a high-level overview of activity trends by date, user, server, object type or data source in your IT infrastructure. The **Enterprise** diagram aggregates data on all monitoring plans and all data sources, while system-specific diagrams provide quick access to important statistics within one data source.

After collecting initial data, making test changes to your environment and running data collection again, you can get at-a-glance statistics for changes with the **Oracle Database Overview**.

To see how your changes are reported with Oracle Database Overview

1. On the main Netwrix Auditor page, navigate to the **Intelligence** section and click the **Reports** tile.
2. Expand the **Predefined** → **Oracle Database** reports.
3. Select the **Oracle Database Overview** report and click **View**.
4. Review your changes.
5. Click on any chart to jump to a table report with the corresponding grouping and filtering of data.



9.3. Review Network Devices Reports

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

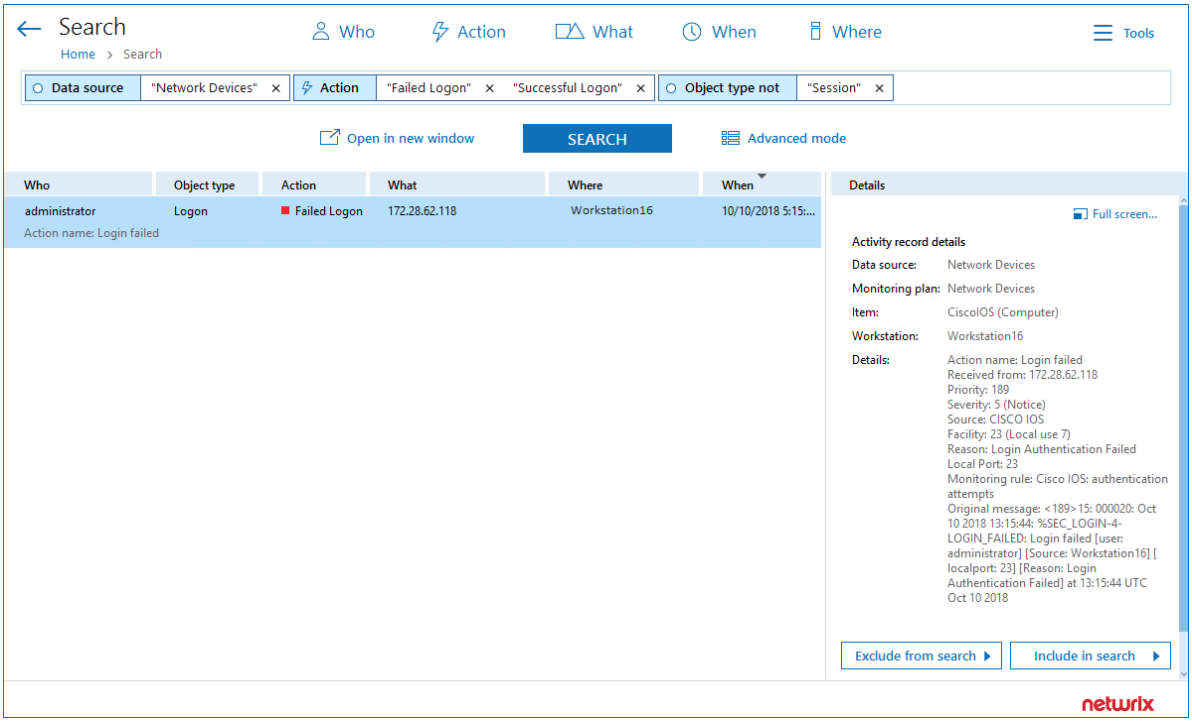
Change and activity reports can be found under the **Reports → Predefined → Network Devices** and provide a narrower insight into what is going on in the audited infrastructure and help you stay compliant with various standards and regulations (FISMA, HIPAA, PCI, SOX, etc.).

