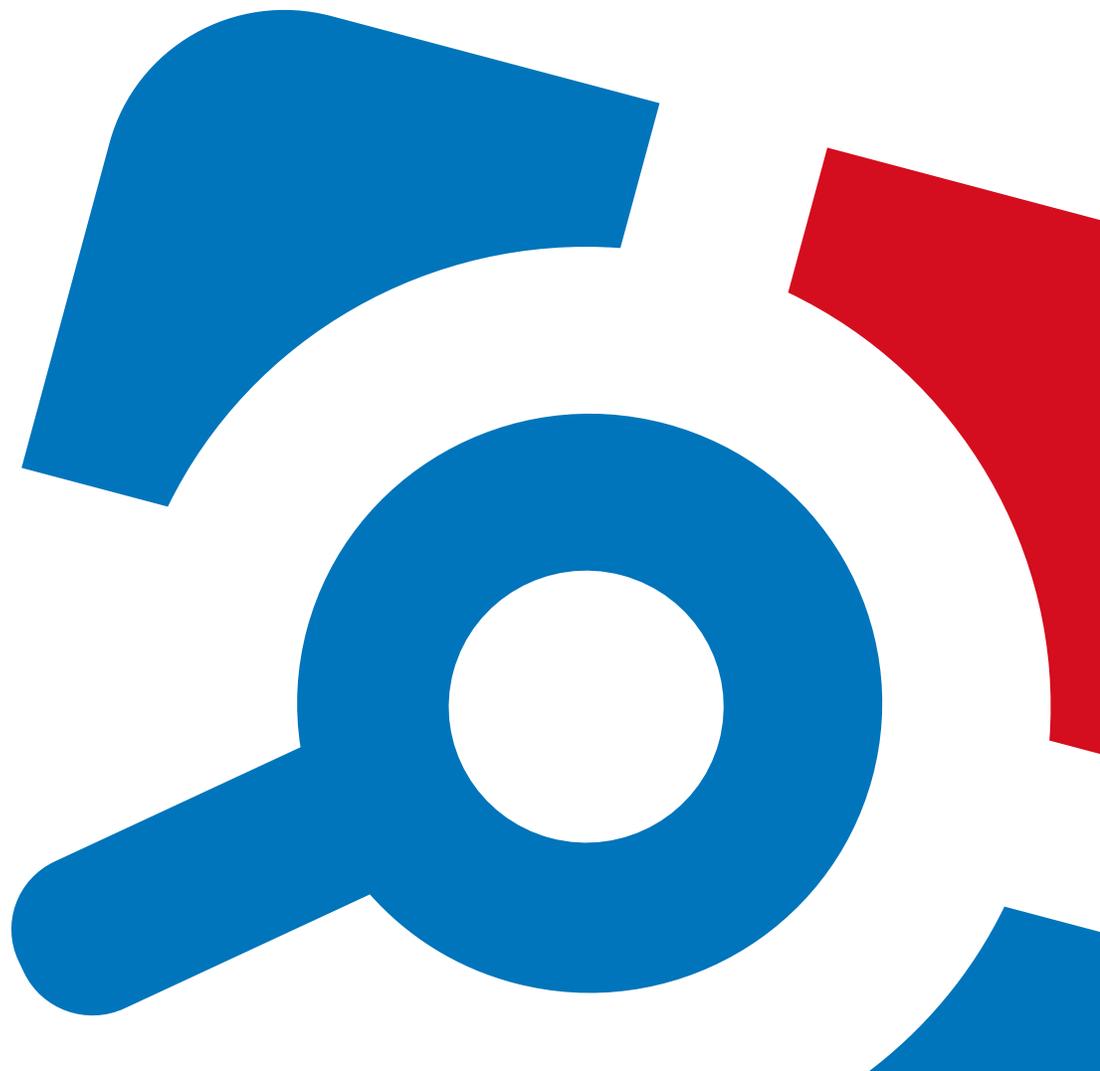netwrix

Netwrix Auditor
for Oracle Database
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.

