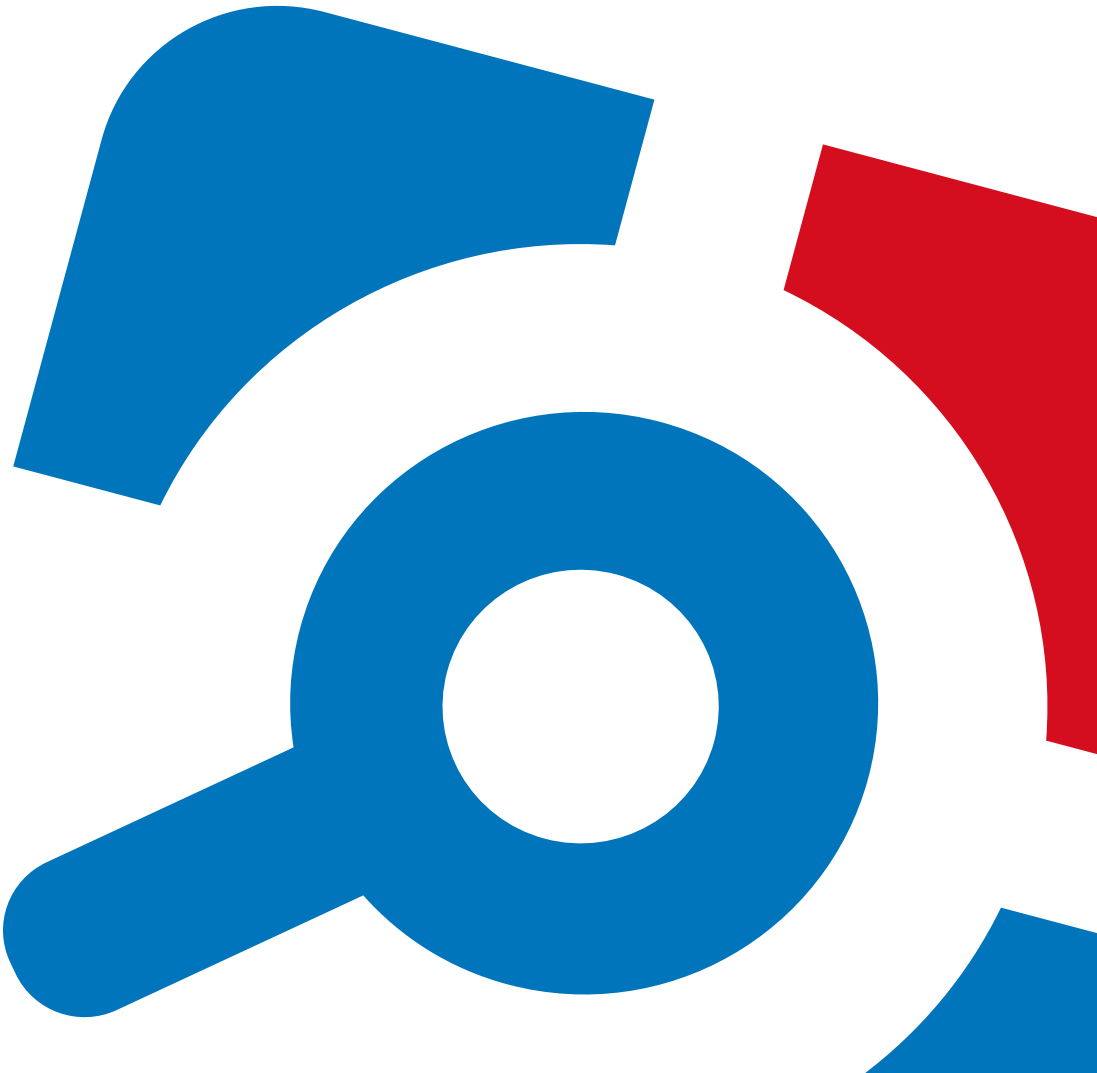
netwrix

Netwrix Auditor for Oracle Database

Quick-Start Guide

Version: 8.5
10/17/2016



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.

© 2016 Netwrix Corporation.

All rights reserved.

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 Managed Object 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 Administrator's Guide
- Netwrix Auditor User Guide

1.1. Netwrix Auditor Overview

Netwrix Auditor is a visibility and governance platform that enables control over changes, configurations and access in hybrid cloud IT environments to protect sensitive 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, 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

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. Netwrix Auditor 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.

2.1. Supported Audited Systems

The table below lists systems that can be audited with Netwrix Auditor for Oracle Database:

Audited System	Supported Versions
Oracle Database	• Oracle Database 11g • Oracle Database 12c

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

Before installing Netwrix Auditor, make sure that your hardware meets the following requirements:

Hardware Component	Minimum	Recommended
Processor	Intel or AMD 32 bit, 2 GHz	Intel Core 2 Duo 2x 64 bit, 3 GHz Preferably a virtual machine
RAM	2 GB	8 GB
Disk space	• 500 MB physical disk space for the product installation • 30 GB for the file-based Long-Term Archive	

Hardware Component	Minimum	Recommended
	• 500 MB for the SQL Server-based Audit Database where audit data is going to be stored **NOTE:** These are rough estimations, calculated for evaluation of Netwrix Auditor for Oracle Database. Refer to Netwrix Auditor Installation and Configuration Guide for complete information on the Netwrix Auditor disk space requirements.	
Screen resolution	1280 x 1024	1920 x 1080 and higher

2.2.2. Software Requirements

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

Component	Requirements
Operating system	• Windows Desktop OS (64-bit): Windows 7 SP1, Windows 8.1 • Windows Server OS (64-bit): Windows Server 2008 R2 SP1, Windows Server 2012/2012 R2
Framework	• .Net Framework 3.5 SP1
Installer	• Windows Installer 3.1 and above

2.2.2.1. Additional Components

Some audited systems may require you to install additional software components.

