PERMISSION REPORTER® V4.1

Report Descriptions

NETsec
13. August 2018

1 Introduction

In this document you will find a brief description of the reports you can create using NETsec Permission Reporter.

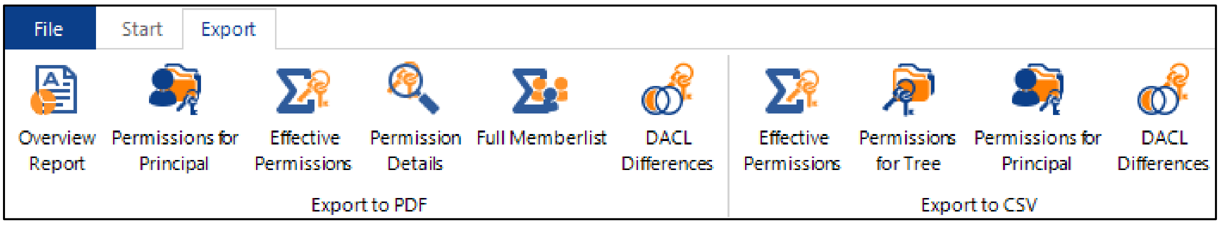
2 Reports

Permission Reporter provides reports to facilitate the communication of permissions granted for security principals[1] on analyzed securable objects[2] (e.g. files, folders, shares).

A report always refers to gathered data of an analysis, which has already been successfully finished. Building a report using "live-data" from the file system or an analysis which is in any state but "done" is not possible.

Permission Reporter also supports your colleagues, who are working in non-technological departments, understanding the result of its analyses by visually-compelling reports.

This is why Permission Reporter offers two file formats for exporting reports.



All Report Types

2.1 CSV Reports

CSV Reports offer extensive collections of permissions. Since spreadsheet like Microsoft Excel are capable of interpreting files containing CSV data, we recommend using these reports for further processing.

2.2 PDF Reports

PDF Reports are visually more appealing then CSV Reports. Therefor PDF Reports may be more suitable for colleagues in non-technological positions by facilitating the comprehensibility of permissions on securable objects.

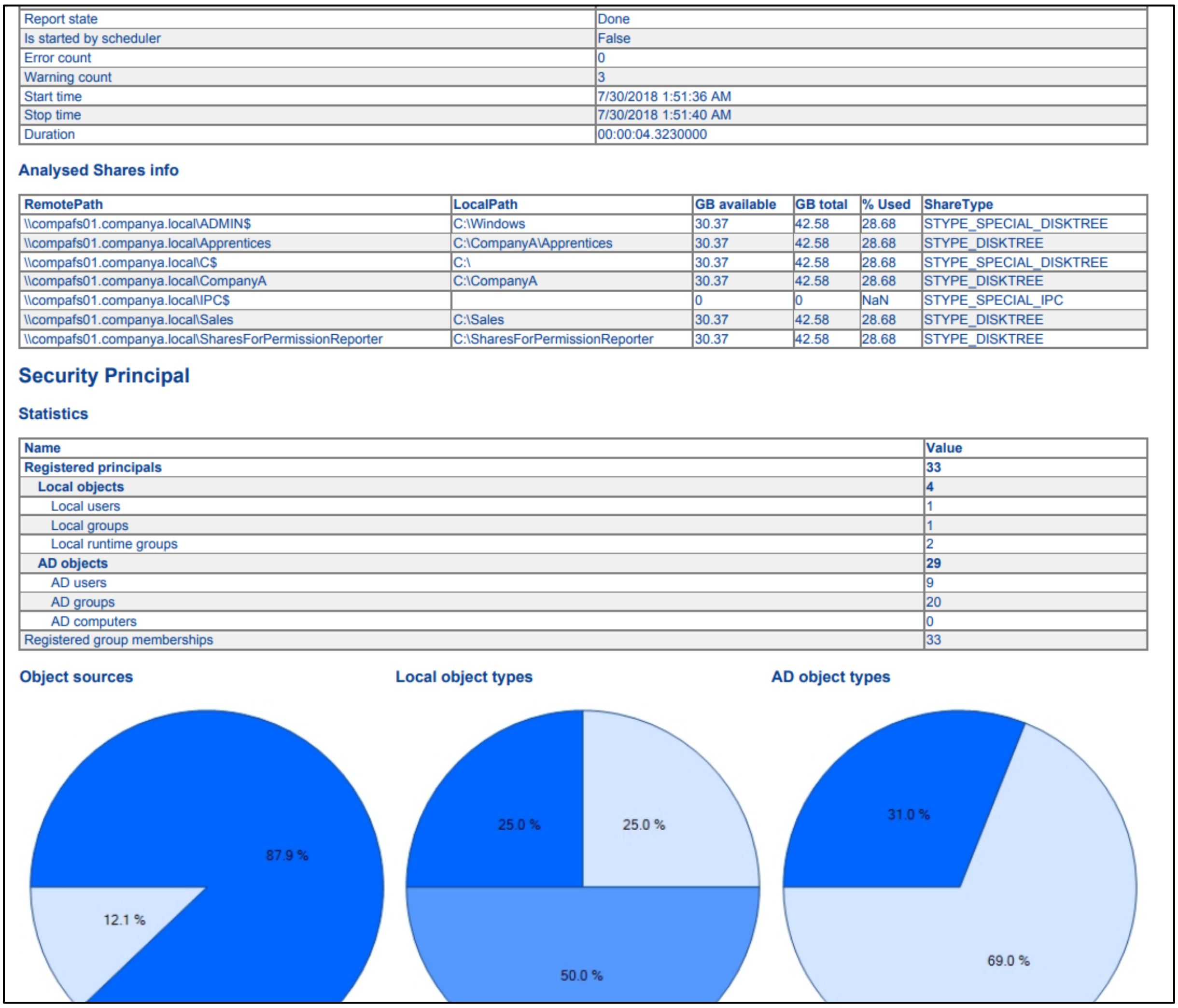
On the other hand PDF Reports are not suitable for processing exported data afterwards and result in large file sizes due to images.

[1] https://technet.microsoft.com/en-us/library/cc780957(v=ws.10).aspx
[2] https://msdn.microsoft.com/en-us/library/windows/desktop/aa379557(v=vs.85).aspx

3 Provided Report Types

3.1 Overview (PDF only)

This report contains general statistical data of an analysis. This report can be send as a status information for administrators.



