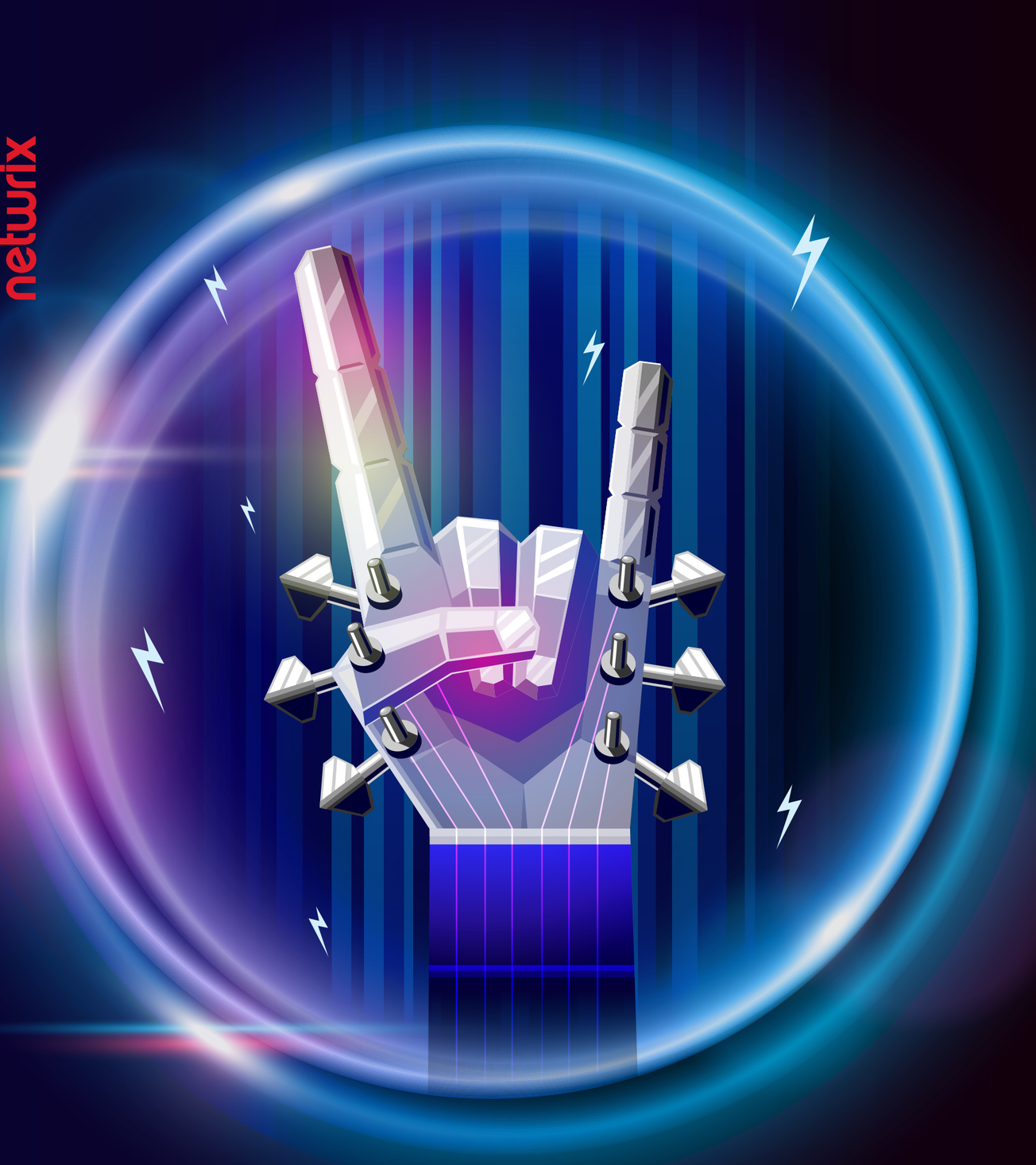
# SysAdmin Magazine

netwrix

№ 28

# Free Stuff Rocks!



# SysAdmin
**Magazine**

№ 28 September ‘17

SysAdmin Magazine is a free source of knowledge for IT Pros who are eager to keep a tight grip on network security and do the job faster.

The Sysadmin Magazine team
sysadmin.magazine@netwrix.com

# Contents

Oleg Lalaev

IT expert,
AD administrator

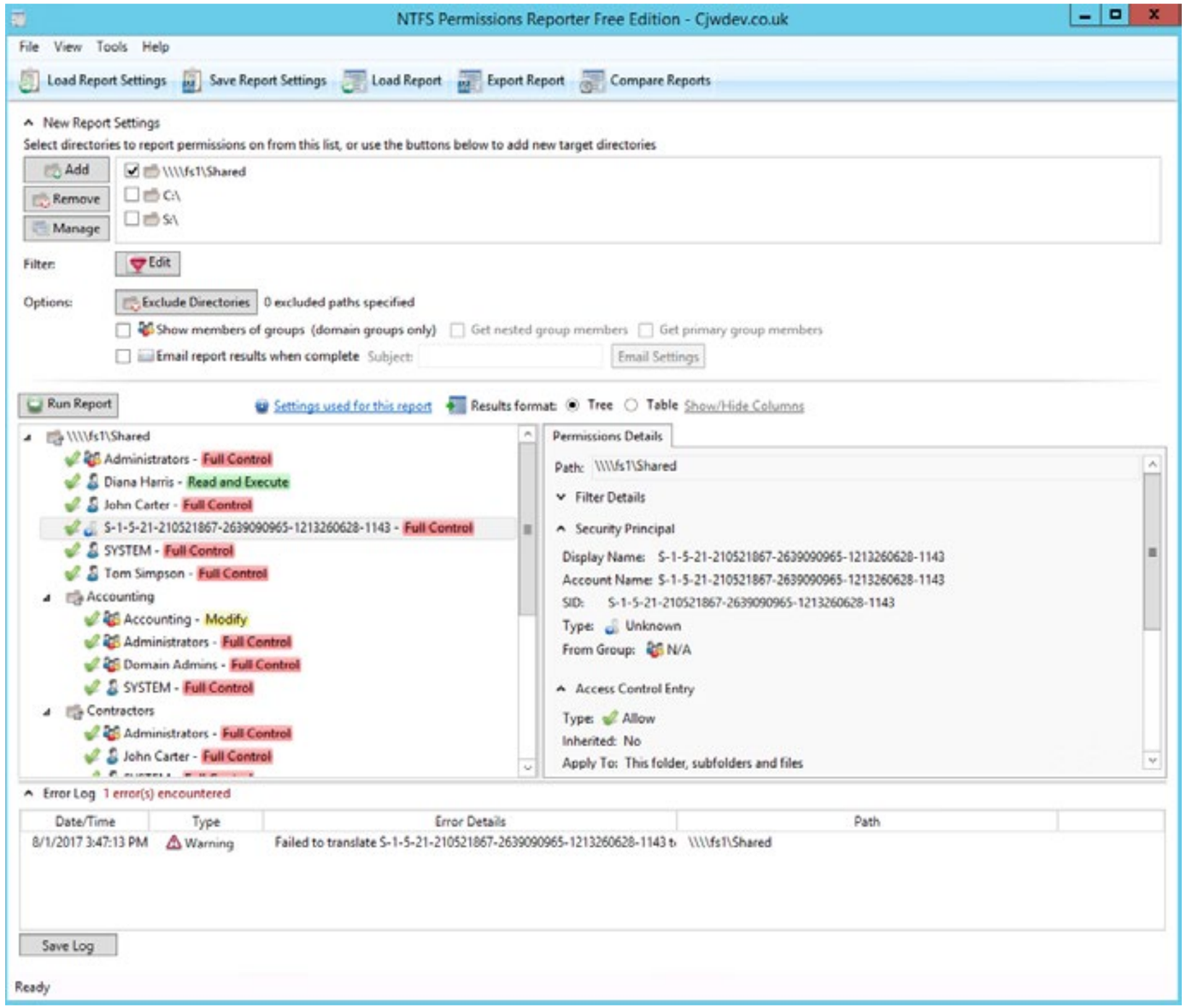
# Top 5 Free Tools for NTFS Permissions Reporting

Managers and compliance auditors often ask IT admins to present a report listing file share permissions granted to a group or a particular user. Here are a few free tools that will help you save time on this report generation and export all permissions granted to a user account on a file share and list of NTFS permissions for particular folder and file.