Audited system	Components
• Oracle Database	• Microsoft Visual C++ 2010 Redistributable Package—can be installed automatically during the Managed Object creation. • Oracle Data Provider for .NET and Oracle Instant Client 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 audited system	Test connectivity to your audited system. Make sure you can access it by its NetBIOS and DNS names from the computer where you intend to install Netwrix Auditor—use the nslookup command-line tool to look up domain names.
SQL Server 2014 with SSRS (optional step)	Although Netwrix Auditor provides a convenient interface for downloading SQL Server 2014 Express right from Netwrix Auditor Administrator Console, it is recommended to deploy SQL Server instance in advance. Test your SQL Server connectivity. **NOTE:** Netwrix Auditor provides an option to verify SSRS settings right in the Netwrix Auditor Administrator Console.

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 Processing Account Rights and Permissions 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 Processing Account Rights and Permissions

The Data Processing Account is used to collect audit data from the target systems. To ensure successful data collection, the Data Processing Account must comply with the following requirements depending on the audited system.

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.

Audited system	Rights and permissions
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` **NOTE:** If you are going to configure Fine Grained Auditing, grant privileges, 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 Auditing

Before you start auditing 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

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;`

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 audit...	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 <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 audit...	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 Direct Path Load`	• 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;`
	• 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.

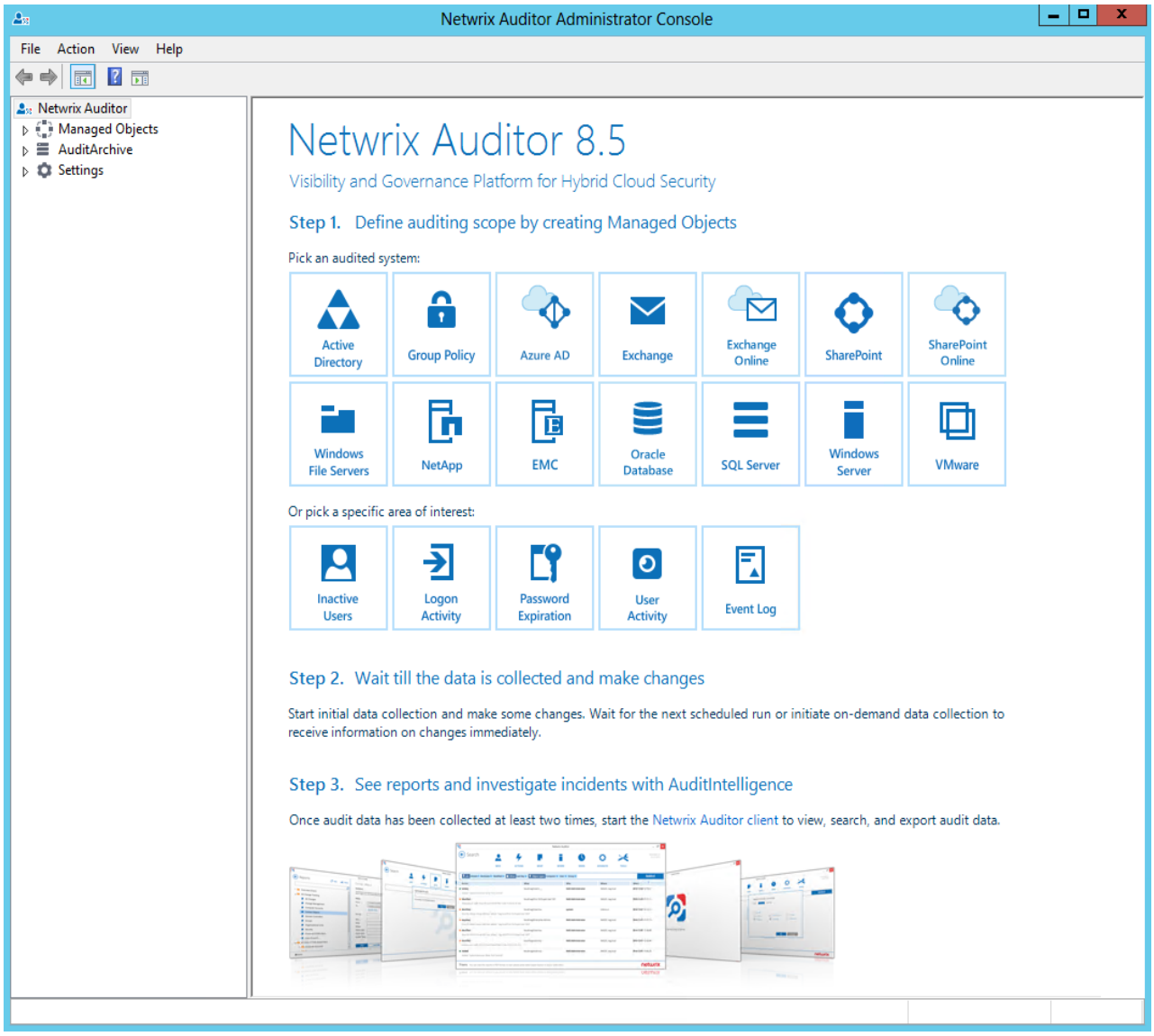
5. Install the Product

To install Netwrix Auditor

1. Download Netwrix Auditor 8.5 on 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. Click **Install**.

After a successful installation, Netwrix Auditor shortcuts will be added to the **Start** menu/screen and Netwrix Auditor Administrator Console will open.


