netwrix
#1 for change auditing

Netwrix Effective Permissions Reporting Tool

Quick-Start Guide

Version: 1.0
2/13/2015

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. Active Directory is a trademark of Microsoft Corporation. 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 Effective Permissions Reporting Tool. 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:

- Start network scanning
- See how effective permissions are reported

1.1. Netwrix Effective Permissions Reporting Tool Overview

Netwrix Effective Permissions Reporting Tool is a freeware product that collects data on effective permissions for selected network resources.

Netwrix Effective Permissions Reporting Tool checks effective permissions granted to a user or group by providing a report on *who* has access to *what* across your Active Directory domain or shared folders/files.

2. System Requirements

This section lists the requirements for the target environments that are going to be audited with Netwrix Effective Permissions Reporting Tool, and for the computer where the product is going to be installed.

2.1. Requirements for Target Environments

The table below provides the requirements for the target environments that can be audited with Netwrix Effective Permissions Reporting Tool:

Target Environment	Supported Versions
Active Directory	• Domain Controllers OS versions: Windows Server 2008 and above
Files and Shares	• Desktop OS: Windows 7 (32 and 64-bit) and above • Server OS: Windows Server 2008 and above

2.2. Requirements to Install Netwrix Effective Permissions Reporting Tool

This section provides the requirements for the computer where Netwrix Effective Permissions Reporting Tool is going to be installed.

Review the following for additional information:

- Hardware Requirements
- Software Requirements

2.2.1. Hardware Requirements

The table below lists the minimum hardware requirements for the Netwrix Effective Permissions Reporting Tool installation:

Hardware Component	Minimum	Recommended
Processor	Intel or AMD 32 bit, 2 GHz	Intel Core 2 Duo 2x or AMD 64 bit, 3GHz
RAM	512 MB	4 GB

Hardware Component	Minimum	Recommended
Disk Space	50 MB physical disk space	100 MB physical disk space
Screen resolution	1024 x 768	Screen resolution recommended by your screen manufacturer.

2.2.2. Software Requirements

The table below lists the minimum software requirements for the Netwrix Effective Permissions Reporting Tool installation:

Component	Requirements
Operating system	• Desktop OS: Windows 7 (32 and 64-bit) and above • Server OS: Windows Server 2008 R2 and above
Framework	• .Net Framework 3.5 SP1

2.3. Deployment Options

The table below provides recommendations on how best to deploy Netwrix Effective Permissions Reporting Tool:

Install on...	To check effective permissions for...
Any computer that belongs to the monitored Active Directory domain or trusted domain	• Domains, OUs, etc. • Domain users and groups • Shared folders/files

3. Configure Rights And Permissions

To ensure successful network resources scanning, the account used by Netwrix Effective Permissions Reporting Tool to collect audit data from the monitored domain or shared folders/files must comply with the following requirements:

To check the effective permissions for...	Required Permissions
Users, Active Directory objects (domains, OUs, etc.)	• Read all properties • List contents • Read permissions
Shared folders/files (based on share permissions)	• Member of the **local Administrators** group on the computer where the target shared folder/file is located.
Shared folders/files (based on the NTFS permissions)	• List folder contents • Read permissions

Perform the following procedures:

- Configure Account to Scan Permissions on Active Directory Objects
- Configure Account to Scan Permissions on Shared Files and Folders

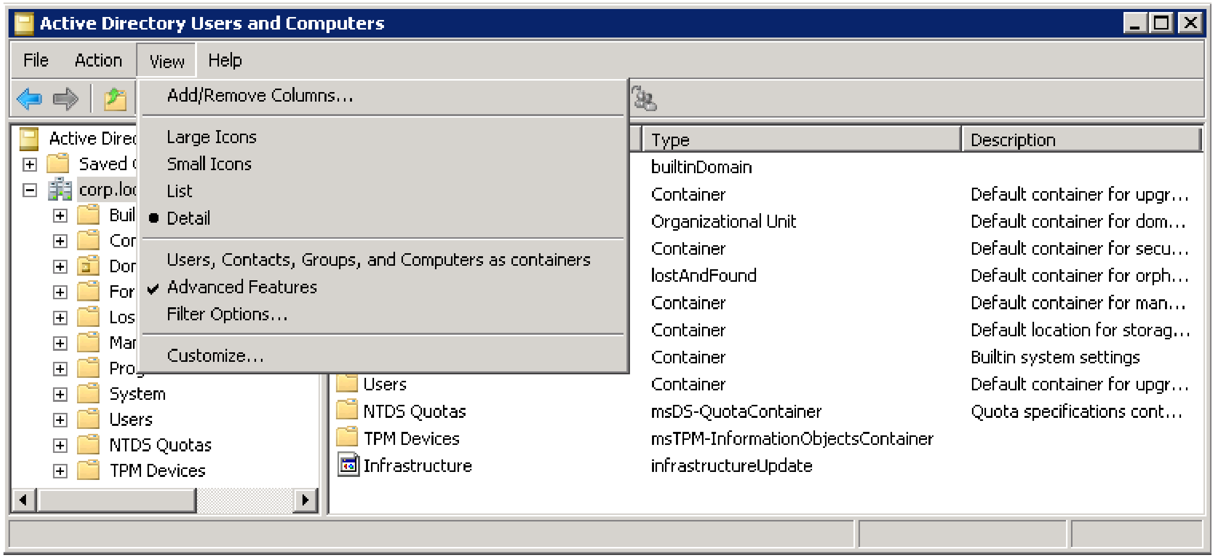
3.1. Configure Account to Scan Permissions on Active Directory Objects

Perform the following procedures:

- To configure account to scan permissions on AD objects on pre-Windows Server 2012 versions
- To configure account to scan permissions on AD objects on Windows Server 2012 and above