Tool #1

# NTFS Permissions Reporter Free Edition

Go to page




Cjwdev delivers a good tool that helps you export file and folder permissions. It displays group members (direct and nested) right in the report; plus, you can pick the report format (a tree or table) as well as highlight different permissions in different colors. Highly customizable, isn't it? It is rather easy to use, but at first, the interface may look a little overloaded, and permission scanning may take additional time. The tool provides you with an option to easily export report results to an HTML file. However, it exports only the report on NTFS permissions to only a folder and cannot export or show permissions of a user.

## Report example

### NTFS Permissions Reporter - Results Export

Report run by: t.simpson
Exported at: 8/1/2017 4:00:55 PM

Target directories: \\\\fs1\Shared
Show group members: False
Get nested group members: False
Get primary group members: False
Excluded directories: None
Filter: No filter specified

(Click column headers to sort)

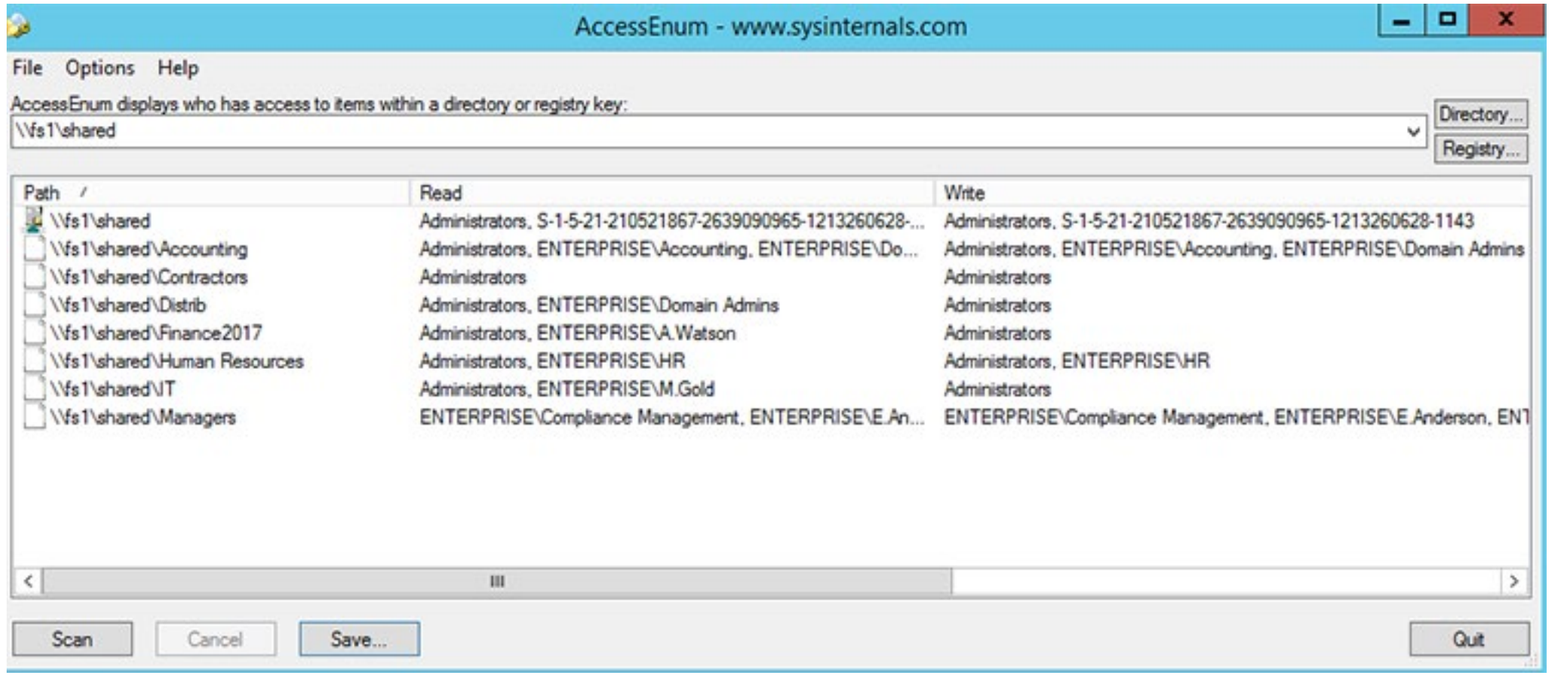
| Path | Account Type | Account | Display Name | Type | Directory Owner | Permission (Simple) | Inherited | |
|---|---|---|---|---|---|---|---|---|
| \\\\fs1\Shared | Group | BUILTIN\Administrators | Administrators | Allow | BUILTIN\Administrators | Full Control | False | Full Control, Traverse Folder / Execute File, List Folder |
| \\\\fs1\Shared | User | ENTERPRISE\D.Harris | Diana Harris | Allow | BUILTIN\Administrators | Read and Execute | False | Traverse Folder / Execute File, List Folder / Read Data, |
| \\\\fs1\Shared | User | ENTERPRISE\J.Carter | John Carter | Allow | BUILTIN\Administrators | Full Control | False | Full Control, Traverse Folder / Execute File, List Folder |
| \\\\fs1\Shared | Unknown | S-1-5-21-210521867-2639090965-1213260628-1143 | S-1-5-21-210521867-2639090965-1213260628-1143 | Allow | BUILTIN\Administrators | Full Control | False | Full Control, Traverse Folder / Execute File, List Folder |
| \\\\fs1\Shared | User | NT AUTHORITY\SYSTEM | SYSTEM | Allow | BUILTIN\Administrators | Full Control | False | Full Control, Traverse Folder / Execute File, List Folder |
| \\\\fs1\Shared | User | ENTERPRISE\t.simpson | Tom Simpson | Allow | BUILTIN\Administrators | Full Control | False | Full Control, Traverse Folder / Execute File, List Folder |
| \\\\fs1\Shared\Accounting | Group | ENTERPRISE\Accounting | Accounting | Allow | BUILTIN\Administrators | Modify | False | Traverse Folder / Execute File, List Folder / Read Data, |
| \\\\fs1\Shared\Accounting | Group | BUILTIN\Administrators | Administrators | Allow | BUILTIN\Administrators | Full Control | False | Full Control, Traverse Folder / Execute File, List Folder |
| \\\\fs1\Shared\Accounting | Group | ENTERPRISE\Domain Admins | Domain Admins | Allow | BUILTIN\Administrators | Full Control | False | Full Control, Traverse Folder / Execute File, List Folder |
| \\\\fs1\Shared\Accounting | User | NT AUTHORITY\SYSTEM | SYSTEM | Allow | BUILTIN\Administrators | Full Control | False | Full Control, Traverse Folder / Execute File, List Folder |
| \\\\fs1\Shared\Contractors | Group | BUILTIN\Administrators | Administrators | Allow | BUILTIN\Administrators | Full Control | False | Full Control, Traverse Folder / Execute File, List Folder |
| \\\\fs1\Shared\Contractors | User | ENTERPRISE\J.Carter | John Carter | Allow | BUILTIN\Administrators | Full Control | False | Full Control, Traverse Folder / Execute File, List Folder |
| \\\\fs1\Shared\Contractors | User | NT AUTHORITY\SYSTEM | SYSTEM | Allow | BUILTIN\Administrators | Full Control | False | Full Control, Traverse Folder / Execute File, List Folder |
| \\\\fs1\Shared\Contractors | User | ENTERPRISE\t.simpson | Tom Simpson | Allow | BUILTIN\Administrators | Full Control | False | Full Control, Traverse Folder / Execute File, List Folder |
| \\\\fs1\Shared\Distrib | Group | BUILTIN\Administrators | Administrators | Allow | BUILTIN\Administrators | Full Control | False | Full Control, Traverse Folder / Execute File, List Folder |
| \\\\fs1\Shared\Distrib | Group | ENTERPRISE\Domain Admins | Domain Admins | Allow | BUILTIN\Administrators | Read and Execute | False | Traverse Folder / Execute File, List Folder / Read Data, |
| \\\\fs1\Shared\Distrib | User | ENTERPRISE\J.Carter | John Carter | Allow | BUILTIN\Administrators | Full Control | False | Full Control, Traverse Folder / Execute File, List Folder |
| \\\\fs1\Shared\Distrib | User | NT AUTHORITY\SYSTEM | SYSTEM | Allow | BUILTIN\Administrators | Full Control | False | Full Control, Traverse Folder / Execute File, List Folder |
| \\\\fs1\Shared\Distrib | User | ENTERPRISE\t.simpson | Tom Simpson | Allow | BUILTIN\Administrators | Full Control | False | Full Control, Traverse Folder / Execute File, List Folder |
| \\\\fs1\Shared\Finance2017 | Group | BUILTIN\Administrators | Administrators | Allow | ENTERPRISE\J.Carter | Full Control | False | Full Control, Traverse Folder / Execute File, List Folder |
| \\\\fs1\Shared\Finance2017 | User | ENTERPRISE\A.Watson | Anna Watson | Allow | ENTERPRISE\J.Carter | Read and Execute | False | Traverse Folder / Execute File, List Folder / Read Data, |
| \\\\fs1\Shared\Finance2017 | User | ENTERPRISE\J.Carter | John Carter | Allow | ENTERPRISE\J.Carter | Full Control | False | Full Control, Traverse Folder / Execute File, List Folder |
| \\\\fs1\Shared\Finance2017 | User | NT AUTHORITY\SYSTEM | SYSTEM | Allow | ENTERPRISE\J.Carter | Full Control | False | Full Control, Traverse Folder / Execute File, List Folder |
| \\\\fs1\Shared\Finance2017 | User | ENTERPRISE\t.simpson | Tom Simpson | Allow | ENTERPRISE\J.Carter | Full Control | False | Full Control, Traverse Folder / Execute File, List Folder |
| \\\\fs1\Shared\Finance2017\ - backup | Group | BUILTIN\Administrators | Administrators | Allow | ENTERPRISE\D.Harris | Full Control | True | Full Control, Traverse Folder / Execute File, List Folder |
| \\\\fs1\Shared\Finance2017\ - backup | User | ENTERPRISE\A.Watson | Anna Watson | Allow | ENTERPRISE\D.Harris | Read and Execute | True | Traverse Folder / Execute File, List Folder / Read Data, |
| \\\\fs1\Shared\Finance2017\ - backup | User | ENTERPRISE\J.Carter | John Carter | Allow | ENTERPRISE\D.Harris | Full Control | True | Full Control, Traverse Folder / Execute File, List Folder |
| \\\\fs1\Shared\Finance2017\ - backup | User | NT AUTHORITY\SYSTEM | SYSTEM | Allow | ENTERPRISE\D.Harris | Full Control | True | Full Control, Traverse Folder / Execute File, List Folder |
| \\\\fs1\Shared\Finance2017\ - backup | User | ENTERPRISE\t.simpson | Tom Simpson | Allow | ENTERPRISE\D.Harris | Full Control | True | Full Control, Traverse Folder / Execute File, List Folder |
| \\\\fs1\Shared\Finance2017\ - backup | Disabled User | ENTERPRISE\G.Black | George Black | Allow | ENTERPRISE\D.Harris | Full Control | False | Full Control, Traverse Folder / Execute File, List Folder |