Netwrix Auditor Administrator Console
File
Action
View
Help
Netwrix Auditor
Managed Objects
AuditArchive
Settings
Netwrix Auditor 8.5
Visibility and Governance Platform for Hybrid Cloud Security
Step 1. Define auditing scope by creating Managed Objects
Pick an audited system:
Active Directory
Group Policy
Azure AD
Exchange
Exchange Online
SharePoint
SharePoint Online
Windows File Servers
NetApp
EMC
Oracle Database
SQL Server
Windows Server
VMware
Or pick a specific area of interest:
Inactive Users
Logon Activity
Password Expiration
User Activity
Event Log
Step 2. Wait till the data is collected and make changes
Start initial data collection and make some changes. Wait for the next scheduled run or initiate on-demand data collection to receive information on changes immediately.
Step 3. See reports and investigate incidents with AuditIntelligence
Once audit data has been collected at least two times, start the Netwrix Auditor client to view, search, and export audit data.

6. Create Managed Object to Audit Oracle Database

To start auditing your IT Infrastructure with Netwrix Auditor, you must create a Managed Object. A Managed Object is a container within Netwrix Auditor that stores information on the auditing scope, the Data Processing Account used for data collection, Audit Database settings, etc.

To create a Managed Object to audit Oracle Database

1. On the main Netwrix Auditor Administrator Console page, click the **Oracle Database** tile to launch the **New Managed Object** wizard.
2. On the **Select Managed Object Type** step, select **Computer Collection** as a Managed Object type.
3. On the **Specify Default Data Processing Account** step, click **Specify Account**.

   Enter the default Data Processing Account that will be used by Netwrix Auditor for data collection. For a full list of the rights and permissions required for the Data Processing Account, and instructions on how to configure them, refer to Netwrix Auditor Installation and Configuration Guide.
4. On the **Specify Email Settings** step, specify the email settings that will be used for Change Summaries, reports and real-time alerts delivery. Netwrix Auditor automatically detects SMTP settings or you can provide them manually. Complete the following fields:

Option	Description
SMTP server	Enter your SMTP server name. It can be your company's Exchange server or any public mail server (e.g., Gmail, Yahoo).
Port	Specify your SMTP server port number.
Sender address	Enter the address that will appear in the **From** field. **NOTE:** It is recommended to click **Verify**. 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.

Option	Description
Password	Enter a password for the SMTP authentication.
Confirm password	Confirm the password.
Use Secure Sockets Layer encrypted connection (SSL)	Select this checkbox if your SMTP server requires SSL to be enabled.
Implicit SSL connection mode	Select this checkbox if the implicit SSL mode is used, which means that an SSL connection is established before any meaningful data is sent.

5. On the **Specify Computer Collection Name** step, enter the computer collection name.
6. On the **Check Prerequisites** step, Netwrix Auditor will automatically look up additional system components and prompt you to install those that are missing. In case all required components have been already installed, this step will be omitted. See Netwrix Auditor Installation and Configuration Guide for more information on software requirements.

   NOTE: You have to download and install components manually. When installing Oracle Data Access Components (ODAC), 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.
7. On the **Audit Database Settings** step, make sure that the **Make audit data available via summary emails only** checkbox is cleared. By default, the Audit Database is created automatically and is used to store collected audit data.

   Select one of the following:

   - **Automatically install and configure a new instance of SQL Server Express Edition** to automatically install and configure SQL Server 2014 Express with Advanced Services.
   - **Use an existing SQL Server instance with SQL Server Reporting Services** to use an already installed SQL Server instance. Netwrix Auditor detects local SQL Server instance automatically and pre-populates the fields.

   Complete the following fields:

Option	Description
	SQL Server Settings
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

Option	Description
	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 Netwrix Auditor Installation and Configuration Guide for more information.
Password	Enter a password.
SQL Server Reporting Services Settings	
Report Server URL	Specify the Report Server URL. Make sure that the resource is reachable.
Report Manager URL	Specify the Report Manager URL. Make sure that the resource is reachable.
User name	Specify the account to be used to connect to SSRS.
Password	Enter a password.

8. On the **Add Items to Computer Collection** step, click **Add** to select items that you want to audit. You can add several items to collection. In the **Computer Collection New Item** dialog that opens, select the item type:

   - **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. You need to specify your Oracle Database name and the Data Processing Account.

     If you want to use a specific account to collect audit data for Computer collection item (other than the one you specified as the default Data Processing Account), select **Custom** and enter credentials. This account must be granted the same permissions and access rights as the default Data Processing Account. Use double quotes for case-sensitive user names.