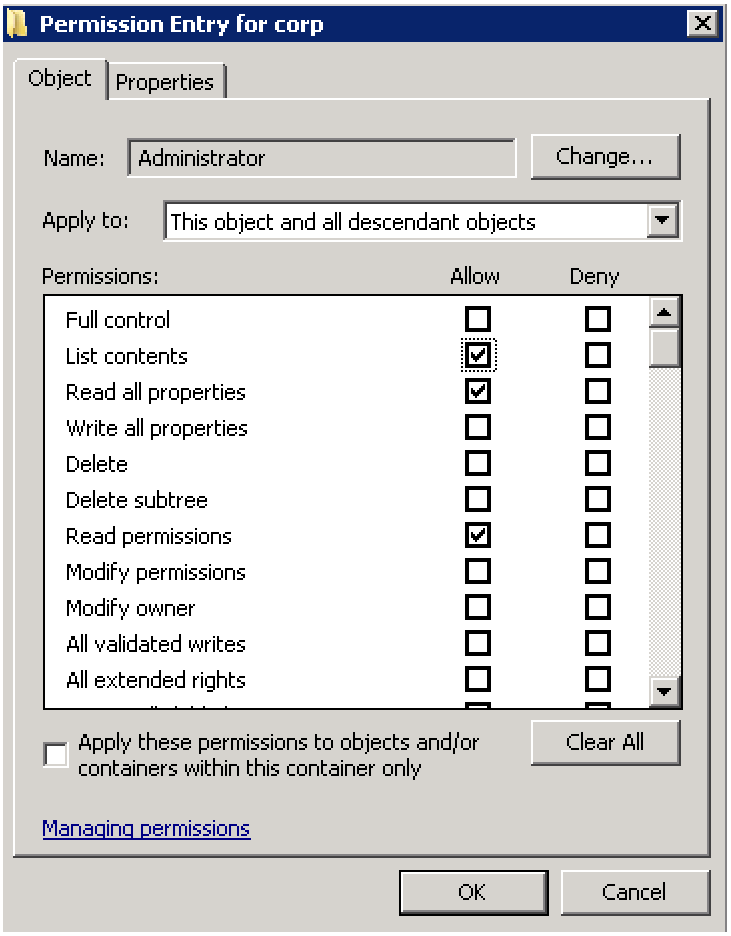
To configure account to scan permissions on AD objects on pre-Windows Server 2012 versions

1. Open the **Active Directory Users and Computers** console on any domain controller in the target domain: Navigate to **Start** → **Administrative Tools** → **Active Directory Users and Computers**.
2. In the **Active Directory Users and Computers** dialog, click **View** in the main menu and ensure that the **Advanced Features** are enabled.



	Type	Description
	builtinDomain	
	Container	Default container for upgr...
	Organizational Unit	Default container for dom...
	Container	Default container for secu...
	lostAndFound	Default container for orph...
	Container	Default container for man...
	Container	Default location for storag...
	Container	Builtin system settings
Users	Container	Default container for upgr...
NTDS Quotas	msDS-QuotaContainer	Quota specifications cont...
TPM Devices	msTPM-InformationObjectsContainer	
Infrastructure	infrastructureUpdate	

3. Right-click the Active Directory object for which you want to be able to check effective permissions and select **Properties**. Select the **Security** tab and click **Advanced**.
4. In the **Advanced Security Settings for <Object_Name>** dialog, click **Add**.
5. In the **Select user, Computer, Service account, or Group** dialog, type the name of the account or group you want to be able to check effective permissions.
6. In the **Permission Entry for <Object_Name>** dialog, set the *"Allow"* flag next to the following options:
   - List contents
   - Read all properties
   - Read permissions



Name: Administrator

Apply to: This object and all descendant objects

Permissions:

Permissions	Allow	Deny
Full control	☐	☐
List contents	☑	☐
Read all properties	☑	☐
Write all properties	☐	☐
Delete	☐	☐
Delete subtree	☐	☐
Read permissions	☑	☐
Modify permissions	☐	☐
Modify owner	☐	☐
All validated writes	☐	☐
All extended rights	☐	☐

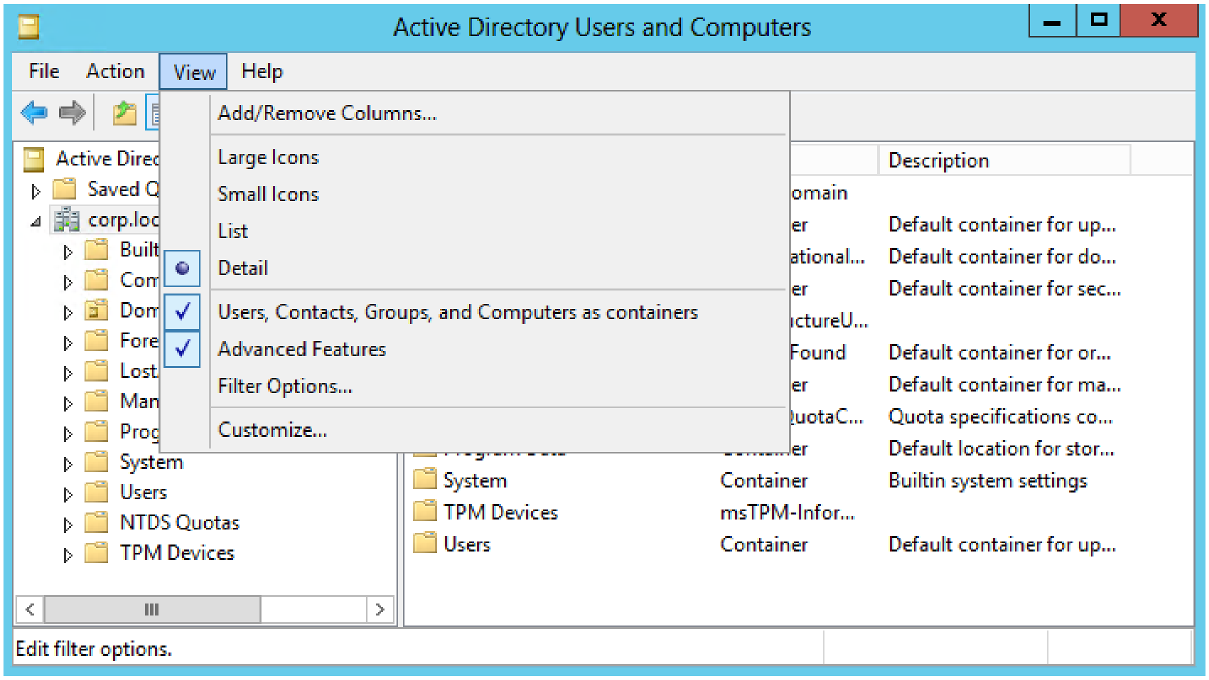
☐ Apply these permissions to objects and/or containers within this container only

NOTE: Make sure that **Apply onto** is set to *"This object and all descendant objects"*, and **Apply these auditing entries to objects and/or containers within this container only** is cleared.