Report state	Done
Is started by scheduler	False
Error count	0
Warning count	3
Start time	7/30/2018 1:51:36 AM
Stop time	7/30/2018 1:51:40 AM
Duration	00:00:04.3230000

Analysed Shares info

RemotePath	LocalPath	GB available	GB total	% Used	ShareType
\\compafs01.companya.local\ADMIN$	C:\Windows	30.37	42.58	28.68	STYPE_SPECIAL_DISKTREE
\\compafs01.companya.local\Apprentices	C:\CompanyA\Apprentices	30.37	42.58	28.68	STYPE_DISKTREE
\\compafs01.companya.local\C$	C:\	30.37	42.58	28.68	STYPE_SPECIAL_DISKTREE
\\compafs01.companya.local\CompanyA	C:\CompanyA	30.37	42.58	28.68	STYPE_DISKTREE
\\compafs01.companya.local\IPC$		0	0	NaN	STYPE_SPECIAL_IPC
\\compafs01.companya.local\Sales	C:\Sales	30.37	42.58	28.68	STYPE_DISKTREE
\\compafs01.companya.local\SharesForPermissionReporter	C:\SharesForPermissionReporter	30.37	42.58	28.68	STYPE_DISKTREE

Security Principal

Statistics

Name	Value
Registered principals	**33**
Local objects	**4**
Local users	1
Local groups	1
Local runtime groups	2
AD objects	**29**
AD users	9
AD groups	20
AD computers	0
Registered group memberships	33

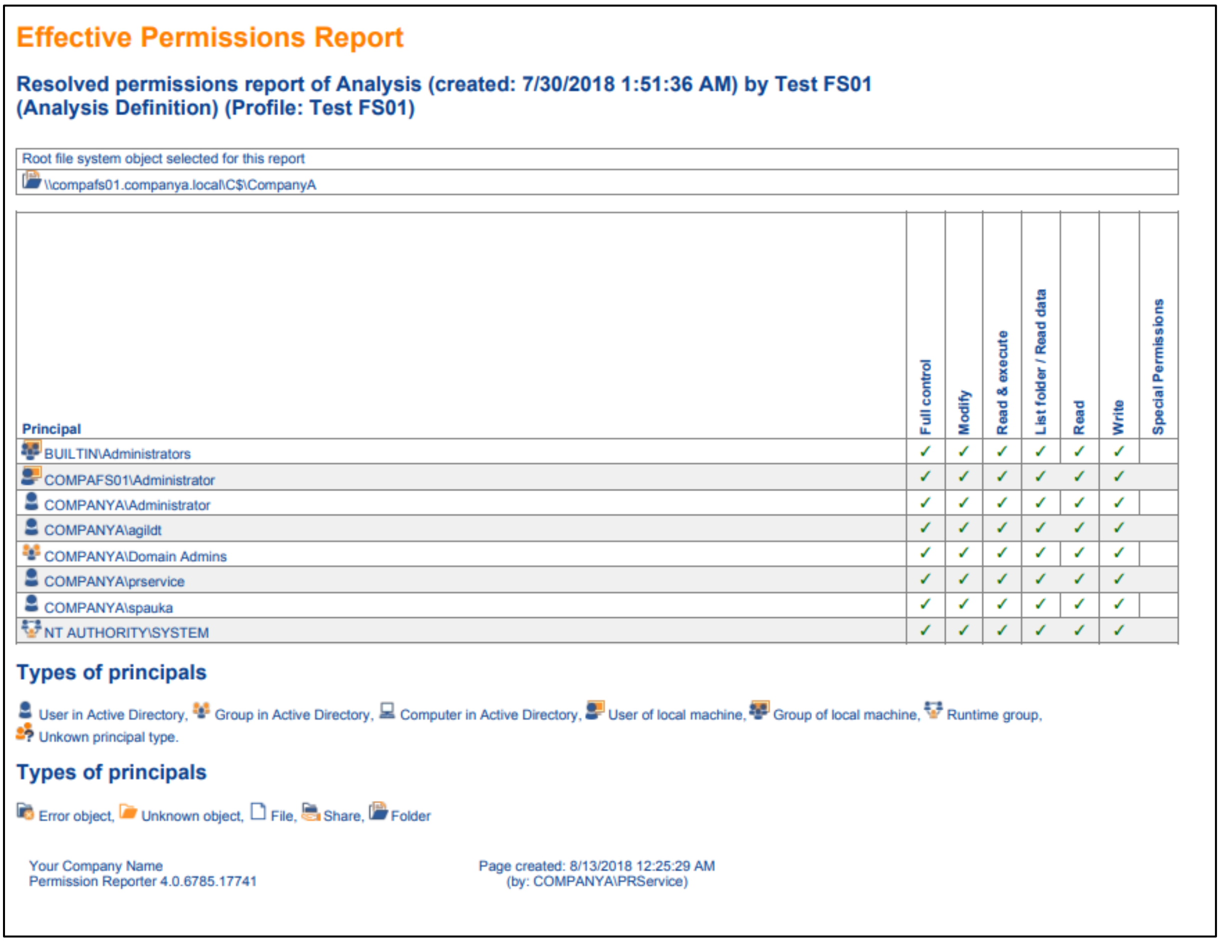
Object sources **Local object types** **AD object types**

3.2 Effective Permissions (CSV, PDF)

By creating this report, an analyzed DACL (Discretionary Access Control List, see chapter 5.1 DACL) of a securable object gets processed.

All security principals which are addressed by being named in (at least) one ACE (Access Control Entry, see chapter 5.2 ACE) or by being a (nested) member in any security group named in the DACL will be resolved.

These security principals will be listed with their effective permission on the securable object.