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 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.

 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

This section lists platforms and systems that can be monitored with Netwrix Auditor for Oracle Database.

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

Supported Data Sources

Databases

Oracle Database

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
Oracle Database	• Oracle Database 19c On-Premise
	• Oracle Database 18c On-Premise
	• Oracle Database 12c On-Premise (12.1, 12.2)
	• Oracle Database 11g
	NOTE: Starting with version 10, Netwrix Auditor provides limited support of Oracle Database 11g. See Considerations for Oracle Database Auditing for more information.
	• Oracle Database Cloud Service (Enterprise Edition)

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 Newrix 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 Oracle Database. 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: • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 Windows Desktop OS (64-bit): • Windows 10 • Windows 8.1
.NET Framework	• .NET Framework 4.5 and above.
Installer	• Windows Installer 3.1 and above

2.2.2.1. Other Components

To monitor your data sources, you will need to install additional software components on Netwrix Auditor Server, in the monitored environment, or in both locations.

Data source	Components
• Oracle Database	**Oracle Database 12c and above:** *On the computer where Netwrix Auditor Server is installed:* • Oracle Instant Client. ○ Download the appropriate package from Oracle website: Instant Client Packages. Netwrix recommends installing the latest available version (Netwrix Auditor is compatible with version 12 and above). ○ Install, following the instructions, for example, Instant Client Installation for Microsoft Windows 64-bit. **NOTE:** Check your Visual Studio Redistributable version. Applicable packages for each Oracle Database version with downloading links are listed in the installation instructions: Instant Client Installation for Microsoft Windows 64-bit. **Oracle Database 11g:** Netwrix Auditor provides limited support of Oracle Database 11g. See

Data source	Components

Considerations for Oracle Database Auditing for more information.

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

  Netwrix recommends the following setup steps:

  a. Download the 64-bit Oracle Data Access Components 12c Release 4 (12.1.0.2.4) for Windows x64 (ODAC121024_x64.zip) package.

  b. Run the setup and select the **Data Provider for .NET** checkbox. Oracle Instant Client will be installed, too.

  c. On the **ODP.NET (Oracle Data Provider)** step make sure the **Configure ODP.NET and/or Oracle Providers for ASP.Net at machine-wide level** checkbox is selected .

2.2.2.2. 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
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 [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. Data Collecting Account

This is a service account that Netwrix Auditor uses to collect audit data from the monitored items (domains, OUs, servers, etc.). Netwrix recommends creating a dedicated service account for that

purpose. Depending on the data source your monitoring plan will process, the account must meet the corresponding requirements (see the table below).

NOTE: If you are going to enable integration with Netwrix Data Classification (NDC Provider), additional server roles must be assigned to the account. See For NDC Provider for more information.

For more information about NDC provider, refer to the

Starting with version 9.96, you can use group Managed Service Account (gMSA) as data collecting account. Currently, the following data sources are supported: Active Directory (also for Group Policy and Logon Activity), Windows Server, File Server (currently for Windows File Servers), SQL Server, SharePoint.

For more details about gMSA usage, see Using Group Managed Service Account (gMSA).

The gMSA should also meet the related requirements (see the table below).

NOTE: The information in this section is outside the quick-start guide scope and is provided for reference only. For detailed instructions on how to configure the data collecting account to access your audited platform or application, see Netwrix Auditor Online Help Center .