To configure account to scan permissions on AD objects on Windows Server 2012 and above

1. Open the **Active Directory Users and Computers** console on any domain controller in the target domain: Navigate to **Start** → **Administrative Tools** → **Active Directory Users and Computers**.

2. In the **Active Directory Users and Computers** dialog, click **View** in the main menu and ensure that the **Advanced Features** are enabled.

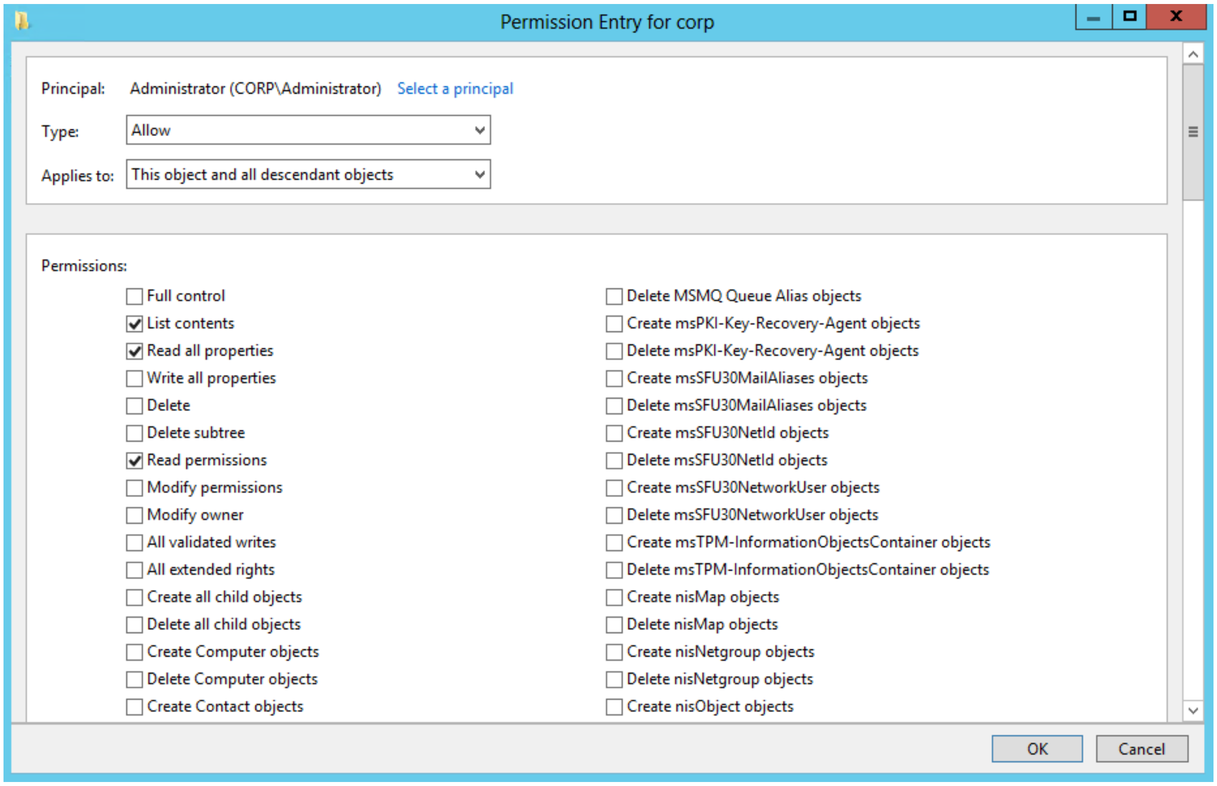


3. Right-click the Active Directory object for which you want to check effective permissions and select **Properties**. Select the **Security** tab and click **Advanced**.

4. In the **Advanced Security Settings for <object name>** dialog, click **Add**.

5. In the **Permission Entry for <Object_Name>** dialog, click **Select a Principal** link .

6. In the **Select user, Computer, Service account, or Group** dialog, type the name of an account or group you want to be able to check effective permissions.



Permission Entry for corp

Principal: Administrator (CORP\Administrator) Select a principal

Type: Allow

Applies to: This object and all descendant objects

Permissions:

- ☐ Full control
- ☑ List contents
- ☑ Read all properties
- ☐ Write all properties
- ☐ Delete
- ☐ Delete subtree
- ☑ Read permissions
- ☐ Modify permissions
- ☐ Modify owner
- ☐ All validated writes
- ☐ All extended rights
- ☐ Create all child objects
- ☐ Delete all child objects
- ☐ Create Computer objects
- ☐ Delete Computer objects
- ☐ Create Contact objects
- ☐ Delete MSMQ Queue Alias objects
- ☐ Create msPKI-Key-Recovery-Agent objects
- ☐ Delete msPKI-Key-Recovery-Agent objects
- ☐ Create msSFU30MailAliases objects
- ☐ Delete msSFU30MailAliases objects
- ☐ Create msSFU30NetId objects
- ☐ Delete msSFU30NetId objects
- ☐ Create msSFU30NetworkUser objects
- ☐ Delete msSFU30NetworkUser objects
- ☐ Create msTPM-InformationObjectsContainer objects
- ☐ Delete msTPM-InformationObjectsContainer objects
- ☐ Create nisMap objects
- ☐ Delete nisMap objects
- ☐ Create nisNetgroup objects
- ☐ Delete nisNetgroup objects
- ☐ Create nisObject objects

7. Set **Type** to *"Allow"* and **Applies to** to *"This object and all descendant objects"*. Under **Permissions**, select the *List Contents*, *Read all properties* and *Read permissions* checkboxes.