Tool #2

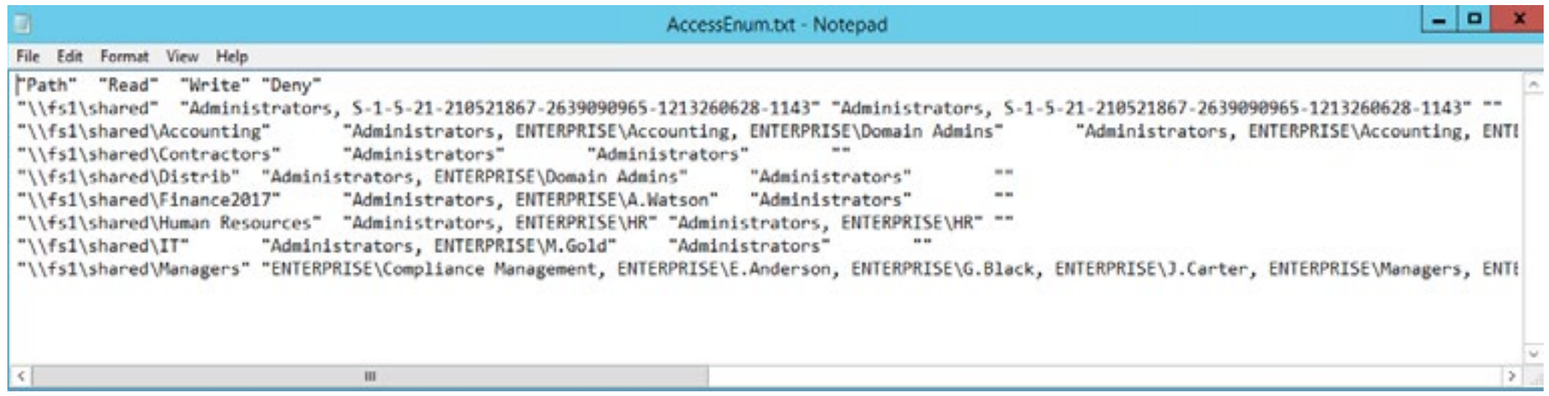
# Access Enum

Go to page

There's no built-in way to quickly view user accesses to a tree of directories or keys. AccessEnum from sysinternals suite gives you a full view of your file system and Registry security settings in seconds, very simple to use, gives you table view of all permissions on your file share or registry, can export only to ".txt" format, which is rather complicate to read, you can copy information from ".txt" file to ".xls" manually and edit it but it will take you some time.




**Report example**

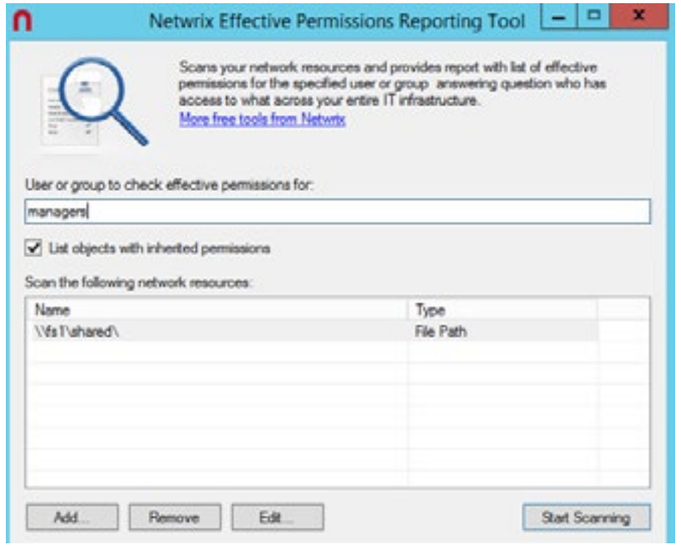


Tool #3

# Netwrix Effective Permissions Reporting Tool

Go to page

This tool helps you make sure that employees' permissions align with their roles in the organization. The freeware tool delivers a file share and Active Directory permissions report that details who has access to what and how that access was gained. Very simple and easy to use tool, you just need to enter the name of a user or group to check its permissions, very fast scan and easy HTML export functionality. It doesn't show folder permissions, such report is available in Netwrix Auditor for File Servers (20 days free trial).




