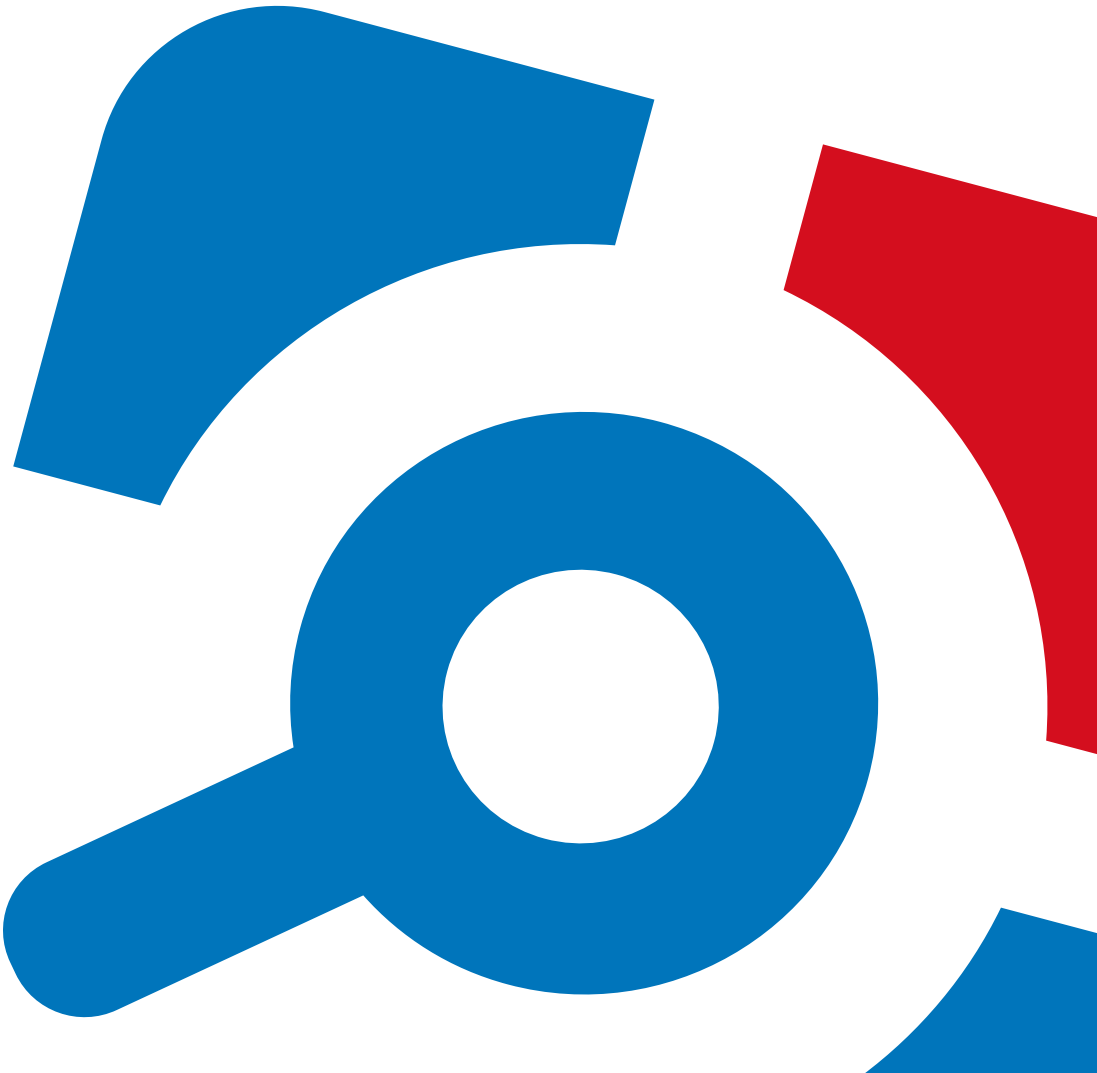
netwrix

Netwrix Auditor

Role-Based Access

Version: 8.0
3/31/2016



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.

Table of Contents

1. Role-Based Access

Security and awareness of *who* has access to *what* is crucial for every organization. Besides notifying you on *who* changed *what*, *when* and *where*, and *who* has access to *what* in your IT infrastructure, Netwrix pays attention to safety of its own configuration and collected audit data.

To keep the auditing process secure, Netwrix suggests configuring role-based access. It helps you ensure that only appropriate users can modify the Netwrix Auditor configuration or view audit data, based on your company policies and the user's job responsibilities. Recommended roles are described briefly in the table below and explained in the further detail in the remainder of this document.

Role	Access level	Recommended use
Administrator	Full access to both Netwrix Auditor configuration and collected audit data	The administrator role should be assigned to a very limited number of employees— typically, only the owner of the Netwrix Auditor host in your environment.
User	Read-only access to all audit data collected by Netwrix Auditor	The user role is appropriate for key employees who need to review audit data collected across various audited systems— typically, IT managers, security officers, and so on.
Recipient	Read-only access to limited scope of audit data defined by an administrator or user	The recipient role enables employees to review a specific set of audit data relevant to their responsibilities. For example, assign this type of access to employees who need to: • Review audit data according to a certain schedule set by your company policies and procedures • Access and review data accumulated over time You can provide recipients with access to the limited audit data they need in two ways: • By configuring report subscriptions • By publishing reports to file shares Typically, email subscriptions to a report with enabled filters work great for an auditor who performs monthly access rights attestation on critical folders. Publishing reports to a file share with granular permissions works great for a multi-level support team.

