

NTFS Permissions Management Best Practices

Enter Your Business Email

Download Free Guide (.PDF)

We never share your data. [Privacy Policy \(/privacy.html\)](/privacy.html)

Configuring NTFS Permissions

- ✓ Create a file server permissions policy that clearly defines your permissions management process.
- ✓ Use Active Directory groups ([active_directory_group_management.html](#)) everywhere. Don't assign NTFS permissions to individuals, even if you have to create hundreds of groups. It's far easier to manage 200 groups than 2,000 one-off permissions.
- ✓ Configure NTFS permissions for the assets, assign roles to those permissions, and assign people to roles. For example, suppose you have a share named **HR** on **fileserver1**. Do the following:



1. For this share, create the following domain local groups in your AD with the permissions shown:

- ✓ *fileserver1_HR_read (Read-only)*
- ✓ *fileserver1_HR_modify (Read and Modify)*
- ✓ *fileserver1_HR_fullcontrol (Full Control)*

We use cookies and other tracking technologies to improve our website and your web experience. To learn more, please read our [Privacy Policy \(/privacy.html#cookie_policy\)](#).

2. Use these groups to set NTFS permissions to the appropriate user rights.

Okay, got it

3. Create a global group in AD named **HR** for your HR people. Add this global group to the domain local group **fileserver1_HR_read**, and then add user accounts to the global group **HR**. What you have now done is tied an asset to a permission, and the permissions to a role. As you expand your network and add different assets and areas of access to the role, you'll be able to easily see what assets a role can access.

People (user accounts) -> Role (AD global group) -> Permissions (AD domain local group) -> Asset (file or folder on a file server)

- ✓ Avoid giving users the Full Control permission. Full Control enables users to change NTFS permissions, which average users should not need to do. Modify rights should be all that's necessary for most users.
- ✓ Assign the most restrictive permissions that still allow users to perform their jobs. For example, if users need only to read information in a folder and not to change, delete or create files, assign the Read permission only.
- ✓ Remove the Everyone permission from every resource except the global folder designated for file exchanges.
- ✓ Create a **Global Deny** group so that when employees leave the company, you can quickly remove all their file server access by making them members of that group.
- ✓ Avoid breaking permissions inheritance as much as possible. There will be a few folders where this may be necessary, but generally avoid it. If something would break inheritance, then it either needs to move up a level or you need to reassess who's got what permissions on the parent folder. For example, if a you need to give someone Read/Write permissions for all of the **\Finance** folder but not **\Finance\Budget**, you're gonna have a bad time later.
- ✓ Have users log on using domain user accounts rather than local accounts. This approach centralizes the administration of share permissions.
- ✓ All permissions changes should be audited ([how_to_audit_file_permission_changes.html](#)) as they occur, and the permissions hierarchy should be audited at least once a year.

Configuring File Shares

We use cookies and other tracking technologies to improve our website and your web experience. To learn more, please read our Privacy Policy ([/privacy.html#cookie_policy](#)).

- ✓ Create a top-level folder that will serve as the root storage folder for all user-created data (for example, **C:\Data**). Create sub-folders in it to segregate and organize data

Okay, got it

according to job roles and security requirements.

- ✓ Ensure that only IT can create root-level folders. Don't even let managers or executive create folders at the top 1 or 2 levels. If you don't lock down the root-level hierarchy, your neat folder structure will quickly be destroyed. Departments can organize their folders how they want, but don't allow junk folders.
- ✓ Organize your resources so that objects with the same security requirements are located in the same folder. For example, if users require the Read permission for several application folders, store those folders in the same parent folder. Then give Read permissions to the parent folder, rather than sharing each individual application folder separately.
- ✓ Make sure access-based enumeration is enabled. Access-based enumeration displays only the files and folders that a user has permissions to access. If a user does not have Read (or equivalent) permissions for a folder, Windows hides the folder from the user's view.
- ✓ Set the Windows file share permissions pretty leniently — give Everyone, Authenticated Users or Domain Users the Full Control or Change permissions — and rely on NTFS for the real permissions management.
- ✓ Avoid having nested shares in your file structures because they can create conflicting behavior for the same network resources if it is accessed through different shares. This can be asking for trouble, especially when the share permissions are different. A nested share is a shared folder that resides in a separate shared folder. There are, of course, the default hidden shares (C\$, D\$, etc.), which make all shares nested beneath them, and they're a default. However, if your users use two separate non-hidden shares that are nested, there can be conflicting share permissions.
- ✓ Know when to copy and when to move. Standard copy and move operations deliver default results that can maintain your configured NTFS permissions — or break them. Copy operations will create the permissions of the destination container, and move operations will maintain that of the parent container. To keep this straight, just remember **CC/MM — Copies Create, Moves Maintain**.