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

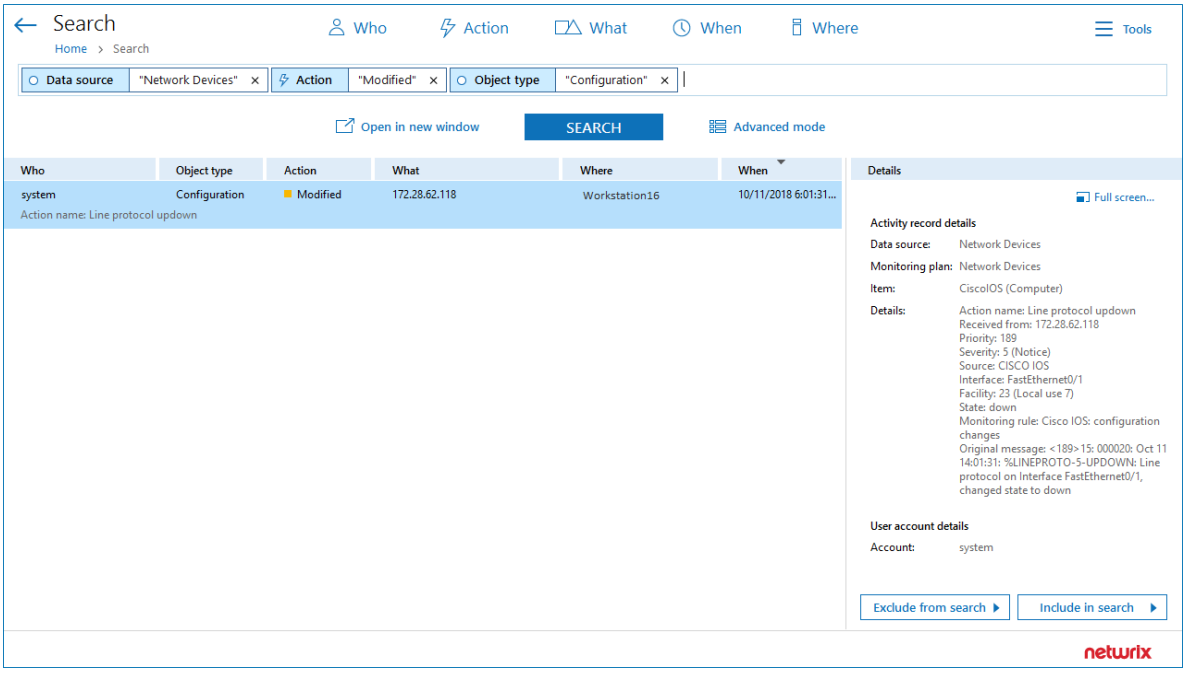
To see how your changes are listed in the report

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

   Logons to network devices:



Configuration changes on network devices:



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

9.4. Review the All Oracle Database Activity by User Report

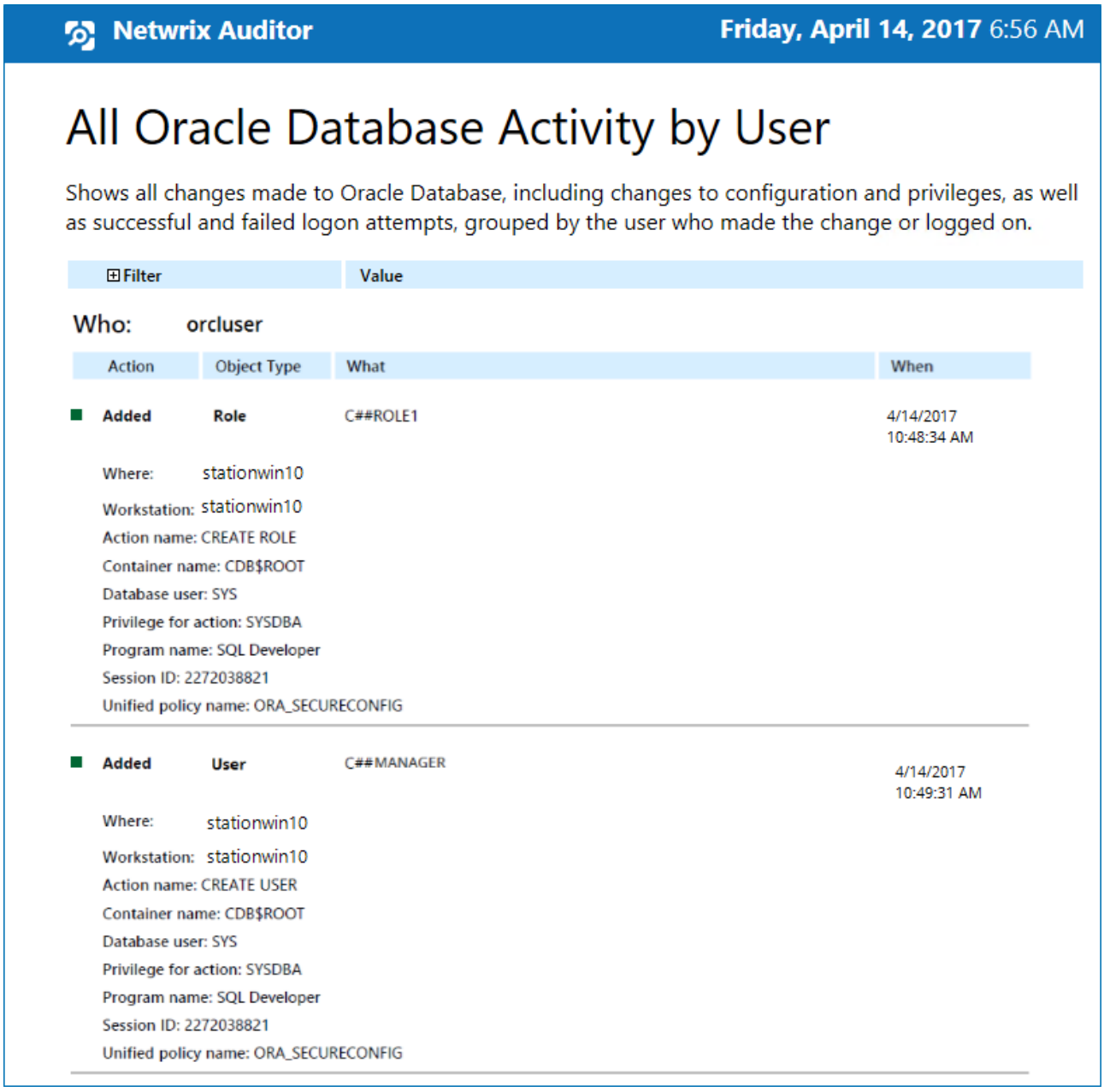
The Netwrix Auditor client provides a variety of predefined reports that aggregate data from the entire audited IT infrastructure or individual data sources.