**Report example**

**Netwrix Effective Permissions Report for enterprise \j.carter**

| enterprise\j.carter is a member of the following groups: |
|---|
| BUILTIN\Administrators |
| BUILTIN\Users |
| ENTERPRISE\Accounting |
| ENTERPRISE\ChangeAuditor Administrators - CA2017 |
| ENTERPRISE\ChangeAuditor Administrators - DEFAULT |
| ENTERPRISE\ChangeAuditor Administrators - ENTERPRISE |
| ENTERPRISE\ChangeAuditor Operators - CA2017 |
| ENTERPRISE\ChangeAuditor Operators - DEFAULT |
| ENTERPRISE\ChangeAuditor Operators - ENTERPRISE |

**Report example**

**Effective permissions for enterprise\j.carter (objects with inherited permissions are hidden):**

**Network Resource: \\fs1\shared\ (File Path)**

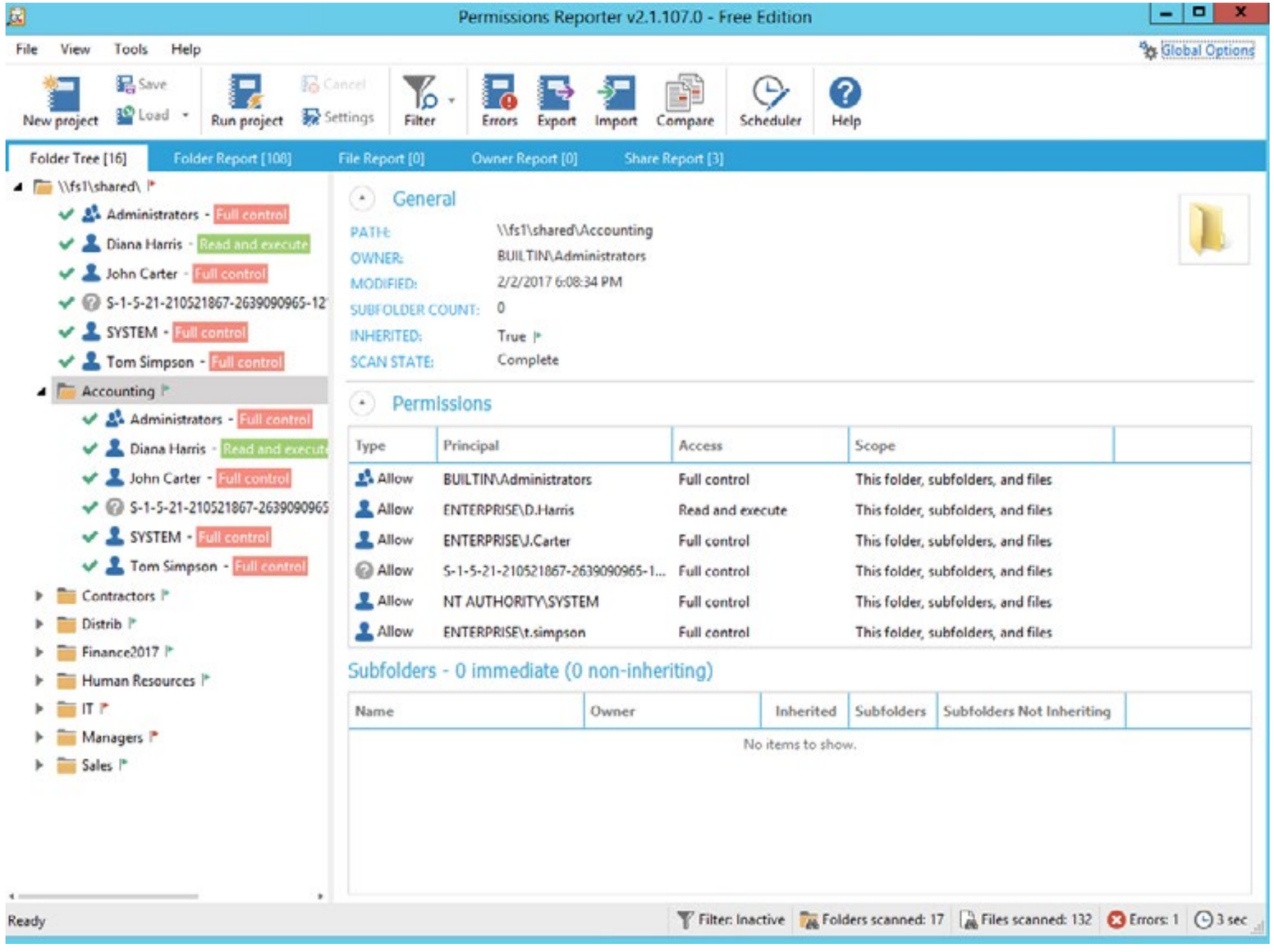
| Object Path | Permissions | Has Access via Groups |
|---|---|---|
| shared [Share-level Permissions] | Full Control | fs1\Administrators |
| shared [Share-level Permissions] | Full Control | Everyone |
| \\fs1\shared\ | Full Control | fs1\Administrators |
| \\fs1\shared\ | Full Control | Direct |
| \\fs1\shared\Accounting\ | Full Control | fs1\Administrators |
| \\fs1\shared\Accounting\ | Full Control | ENTERPRISE\Domain Admins |
| \\fs1\shared\Accounting\ | Modify, List Folder Contents, Read & Execute, Read, Write | ENTERPRISE\Accounting |
| \\fs1\shared\Contractors\ | Full Control | fs1\Administrators |
| \\fs1\shared\Contractors\ | Full Control | Direct |
| \\fs1\shared\Distrb\ | Full Control | fs1\Administrators |
| \\fs1\shared\Distrb\ | List Folder Contents, Read & Execute, Read | ENTERPRISE\Domain Admins |
| \\fs1\shared\Distrb\ | Full Control | Direct |
| \\fs1\shared\Finance2017\ | Full Control | fs1\Administrators |
| \\fs1\shared\Finance2017\ | Full Control | Direct |
| \\fs1\shared\Human Resources\ | Full Control | fs1\Administrators |
| \\fs1\shared\Human Resources\ | Full Control | Direct |
| \\fs1\shared\IT\ | Full Control | fs1\Administrators |
| \\fs1\shared\IT\ | Full Control | Direct |
| \\fs1\shared\IT\JSmith\ | Full Control | fs1\Administrators |

Tool #4

# Permissions Reporter

Go to page

This is a very good Windows NTFS permissions reporting tool. It resembles Cjwdev's NTFS Permissions Reporter tool a little, as it has the same functionality but a prettier interface. It's easy to use. However, permission scanning takes some time, and you can export only the report on NTFS permissions to a folder or HTML file; a report on the permissions of a user is not shown and can't be exported.



**Report example**

# Permissions Reporter

## Permissions Report - 8/1/2017 5:03:18 PM

**Path(s): \\fs1\shared**
**Excluded Path(s): None**

Contents:



### Folder Permissions

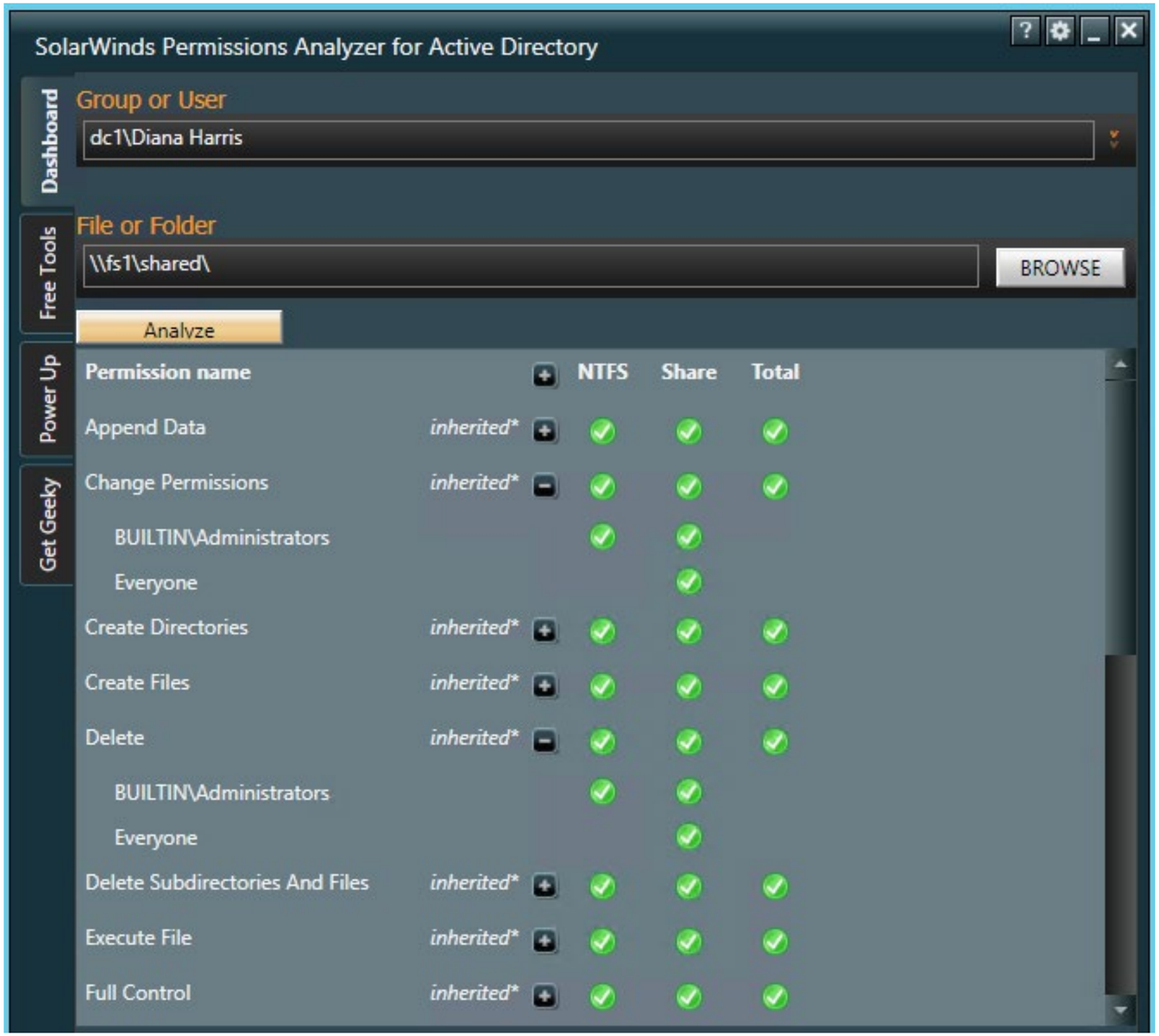
| Path | Account Type | Account Name | Display Name | Security Identifier | Parent Group | Access Type | Inherited | Owner | Modified | Basic Permissions | Access Scope | Advanced Permissions |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| \\fs1\shared\ | Group | BUILTIN\Administrators | Administrators | S-1-5-32-544 | N/A | Allow | False | BUILTIN\Administrators | 10/21/2016 9:09:08 AM | Full control | This folder, subfolders, and files | 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 |
| \\fs1\shared\ | User | ENTERPRISE\D.Harris | Diana Harris | S-1-5-21-210521867-2639090965-1213260628-1182 | N/A | Allow | False | BUILTIN\Administrators | 10/21/2016 9:09:08 AM | Read and execute | This folder, subfolders, and files | Traverse folder / Execute file, List folder / Read data, Read attributes, Read extended attributes, Read permissions |
| \\fs1\shared\ | User | ENTERPRISE\J.Carter | John Carter | S-1-5-21-210521867-2639090965-1213260628-1106 | N/A | Allow | False | BUILTIN\Administrators | 10/21/2016 9:09:08 AM | Full control | This folder, subfolders, and files | 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 |
| \\fs1\shared\ | Unknown | S-1-5-21-210521867-2639090965-1213260628-1143 | S-1-5-21-210521867-2639090965-1213260628-1143 | S-1-5-21-210521867-2639090965-1213260628-1143 | N/A | Allow | False | BUILTIN\Administrators | 10/21/2016 9:09:08 AM | Full control | This folder, subfolders, and files | 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 |
| \\fs1\shared\ | User | NT AUTHORITY\SYSTEM | SYSTEM | S-1-5-18 | N/A | Allow | False | BUILTIN\Administrators | 10/21/2016 9:09:08 AM | Full control | This folder, subfolders, and files | 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 |
| \\fs1\shared\ | User | ENTERPRISE\t.simpson | Tom Simpson | S-1-5-21-210521867-2639090965-1213260628-1138 | N/A | Allow | False | BUILTIN\Administrators | 10/21/2016 9:09:08 AM | Full control | This folder, subfolders, and files | 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 |
| \\fs1\shared\Contractors | Group | BUILTIN\Administrators | Administrators | S-1-5-32-544 | N/A | Allow | True | BUILTIN\Administrators | 3/30/2017 6:48:14 PM | Full control | This folder, subfolders, and files | 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 |
| \\fs1\shared\Contractors | User | ENTERPRISE\D.Harris | Diana Harris | S-1-5-21-210521867-2639090965-1213260628-1182 | N/A | Allow | True | BUILTIN\Administrators | 3/30/2017 6:48:14 PM | Read and execute | This folder, subfolders, and files | Traverse folder / Execute file, List folder / Read data, Read attributes, Read extended attributes, Read permissions |
| \\fs1\shared\Contractors | User | ENTERPRISE\J.Carter | John Carter | S-1-5-21-210521867-2639090965-1213260628-1106 | N/A | Allow | True | BUILTIN\Administrators | 3/30/2017 6:48:14 PM | Full control | This folder, subfolders, and files | 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 |

Tool #5

# SolarWinds Permissions Analyzer

Go to page

This is the last tool in our list and the worst one, in my opinion. The main reason why I'm not fond of this tool is because you cannot export information from it, but for those who just need detailed information about user permissions, it can be rather handy. It quickly identifies how users' permissions were inherited, browses permissions by group or by individual user and analyzes them based on group membership and permissions.



## (BONUS) PowerShell

Despite all the tools on the market, you know that you can always rely on an old friend, PowerShell. Here's a ready-to-use script for you in case you need to export folder permissions and user permissions into ".csv" file format:

**PowerShell code for exporting folder permissions:**

```
$OutFile = "C:\Temp\permissions.csv"
$Header = "Folder Path,IdentityReference,AccessControlType,IsInherited,InheritanceFlags,PropagationFlags"
Del $OutFile
Add-Content -Value $Header -Path $OutFile

$RootPath = "\\fs1\shared"

$Folders = dir $RootPath -recurse | where {$_.psiscontainer -eq $true}

foreach ($Folder in $Folders){
    $ACLs = get-acl $Folder.fullname | ForEach-Object { $_.Access  }
    Foreach ($ACL in $ACLs){
    $OutInfo = $Folder.Fullname + "," + $ACL.IdentityReference  + "," + $ACL.AccessControlType + "," + $ACL.IsInherited + "," + $ACL.InheritanceFlags +
"," + $ACL.PropagationFlags
    Add-Content -Value $OutInfo -Path $OutFile
    } }
```

**Report Example**

| | |
|---|---|
| 1 | Folder Path,IdentityReference,AccessControlType,IsInherited,InheritanceFlags,PropagationFlags |
| 2 | \\fs1\shared\Accounting,NT AUTHORITY\SYSTEM,Allow,False,ContainerInherit, ObjectInherit,None |
| 3 | \\fs1\shared\Accounting,BUILTIN\Administrators,Allow,False,ContainerInherit, ObjectInherit,None |
| 4 | \\fs1\shared\Accounting,ENTERPRISE\Domain Admins,Allow,False,ContainerInherit, ObjectInherit,None |

**PowerShell code for exporting user permissions:**

```
dir -Recurse | where { $_.PsIsContainer } | % { $path1 = $_.fullname;
Get-Acl $_.Fullname | % { $_.access | where { $_.IdentityReference
-like "ENTERPRISE\J.Carter" } | Add-Member -MemberType
NoteProperty -name "\\fs1\shared\" -Value $path1 -passthru }} |
export-csv "C:\temp\permissions.csv"
```