Effective Permissions Report

Resolved permissions report of Analysis (created: 7/30/2018 1:51:36 AM) by Test FS01 (Analysis Definition) (Profile: Test FS01)

Root file system object selected for this report
\\compafs01.companya.local\C$\CompanyA

Principal	Full control	Modify	Read & execute	List folder / Read data	Read	Write	Special Permissions
BUILTIN\Administrators	✓	✓	✓	✓	✓	✓	
COMPAFS01\Administrator	✓	✓	✓	✓	✓	✓	
COMPANYA\Administrator	✓	✓	✓	✓	✓	✓	
COMPANYA\agildt	✓	✓	✓	✓	✓	✓	
COMPANYA\Domain Admins	✓	✓	✓	✓	✓	✓	
COMPANYA\prservice	✓	✓	✓	✓	✓	✓	
COMPANYA\spauka	✓	✓	✓	✓	✓	✓	
NT AUTHORITY\SYSTEM	✓	✓	✓	✓	✓	✓	

Types of principals

User in Active Directory, Group in Active Directory, Computer in Active Directory, User of local machine, Group of local machine, Runtime group, Unkown principal type.

Types of principals

Error object, Unknown object, File, Share, Folder

Your Company Name
Permission Reporter 4.0.6785.17741

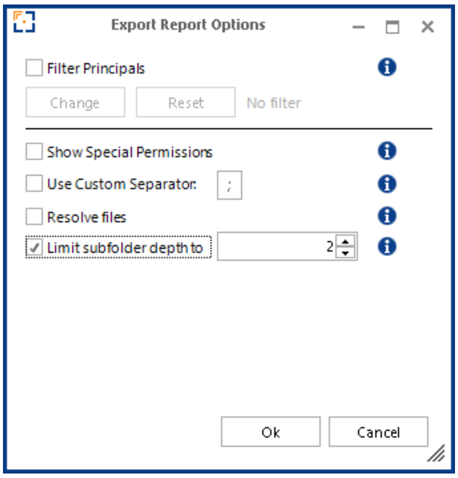
Page created: 8/13/2018 12:25:29 AM
(by: COMPANYA\PRService)

3.3 Permissions for Tree (CSV)

Similar to the “Effective Permissions Report” this report lists all security principals having any permission and their effective permissions on securable objects at the time of the chosen analysis.

But other than in the “Effective Permissions Report” the chosen securable object serves as entry point. Sub-objects of this object will also be included in this report.

In order to avoid excessive memory consumption, this reports may be limited to a maximum level of sub-folder. If this level is reached, no further sub-folder will be included in the report. E.g. C:\ is analyzed and the limit is set to 2, the folder C:\Root\Sub1\ will be included to the report, but C:\Root\Sub1\Sub2\ will not be included.



□ Filter Principals

No filter

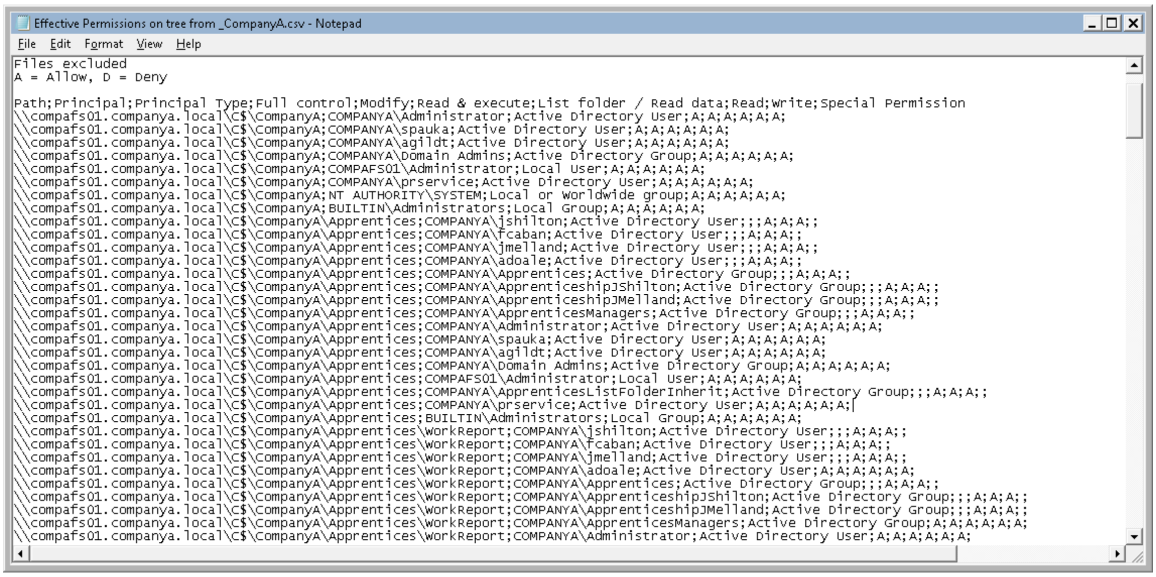
□ Show Special Permissions

□ Use Custom Separator: ;

□ Resolve files

☑ Limit subfolder depth to 2

If no limitation is set, the report will include every securable object starting from the selected entry point.



Effective Permissions on tree from _CompanyA.csv - Notepad
File Edit Format View Help