Data source	Required rights and permissions:
Oracle Database	For Oracle Database Auditing
NDC Provider	

4. Configure Oracle Database for Monitoring

Before you start monitoring your Oracle Database with Netwrix Auditor, you should configure it to provide audit trails. Depending on your current database version and edition, Oracle supports different auditing types:

Auditing type	Oracle version	Details
Unified Auditing	Oracle Database 19c, 18c, 12c	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, 18c, 19c for Auditing for more information.
Fine Grained Auditing	Oracle Database 19c, 18c, 12c, 11g Available for **Enterprise Edition** only.	Supports auditing of actions associated with columns in application tables — along with conditions necessary for an audit record to be generated. Helps to focus on security-relevant columns and rows, ignoring areas that are less important. See Configure Fine Grained Auditing for more information.
Standard Auditing (trail auditing mode)	Oracle Database 11g	See Configure Oracle Database 11g for Auditing for more information. Use initialization parameters and the `AUDIT` and `NOAUDIT` SQL statements to audit: ○ SQL statements ○ privileges ○ schema objects ○ network and multitier activities See Oracle documentation for more information. **NOTE:** Starting with version 10, Netwrix Auditor provides limited support of Oracle Database 11g and trail auditing mode, in

Auditing type	Oracle version	Details
		particular: Netwrix Auditor client UI does not display any warnings and / or errors related to Standard Auditing mode operation.

- If you are going to use **Oracle Wallet** to connect to your database, see the Create and Configure Oracle Wallet section for configuration details.

NOTE: Oracle Wallet is not supported for Oracle 11g.

- If you are unsure of your audit settings, refer to the 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 Access Oracle Database

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

This section explains how to configure **Standard Auditing** on your Oracle Database 11g, preparing for monitoring with Netwrix Auditor.

NOTE: Starting with version 10, Netwrix Auditor provides limited support of Oracle Database 11g. See Considerations for Oracle Database Auditing for more information.

IMPORTANT! Verify that Oracle Data Provider for .NET and Oracle Instant Client are installed and properly configured on the computer where Netwrix Auditor Server is installed. Netwrix Auditor does not provide any special notification for that.

To configure **Standard Auditing** on your Oracle Database 11g, take these steps:

1. Select the audit trail to store audit records. Oracle Database has the following options:

   - **Database audit trail**— Set by default.

   - **XML audit trail**— Recommended.

   - **OS files**—Not supported by current version of Netwrix Auditor.

2. Enable auditing of Oracle Database changes, using the corresponding command.

4.1.1. Select audit trail to store Oracle audit records

1. On the computer where your database is deployed, run the **sqlplus** tool.

2. Connect to your Oracle Database using Oracle account with the `SYSDBA` privilege. For example:

   `OracleUser as sysdba`

   Enter your password.

3. Depending on where you want to store audit records, execute the required command.

Store to...	Execute...

Store audit records to XML audit trail (recommended).
 	
NOTE: Use this audit trail if you want Netwrix Auditor to report on actions performed by users with SYSDBA and SYSOPER privileges. Otherwise, these actions will not be audited.
	`ALTER SYSTEM SET audit_trail=XML SCOPE=SPFILE;`
	
	If you want to enable auditing of actions performed by SYS user and by users connecting with SYSDBA and SYSOPER privileges, execute:
	
	`ALTER SYSTEM SET audit_sys_ operations=TRUE SCOPE=SPFILE;`

Database audit trail (default setting) **NOTE:** In this case, actions performed by user SYS and users connecting with SYSDBA and SYSOPER privileges will not be audited.	`ALTER SYSTEM SET audit_trail=DB SCOPE=SPFILE;`

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. If you turned auditing on or off, you will need to restart the database. For that, run the following:

   `SHUTDOWN IMMEDIATE`

   `STARTUP`

NOTE: If you only changed auditing settings, database restart is not required.

NOTE: If you are using 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.

4.1.2. 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. Depending on your monitoring requirements, enable auditing of the database parameters with the related command.

To monitor for...	Execute...

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 <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>;`

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

- AUDIT_TRAIL

- AUDIT

After an audit parameter has been enabled or disabled, Netwrix Auditor will start collecting data after successful logon session.

Also, remember to do the following:

- Configure Data Collecting Account as described in the For Oracle Database Auditing section.

- Configure ports as described in Protocols and Ports Required for Monitoring Oracle Database.