3.2. Configure Account to Scan Permissions on Shared Files and Folders

Perform the following procedures:

- Configure Account to Scan NTFS Permissions on Shared Files and Folders
- Configure Account to Scan Share Permissions on Shared Files and Folders

3.2.1. Configure Account to Scan NTFS Permissions on Shared Files and Folders

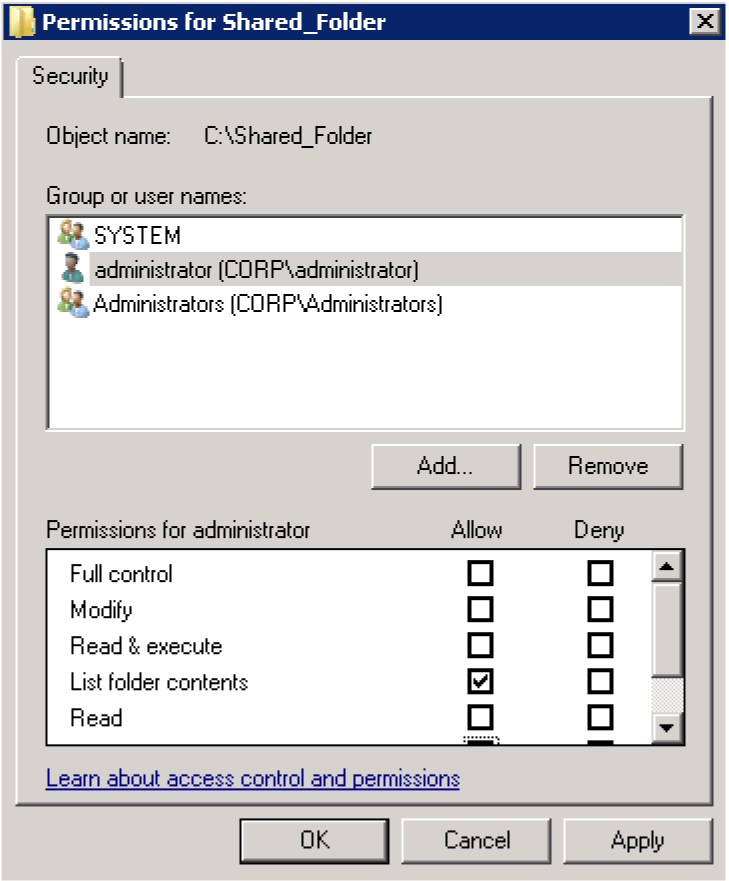
Do one of the following depending on the OS:

- To configure account to scan NTFS permissions on pre-Windows Server 2012 versions
- To configure account to scan NTFS permissions on Windows Server 2012 and above

To configure account to scan NTFS permissions on pre-Windows Server 2012 versions

- *To grant the List Folder Content permission on pre-Windows Server 2012 versions*

1. Navigate to the target shared folder/file, right-click it and select **Properties**.
2. In the **<Share_Name> Properties** dialog, select the **Security** tab and click **Edit**.
3. In the **Permissions for <Share_Name>** dialog, click **Add** to add an account or group you want to be able to check effective permissions.


Permissions for Shared_Folder
Security
Add...
Remove
Learn about access control and permissions
OK
Cancel
Apply

Object name: C:\Shared_Folder

Group or user names:

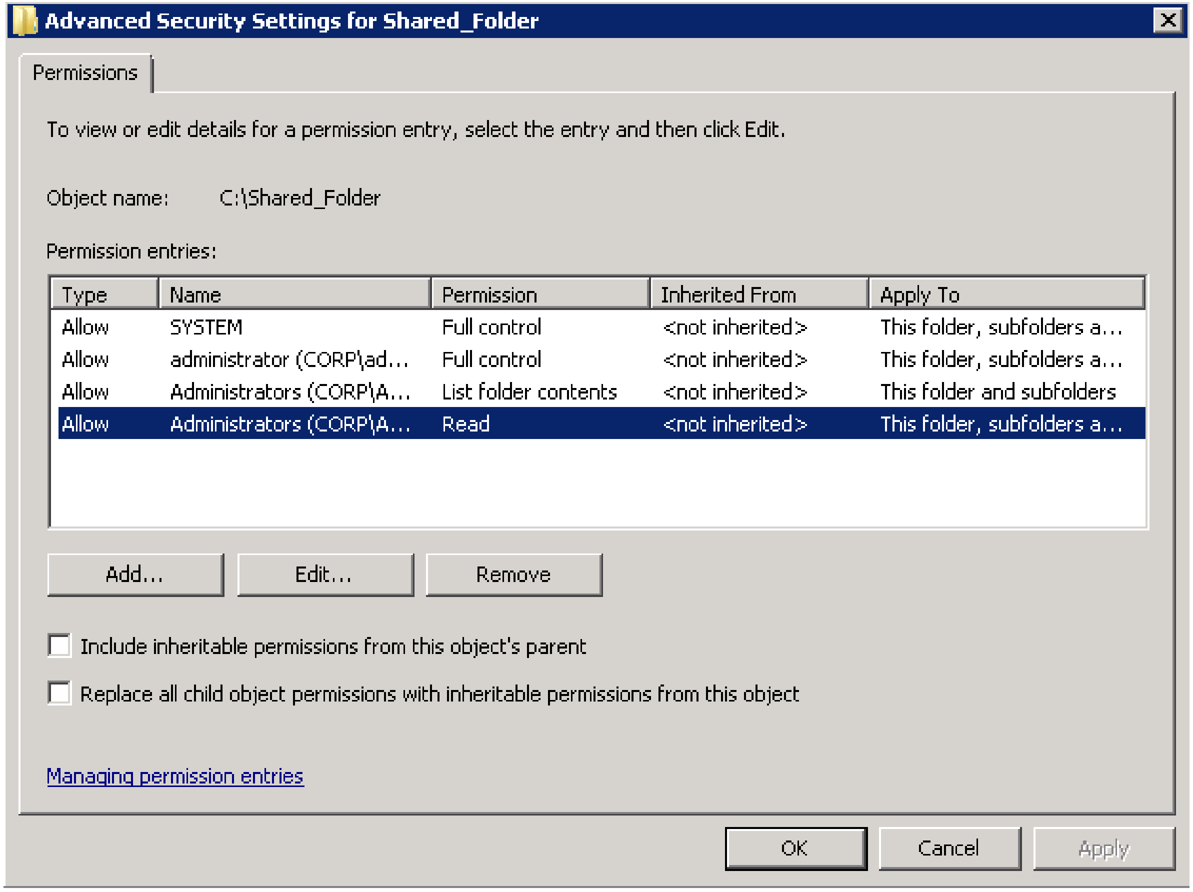
- SYSTEM
- administrator (CORP\administrator)
- Administrators (CORP\Administrators)

Permissions for administrator	Allow	Deny
Full control	□	□
Modify	□	□
Read & execute	□	□
List folder contents	☑	□
Read	□	□

4. Locate the newly added account or group and set the *"Allow"* flag next to the following options:
   - List folder contents

- *To grant Read Permissions on pre-Windows Server 2012 versions*

1. Navigate to the target shared folder/file, right-click it and select **Properties**.
2. In the **<Share_Name> Properties** dialog, select the **Security** tab and click **Advanced**.
3. In the **Advanced Security Settings for <Share_Name>** dialog, click **Change Permissions**.