Top 5 NTFS Permissions Tools

We use cookies and other tracking technologies to improve our website and your web experience. To learn more, please read our Privacy Policy (/privacy.html#cookie_policy).

Okay, got it

✓ **Effective Permissions Reporting Tool**

([netwrix_effective_permissions_reporting_tool.html](#)) from Netwrix

✓ **NTFS Permissions Reporter**

(<http://www.cjwdev.com/Software/NtfsReports/Info.html>) from Cjwdev

✓ **Access Enum** (<https://docs.microsoft.com/en-us/sysinternals/downloads/accessenum>)

(Microsoft utility)

✓ **Permissions Reporter** (<http://www.permissionsreporter.com/download>) from Key

Metric Software

✓ **Permissions Analyzer** (<http://www.solarwinds.com/free-tools/permissions-analyzer-for-active-directory>) from SolarWinds

Exporting NTFS Permissions via Powershell

✓ Exporting folder permissions using PowerShell

([how_to_get_ntfs_permissions_report.html](#))

✓ Exporting user permissions using PowerShell

([how_to_monitor_excessive_permissions_in_everyone_group_on_windows_file_servers.html](#))

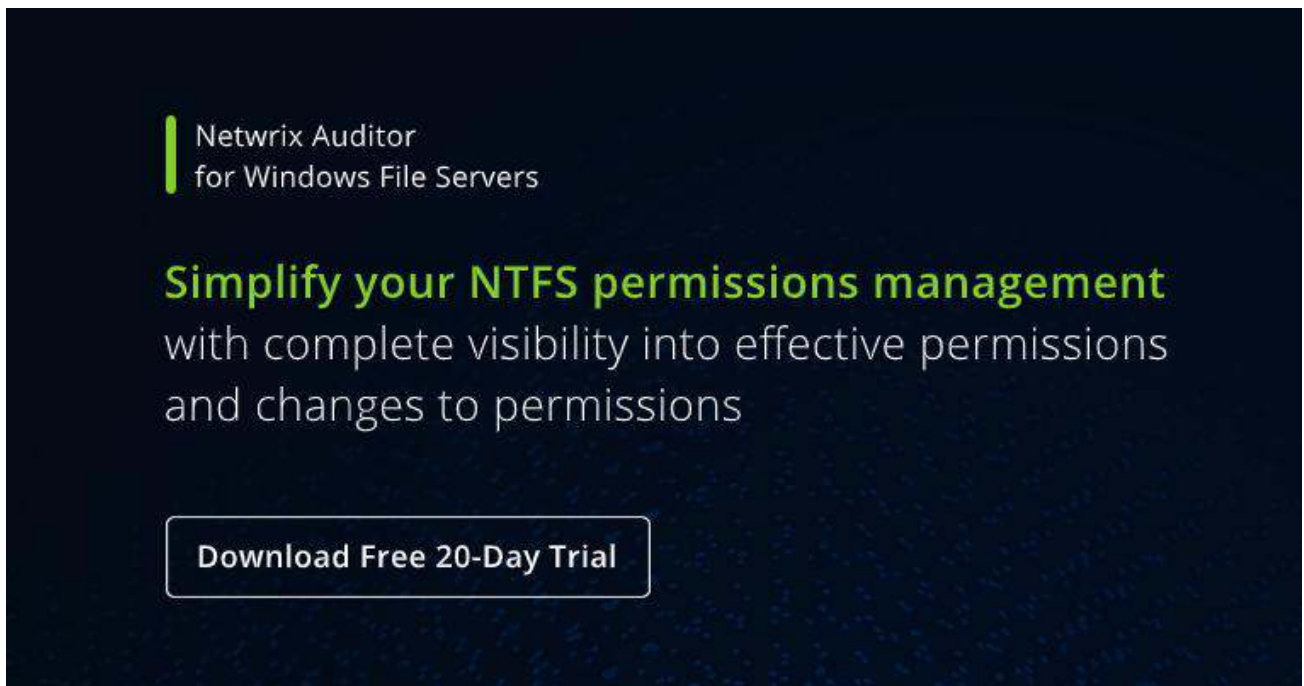
What are NTFS Permissions

NTFS (New Technology File System) is the standard file system for Windows NT and all later Windows operating systems. With NTFS, you use shared folders to provide network users with access to file resources and thereby manage permissions for drives and folders. NTFS permissions are available to all drives formatted with this file system. Each user can choose to share entire drives or individual folders with the network.

The main advantages of NTFS permissions are that they affect local users as well as network users and they are based on the permissions granted to each individual user at the Windows login, regardless of where the user is connecting. Administrators can use the NTFS utility to control access to files and folders, containers, and objects on the network as part of system security.

We use cookies and other tracking technologies to improve our website and your web experience. To learn more, please read our Privacy Policy ([/privacy.html#cookie_policy](#)).