4.2. Configure Oracle Database 12c, 18c, 19c for Auditing

The following auditing modes are available for Oracle Database 12c, 18c, 19c:

- **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:

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

     NOTE: After an audit policy has been enabled or disabled, Netwrix Auditor starts collecting data after a successful logon session.

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

- **Mixed Mode**—Default auditing in a newly installed database. It enables both traditional and the new **Unified Auditing** facilities. Netwrix recommends using **Unified Auditing** mode if you do not have any trail audit facilities in your infrastructure.

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

To configure Oracle Database 12c, 18c, 19c 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. You can set them to audit the following:

   - Configuration changes

   - Successful and failed data access and changes

   - `Oracle Data Pump`, `Oracle Recovery Manager (RMAN)` and `Oracle SQL*Loader Direct Path Load` components

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,`

To monitor…	Execute the command…
| | ```
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;
``` <br><br> • Enable the audit policy: <br><br> ```AUDIT POLICY nwx_actions_pol;``` |
| Data access and changes (successful and failed) | • Create the audit policy (e.g., `nwx_actions_obj_pol`): <br><br> ```
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;
``` <br><br> • Enable the audit policy (e.g., `nwx_actions_obj_pol`): <br><br> ```AUDIT POLICY nwx_actions_obj_pol;``` |
| Component actions: `Oracle Data Pump`, `Oracle Recovery Manager`, and `Oracle SQL*Loader Direct Path Load` | • Create the audit policies (e.g., `nwx_sqlloader_dp_pol`, etc.): <br><br> **NOTE:** No special configuration required to audit RMAN events. <br><br> ```
CREATE AUDIT POLICY nwx_datapump_expimp_pol ACTIONS
COMPONENT=DATAPUMP ALL;
``` <br><br> ```
CREATE AUDIT POLICY nwx_sqlloader_dp_pol ACTIONS
COMPONENT=DIRECT_LOAD LOAD;
``` <br><br> • Enable these policies: <br><br> ```AUDIT POLICY nwx_datapump_expimp_pol;``` <br><br> ```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.

Also, remember to do the following:

- Configure Data Collecting Account as described in the For Oracle Database Auditing section.

- Configure ports as described in Protocols and Ports Required for Monitoring Oracle Database.

4.3. Configure Fine Grained Auditing

When configuring Fine Grained Auditing, you need to create an audit policy with required parameters set. The section below explains 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.

Fine Grained Auditing is not supported in **Mixed** mode.

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.

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 19c (Unified Auditing)	`select ENTITY_NAME, ENABLED_OPTION, SUCCESS, FAILURE from AUDIT_UNIFIED_ENABLED_POLICIES;`
Oracle Database 12c, 18c, 19c (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;`
Oracle Database 11g (Standard Auditing)	`SELECT audit_option, success, failure FROM dba_stmt_audit_opts;`
IMPORTANT! Starting with version 10, Netwrix Auditor provides limited support of Oracle Database 11g and trail auditing mode accordingly. See [Netwrix Auditor for Oracle Database Overview](#) for more information.	**NOTE:** To review your initialization parameters, execute the following command: `SHOW PARAMETERS audit%r;`