9. On the **Configure Oracle Database Auditing Scope** step, select Oracle Database objects and events to be audited with the product. Review the following for additional information:

Option	Description
Audit Oracle Database configuration changes	Always enabled. Includes changes to database structure, etc.
Audit data access and changes	Click **Specify** to create rules for objects and actions that you want to audit. Click **Add**, specify a name of Oracle object or schema and check actions (successful or failed reads, successful or failed changes). **NOTE:** Schema and object names are case sensitive.
Audit Oracle Database logons	Netwrix Auditor allows specifying what types of logon events you want to audit: successful logon, failed logon, or logoff.

10. On the **Specify Oracle Database Change Summary Recipients** step, enter your email.

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

11. On the last step, review your Managed Object settings and make sure **Run data collection now** is enabled. Click **Finish** to exit the wizard. The newly created Managed Object will appear under the **Managed Objects** node.

    When a new Managed Object is created, Netwrix Auditor starts collecting data from the audited IT infrastructure. The first data collection runs automatically and gathers information on the audited system's current configuration state. After the first data collection has finished, an email notification is sent to your email stating that the analysis has completed.

7. Make Test Changes

Now that the product has collected a snapshot of the audited system'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

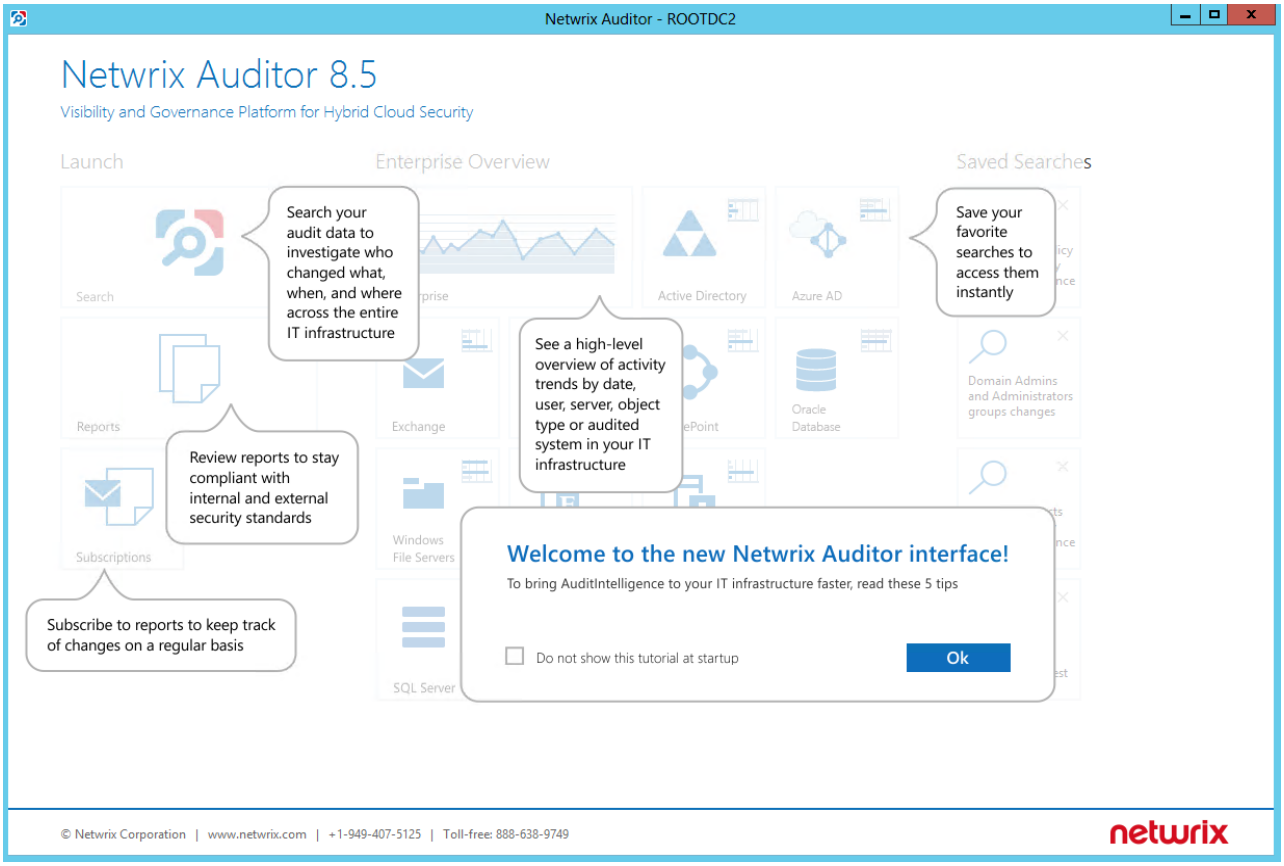
NOTE: Before making any test changes to your environment, ensure that you have the sufficient rights, and that the changes conform to your security policy.

8. See How Netwrix Auditor Enables Complete Visibility

After you have made test changes to the audited environment, you can see how Netwrix Auditor brings AuditIntelligence into your IT infrastructure and enables its complete visibility. This section explains how to review your test changes in the Netwrix Auditor client and Change Summary.

To launch the Netwrix Auditor client

- Navigate to **Start** → **Netwrix Auditor**.



Review the following for additional information:

- Review a Change Summary
- Browse Data with AuditIntelligence Search
- Review Oracle Database Overview
- Review the All Oracle Database Activity by User Report

In order not to wait for a scheduled data collection and a Change Summary generation, launch data collection manually.