Change and activity reports can be found under the **Reports** → **Predefined** → **Oracle Database** 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** → **Oracle Database**.
2. Select the **All Oracle Database Activity by User** report.
3. Click **View** to open the report.



Netwrix Auditor Friday, April 14, 2017 6:56 AM

All Oracle Database Activity by User

Shows all changes made to Oracle Database, including changes to configuration and privileges, as well as successful and failed logon attempts, grouped by the user who made the change or logged on.

Filter	Value

Who: orcluser

Action	Object Type	What	When
Added	Role	C##ROLE1	4/14/2017 10:48:34 AM

Where: stationwin10
Workstation: stationwin10
Action name: CREATE ROLE
Container name: CDB$ROOT
Database user: SYS
Privilege for action: SYSDBA
Program name: SQL Developer
Session ID: 2272038821
Unified policy name: ORA_SECURECONFIG

Action	Object Type	What	When
Added	User	C##MANAGER	4/14/2017 10:49:31 AM

Where: stationwin10
Workstation: stationwin10
Action name: CREATE USER
Container name: CDB$ROOT
Database user: SYS
Privilege for action: SYSDBA
Program name: SQL Developer
Session ID: 2272038821
Unified policy name: ORA_SECURECONFIG

9.5. 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.

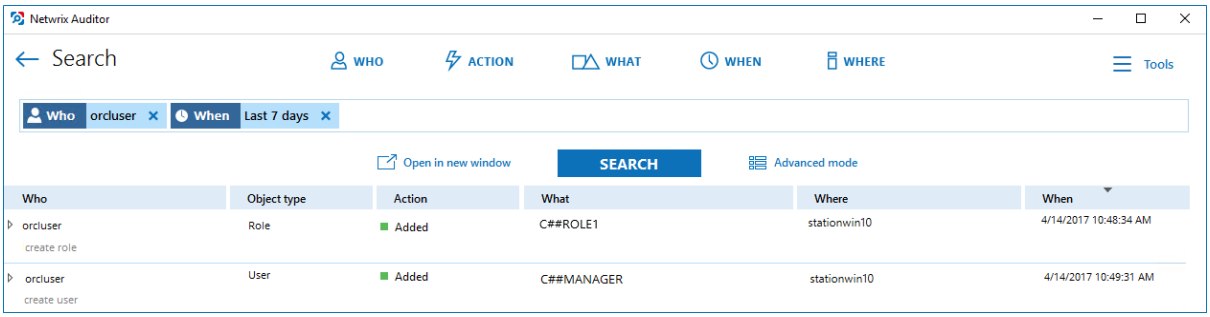
   For example, consider adding these filters:

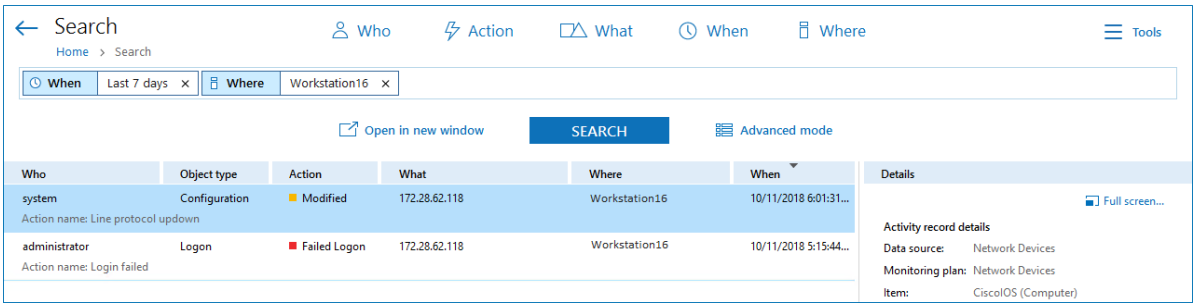
Filter	Value
 WHO	Specify your Oracle Database account name, as you performed test changes.
 WHEN	Specify a timeframe.

   NOTE: Refer to Netwrix Online Helpcenter for detailed instructions on how to apply filters and change match types.

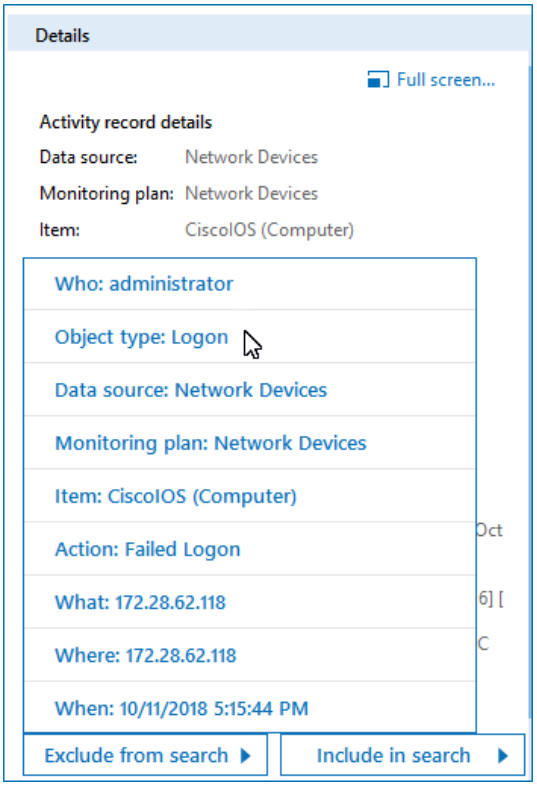
   As a result, you will see the following filters in the **Search** field:

3. Click **Search**.

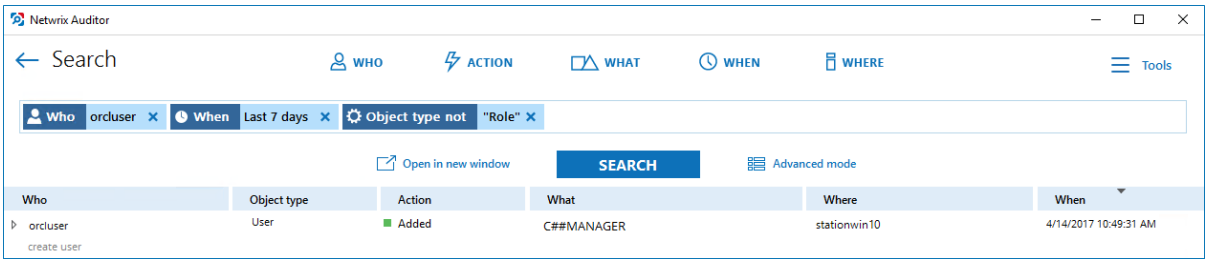


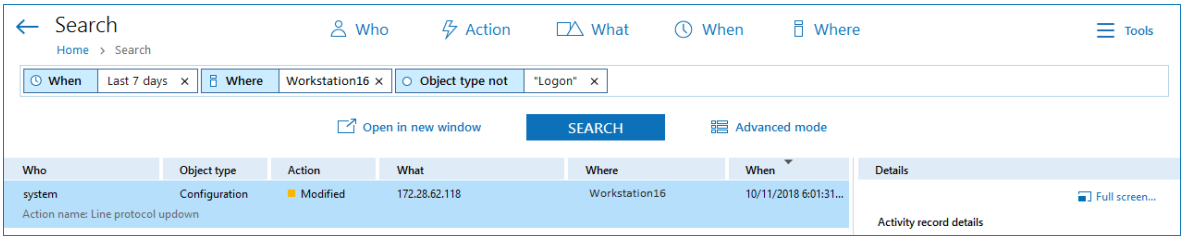


4. Now, you can narrow your search and modify it right from the search results pane. Click any entry that contains excess data, select **Exclude from search** in the **Details** section and specify a filter, e.g., **Object type:** *Role* to leave information on new users only.**Object type:** *Logon* to leave information on network device configuration changes only.