**Report Example**

| | A | B | C | D | |
|---|---|---|---|---|---|
| 1 | | | | | |
| 2 | System.Security. Access Control. FileSystem AccessRule | FileSystem Rights | Access Control Type | Identity Reference | IsInherited |
| 3 | \\FS\Shared | FullControl | Allow | NA\Suspicious | TRUE |
| 4 | \\FS\Shared\Finance | FullControl | Allow | NA\Suspicious | TRUE |
| 5 | \\FS\Shared | FullControl | Allow | NA\Suspicious | TRUE |
| 6 | \\FS\Shared\IT | FullControl | Allow | NA\Suspicious | TRUE |

Oleg Lalaev

IT expert,
AD administrator

# Top 5 Free Tools for Account Lockout Troubleshooting

How many account lockouts do you deal with every day? Troubleshooting account lockouts has always been an IT admin's daily task: either employees forget their passwords or accounts lockout due to a significant increase in authentication requests on domain controllers. On top of that, account lockouts can also be a sign of the Conficker virus (also known as Downup, Downadup or Kido), which performs brute-force attacks against accounts in a network, or of a password change on a service account. For more cases of account lockouts, check out the Account lockout troubleshooting guide.

Tool #1

# Netwrix Account Lockout Examiner

Go to page

This is a free tool that gives alerts about account lockouts and helps you troubleshoot each event and determine the root cause so you can quickly restore vital services. The freeware enables you to do the following:

- **Quickly spot account lockouts**

  The tool scans the logs related to locked accounts and gives you the info about an IP address or computer namefrom which failed logons came. Plus, it examines mapped drives, services, RDP sessions and scheduled tasks for bad credentials.

- **Identify the root cause**

  The tool helps find the root cause of a lockout, such as improperly mapped network drives, services or scheduled tasks running under stale credentials, or disconnected remote desktop sessions.

- **Unlock accounts**

  Unlock accounts faster through a web-based console or even via email sent from your mobile device.

Tool #2

# Account Lockout Status tools

Go to page

This is a set of tools Microsoft offers to help you with account lockout troubleshooting:

- **exe** collects and filters events from the event logs of domain controllers. This tool has a built-in search for account lockouts. It gathers the event IDs related to a certain account lockout in a separate text file

- **exe** examines all DCs in a domain, letting you know when the target account last locked out and from which DC. In addition, it provides the locked-out account's current status and the number of bad password attempts

- Netlogon logging is used to track Netlogon and NT LAN Manager (NTLM) events. Enabling Netlogon logging on all DCs is an effective way to isolate a locked-out account and see where the account is being locked out. Although Netlogon logging isn't part of the account lockout and management tools, NLParse.exe is used to parse the Netlogon logs, and NLParse.exe is one of the account lockout tools

- **Acctinfo** exposes more properties in ADUC (Active Directory Users and Computers) (e.g., last logon and password expires). Specifically, with this add-on, you get an extra tab in ADUC called additional account info that helps isolate and troubleshoot account lockouts and change a user's password on a domain controller on that user's site

Tool #3

# Active Directory Lockouts

Go to page

This simple utility tries to track the origin of Active Directory bad password attempts and lockouts. It can search each domain/domain controller for bad password attempts to access an account. It will then parse any related events on each domain controller and work out where the origin of the lockout came from. After that, it analyzes each machine and outputs and the common causes of account lockouts that are present (e.g., mapped drives, old rdp sessions, scheduled tasks).

Tool #4

# PowerShell

Using the following PowerShell script, you can easily filter the event log for events that are related to a
Using the following PowerShell script, you can easily filter the event log for events that are related to a
certain account and try to figure out what caused its lockout:

```
Get-EventLog -LogName Security | ?{$_.message -like
"*locked*USERNAME*"} | fl -property *
```

You can also use Get-UserLockoutStatus function to troubleshoot persistent account lockout problems. The function searches all domain controllers for a user in a domain for account lockout status: bad password count, last bad password time, and when the password was set last. You can find the full code here.

> **Good old PowerShell is coming to your rescue!**

Tool #5

# N/A

Actually I couldn't find the 5th free tool; my bad. However, there are some paid tools such as the Manage Engine and Jiji account lockout tools. Algoware AD tool didn't work in my test environment, so I have no clue what it is actually capable of doing. Maybe you can recommend one? Which account lockout troubleshooting free tool do you use?

[Infographics]

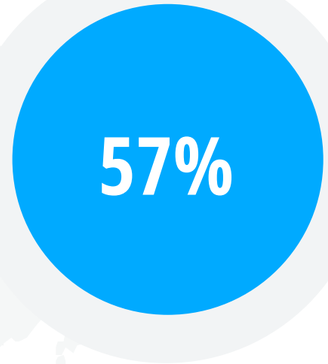
# Top Cybersecurity Risks in Government

Netwrix conducted its 2017 IT Risks Survey to learn more about the security, compliance and operational issues that bother organizations worldwide. As part of the survey, we've extracted some pretty interesting findings about government entities.

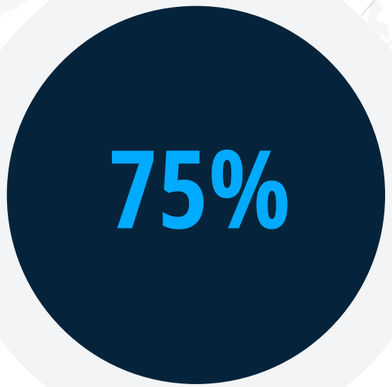
How do government agencies have dealt with IT risks over the past year and what they plan to do to mitigate them in the future? Let's look at our findings.

Read Full Report


of government entities see their own employees as the biggest threat to security




of government entities do not have a separate information security function




of government entities have been focusing their security efforts on protecting endpoints, rather than data

# IT RISKS Government 2017

netwrix

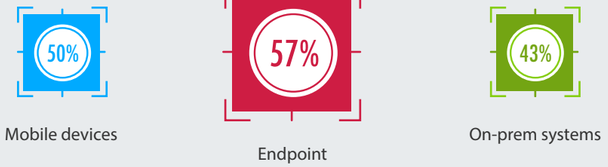
## CONTEXT

**88%** Of organizations do not use any software for information security governance or risk management

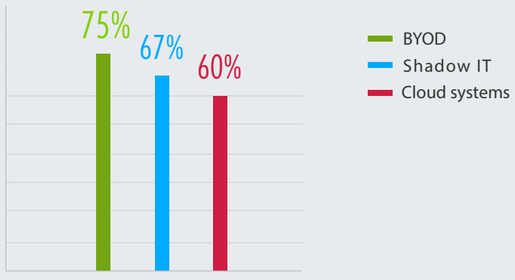
**88%** Of IT operations teams are at least partially responsible for security

**75%** Of organizations do not have a separate information security function

## MAIN SECURITY FOCUS




## MOST NEGLECTED AREAS

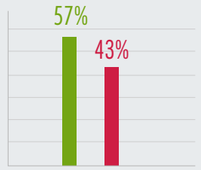



## BIGGEST SECURITY RISKS

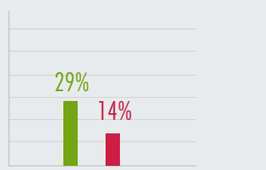
100% Employees

**33%** of organizations had compliance issues in 2016

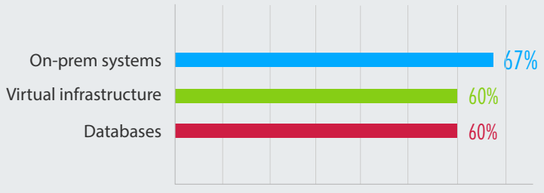
## MAIN CAUSES OF SECURITY INCIDENTS IN 2016




## MAIN CAUSES OF SYSTEM DOWNTIME IN 2016




## WHERE VISIBILITY INTO USER ACTIVITY IS MOST NEEDED




**ONLY 14%** of organizations are well prepared to beat cyber risks

## WHY?

**57%** Lack of time

**54%** Lack of budget

**43%** Complexity of IT infrastructure

**43%** Growth of data assets

## FOCUS OF FUTURE INVESTMENTS

**43%** Intellectual property theft

**29%** Data breach

**14%** Fraud

## WHY ORGANIZATIONS NEED VISIBILITY

**86%** To detect and mitigate human factor (errors, misuse, etc.)

**71%** To investigate security incidents

**71%** To optimize IT processes and operations


# Jonathan Hassell

IT Pro, Entrepreneur


Cybersecurity Best Practices

# How to Get Rid of Ransomware at No Cost

Ransomware is one of the biggest scourges we face as Internet citizens today. What happens when you have been struck by it? The most obvious option would be to pay the ransom. You would not be alone if you did – even large companies and non-profits have had to pay, or at least negotiate, a ransom. But should that be your first option? Hardly.