2. Netwrix Auditor Administrator Role

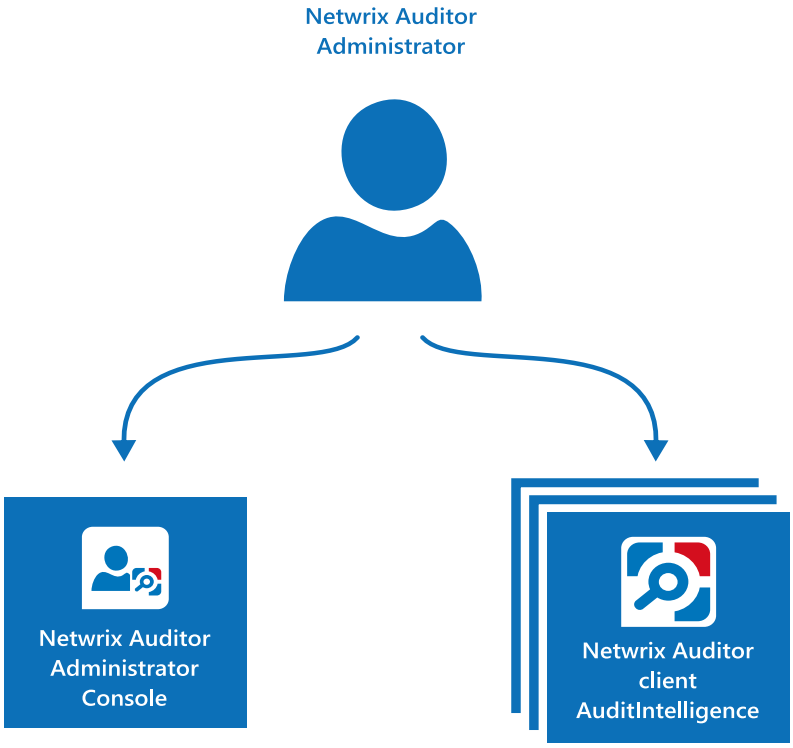
2.1. Access Rights of the Role

The administrator role grants full access to both Netwrix Auditor configuration and collected audit data. Therefore, this role should be assigned to a very limited number of employees—typically, only the owner of the Netwrix Auditor host in your environment.

It is reasonable to assign the Netwrix Auditor administrator role to your system administrator who has access to your IT infrastructure configuration (Active Directory, etc.) because configuring Netwrix Auditor requires additional actions.

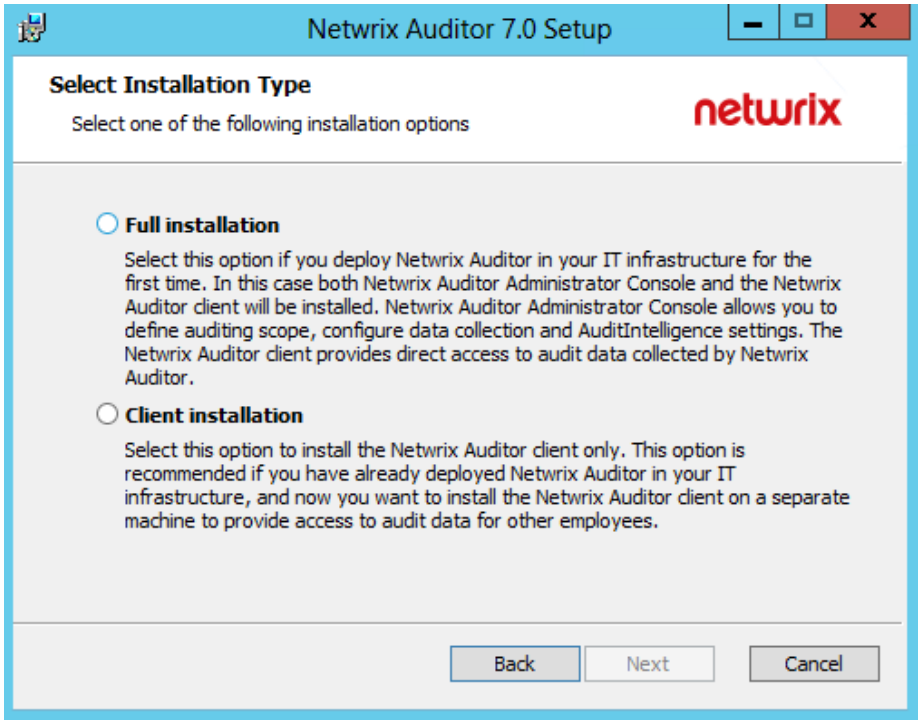
Specifically, anyone assigned the Netwrix Auditor administrator role has full access to:

- Netwrix Auditor Administrator Console. The administrator can:
  - Create, edit and remove Managed Objects that define auditing scope
  - Start and stop auditing
  - Modify the delivery schedule for Change Summaries
  - Enable or disable real-time alerts
  - Specify whether collected audit data will be written to the Audit Database (and therefore whether it is available in the Netwrix Auditor client)
- The Netwrix Auditor client. The administrator can:
  - View any collected audit data while generating reports and diagrams or running AuditIntelligence searches
  - Export AuditIntelligence search results and configure reports to be sent by email or saved to file shares or local folders
  - Create, modify and remove saved searches