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

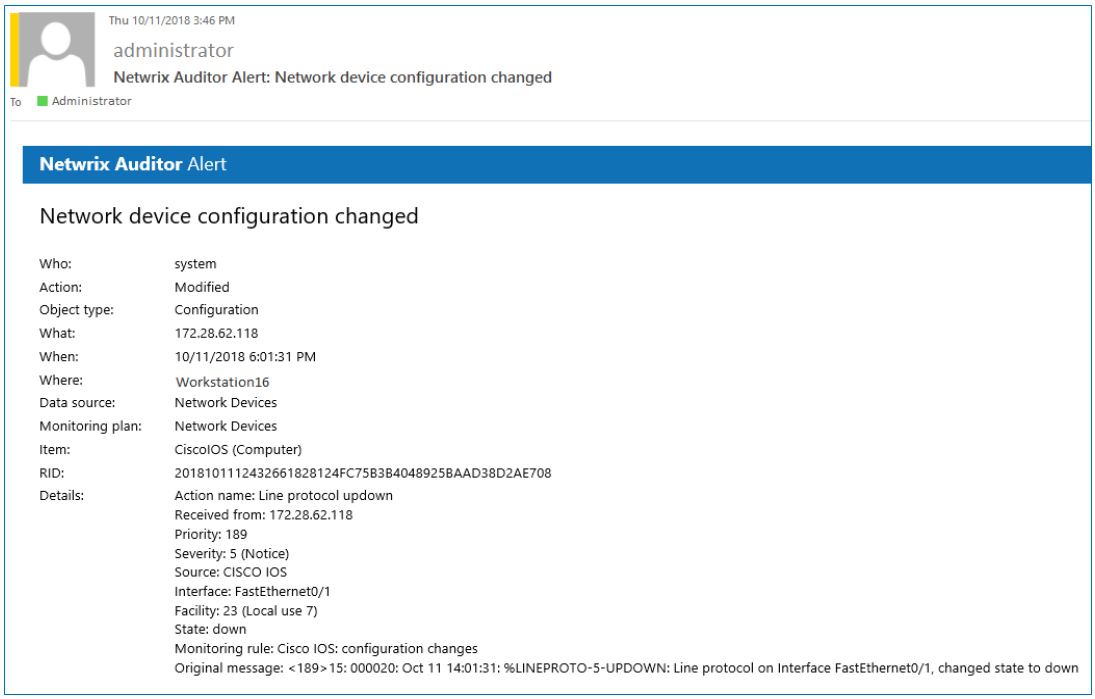


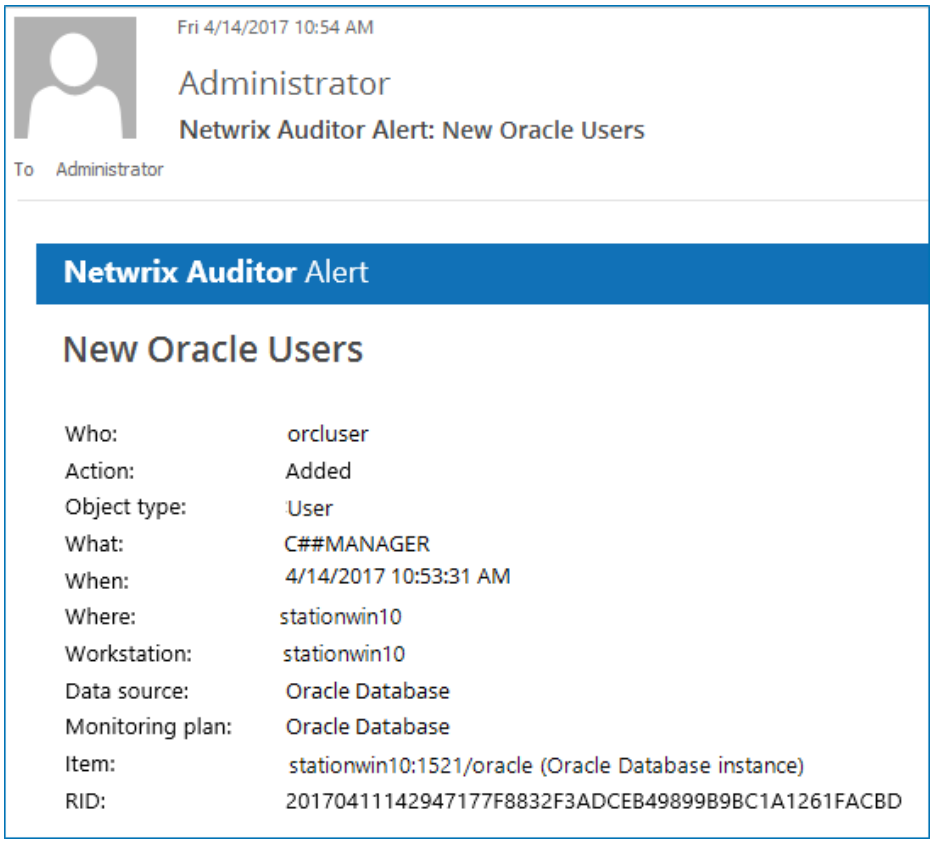


5. Having reviewed your search results, navigate to **Tools**.

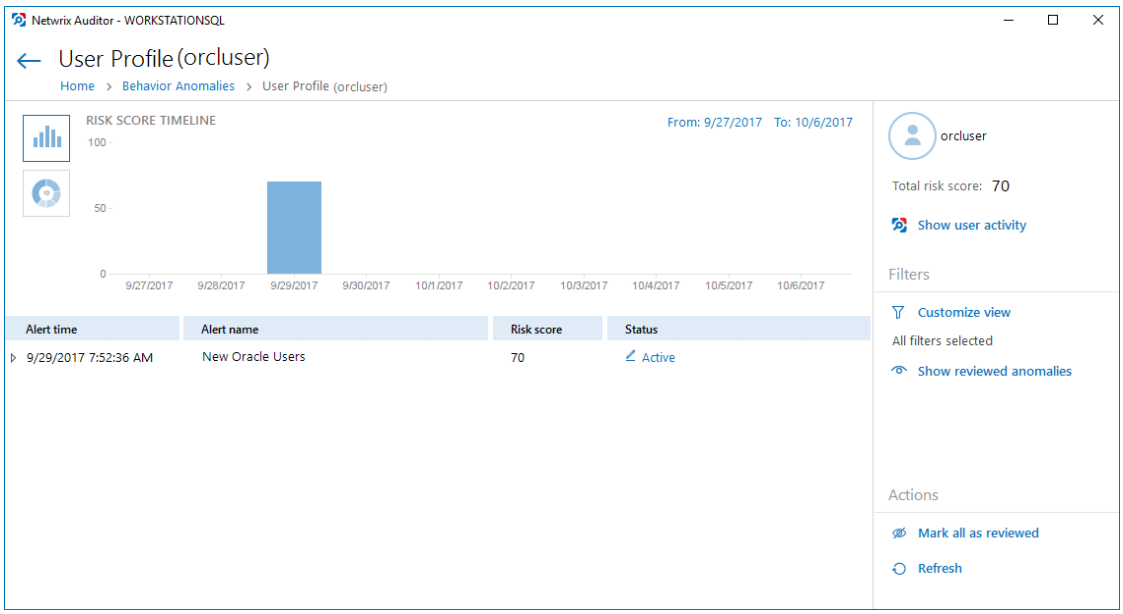
   - Click **Save as report** to save the selected set of filters. This search will be added to the **Custom** section inside **Reports**, so that you will be able to access it instantly. Refer to Custom Search-Based Reports for detailed instructions on how to create saved searches.
   - Click **Create alert** to get instant email or SMS notifications on suspicious activity that matches your current search criteria. You only need to specify a name for a new alert, add recipient and assign a risk score. The selected set of search criteria will be associated with the new alert automatically. Refer to Alerts for detailed instructions on how to create and configure alerts.

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





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



10. Related Documentation

The table below lists all documents available to support Netwrix Auditor for Oracle Database:

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 9.7, and suggests workarounds for these issues.