Advanced Security Settings for Shared_Folder

Permissions

To view or edit details for a permission entry, select the entry and then click Edit.

Object name: C:\Shared_Folder

Permission entries:

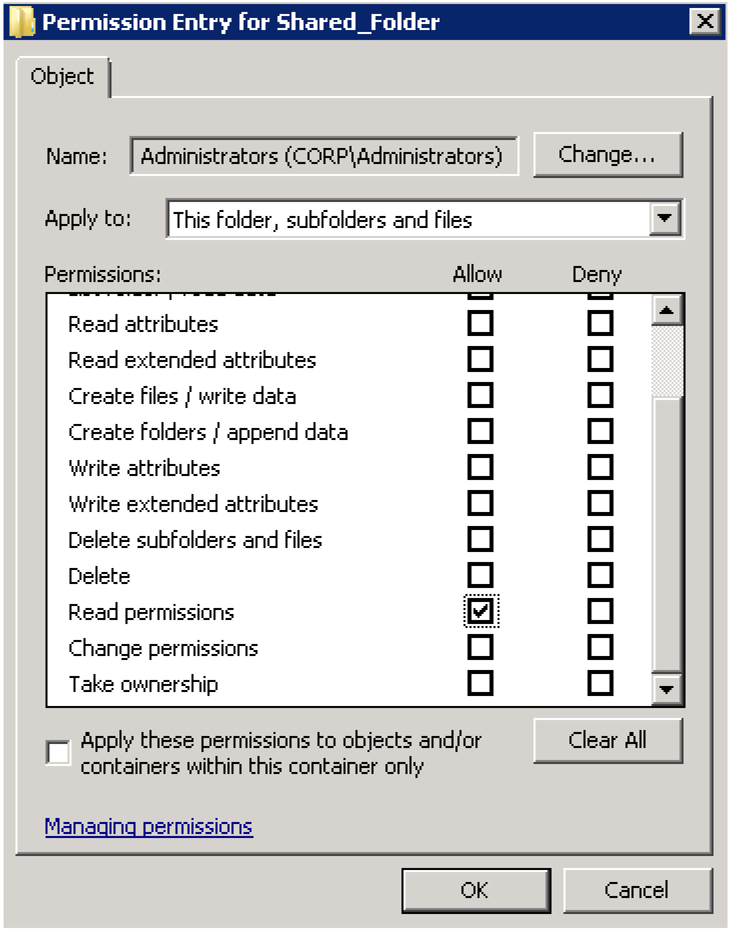
Type	Name	Permission	Inherited From	Apply To
Allow	SYSTEM	Full control	<not inherited>	This folder, subfolders a...
Allow	administrator (CORP\ad...	Full control	<not inherited>	This folder, subfolders a...
Allow	Administrators (CORP\A...	List folder contents	<not inherited>	This folder and subfolders
Allow	Administrators (CORP\A...	Read	<not inherited>	This folder, subfolders a...

☐ Include inheritable permissions from this object's parent

☐ Replace all child object permissions with inheritable permissions from this object

Managing permission entries

4. Click **Add** to add an account or group you want to be able to check effective permissions.
5. In the **Select user, Computer, Service account, or Group** dialog, type the name of the account or group you want to be able to check effective permissions.
6. In the **Permissions Entry for <Share_Name>** dialog, set the *"Allow"* flag next to the following options:
   - Read permissions



Permission Entry for Shared_Folder

Object

Name: Administrators (CORP\Administrators) Change...

Apply to: This folder, subfolders and files

Permissions:	Allow	Deny
Read attributes	□	□
Read extended attributes	□	□
Create files / write data	□	□
Create folders / append data	□	□
Write attributes	□	□
Write extended attributes	□	□
Delete subfolders and files	□	□
Delete	□	□
Read permissions	☑	□
Change permissions	□	□
Take ownership	□	□

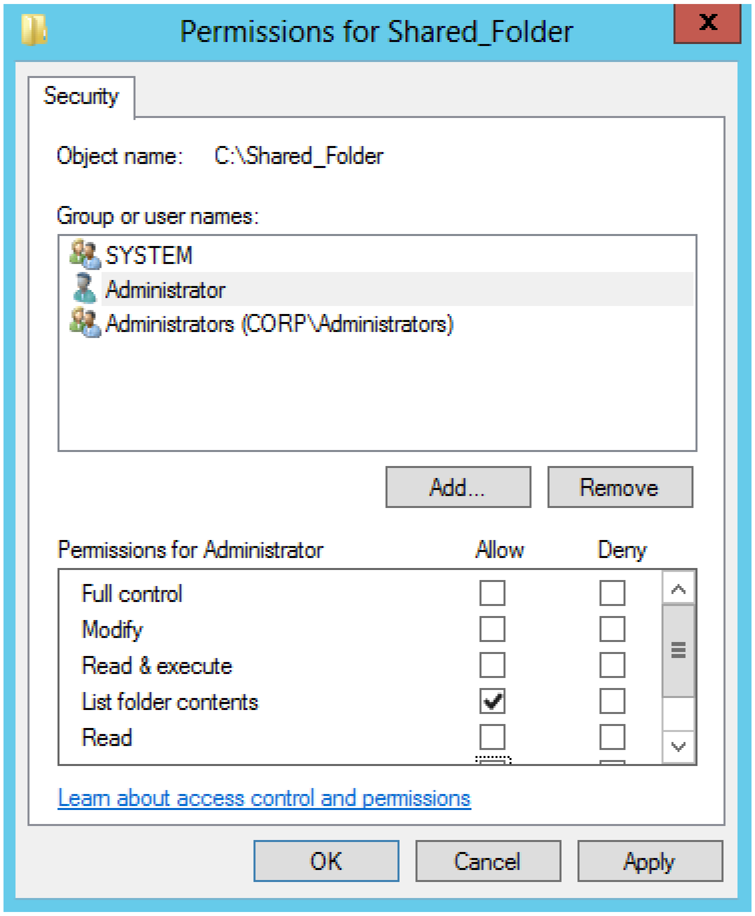
□ Apply these permissions to objects and/or containers within this container only

NOTE: Make sure that **Apply to:** is set to *"This folder, subfolders and files"*, and **Apply these auditing entries to objects and/or containers within this container only** is cleared.