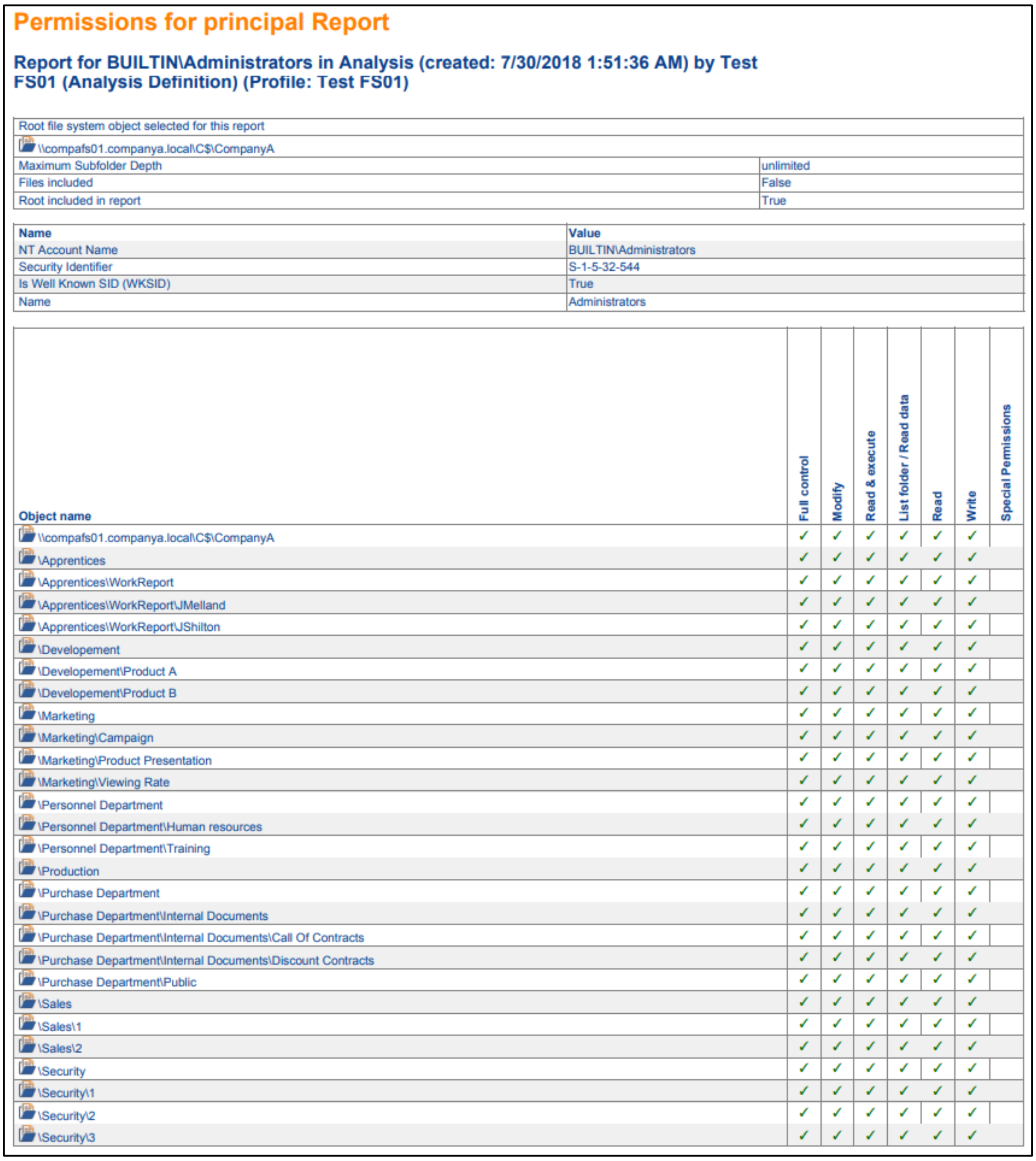
```
Files excluded
A = Allow, D = Deny

Path;Principal;Principal Type;Full control;Modify;Read & execute;List folder / Read data;Read;Write;Special Permission
\\compafs01.companya.local\C$\CompanyA;COMPANYA\Administrator;Active Directory User;A;A;A;A;A;A;
\\compafs01.companya.local\C$\CompanyA;COMPANYA\spauka;Active Directory User;A;A;A;A;A;A;
\\compafs01.companya.local\C$\CompanyA;COMPANYA\agildt;Active Directory User;A;A;A;A;A;A;
\\compafs01.companya.local\C$\CompanyA;COMPANYA\Domain Admins;Active Directory Group;A;A;A;A;A;A;
\\compafs01.companya.local\C$\CompanyA;COMPAFS01\Administrator;Local User;A;A;A;A;A;A;
\\compafs01.companya.local\C$\CompanyA;COMPANYA\prservice;Active Directory User;A;A;A;A;A;A;
\\compafs01.companya.local\C$\CompanyA;NT AUTHORITY\SYSTEM;Local or Worldwide group;A;A;A;A;A;A;
\\compafs01.companya.local\C$\CompanyA;BUILTIN\Administrators;Local Group;A;A;A;A;A;A;
\\compafs01.companya.local\C$\CompanyA\Apprentices;COMPANYA\jshilton;Active Directory User;;;A;A;A;;
\\compafs01.companya.local\C$\CompanyA\Apprentices;COMPANYA\fcaban;Active Directory User;;;A;A;A;;
\\compafs01.companya.local\C$\CompanyA\Apprentices;COMPANYA\jmelland;Active Directory User;;;A;A;A;;
\\compafs01.companya.local\C$\CompanyA\Apprentices;COMPANYA\adoale;Active Directory User;;;A;A;A;;
\\compafs01.companya.local\C$\CompanyA\Apprentices;COMPANYA\Apprentices;Active Directory Group;;;A;A;A;;
\\compafs01.companya.local\C$\CompanyA\Apprentices;COMPANYA\ApprenticeshipJShilton;Active Directory Group;;;A;A;A;;
\\compafs01.companya.local\C$\CompanyA\Apprentices;COMPANYA\ApprenticeshipJMelland;Active Directory Group;;;A;A;A;;
\\compafs01.companya.local\C$\CompanyA\Apprentices;COMPANYA\ApprenticesManagers;Active Directory Group;;;A;A;A;;
\\compafs01.companya.local\C$\CompanyA\Apprentices;COMPANYA\Administrator;Active Directory User;A;A;A;A;A;A;
\\compafs01.companya.local\C$\CompanyA\Apprentices;COMPANYA\spauka;Active Directory User;A;A;A;A;A;A;
\\compafs01.companya.local\C$\CompanyA\Apprentices;COMPANYA\agildt;Active Directory User;A;A;A;A;A;A;
\\compafs01.companya.local\C$\CompanyA\Apprentices;COMPANYA\Domain Admins;Active Directory Group;A;A;A;A;A;A;
\\compafs01.companya.local\C$\CompanyA\Apprentices;COMPAFS01\Administrator;Local User;A;A;A;A;A;A;
\\compafs01.companya.local\C$\CompanyA\Apprentices;COMPANYA\ApprenticesListFolderInherit;Active Directory Group;;;A;A;A;;
\\compafs01.companya.local\C$\CompanyA\Apprentices;COMPANYA\prservice;Active Directory User;A;A;A;A;A;A;
\\compafs01.companya.local\C$\CompanyA\Apprentices;BUILTIN\Administrators;Local Group;A;A;A;A;A;A;
\\compafs01.companya.local\C$\CompanyA\Apprentices\WorkReport;COMPANYA\jshilton;Active Directory User;;;A;A;A;;
\\compafs01.companya.local\C$\CompanyA\Apprentices\WorkReport;COMPANYA\fcaban;Active Directory User;;;A;A;A;;
\\compafs01.companya.local\C$\CompanyA\Apprentices\WorkReport;COMPANYA\jmelland;Active Directory User;;;A;A;A;;
\\compafs01.companya.local\C$\CompanyA\Apprentices\WorkReport;COMPANYA\adoale;Active Directory User;A;A;A;A;A;A;
\\compafs01.companya.local\C$\CompanyA\Apprentices\WorkReport;COMPANYA\Apprentices;Active Directory Group;;;A;A;A;;
\\compafs01.companya.local\C$\CompanyA\Apprentices\WorkReport;COMPANYA\ApprenticeshipJShilton;Active Directory Group;;;A;A;A;;
\\compafs01.companya.local\C$\CompanyA\Apprentices\WorkReport;COMPANYA\ApprenticeshipJMelland;Active Directory Group;;;A;A;A;;
\\compafs01.companya.local\C$\CompanyA\Apprentices\WorkReport;COMPANYA\ApprenticesManagers;Active Directory Group;A;A;A;A;A;A;
\\compafs01.companya.local\C$\CompanyA\Apprentices\WorkReport;COMPANYA\Administrator;Active Directory User;A;A;A;A;A;A;
```