## Why Are Ransomware Attacks so Successful?

The core reason for ransomware "success" is the sophisticated manner of attack. Hackers create smart campaigns based on social behavior insights. Moreover, technology enables them to hide encryption software in almost any document. Imagine getting an email that includes the text "If the encoding of the attached Word document seems incorrect, please activate macros. This is done as follows..."

Another reason lies in the weakness of IT networks' security policies. Factors such as inadequate backups, the lack of disaster recovery plans, poor updates of operating systems and applications, inadequate control over changes in IT infrastructure and user permissions, and lack of employee security education and training can all put organizations at serious risk of ransomware encryption.

## How to Fix ransomware: Practical Tips and Free Tools

### Have good backups

The best defense is a good offense – having good backups. This can come in a couple of forms.

#### 1. Shadow copies.

If you are a Windows administrator, you may be familiar with the Volume Shadow Copy Service, a piece of software, first introduced in Windows Server 2003, that takes snapshots of data on specifically

configured volumes at predetermined points in time. This service informs the Previous Versions feature in Windows client, which allows users to right-click a file on the disk and open a previous version if, for example, they make a mistake in a spreadsheet. If you catch a ransomware infection early, shadow copies are likely a good way to restore an unencrypted version of your files. If you are not using shadow copies, configure them today. Unfortunately, some variants of ransomware have caught onto this procedure. During their silent infection process, prior to encrypting files, they delete all shadow copies found on a disk.

### 2. Regular backups that you restore from a tape or archive disk.

You are making regular backups of your storage system, right? And you are regularly testing them to verify the files can be restored intact? If not, then stop reading right now and go configure a backup scheme. If you are, then rest a little easier, as the worst case for a ransomware infection in this case would be wiping your machines and restored their data from backups. Sure, it is an investment of time, but you will absolutely not need to pay any ransom, and you might just be seen as a hero.

## Look for available free anti-ransomware tools

If you do find yourself on the other end of a completed ransomware attack, you have a couple of options that don't involve paying the ransom.

As governments and security researchers continue to make progress against ransomware threats, these parties have managed to break the encryption schemes used by some variants of ransomware. It is important to keep in mind that not every variant of ransomware has been "broken" by the good guys, so you should not rely solely on the hope that these encryption schemes have been foiled. Do not rest on your laurels when it comes to building defenses against this type of attack.

If you have already been victimized, then head over to the No More Ransom Project at https://www.nomoreransom.org and look for the variant you have been hit with. This site is sponsored jointly by the European Cybercrime Center, Politie, Kaspersky Lab, and Intel Security, and contains current decryption tools for the following variants:

- Crysus
- Marsjoke/Polyglot
- Wildfire
- Chimera
- Teslacrypt
- Shade
- Coinvault
- Rannoh
- Rakhni

The aforementioned organizations are working on breaking other variants as well, but breaking good encryption takes time, and malware creators

have a perverse incentive to make their encryption stronger and even more difficult to break. It is an unfortunate dance, but for now, you might be able to save yourself with the decryption tools on the site. Beware of ransomware removal tools from other sources—they may actually be ransomware disguised as a prevention tools.

## Use the File Server Resource Manager to catch bad actors

Even if you have been infected by ransomware, it is not too late to prevent further damage. You will likely have some encrypted files, but the sooner you stop the spread of the infection, the fewer files end up being held hostage, and the easier your cleanup task is. As we have covered on this blog before, you can use the tool built into Windows Server called File Server Resource Manager to catch ransomware attacks as they happen. Essentially, you create a honeypot share with a dollar sign in front of the name to fool ransomware into starting with that particular share in its efforts to encrypt files. Let the group Authenticated Users have full control of this share so that any process wanting to write to the share can do so. This is not a drop box for other files, so do not publicize this share to actual users; its only legitimate use is to catch things that should not be on your systems. When the File Server Resource Manager screen notices activity happening within that share, it assumes that someone has been infected and will cut off that user's access to any share to stop the encryption attack in its tracks. There is a simple PowerShell script that can be fired by the File Server Resource Manager in order to accomplish this:

```
Get-SmbShare -Special $false | ForEach-Object { Block-SmbShareAccess -Name $_.Name -AccountName '[Source Io Owner]' -Force }
```

Once these permissions have been removed, ransomware cannot access files for encryption, and basically just stop. You can then remove the malware, restore the files that were encrypted, and move on with your life.

For much more detail on this method of stopping a pending attack or an attack that has just begun, check out Ransomware Protection Using FSRM and PowerShell on our blog.


# Matt Hopton

**Network Architect**


Exchange Email Security

# 5 Free Exchange Security Tools You Probably Don't Know About

Exchange email security is a huge front to defend. There are now so many attack surfaces that it can be hard to decide how to start. Here are a few things that you might want to consider when thinking about your Exchange infrastructure security setup.

This is by no means a full list.

## 1. Full Access and Send As Permissions

A brilliant feature of Exchange is the ability to grant users access to others' mailboxes. You can do this in two ways, either by using the "Full Access" permission, which effectively gives them the same rights as the owner of the mailbox, or by granting "Send As," which just gives them the permissions to change the "from" field to a specified user.

To grant full access, you can use a PowerShell command like the following:

```
Get-Mailbox "MailboxToView" | Add-ADPermission
-User "PersonWhoNeedsPermission" -ExtendedRights "Full
Access"
```

Be aware that in Exchange 2013 and later, any member of 'Domain Admins' cannot view other users' mailboxes.

To list users who have access, you can run the following PowerShell command:

```
Get-Mailbox | Get-MailboxPermission | Where {
$_.AccessRights -eq "FullAccess" -and $_.User.ToString()
-ne "NT AUTHORITY\SYSTEM" -and $_.User.ToString()
-ne "NT AUTHORITY\SELF"} | Select Identity, User | fl
```

This will give you a list of mailboxes with users and groups that are able to access them.

Note: this may take a while to run across many mailboxes!

## 2. Transport Rules

One of the most commonly overlooked Exchange security points is the humble transport rule. If you have a malicious administrator, they can potentially view everyone's email just by setting up a transport rule.

I know of an organization where someone had modified the default signature transport rule to blind carbon themselves on every single email that left the company. It was only by chance when another sysadmin was asked to modify the signature that they noticed this.

```
Get-TransportRule | Where {$_.BlindCopyTo -ne $null} |
fl Name, BlindCopyTo
```


Other actions that could potentially be used for malicious purposes are as follows:

```
Get-TransportRule | Where {$_.
ModerateMessageByUser -ne $null} | fl Name,
ModerateMessageByUser
```

This command will list any rules where approval is needed before the message is delivered.

```
Get-TransportRule | Where {$_.DeleteMessage -eq
$true} | fl Name
```

This command will list any rules that simply delete the message.

## 3. Exchange Roles

Microsoft has used the Role-Based Access Control model (RBAC) since Exchange 2010, and it became more prominent in Exchange 2013 and later. In essence, you assign users and groups permissions to perform actions and tasks using the "who, what, where" method.