Okay, got it

A dark blue banner with a subtle pattern of small white dots. In the top left, there is a green vertical bar followed by the text "Netwrix Auditor for Windows File Servers". In the center, the text "Simplify your NTFS permissions management" is written in a large, bold, green font, followed by "with complete visibility into effective permissions and changes to permissions" in a smaller, white font. At the bottom center, there is a white rectangular button with rounded corners containing the text "Download Free 20-Day Trial" in a bold, black font.

Netwrix Auditor
for Windows File Servers

Simplify your NTFS permissions management
with complete visibility into effective permissions
and changes to permissions

Download Free 20-Day Trial

(https://www.netwrix.com/file_server_auditing.html)

Previous

([active_directory_delegation.html](#))

Next

([audit_policy_best_practice.html](#))

Related best practices



([prevent_ransomware_best_practice.html](#))

How to Prevent Ransomware Infections: Best Practices



([active_directory_group_management.html](#))

Active Directory Group Management Best Practices

We use cookies and other tracking technologies to improve our website and your web experience. To learn more, please read our Privacy Policy ([/privacy.html#cookie_policy](#)).



([Data_Access_Governance_Best_Practice_Guide.html](#))

Okay, got it

Data Access Governance Best Practices



(file_analysis_best_practice_guide.html)

File Analysis Best Practices

Netwrix Auditor

- [Platform Overview \(./auditor.html\)](#)
- [Request a Price Quote \(./how_to_buy.html\)](#)
- [Solutions \(./solutions.html\)](#)
- [Virtual Appliance \(./virtual_appliances.html\)](#)
- [Cloud Vision \(./cloud_opportunities.html\)](#)

Netwrix Freeware

- [Free Netwrix Auditor for Active Directory \(./netwrix_change_notifier_for_active_directory.html\)](#)
- [Account Lockout Examiner \(./account_lockout_examiner.html\)](#)
- [Top 7 Free Tools \(./top_7_freeware_tools.html\)](#)

Audited Systems

- [Active Directory \(./active_directory_auditing.html\)](#)
- [Azure AD \(./azure_ad_auditing.html\)](#)
- [Office 365 \(./office_365_auditing.html\)](#)
- [Windows File Servers \(./file_server_auditing.html\)](#)
- [EMC \(./emc_storage_monitoring.html\)](#)

Compliance

- [PCI compliance \(./PCI_Compliance.html\)](#)
- [HIPAA compliance \(./HIPAA_Compliance.html\)](#)
- [SOX compliance \(./SOX_Compliance.html\)](#)
- [FISMA compliance \(./FISMA_Compliance.html\)](#)

- [NetApp \(./netapp_monitoring_software.html\)](#)
- [Windows Server \(./windows_server_auditing.html\)](#)
- [ISO 27001 compliance \(./ISO_27001_Compliance.html\)](#)
- [GLBA compliance \(./GLBA_Compliance.html\)](#)

We use cookies and other tracking technologies to improve our website and your web experience. To learn more, please read our Privacy Policy (./privacy.html#cookie_policy).

Okay, got it

Exchange (./exchange_server_auditing.html)	FERPA compliance (./FERPA_Compliance.html)
SQL Server (./sql_server_auditing.html)	NERC compliance (./NERC_Compliance.html)
Oracle Database (./oracle_database_monitoring_and_auditing.html)	GDPR compliance (./GDPR_Compliance.html)
VMware (./vmware_auditing_reporting.html)	CJIS compliance (./cjis_compliance.html)
SharePoint (./sharepoint_auditing.html)	CCPA compliance (./CCPA_Compliance.html)
Nutanix Files (./nutanix_afs_auditing.html)	
Network Devices (./network_auditing_software_features.html)	

Support

Online Help Center (https://helpcenter.netwrix.com/)
Support Programs (./support.html)
Knowledge Base (/kb.netwrix.com)
Submit Ticket (./open_a_ticket.html)
Customer Portal (./tickets.html)
Renew Maintenance (./support.html#renewform)
Freeware Support (https://forum.netwrix.com)

Company

About Us (./company.html)
Contact Us (./contact.html)
Our Customers (./customer_case_studies.html)
News (./news.html)

© 2019 Netwrix Corporation

[Privacy Policy \(/privacy.html\)](/privacy.html) | [EU Privacy Policy \(/privacy_eu.html\)](/privacy_eu.html) | [EULA \(/eula.html\)](/eula.html)

Corporate Headquarters: 300 Spectrum Center Drive,
Suite 200 Irvine, CA 92618

Phone: 1-949-407-5125 | Toll-free: 888-638-9749

 [Select region](#) ▼

We use cookies and other tracking technologies to improve our website and your web experience. To learn more, please read our [Privacy Policy \(/privacy.html#cookie_policy\)](/privacy.html#cookie_policy).

Okay, got it