3.4 Permissions for Principal (CSV, PDF)

To create a “Permissions for Principal Report” an analyzed security principal as well as a securable object has to be selected.

The selected securable object will be used as entry point similar to the selected securable object in a “Permissions for Tree Report”.

This report will contain all securable objects and the individual effective permissions the selected principal has on them starting with the entry point.



Permissions for principal Report

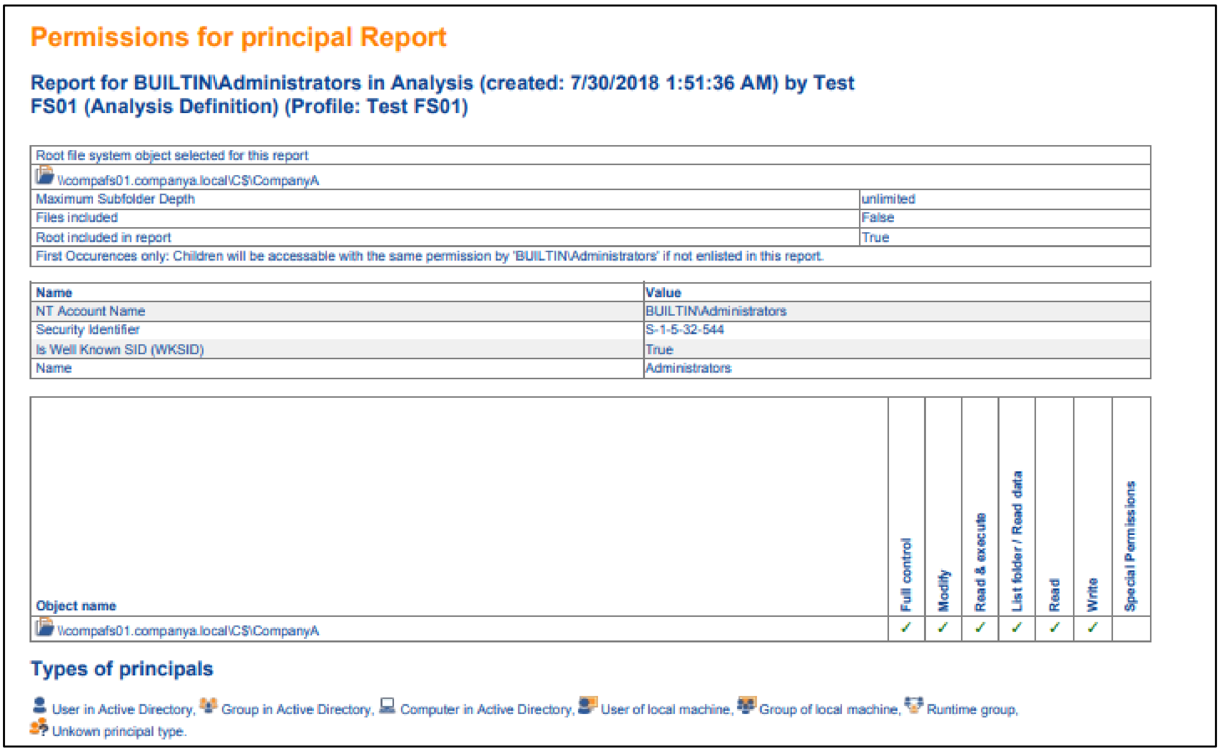
Report for BUILTIN\Administrators in Analysis (created: 7/30/2018 1:51:36 AM) by Test FS01 (Analysis Definition) (Profile: Test FS01)

Root file system object selected for this report	
\\compafs01.companya.local\C$\CompanyA	
Maximum Subfolder Depth	unlimited
Files included	False
Root included in report	True

Name	Value
NT Account Name	BUILTIN\Administrators
Security Identifier	S-1-5-32-544
Is Well Known SID (WKSID)	True
Name	Administrators

Object name	Full control	Modify	Read & execute	List folder / Read data	Read	Write	Special Permissions
\\compafs01.companya.local\C$\CompanyA	✓	✓	✓	✓	✓	✓	
\Apprentices	✓	✓	✓	✓	✓	✓	
\Apprentices\WorkReport	✓	✓	✓	✓	✓	✓	
\Apprentices\WorkReport\JMelland	✓	✓	✓	✓	✓	✓	
\Apprentices\WorkReport\JShilton	✓	✓	✓	✓	✓	✓	
\Developement	✓	✓	✓	✓	✓	✓	
\Developement\Product A	✓	✓	✓	✓	✓	✓	
\Developement\Product B	✓	✓	✓	✓	✓	✓	
\Marketing	✓	✓	✓	✓	✓	✓	
\Marketing\Campaign	✓	✓	✓	✓	✓	✓	
\Marketing\Product Presentation	✓	✓	✓	✓	✓	✓	
\Marketing\Viewing Rate	✓	✓	✓	✓	✓	✓	
\Personnel Department	✓	✓	✓	✓	✓	✓	
\Personnel Department\Human resources	✓	✓	✓	✓	✓	✓	
\Personnel Department\Training	✓	✓	✓	✓	✓	✓	
\Production	✓	✓	✓	✓	✓	✓	
\Purchase Department	✓	✓	✓	✓	✓	✓	
\Purchase Department\Internal Documents	✓	✓	✓	✓	✓	✓	
\Purchase Department\Internal Documents\Call Of Contracts	✓	✓	✓	✓	✓	✓	
\Purchase Department\Internal Documents\Discount Contracts	✓	✓	✓	✓	✓	✓	
\Purchase Department\Public	✓	✓	✓	✓	✓	✓	
\Sales	✓	✓	✓	✓	✓	✓	
\Sales\1	✓	✓	✓	✓	✓	✓	
\Sales\2	✓	✓	✓	✓	✓	✓	
\Security	✓	✓	✓	✓	✓	✓	
\Security\1	✓	✓	✓	✓	✓	✓	
\Security\2	✓	✓	✓	✓	✓	✓	
\Security\3	✓	✓	✓	✓	✓	✓	