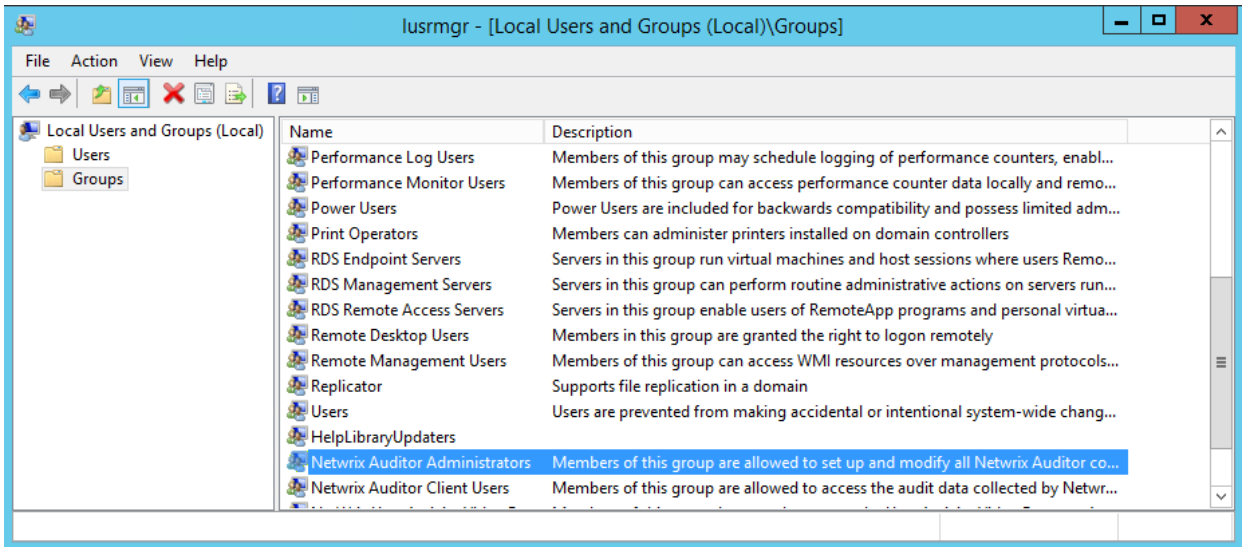
2.2. Grant Full Access

Full access permissions are granted through membership in the local **Netwrix Auditor Administrators** group. This group is created during the first installation (Full installation), and the user who performs the installation is automatically included into this group.



To add additional administrators, navigate to **Local Users and Groups** and add users to this group.

NOTE: Every Netwrix Auditor administrator must also be a member of the local **Administrators** group on the computer where Netwrix Auditor Server is installed.



For more information on how to grant administrator permissions, refer to the *"Configure Netwrix Auditor Roles"* chapter in the Netwrix Auditor Installation and Configuration Guide.

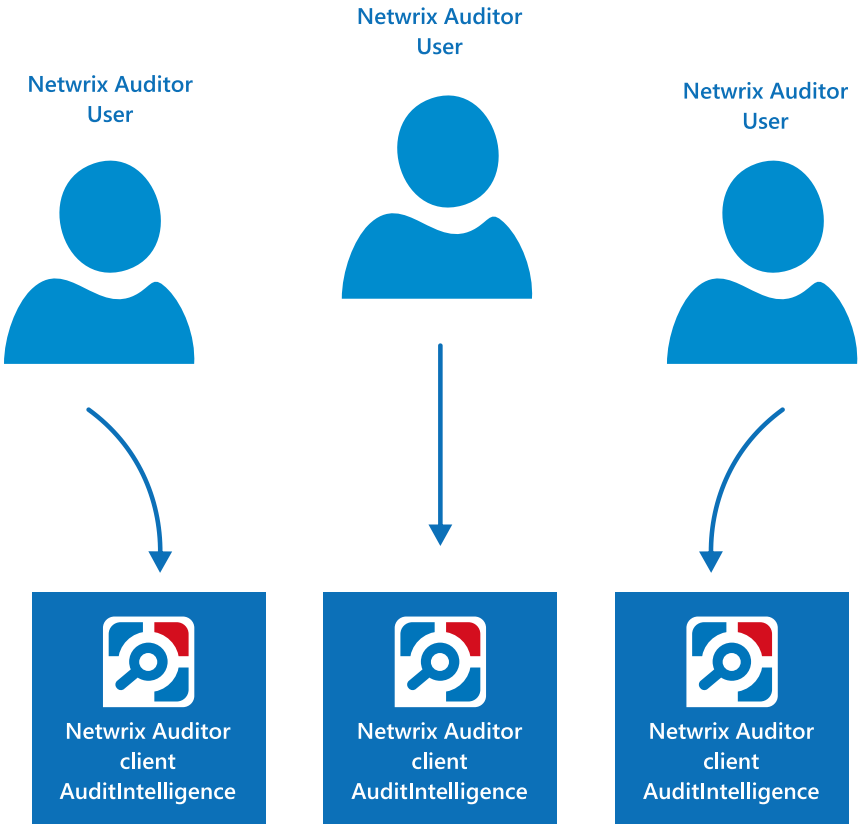
3. Netwrix Auditor User Role

3.1. Access Rights of the Role

The user role grants read-only access to all audit data through the Netwrix Auditor client. Although you can install client on multiple workstations, you should grant read access only to those employees who deal with data collected across all audited systems, such as IT managers, security officers and internal auditors. Granting read permissions to a significant number of employees may lead to uncontrollable audit data distribution.