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. 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:
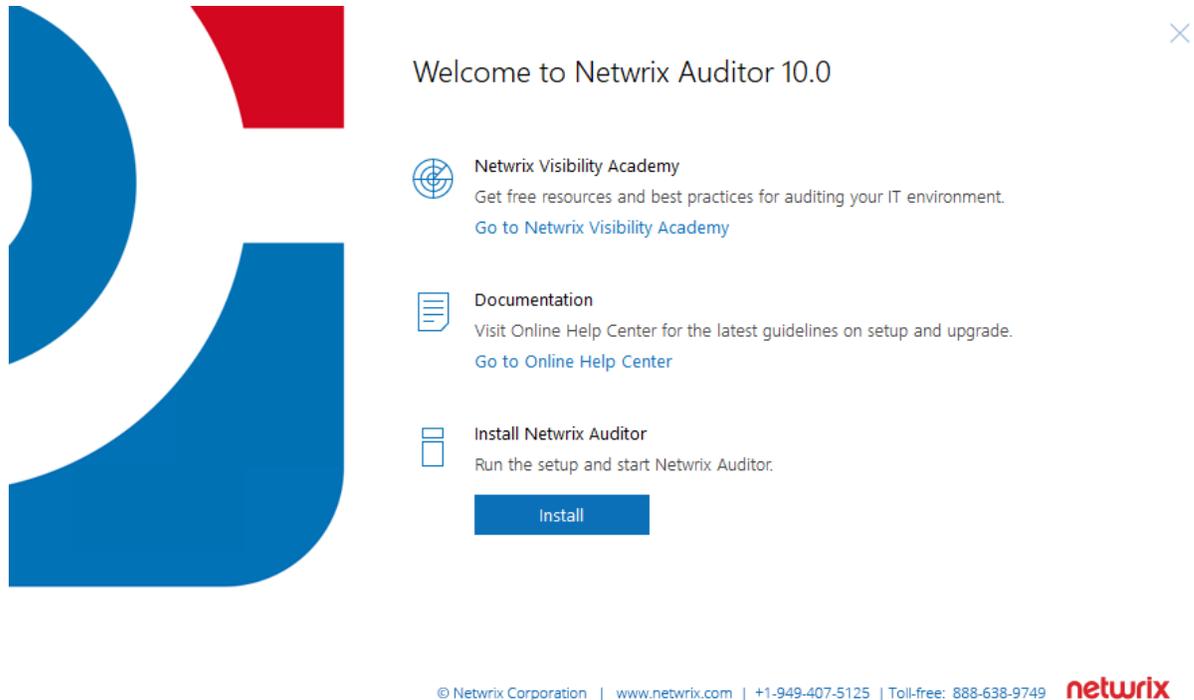
3. Follow the instructions of the setup wizard. When prompted, accept the license agreement.

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.

Netwrix Auditor - CORPSQL (CORP\Administrator)

Netwrix Auditor 10.0

Customize   Settings   Help

NEW MONITORING PLAN   SEARCH ACTIVITY RECORDS

REPORTS   BEHAVIOR ANOMALIES

Welcome to Netwrix Auditor
Get started to collect data in your IT infrastructure

✓ Create a monitoring plan to start auditing your environment
• Make sure that your monitoring plan is configured properly
• Run search to investigate incidents and browse collected data

ALERTS   7 days

TRIGGERED

0

0% over previous 7 days

CONFIGURATION

Monitoring plans

Subscriptions

Alert settings

Close to view statistics across the audited IT infrastructure

ENVIRONMENT STATS

Users	5
Groups	48
Files and folders	0

Recalculate

RISK ASSESSMENT

Take action

FAVORITE REPORTS

Enterprise Overview
Failed Activity Trend
User Account Status Changes
Activity Outside Business Hours
Logons by Single User from Multiple Endpoints
Administrative groups and role changes
AD or Group Policy modifications by Administrator since yesterday