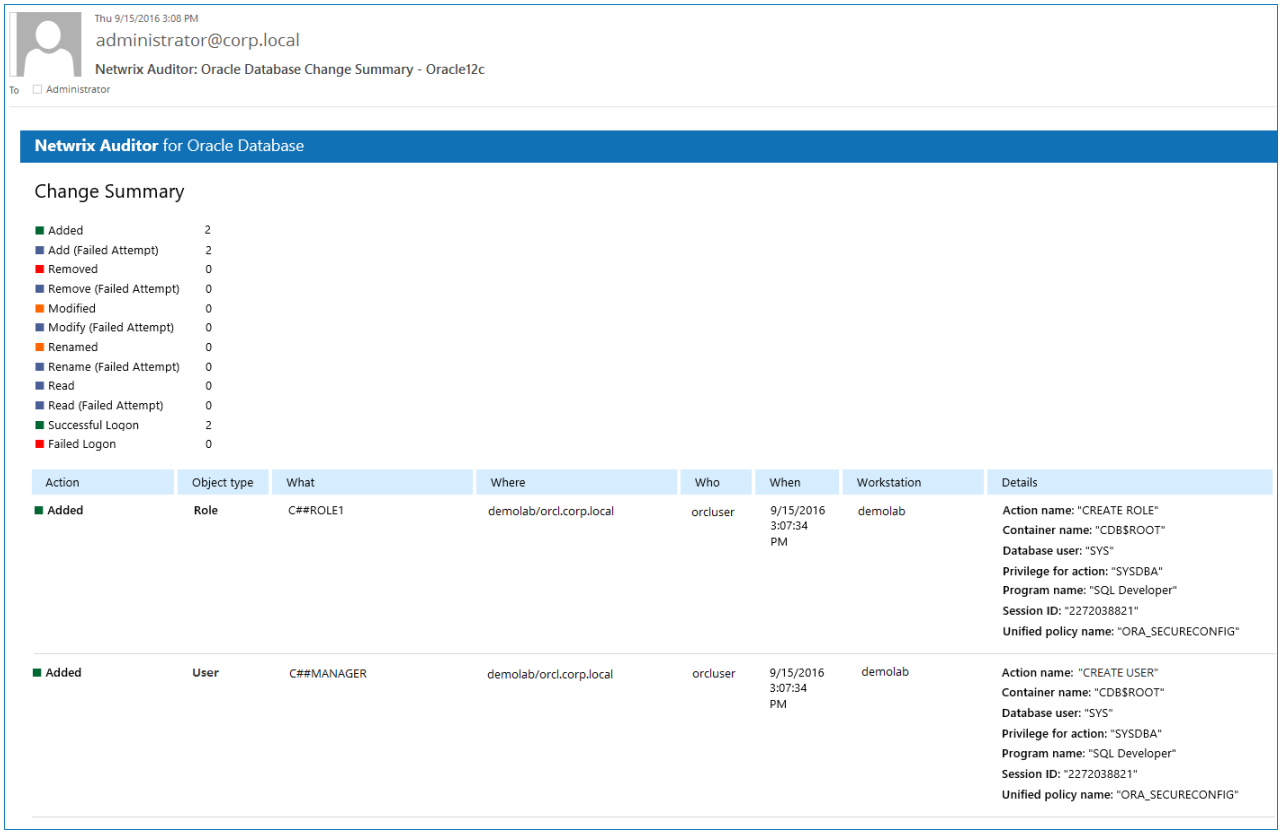
To launch data collection manually

1. In the Netwrix Auditor Administrator Console, navigate to **Managed Objects** → **your_Managed_Object_name**.
2. In the right pane, click **Run**.
3. Check your mailbox for an email notification and make sure that the data collection has completed successfully.

8.1. Review a Change Summary

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

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



Thu 9/15/2016 3:08 PM
administrator@corp.local
Netwrix Auditor: Oracle Database Change Summary - Oracle12c
To Administrator

Netwrix Auditor for Oracle Database

Change Summary

Added	2
Add (Failed Attempt)	2
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	Where	Who	When	Workstation	Details
Added	**Role**	C##ROLE1	demolab/orcl.corp.local	orcluser	9/15/2016 3:07:34 PM	demolab	**Action name:** "CREATE ROLE" **Container name:** "CDB$ROOT" **Database user:** "SYS" **Privilege for action:** "SYSDBA" **Program name:** "SQL Developer" **Session ID:** "2272038821" **Unified policy name:** "ORA_SECURECONFIG"
Added	**User**	C##MANAGER	demolab/orcl.corp.local	orcluser	9/15/2016 3:07:34 PM	demolab	**Action name:** "CREATE USER" **Container name:** "CDB$ROOT" **Database user:** "SYS" **Privilege for action:** "SYSDBA" **Program name:** "SQL Developer" **Session ID:** "2272038821" **Unified policy name:** "ORA_SECURECONFIG"

The example Change 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.
Where	Shows the name of Oracle 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.

8.2. Browse Data with AuditIntelligence Search

Netwrix Auditor delivers complete visibility into your IT infrastructure. Its convenient AuditIntelligence search interface enables you to investigate incidents and browse audit data collected across the entire IT infrastructure. When running a search in Netwrix Auditor, you are not limited to a certain audited system, 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 AuditIntelligence search.