To configure account to scan NTFS permissions on Windows Server 2012 and above

- *To grant the List Folder Content permission on Windows Server 2012 and above*

1. Navigate to the target shared folder/file, right-click it and select **Properties**.
2. In the **<Share_Name> Properties** dialog, select the **Security** tab and click **Edit**.
3. In the **Permissions for <Share_Name>** dialog, click **Add** to add an account or group you want to be able to check effective permissions.



Permissions for Shared_Folder

Security

Object name: C:\Shared_Folder

Group or user names:

- SYSTEM
- Administrator
- Administrators (CORP\Administrators)

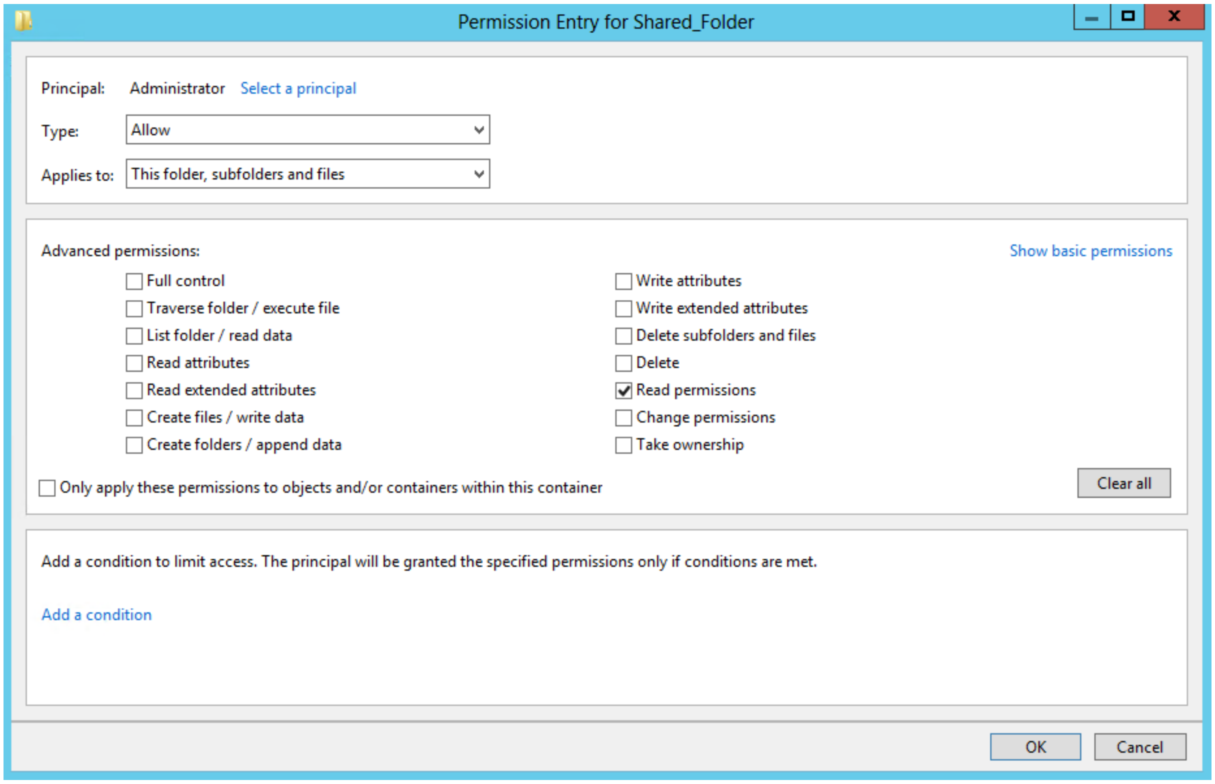
Permissions for Administrator	Allow	Deny
Full control	□	□
Modify	□	□
Read & execute	□	□
List folder contents	☑	□
Read	□	□

4. Locate the newly added account or group and set the *"Allow"* flag next to the following options:

   - List folder contents

- ***To grant Read Permissions on Windows Server 2012 and above***

1. Navigate to the target shared folder/file, right-click it and select **Properties**.
2. In the **<Share_Name> Properties** dialog, select the **Security** tab and click **Advanced**.
3. In the **Advanced Security Settings for <Share_Name>** dialog, click **Add**.
4. In the **Permission Entry for <Share_Name>** dialog, click the **Select a principal** link.
5. In the **Select user, Computer, Service account, or Group** dialog, type the name of an account or group you want to be able to check effective permissions.
6. In the **Permission Entry for <Share_Name>** dialog, click **Advanced**.



Permission Entry for Shared_Folder

Principal: Administrator Select a principal

Type: Allow

Applies to: This folder, subfolders and files

Advanced permissions:

Show basic permissions

□ Full control
□ Traverse folder / execute file
□ List folder / read data
□ Read attributes
□ Read extended attributes
□ Create files / write data
□ Create folders / append data

□ Write attributes
□ Write extended attributes
□ Delete subfolders and files
□ Delete
☑ Read permissions
□ Change permissions
□ Take ownership

□ Only apply these permissions to objects and/or containers within this container

Clear all

Add a condition to limit access. The principal will be granted the specified permissions only if conditions are met.

Add a condition

OK Cancel

7. Set Type to *"Allow"* and **Applies to** to *"This folder, subfolders and files"*. Under **Permissions**, select the *Read permissions* checkbox.

NOTE: Make sure that the **Only apply these auditing settings to objects and/or containers within this container** checkbox is cleared.