Specifically, anyone assigned the Netwrix Auditor user role can:

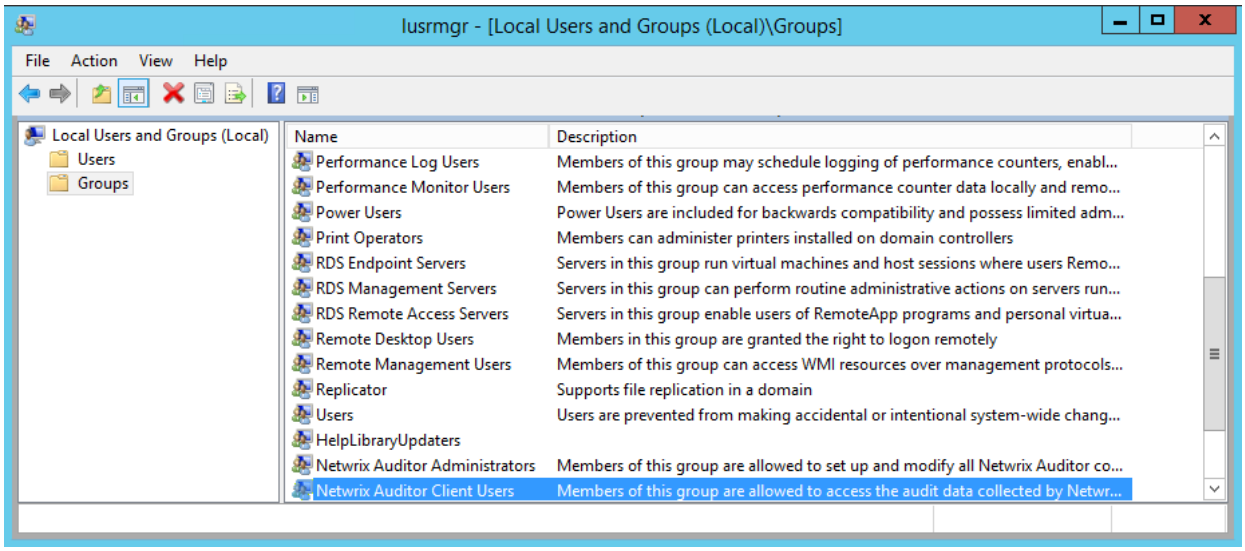
- View any collected audit data while generating reports and diagrams or running AuditIntelligence searches
- Export AuditIntelligence search results and configure reports to be sent by email or saved to file shares or local folders
- Create, modify and remove saved searches



3.2. Grant Read Access to Audit Data

Read permissions are granted through membership in the **Netwrix Auditor Client Users** group on the computer where Netwrix Auditor Server resides.

For security reasons, you have to add users to this group manually. To do this, on the computer where Netwrix Auditor Server resides, navigate to **Local Users and Groups**. Anyone with the Netwrix Auditor user role must be assigned the **Browser** role on the Report Server.



For more information on how to grant user permissions, refer to the *"Configure Netwrix Auditor Roles"* chapter in the Netwrix Auditor Installation and Configuration Guide.

4. Netwrix Auditor Recipient Role

By default, only Netwrix Auditor administrators and users are allowed to view audit data collected by Netwrix Auditor. This policy ensures that only authorized and trustworthy users access sensitive data.

However, in some cases, organizations need to provide certain employees with access to a limited set of audit data. For example, an auditor might need to review particular access reports once or twice a year. You can provide this limited access using the recipient role. Users with this role are allowed to review a piece of collected audit data but have no access to the rest of the audit data or the Netwrix Auditor configuration. This ensures that dedicated specialists have access to the data they need (without actually running Netwrix Auditor) while preventing data breaches and ensuring that sensitive data is not being distributed across the whole company.

NOTE: Netwrix recommends granting limited access permissions to employees who need to:

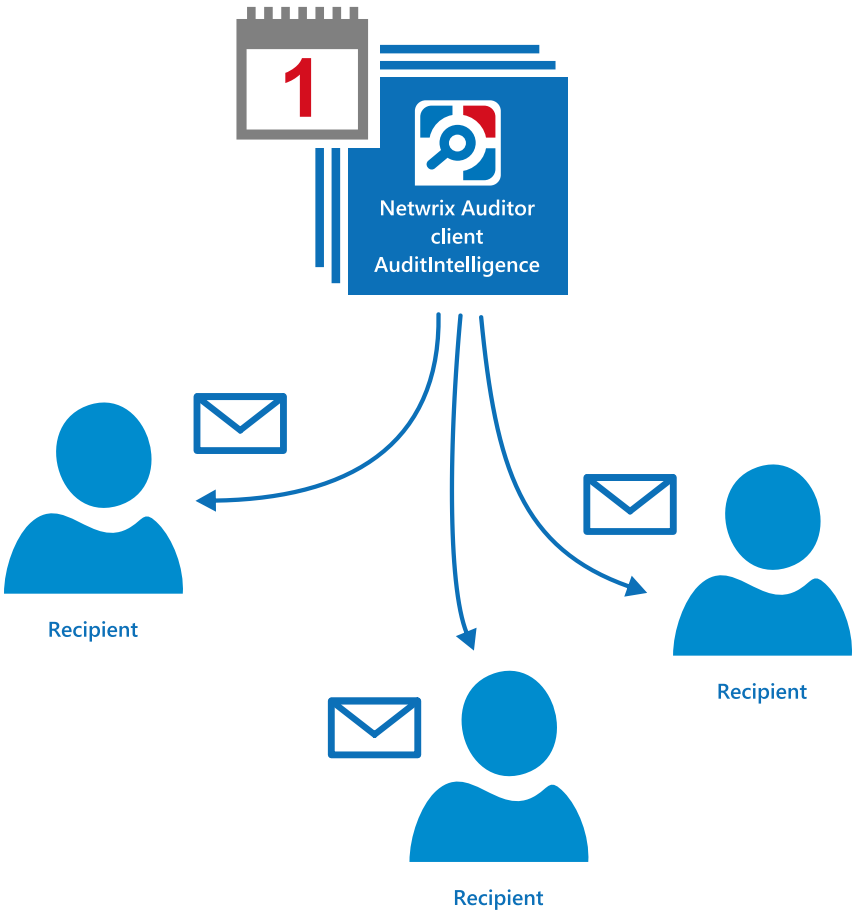
- Review audit data periodically in accordance with company policy
- Review audit data accumulated over time

To grant limited access to audit data, you can:

- Schedule email report subscriptions
- Publish reports to file shares

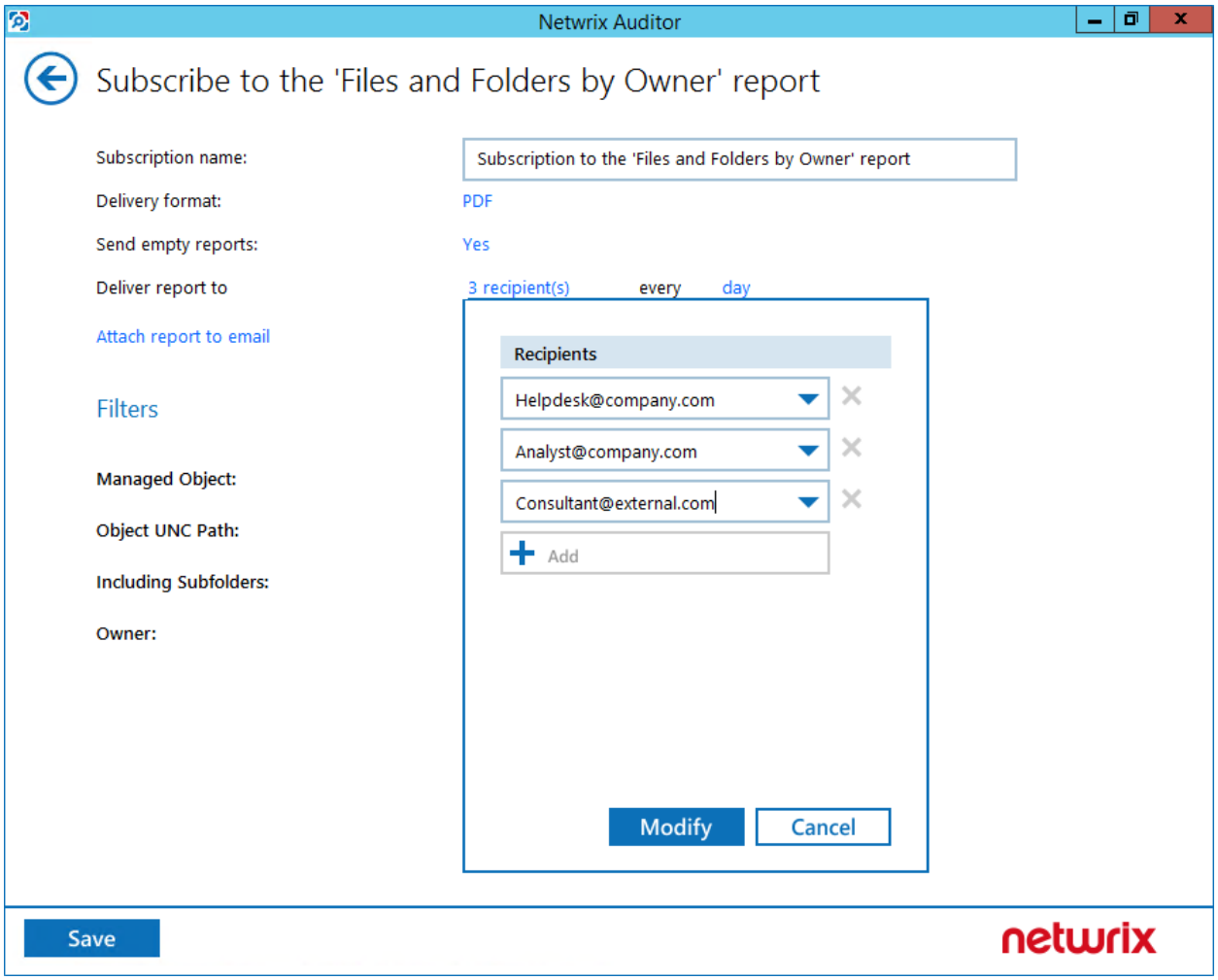
4.1. Grant Limited Access by Configuring Report Subscriptions

Netwrix Auditor administrators and users can provide recipients with limited access to audit data by scheduling email subscriptions. This is helpful when you want to share information with a group of employees, external consultants, auditors, and so on. Reports are sent according to a specified schedule and recipients can review them, but they do not have any other means to access audit data. Basically, this option is enough for employees who are interested in a high-level summary—for example, an auditor who performs monthly access rights attestation on critical folders.