To browse your audit data and see you test changes

1. On the main Netwrix Auditor page, navigate to **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.

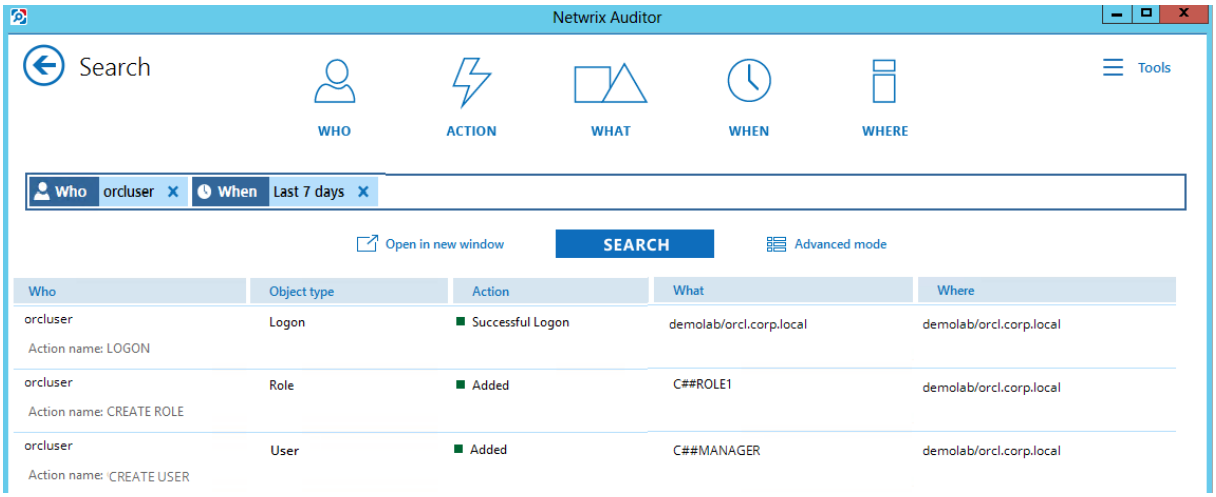
   For example, consider adding these filters:

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

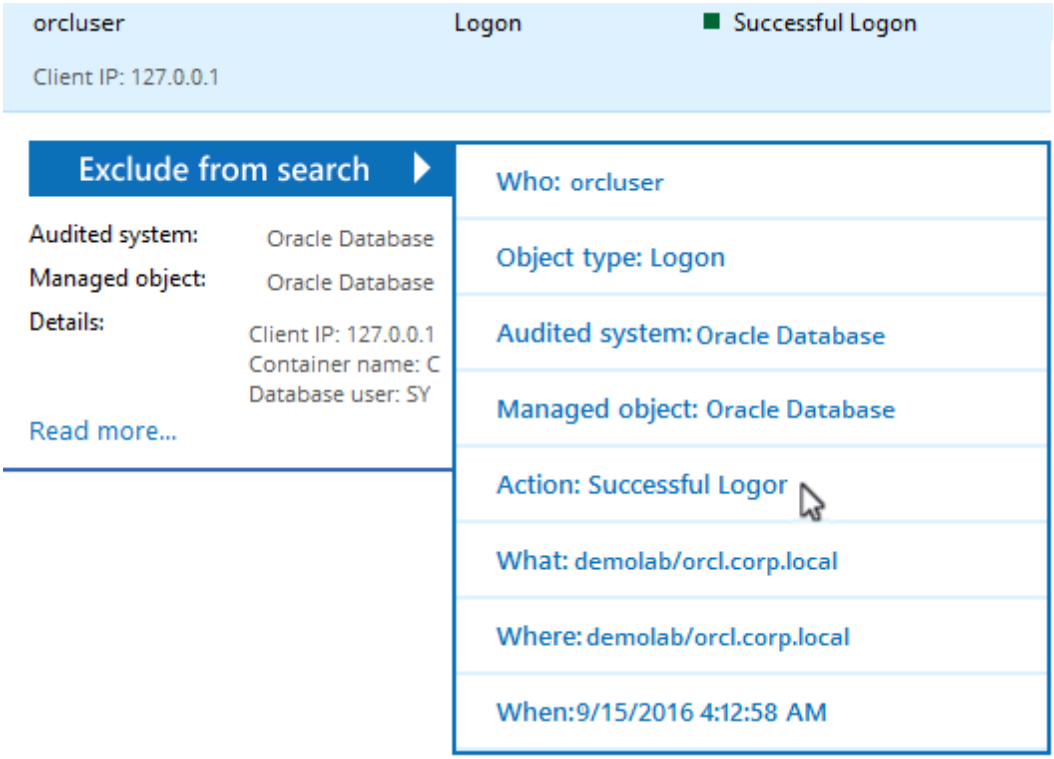
NOTE: Refer to Netwrix Auditor User Guide for detailed instructions on how to apply filters and change match types.