3.2.2. Configure Account to Scan Share Permissions on Shared Files and Folders

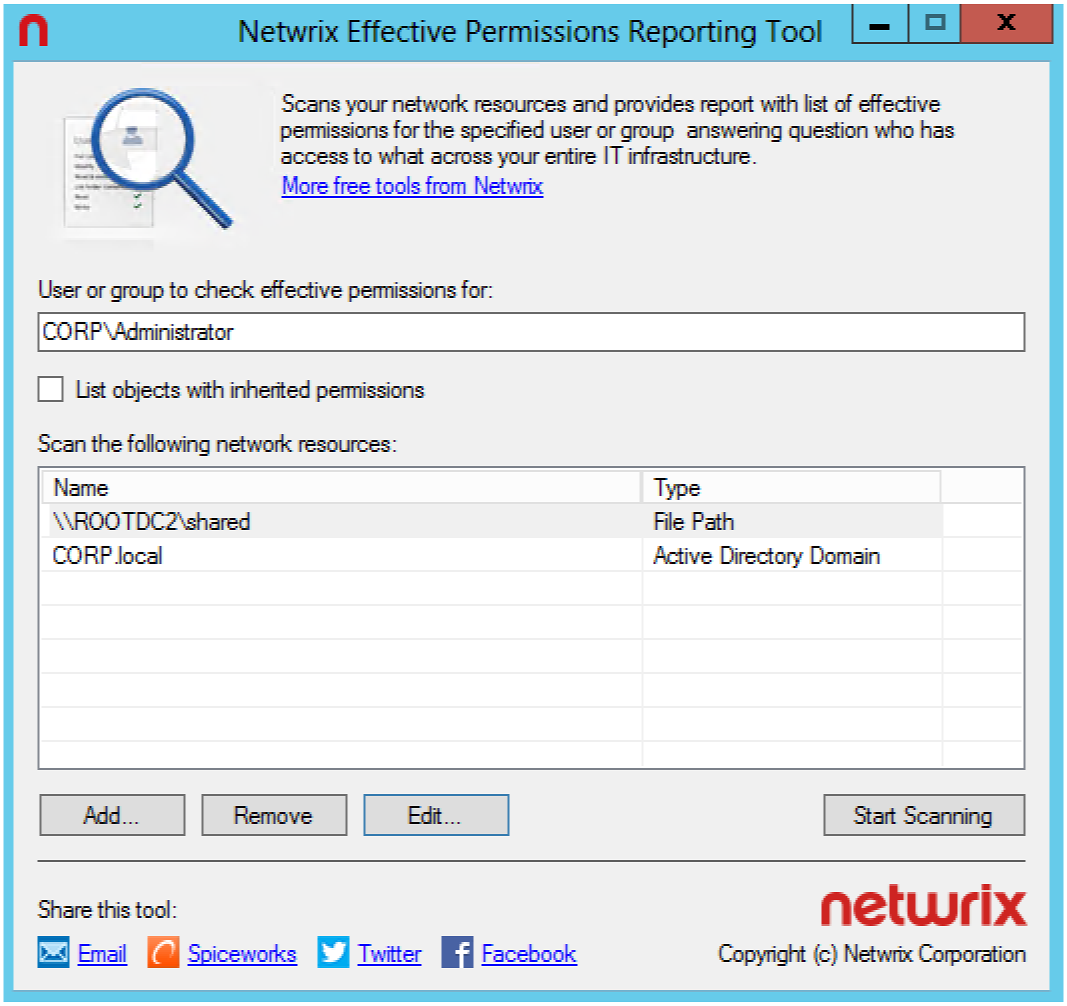
To ensure successfull scanning your shared folder/file, the account used by Netwrix Effective Permissions Reporting Tool to check permissions must be a member of the **local Administrators** group on the computer where the target shared folder/file is located.

4. Start Using Netwrix Effective Permissions Reporting Tool

To start collecting data on your IT Infrastructure, you must configure Netwrix Effective Permissions Reporting Tool.

1. Run the installation package.

   NOTE: To invoke Netwrix Effective Permissions Reporting Tool again, navigate to the *%Netwrix Effective Permissions Reporting Tool installation folder%* and click on the product icon.



Netwrix Effective Permissions Reporting Tool

Scans your network resources and provides report with list of effective permissions for the specified user or group answering question who has access to what across your entire IT infrastructure.

More free tools from Netwrix

User or group to check effective permissions for:

CORP\Administrator

☐ List objects with inherited permissions

Scan the following network resources:

Name	Type
\\ROOTDC2\shared	File Path
CORP.local	Active Directory Domain

2. Complete the following fields:

Option	Description
User or group to check effective permissions for:	Specify a user name or group name for whom you want to check effective permissions in the *DOMAIN\user* format.
List objects with inherited permissions	Enable the checkbox to include objects with inherited permissions to the report. **NOTE:** Refer to the Windows Server TechCenter article for more information: Inherited Permissions.
Scan the following network resources:	1. Click **Add**. 2. In the **Specify Network Resource** dialog, select one of the following: • **Active Directory**—Provide the audited Active Directory object name (domain, OU, etc.) in the FQDN format, e.g. **CORP.local**. In the screenshot above, the report on effective permissions granted to the **CORP\Administrator** user for the **CORP.local** domain will be shown. • **File Path**—Provide the UNC file path, e.g. **\\ROOTDC2\shared**. In the screenshot above, the report on effective permissions granted to the **CORP\Administrator** user for the **\\ROOTDC2\shared** file share will be shown.