By setting “Show Only First Occurrence” in export options for *Permissions for Principal*, the report will look like following.



Permissions for principal Report

Report for BUILTIN\Administrators in Analysis (created: 7/30/2018 1:51:36 AM) by Test FS01 (Analysis Definition) (Profile: Test FS01)

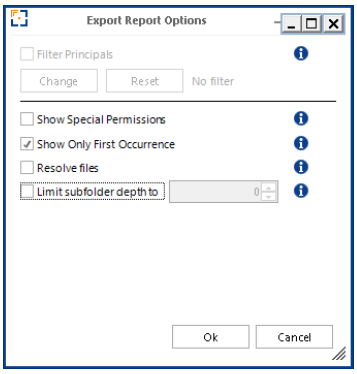
Root file system object selected for this report	
\\compafs01.companya.local\C$\CompanyA	
Maximum Subfolder Depth	unlimited
Files included	False
Root included in report	True
First Occurences only: Children will be accessable with the same permission by 'BUILTIN\Administrators' if not enlisted in this report.	

Name	Value
NT Account Name	BUILTIN\Administrators
Security Identifier	S-1-5-32-544
Is Well Known SID (WKSID)	True
Name	Administrators

Object name	Full control	Modify	Read & execute	List folder / Read data	Read	Write	Special Permissions
\\compafs01.companya.local\C$\CompanyA	✓	✓	✓	✓	✓	✓	

Types of principals

User in Active Directory, Group in Active Directory, Computer in Active Directory, User of local machine, Group of local machine, Runtime group, Unkown principal type.



Export Report Options

□ Filter Principals

□ Show Special Permissions

☑ Show Only First Occurrence

□ Resolve files

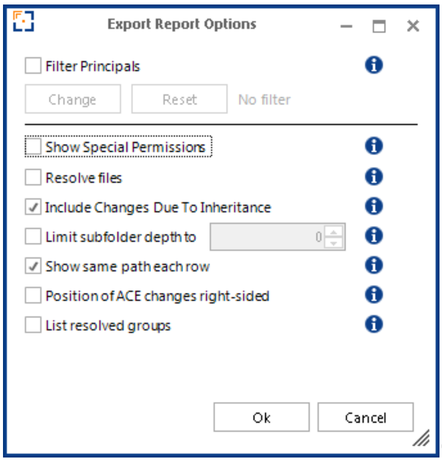
□ Limit subfolder depth to 0

3.5 DACL Differences (CSV, PDF)

Starting with a chosen securable object as an entry point this report shows all differences between DACLs of sub-objects and their direct parents at the time of the chosen analysis.

Therefore a DACL of a securable object will be compared with the DACL of the object which is the direct parent. All disparities between DACLs will be listed in this report in the form of ACEs, causing disparities, and a phrase characterizing the kind of disparity.

You also can use the Principal Filter (see chapter 0 Filter Principals) to see only principals you want to see.