As an example, let's take a branch manager of ExampleCo's London office (who). Management want the branch manager to be able to change the out-of-office replies (what) for their branch (where).
Exchange role security allows us to do this by creating a custom role group:

```
New-RoleGroup -Name ExampleCo_London -Roles (See
Later) -Members BranchMgr1
```

This will create a role group with no scope applied – no "where," i.e., BranchMgr1 will be able to use their permissions on all Exchange objects that support it.

We can limit the scope to a single organizational unit  by omitting -Members and supplying -RecipientOrganizationalUnitScope instead:

```
New-RoleGroup -Name ExampleCo_London -Roles (See Later) -RecipientOrganizationalUnitScope "LondonOU"
```

In order to achieve our goal of allowing BranchMgr1 to change the out-of-office replies, we can assign them the "Help Desk" built-in role:

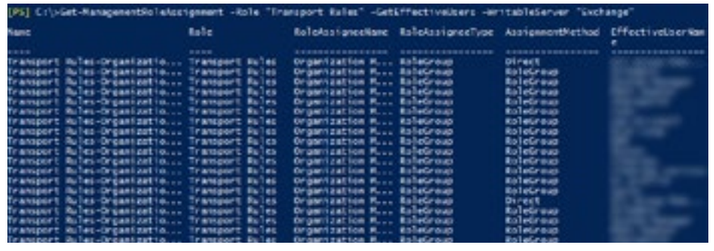
```
New-RoleGroup -Name ExampleCo_London -Roles "Help Desk"
```

You can also create your own roles with a custom set of permissions.

We had a situation recently where we needed to find out who had changed a transport rule on one of our Exchange servers; luckily, there is an easy PowerShell command to view who has permissions to change a mailbox or server:

```
Get-ManagementRoleAssignment -Role "Transport Rules" -WritableServer Exchange -GetEffectiveUsers
```

Running this on our environment yielded a list of groups who could perform this task:



## 4. Exchange Edge Servers

I cannot stress enough how important it is to have an Exchange Edge server. These are highly cut-down servers that just expose port 25 (SMTP) to the outside world. This narrows their attack surface dramatically and offloads spam and anti-virus processing to another (virtual) server.

Edge servers are not members of your active directory domain, so as long as you're not sharing passwords between admin accounts (you're not, are you?), then an attacker who manages to get control of your Edge Server doesn't really have much of a foothold.

Required information from Active Directory that is used for early recipient rejection for example, is sent via a one-way Edge Sync process.

## 5. Hybrid Configurations

I'll finish by just drawing your attention to Office 365 and Hybrid configurations. It is possible to apply most of the on-premise configurations to the cloud or hybrid part of your Exchange configuration.

You can use the following command to establish a connection to the Exchange Online servers:

```
$creds = Get-Credential
```

```
$eonlinesession = New-PSSession – ConfigurationName Microsoft.Exchange -ConnectionUri https://outlook.office365.com/powershell-liveid/ -Credential $creds -Authentication Basic -AllowRedirection
```

```
Import-PsSession $eonlinesession
```

Check that you've connected successfully by issuing something like get-mailbox and see if it returns mailboxes that you know are offsite.

Once you're done, don't forget to disconnect; otherwise, you can run into issues later on in which you use up all of the available PowerShell sessions for your user (you then have to wait for them to timeout, which is not fun.).

```
Remove-PsSession $eonlinesession
```

## Free Tool of the Month

# Effective Permissions Reporting Tool

Download Free Tool

Permissions Reporting Tool helps you make sure that employees' permissions align with their roles in the organization.

The freeware tool delivers a file share and Active Directory permissions report that details who has access to what and how that access was gained.

**Report example**

**Netwrix Effective Permissions Report for ENTERPRISE\T.Simpson**

ENTERPRISE\T.Simpson is a member of the following groups:
BUILTIN\Users

**Effective permissions for ENTERPRISE\T.Simpson (object with inherited permissions are hidden):**

**Network Resource: \\PDC\Users\Administrator\Documents\Shared documents (File Path)**

| Object Path | Permissions | Has Access via Groups |
|---|---|---|
| Users [Share-level Permissions] | Full Control | Everyone |
| \Documents\Shared documents\ | Full Control | Everyone |
| \Documents\Shared documents\Customer Care\ | Read & Execute, Read | Everyone |
| \Documents\Shared documents\Misc\ | Read & Execute, Read | Everyone |
| \Documents\Shared documents\Operations\ | Modify, List Folder Contents | Everyone |
| \Documents\Shared documents\Personnel Folders\ | Full Control | Direct |
| \Documents\Shared documents\Workflow\ | List Folder Contents | Everyone |

# How-to for IT Pro

## How to Detect Password Changes in Active Directory

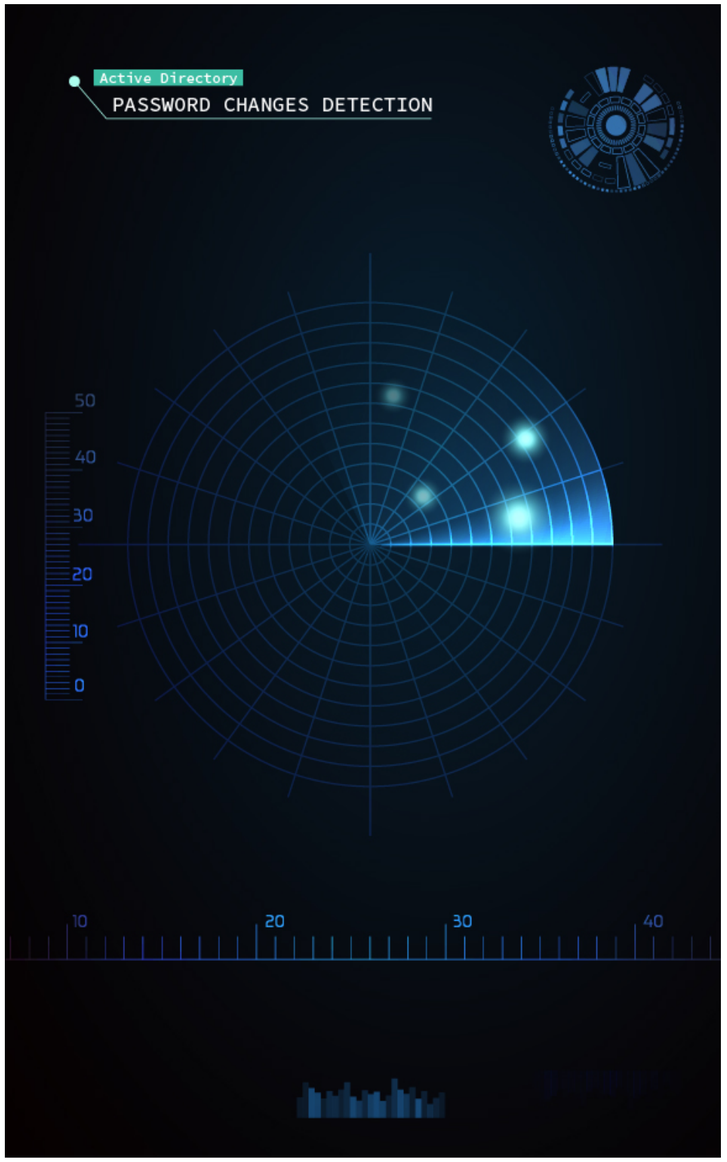
1. Run GPMC.msc (url2open.com/gpmc) > open “Default Domain Policy” > Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Audit Policy:

   - Audit account management > Define > Success and Failure.

2. Run GPMC.msc > open “Default Domain Policy” > Computer Configuration > Policies > Windows Settings > Security Settings > Event Log > Define:

   - Maximum security log size to 1GB
   - Retention method for security log to Overwrite events as needed

3. Open Event viewer and search Security log for event id’s: 628/4724 – password reset attempt by administrator and 627/4723 – password change attempt by user.

# Try Netwrix Auditor 9.0:

**Shield Your IT Environment from Ransomware & Malicious Insiders**

netwrix.com/auditor9.html


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

**Phone:** 1-949-407-5125
**Toll-free:** 888-638-9749
**EMEA:** +44 (0) 203-318-02