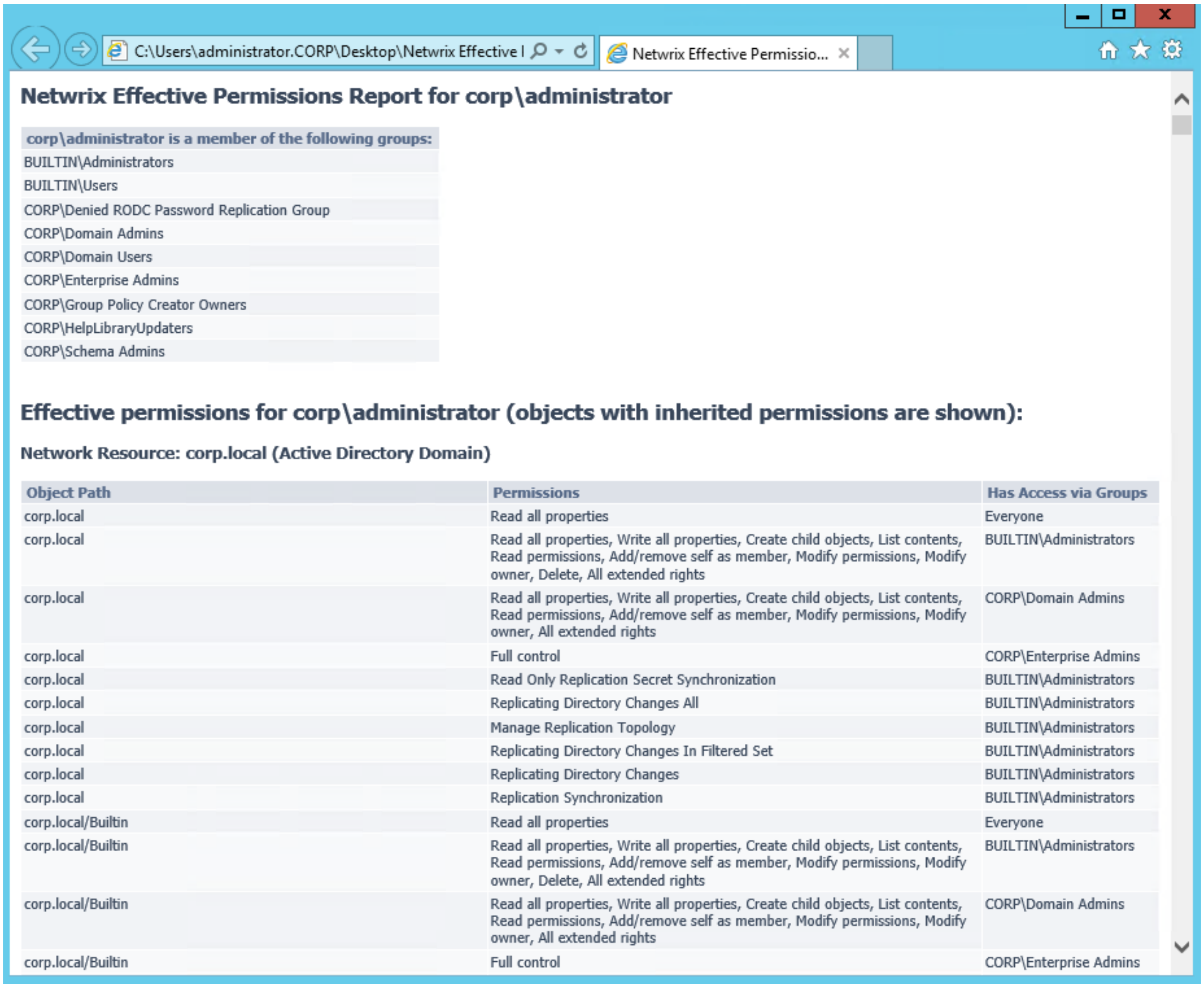
3. Click **Start scanning** to launch data collection.

4. In the **Save Effective Permissions Report** dialog that opens, specify the name of the new report and select its location. The report file will be saved in the HTML format and displayed in a default web browser.

5. In the **Netwrix Effective Permissions Reporting Tool** dialog, click **OK** to save the report.

5. See How Effective Permissions Are Reported

After the data collection has completed, see how effective permissions are reported by the product. This section explains how to review the Effective Permissions Report.


C:\Users\administrator.CORP\Desktop\Netwrix Effective I
Netwrix Effective Permissio...

Netwrix Effective Permissions Report for corp\administrator

corp\administrator is a member of the following groups:
BUILTIN\Administrators
BUILTIN\Users
CORP\Denied RODC Password Replication Group
CORP\Domain Admins
CORP\Domain Users
CORP\Enterprise Admins
CORP\Group Policy Creator Owners
CORP\HelpLibraryUpdaters
CORP\Schema Admins

Effective permissions for corp\administrator (objects with inherited permissions are shown):

Network Resource: corp.local (Active Directory Domain)

Object Path	Permissions	Has Access via Groups
corp.local	Read all properties	Everyone
corp.local	Read all properties, Write all properties, Create child objects, List contents, Read permissions, Add/remove self as member, Modify permissions, Modify owner, Delete, All extended rights	BUILTIN\Administrators
corp.local	Read all properties, Write all properties, Create child objects, List contents, Read permissions, Add/remove self as member, Modify permissions, Modify owner, All extended rights	CORP\Domain Admins
corp.local	Full control	CORP\Enterprise Admins
corp.local	Read Only Replication Secret Synchronization	BUILTIN\Administrators
corp.local	Replicating Directory Changes All	BUILTIN\Administrators
corp.local	Manage Replication Topology	BUILTIN\Administrators
corp.local	Replicating Directory Changes In Filtered Set	BUILTIN\Administrators
corp.local	Replicating Directory Changes	BUILTIN\Administrators
corp.local	Replication Synchronization	BUILTIN\Administrators
corp.local/Builtin	Read all properties	Everyone
corp.local/Builtin	Read all properties, Write all properties, Create child objects, List contents, Read permissions, Add/remove self as member, Modify permissions, Modify owner, Delete, All extended rights	BUILTIN\Administrators
corp.local/Builtin	Read all properties, Write all properties, Create child objects, List contents, Read permissions, Add/remove self as member, Modify permissions, Modify owner, All extended rights	CORP\Domain Admins
corp.local/Builtin	Full control	CORP\Enterprise Admins

The example report provides the following information:

Parameter	Description
Netwrix Effective Permissions Report for <User_Name>	
<User_Name> is a member of the following groups:	The list of Active Directory groups where the user belongs to.

Parameter	Description
Effective permissions for <User_Name> (objects with inherited permissions are shown/hidden)	
Network Resource: **<Resource_Name>**	The name of the network resource: **Active Directory domain** or **File Path**.
Object Path	• When **Active Directory domain** selected: Active Directory object (the audited OU, container within a domain, domain user, etc.) name in the FQDN format. • When **Files and Shares** selected: the UNC file path.
Permissions	Contains a list of effective permissions granted to groups which are shown in the **Has Access via Groups** column for the selected network resource.
Has Access via Groups	The list of Active Directory groups where the user belongs to with effective permissions for the selected network resource.