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

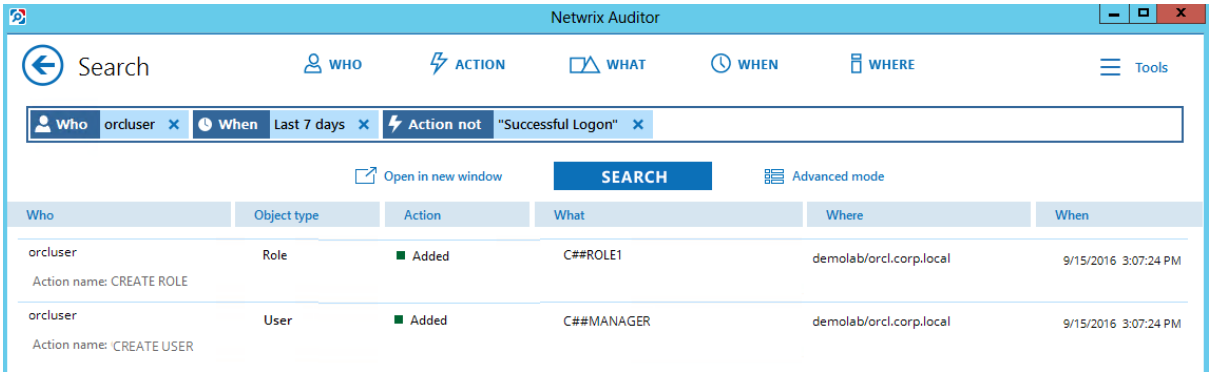
3. Click **Search**.



4. Now, you can narrow your search and modify it right from the search results pane. Double-click any entry that contains excess data, select **Exclude from search** and specify a filter, e.g., **Action:** *Successful Logon* to leave infomration on changes only.



Your **Search** field will be updated, the **Action 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 **Export data** to save your search results as a *.pdf or *.csv file.
   - Click **Save search** to save the selected set of filters. This search will be added to the **Saved Searches** section on the main Netwrix Auditor page, so that you will be able to access it instantly. Refer to Netwrix Auditor User Guide for detailed instructions on how to create saved searches.

8.3. Review Oracle Database Overview

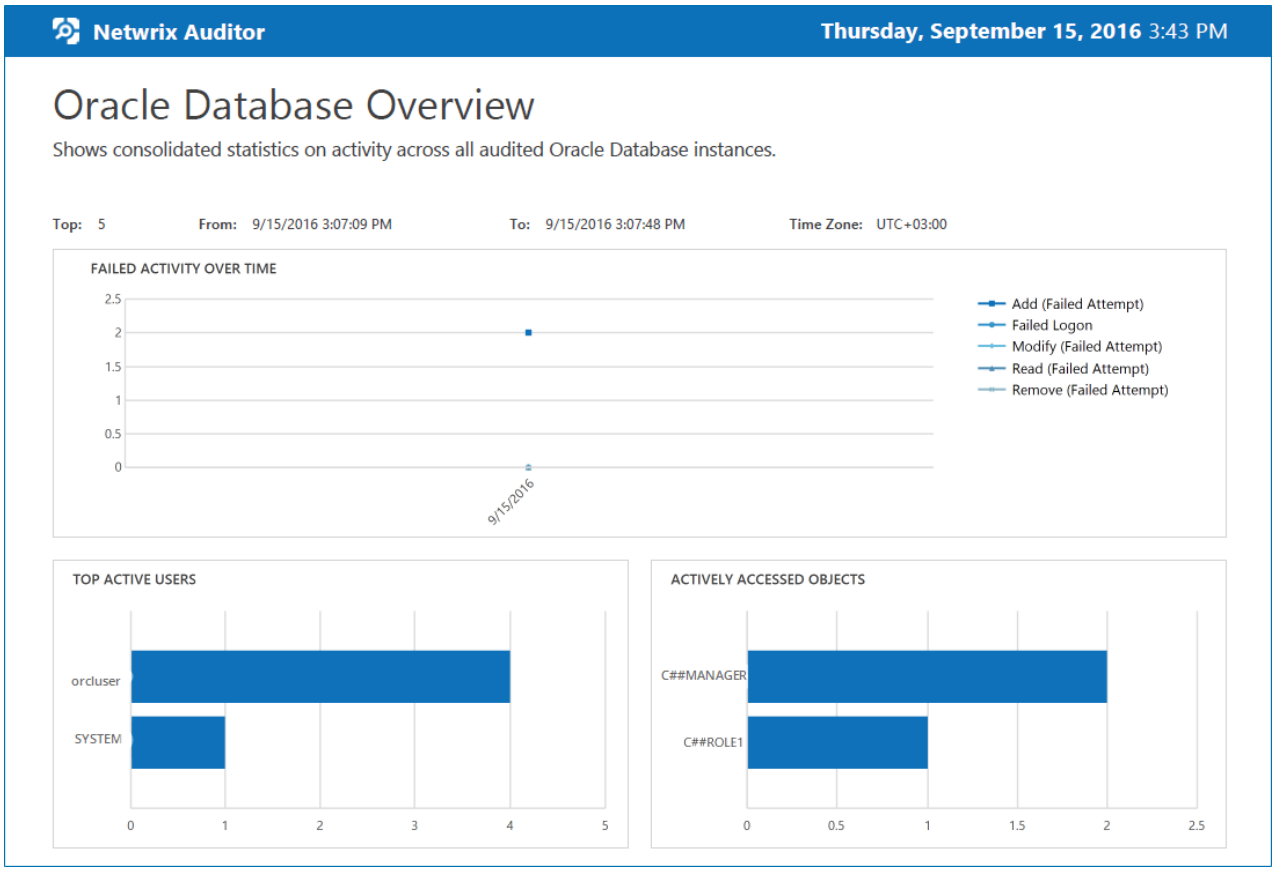
Enterprise Overview provides a high-level overview of activity trends by date, user, server, object type or audited system in your IT infrastructure. The **Enterprise** diagram aggregates data on all Managed Objects

and all audited systems, while system-specific diagrams provide quick access to important statistics within one audited system.