☐ Filter Principals

No filter

☐ Show Special Permissions

☐ Resolve files

☑ Include Changes Due To Inheritance

☐ Limit subfolder depth to 0

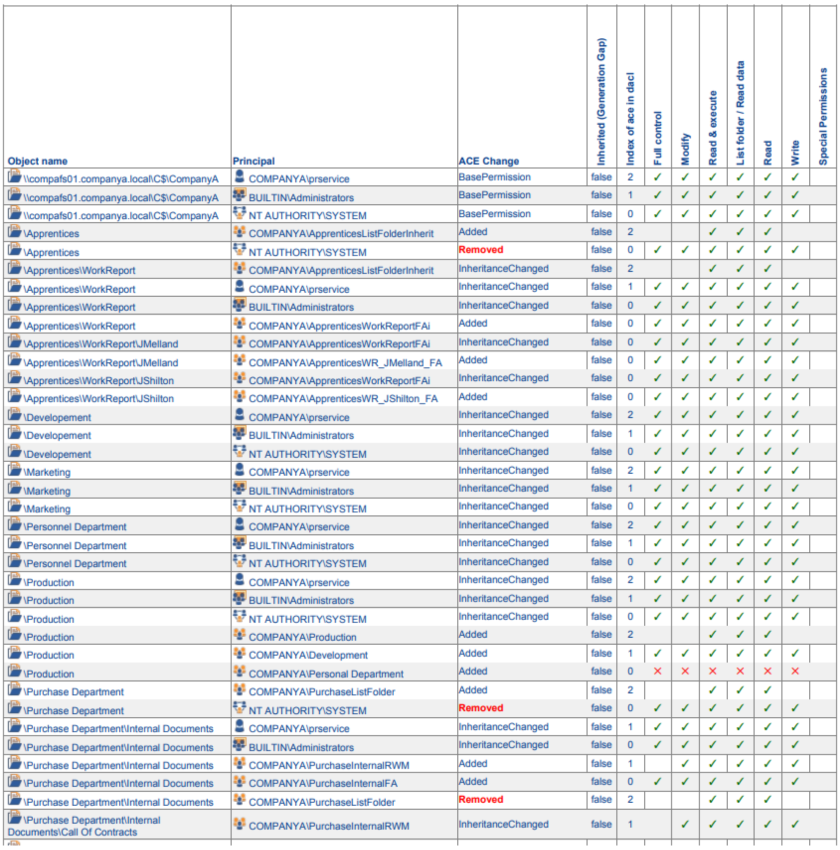
☑ Show same path each row

☐ Position of ACE changes right-sided

☐ List resolved groups

0

3.5.1 Kinds of disparity



Object name	Principal	ACE Change	Inherited (Generation Gap)	Index of ace in dacl	Full control	Modify	Read & execute	List folder / Read data	Read	Write	Special Permissions
\\compafs01.companya.local\C$\CompanyA	COMPANYA\prservice	BasePermission	false	2	✓	✓	✓	✓	✓	✓	
\\compafs01.companya.local\C$\CompanyA	BUILTIN\Administrators	BasePermission	false	1	✓	✓	✓	✓	✓	✓	
\\compafs01.companya.local\C$\CompanyA	NT AUTHORITY\SYSTEM	BasePermission	false	0	✓	✓	✓	✓	✓	✓	
\Apprentices	COMPANYA\ApprenticesListFolderInherit	Added	false	2			✓	✓	✓		
\Apprentices	NT AUTHORITY\SYSTEM	Removed	false	0	✓	✓	✓	✓	✓	✓	
\Apprentices\WorkReport	COMPANYA\ApprenticesListFolderInherit	InheritanceChanged	false	2			✓	✓	✓		
\Apprentices\WorkReport	COMPANYA\prservice	InheritanceChanged	false	1	✓	✓	✓	✓	✓	✓	
\Apprentices\WorkReport	BUILTIN\Administrators	InheritanceChanged	false	0	✓	✓	✓	✓	✓	✓	
\Apprentices\WorkReport	COMPANYA\ApprenticesWorkReportFAi	Added	false	0	✓	✓	✓	✓	✓	✓	
\Apprentices\WorkReport\JMelland	COMPANYA\ApprenticesWorkReportFAi	InheritanceChanged	false	0	✓	✓	✓	✓	✓	✓	
\Apprentices\WorkReport\JMelland	COMPANYA\ApprenticesWR_JMelland_FA	Added	false	0	✓	✓	✓	✓	✓	✓	
\Apprentices\WorkReport\JShilton	COMPANYA\ApprenticesWorkReportFAi	InheritanceChanged	false	0	✓	✓	✓	✓	✓	✓	
\Apprentices\WorkReport\JShilton	COMPANYA\ApprenticesWR_JShilton_FA	Added	false	0	✓	✓	✓	✓	✓	✓	
\Developement	COMPANYA\prservice	InheritanceChanged	false	2	✓	✓	✓	✓	✓	✓	
\Developement	BUILTIN\Administrators	InheritanceChanged	false	1	✓	✓	✓	✓	✓	✓	
\Developement	NT AUTHORITY\SYSTEM	InheritanceChanged	false	0	✓	✓	✓	✓	✓	✓	
\Marketing	COMPANYA\prservice	InheritanceChanged	false	2	✓	✓	✓	✓	✓	✓	
\Marketing	BUILTIN\Administrators	InheritanceChanged	false	1	✓	✓	✓	✓	✓	✓	
\Marketing	NT AUTHORITY\SYSTEM	InheritanceChanged	false	0	✓	✓	✓	✓	✓	✓	
\Personnel Department	COMPANYA\prservice	InheritanceChanged	false	2	✓	✓	✓	✓	✓	✓	
\Personnel Department	BUILTIN\Administrators	InheritanceChanged	false	1	✓	✓	✓	✓	✓	✓	
\Personnel Department	NT AUTHORITY\SYSTEM	InheritanceChanged	false	0	✓	✓	✓	✓	✓	✓	
\Production	COMPANYA\prservice	InheritanceChanged	false	2	✓	✓	✓	✓	✓	✓	
\Production	BUILTIN\Administrators	InheritanceChanged	false	1	✓	✓	✓	✓	✓	✓	
\Production	NT AUTHORITY\SYSTEM	InheritanceChanged	false	0	✓	✓	✓	✓	✓	✓	
\Production	COMPANYA\Production	Added	false	2			✓	✓	✓		
\Production	COMPANYA\Development	Added	false	1	✓	✓	✓	✓	✓	✓	
\Production	COMPANYA\Personal Department	Added	false	0	✗	✗	✗	✗	✗	✗	
\Purchase Department	COMPANYA\PurchaseListFolder	Added	false	2			✓	✓	✓		
\Purchase Department	NT AUTHORITY\SYSTEM	Removed	false	0	✓	✓	✓	✓	✓	✓	
\Purchase Department\Internal Documents	COMPANYA\prservice	InheritanceChanged	false	1	✓	✓	✓	✓	✓	✓	
\Purchase Department\Internal Documents	BUILTIN\Administrators	InheritanceChanged	false	0	✓	✓	✓	✓	✓	✓	
\Purchase Department\Internal Documents	COMPANYA\PurchaseInternalRWM	Added	false	1		✓	✓	✓	✓	✓	
\Purchase Department\Internal Documents	COMPANYA\PurchaseInternalFA	Added	false	0	✓	✓	✓	✓	✓	✓	
\Purchase Department\Internal Documents	COMPANYA\PurchaseListFolder	Removed	false	2			✓	✓	✓		
\Purchase Department\Internal Documents\Call Of Contracts	COMPANYA\PurchaseInternalRWM	InheritanceChanged	false	1		✓	✓	✓	✓	✓	

3.5.1.1 BasePermission

Represents an ACE of the entry point’s DACL. This ACE does not necessarily cause a disparity between its DACL and the DACL of the direct parent.

Note: Since the direct parent is not part of this report you will not be able to make an objective statement whether the ACE is responsible for a different DACL or not.

3.5.1.2 Added

An ACE tagged with the “Added‟-keyword means in effect that the DACL of the parent object does not contain an ACE which grants the same permissions to the same security principal.

This means that a new permission has been added to the child object’s DACL.

3.5.1.3 Removed

ACEs which are listed as “Removed” representing missing ACEs compared to the parent object’s DACL.

3.5.1.4 InheritanceChanged

If an ACE is tagged as “InheritanceChanged”, no new permission is added or removed from the DACL of the securable object compared to its parent.

The given ACE differs in its properties concerning inheritance rules. So this ACE may be either the first inherited entry after a new ACE is applied to a securable object or this ACE will not be inherited to the same types of objects as the related ACE of the parent object.