To subscribe to a report

1. In the Netwrix Auditor client, navigate to **Reports**.
2. Select a report and click **Subscribe**.
3. In the **Subscribe to report** window, select **Attach report to email**, define a schedule (such as daily or weekly on Mondays), add recipients, and specify filters to control what information is included in the report.

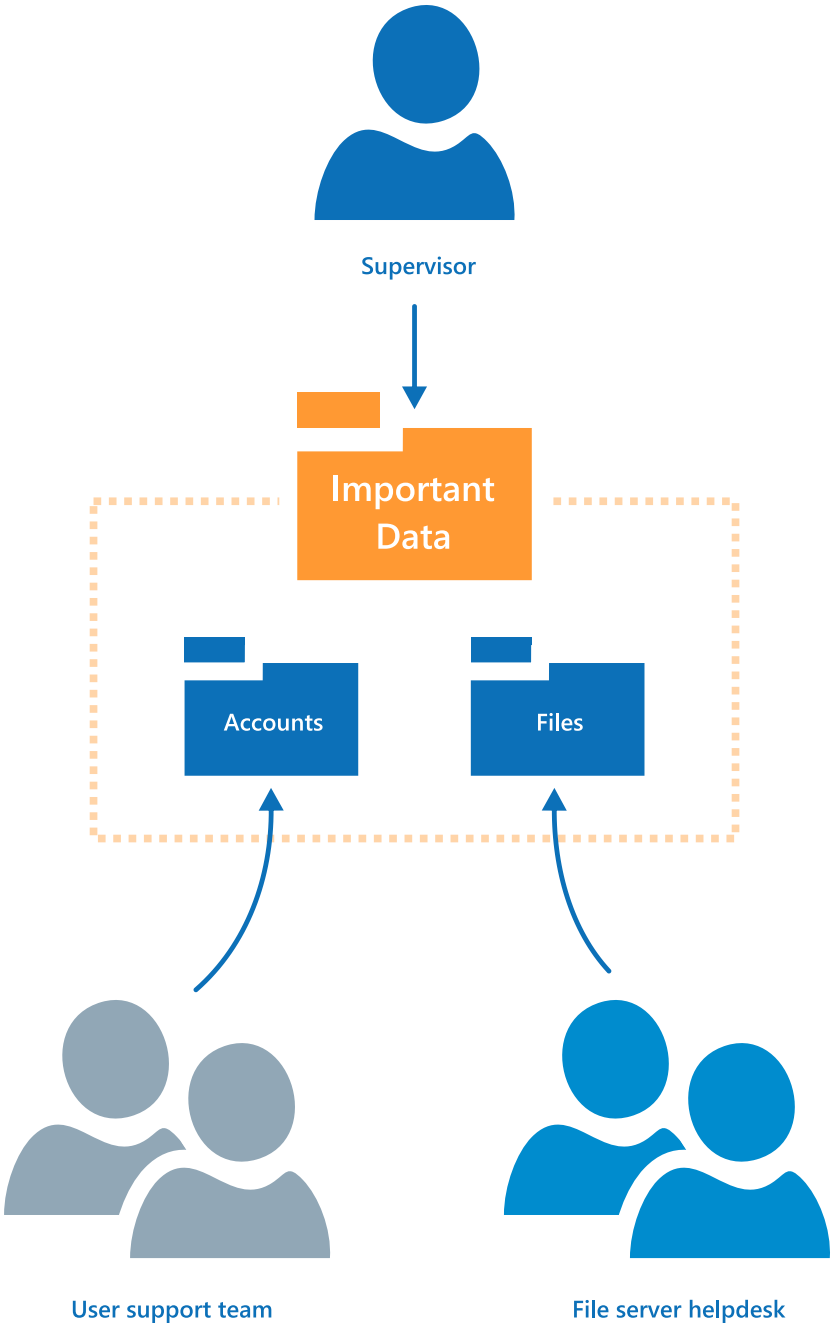


4.2. Grant Limited Access by Publishing Reports To File Share

Netwrix Auditor administrators and users can provide recipients with limited access to audit data by publishing reports to file servers. By granting individuals access to the file share, you grant them access to the reports in it.