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 **Enterprise Overview** section.
2. Click the **Oracle Database** tile to open it.
3. Review your changes.
4. Click on any chart to jump to a table report with the corresponding grouping and filtering of data.



8.4. Review the All Oracle Database Activity by User Report

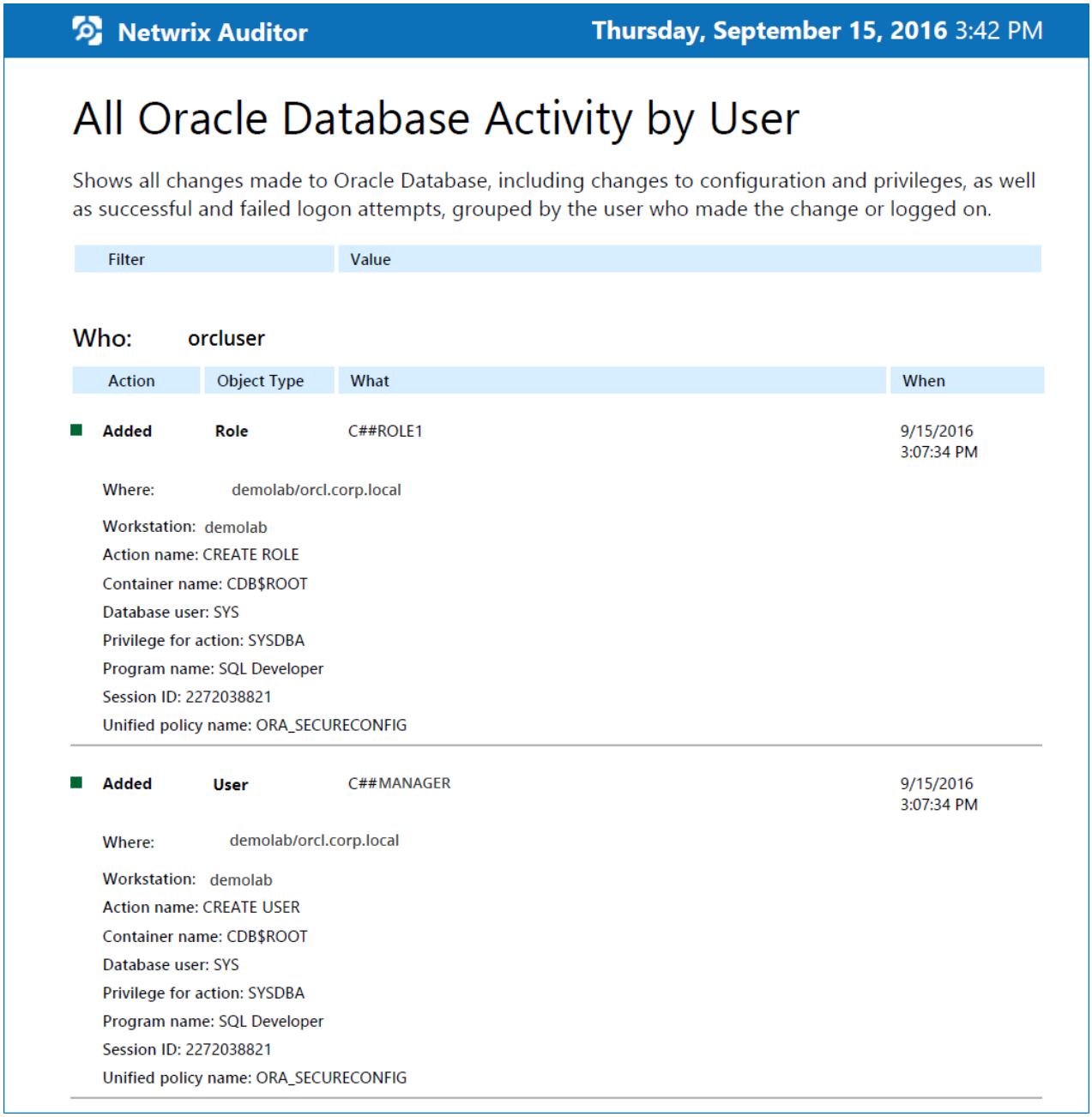
Netwrix Auditor allows generating audit reports based on Microsoft SQL Server Reporting Services (SSRS). The Netwrix Auditor client provides a variety of predefined reports that aggregate data from the entire audited IT infrastructure, an individual system, or a Managed Object.

Change reports can be found under the **Reports** → **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. In the Netwrix Auditor client, navigate to **Reports** → **Oracle Database**.
2. Select the **All Oracle Database Activity by User** report.
3. Click **View** to open the report.



Netwrix Auditor — Thursday, September 15, 2016 3:42 PM

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	9/15/2016 3:07:34 PM

Where: demolab/orcl.corp.local
Workstation: demolab
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	9/15/2016 3:07:34 PM

Where: demolab/orcl.corp.local
Workstation: demolab
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. Related Documentation

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

Document	Description
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 Administrator's Guide	Provides step-by-step instructions on how to configure and use the product.
Netwrix Auditor User Guide	Provides detailed instructions on how to enable complete visibility with AuditIntelligence.
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 8.5, and suggests workarounds for these issues.