View all

MONITORING PLANS OVERVIEW

● Ready	4
● Pay attention	0
● Take action	3

COMPLIANCE MAPPING   LIVE NEWS

8

HEALTH STATUS

● Some issues occurred

ACTIVITY RECORDS   7 days

COLLECTED

30
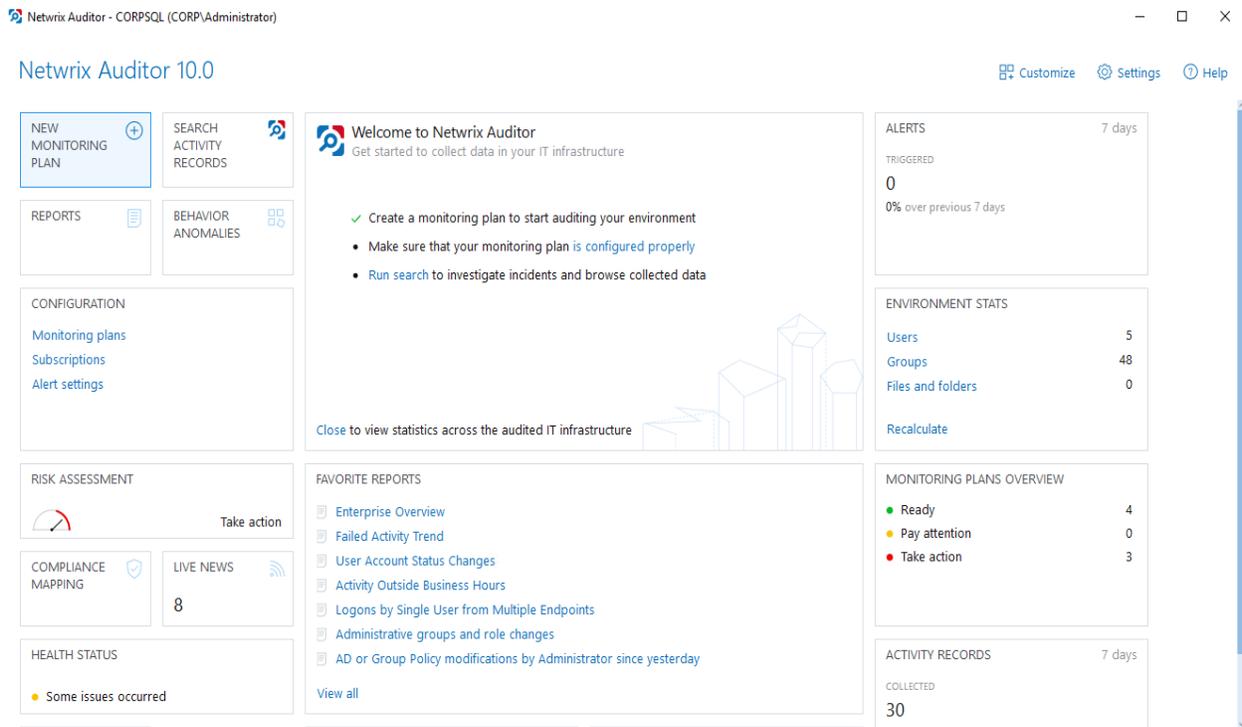
netwrix

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 Netwrix Auditor page, click the **All data sources** tile in the **Quick Start** section.

Then follow the steps of the Monitoring Plan Wizard:

- 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

6.2.1. Settings for Data Collection

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

Option	Description
Specify the account for collecting data	Provide a user name and a password for the account that Netwrix Auditor will use to collect data. By default, the user name is prepopulated with your account name.
	Make sure the account has sufficient permissions to collect data. For a full list of the rights and permissions, and instructions on how to configure them, refer to Data Collecting Account. Netwrix recommends creating a special service account with extended permissions.
	NOTE: If you want to audit network devices or Azure AD/Office 365 infrastructure, you can use any account here.

6.2.2. Default SQL Server Instance

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

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

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

Select one of the following options:

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

- **Use an existing SQL Server instance** — select this option to use an existing SQL Server instance.

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

    Complete the following fields:

Option	Description
SQL Server instance	Specify the name of the SQL Server instance to store audit data.
Authentication	Select the authentication type you want to use to connect to the SQL Server instance: • Windows authentication • SQL Server authentication
User name	Specify the account to be used to connect to the SQL Server instance. NOTE: This account must be granted the **database owner (db_owner)** role and the **dbcreator** server role.
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.

Configure the following:

Setting	Description
Disable security intelligence ...	Only select this option if you do not want your data to be stored in the database. In this case, you will only be able to receive activity summaries. Reporting and alerting capabilities will not be provided. To store data to the database, leave this check box cleared.
Database	Default database name is *Netwrix_Auditor_<monitoring_ plan_name>*. It is recommended that you enter a meaningful name for the database here. It may include the data source type (e.g. *Exchange_Audit_Data* or *OracleSrv02_Audit_ Data*), or so. If you decided to use the existing SQL Server instance instead of dedicated, you may want to use *Netwrix_ Auditor* prefix to distinguish Netwrix Auditor databases

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 **Send Test Email**. 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.