For example, this scenario works great for a helpdesk with several departments. Assume, each department has its own field of responsibility and must not disclose information to other departments. You can configure Netwrix Auditor to publish reports to folders that can be accessed by employees from a specific department only. You might set up the following folders and permissions:

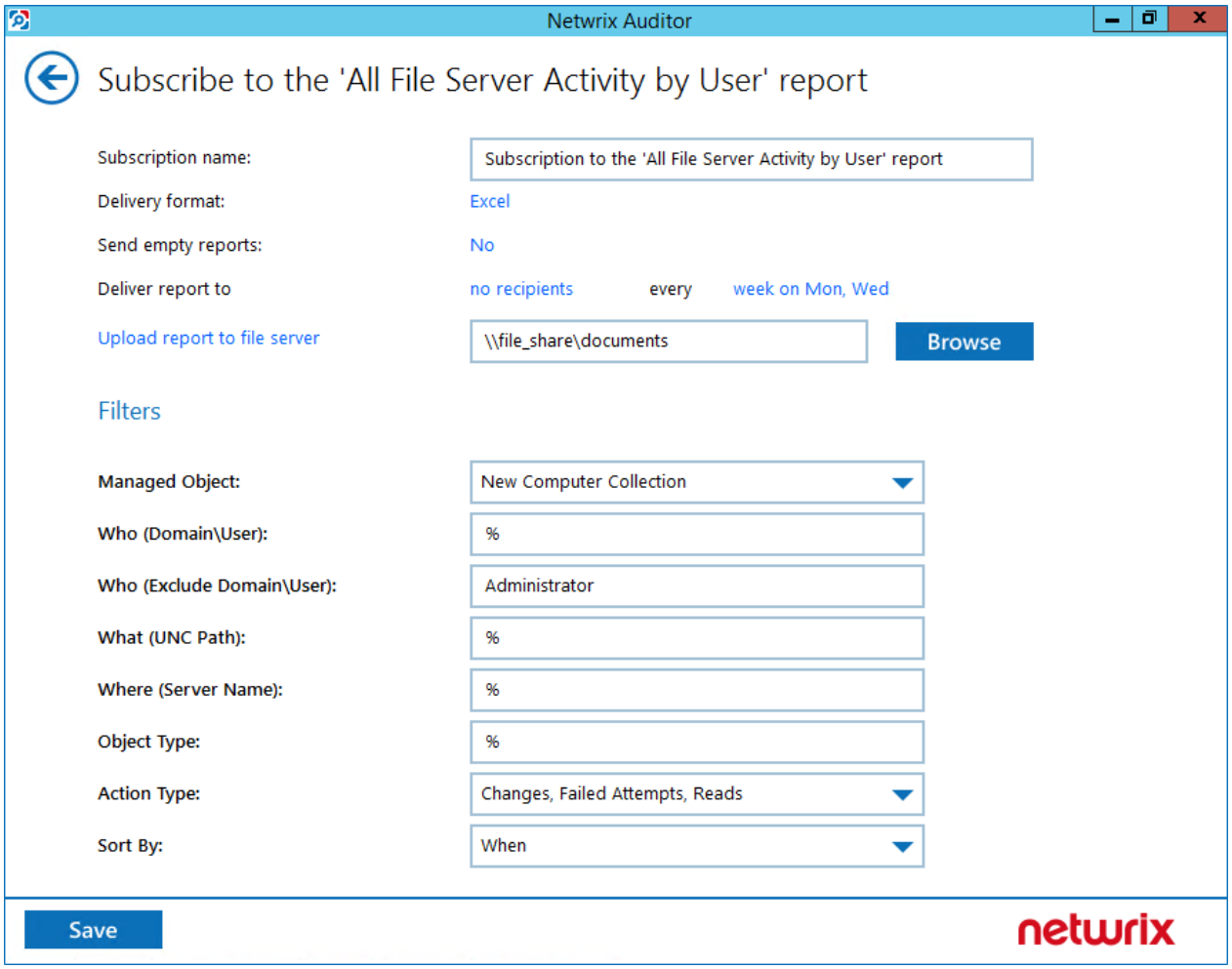
- The user support team has access to a folder with reports on account lockouts and password resets.
- File server helpdesk personnel have access to a different folder with daily reports listing all file removals.
- The helpdesk supervisor has access to both folders.



To publish reports to a file share

NOTE: Make sure that users who are going to access a file share have the **Read** share permissions. You can assign these permissions through folder properties.

1. In the Netwrix Auditor client, navigate to **Reports**.
2. Select a report and click **Subscribe**.
3. In the **Subscribe to report** window, select **Upload report to file server**, define a schedule (such as daily or weekly on Mondays), and specify filters to control what information is included in the report.



For more information on how to subscribe to reports, refer to the *"Subscriptions"* chapter in the Netwrix Auditor User Guide.

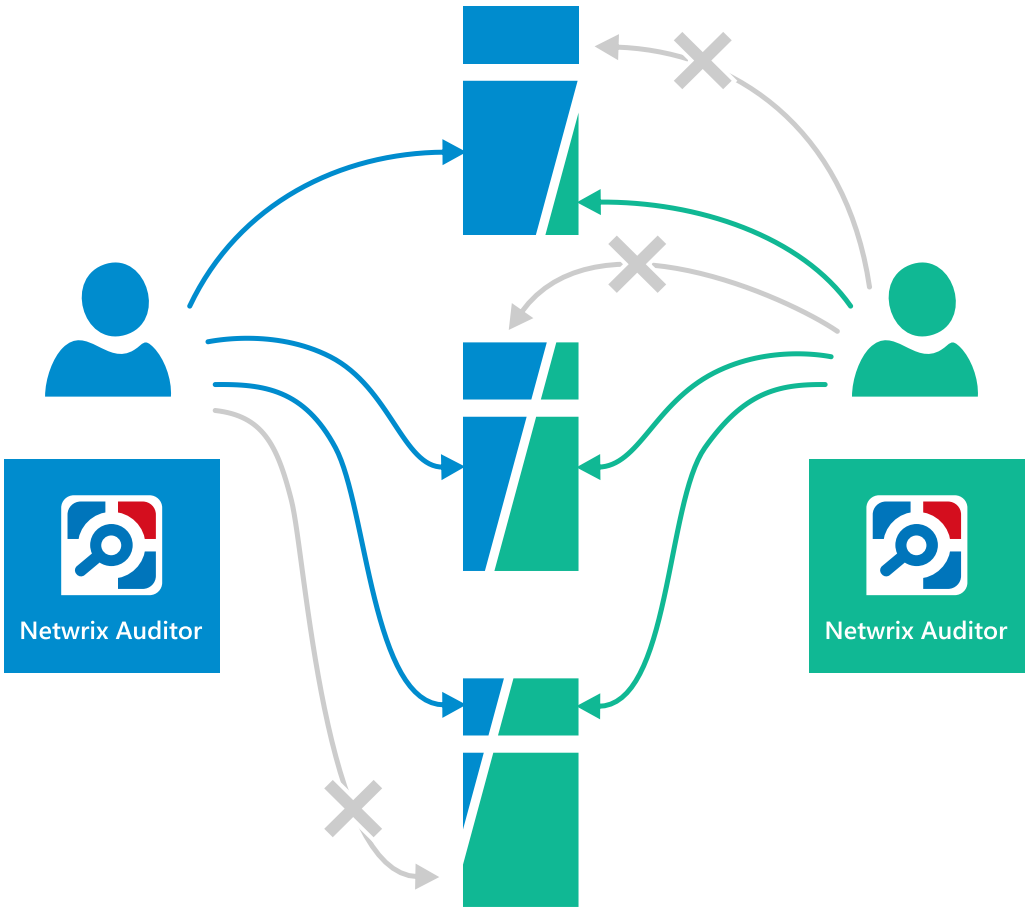
5. Additional Scenarios

Besides configuring role-based access, Netwrix suggests additional deployment and configuration scenarios. Review the scenarios below to achieve more granular separation of duties with Netwrix Auditor.

5.1. Install Multiple Instances of Netwrix Auditor

Some organizations require complete isolation of IT departments or groups. For example, database administrators (DBAs) have no access to Active Directory management data, domain administrators have no permissions to view database schemas. Both groups are interested in auditing changes with Netwrix Auditor, but must keep their data separately.

In this case, Netwrix recommends installing several instances of Netwrix Auditor in your IT infrastructure—one per group or department. For example, DBAs have their own instance of Netwrix Auditor and configure audit for SQL Server and underlying Windows Server configuration changes. Likewise, Active Directory administrators have their isolated installation of Netwrix Auditor configured to audit changes and configuration within their scope of responsibility. Both instances work independently.



Each IT group can leverage role separation capabilities within their instance of Netwrix Auditor: designate administrators, delegate read access to users, and publish reports for the recipients as needed.

NOTE: You can install as many Netwrix Auditors as needed. The number of installations is not limited by Netwrix policy as long as the total license count across all audited systems stays within the license terms.

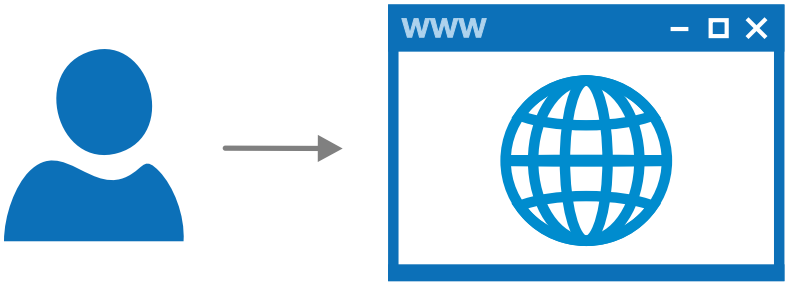
You cannot install several Netwrix Auditors side-by-side. Make sure to deploy them on different servers. Also, each Netwrix Auditor Administrator Console requires its own instance of SQL Server to store Audit Database.

The obvious caveat of this deployment scenario is that reports and search results are specific to the instance of Netwrix Auditor. At the same time, this scenario ensures complete isolation and data security—Netwrix Auditor configuration and data cannot be reviewed or modified outside the department or group.

5.2. Grant Access to Reports Through SSRS Web Interface

By default, recipients can review reports published on file shares or delivered by email. These reports are generated according to a schedule, have preset filtering and cannot be modified.

However, in a specific process, users need to access reports on demand. To provide this possibility, you can leverage the SQL Server Reporting Services (SSRS) web interface. Assign the **Browser** role to a user to enable access to a specific report or the entire report folder (all reports for an audited system). And then share the report URL with the user.



Report

Specifically, anyone granted access to a report through SSRS can:

- Generate report any time
- Review data for any configured Managed Object (e.g., across multiple servers or domains)
- Apply filters

For more information on how to grant such access, refer to the *"Configure Netwrix Auditor Roles"* chapter in the Netwrix Auditor Installation and Configuration Guide.

6. Related Documentation

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

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 integration 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 8.0, and suggests workarounds for these issues.