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.

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. Oracle Database Instance

Complete the following fields:

Option	Description
Connection type	Select how the product connects to Oracle Database: • **Oracle Database instance** – select if you want to connect to a database by instance name. • **Oracle Wallet** – select if you want to use Oracle Wallet – password‑protected container used to store authentication and signing credentials, including private keys, certificates, and trusted certificates needed by SSL.
Instance name	Provide connection details in the following format: *host:port/service_name.* Make sure audit settings are configured for your Oracle Database instance.
Wallet alias	Provide the alias you set while creating wallet. For example, "*MyOracle*".

Option	Description
	NOTE: Alias name in Netwrix Auditor should exactly match the alias in the `tnsnames.ora` file. See Configure Oracle Instant Client for HTTP Proxy Connections for more information.
Specify the account for collecting data	Select the account that will be used to collect data for this item.

> **NOTE:** For **Oracle Database instance** connection type only.

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:

- Create a new user

- Create a new role

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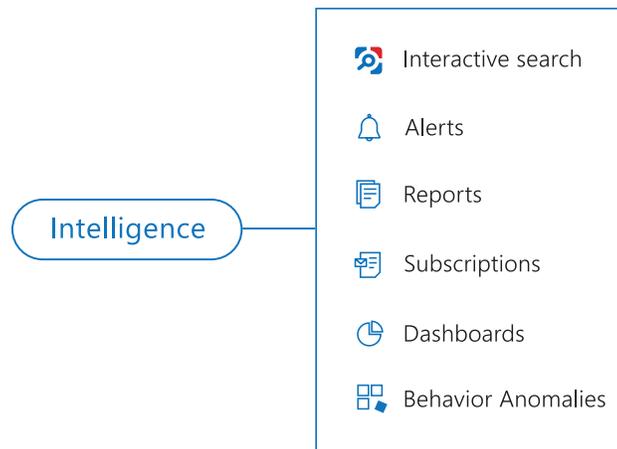
This chapter explains how to review your test changes with some of the Intelligence options and Activity Summary. Review the following for additional information:

- Review an Activity Summary

- Review Overview Dashboard

- Review the All Changes 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.

8.1. Review an Activity Summary

Activity Summary email is generated automatically by Netwrix Auditor and lists all changes that occurred since the last Activity Summary delivery. By default, an Activity Summary is generated daily at 3:00 AM and delivered to the specified recipients. You can also launch data collection and Activity Summary generation manually.

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

The example Activity Summary 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.

| Column	Description
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.

8.2. Review Overview Dashboard

Overview diagram provides a high-level overview of activity trends by date, user, server, object type or data source in your IT infrastructure. The **Overview** 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.
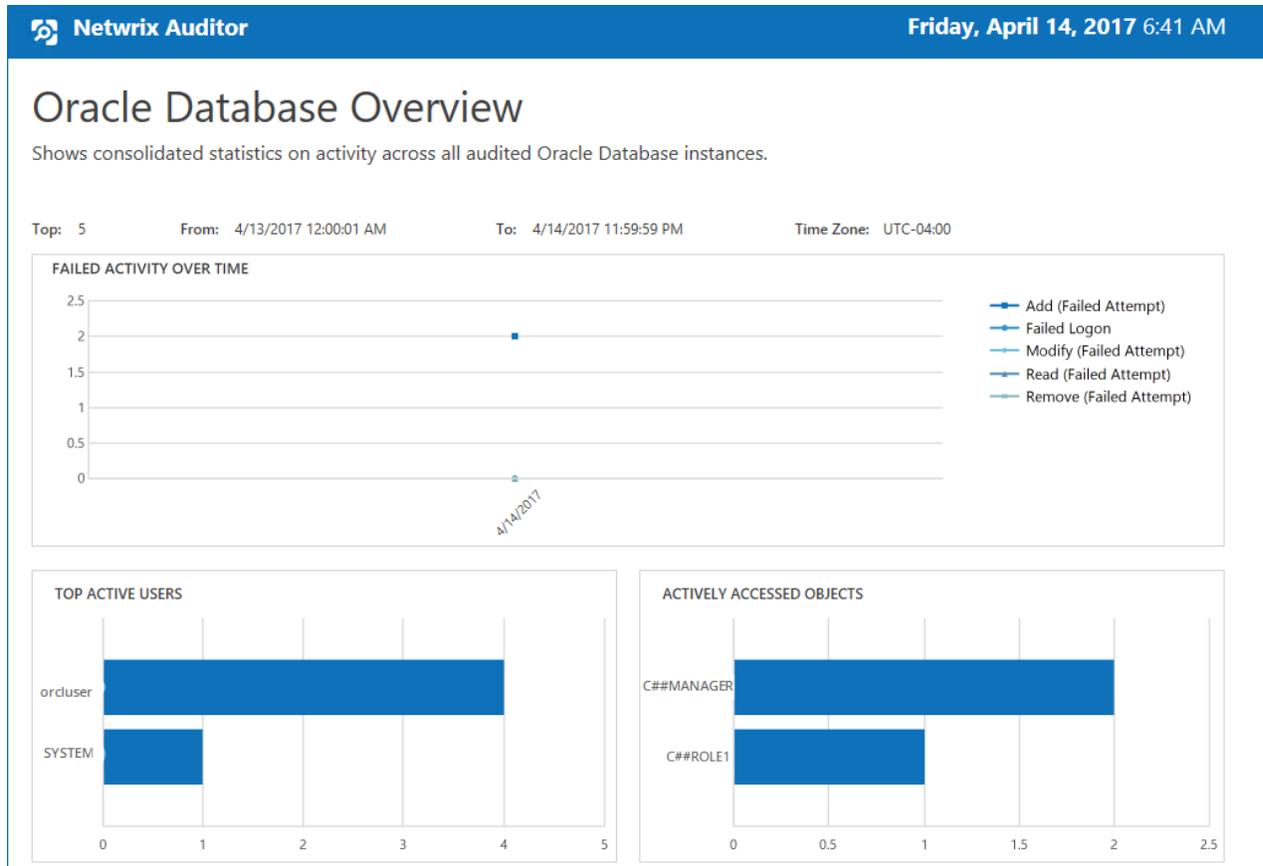
8.3. Review the All Changes Report

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 → your data source type** 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 → your data source**.

2. Select the **All Oracle Database Activity by User** report.

3. Click **View** to open the report.

8.4. 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:** *Role* to leave information on new users only.

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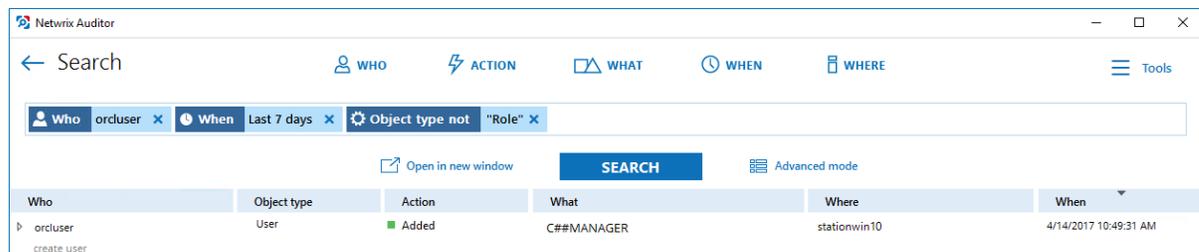
5. Having reviewed your search results, navigate to **Tools**.

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

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

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

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

9. Related Documentation

The table below lists all documents available to support Netwrix Auditor for 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 10, and suggests workarounds for these issues.