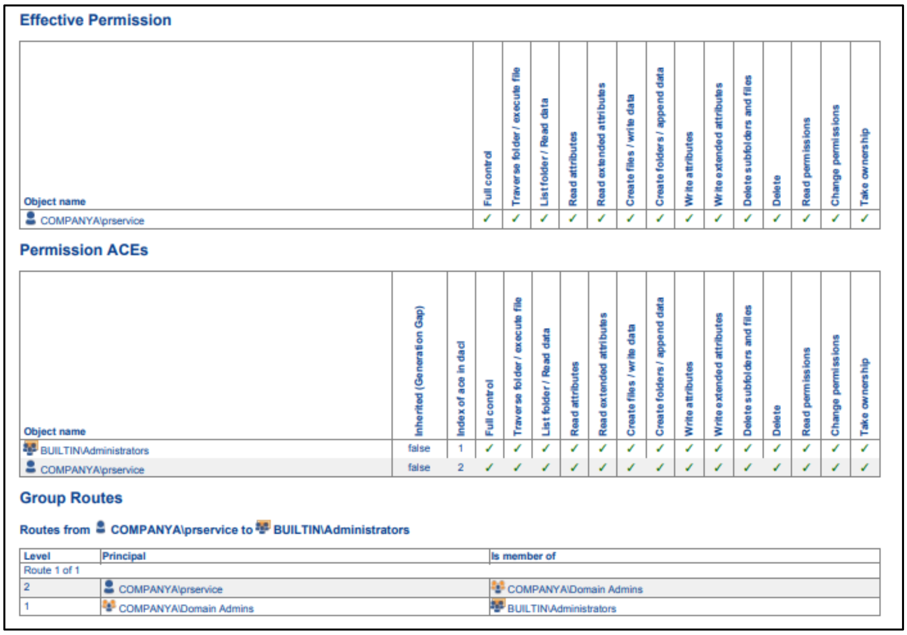
3.6 Permissions Details Report (PDF)

Shows the analyzed effective permission granted for a selected security principal on a securable object.

Furthermore all ACEs of the DACL, which contributed to the effective permission on the selected securable object, are listed in this report.

If listed ACEs are granted permissions over (security) groups, this report will also show the nested memberships of the group, which are leading to the selected security principal.

Example: In the image below the user *prservice* is granted with the permission via the group *BULTIN\Administrators*. prservice is not a direct member of this group. *BULTIN\Administrators* has a member, which is also a group called *COMPANYA\Domain Admins*. prservice is member of the *Domain Admins* group. You can see the resolved membership in this report in the chapter *Group Routes.*



Effective Permission

Object name	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
COMPANYA\prservice	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Permission ACEs

Object name	Inherited (Generation Gap)	Index of ace in dacl	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
BUILTIN\Administrators	false	1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
COMPANYA\prservice	false	2	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Group Routes

Routes from COMPANYA\prservice to BUILTIN\Administrators

Level	Principal	Is member of
Route 1 of 1		
2	COMPANYA\prservice	COMPANYA\Domain Admins
1	COMPANYA\Domain Admins	BUILTIN\Administrators

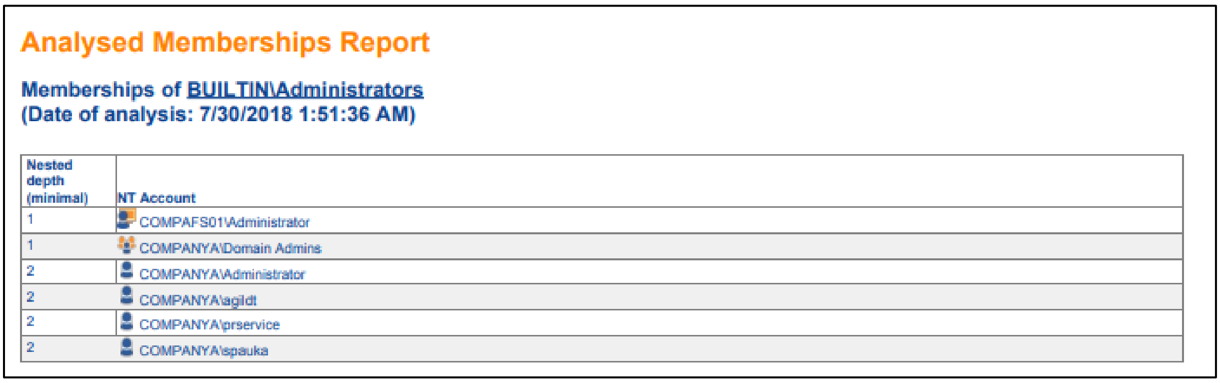
3.7 Full Memberlist Report (PDF)

Shows all analyzed members of a selected group.

This report includes nested memberships and displays the minimal nesting depth.

A nested depth of *1* stands for a direct membership. A depth value of 2 means that the listed security principal is member of a group which itself is a direct member of the selected group.

If a security principal is a member of the group via different routes, the shortest route and the minimal nesting depth will be listed.



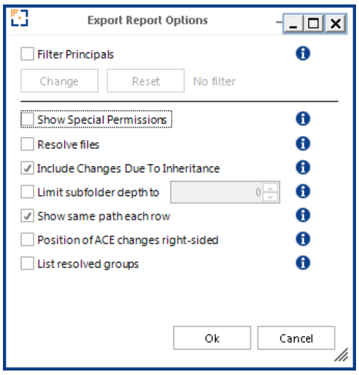
Analysed Memberships Report

Memberships of BUILTIN\Administrators
(Date of analysis: 7/30/2018 1:51:36 AM)

Nested depth (minimal)	NT Account
1	COMPAFS01\Administrator
1	COMPANYA\Domain Admins
2	COMPANYA\Administrator
2	COMPANYA\agildt
2	COMPANYA\prservice
2	COMPANYA\spauka

4 Export Report Options

The provided report types offer options, which allow to filter the amount of results. This allows you to export the information you need keeping the resulting size of the exported file as small as possible.



□ Filter Principals

No filter

□ Show Special Permissions
□ Resolve files
☑ Include Changes Due To Inheritance
□ Limit subfolder depth to 0
☑ Show same path each row
□ Position of ACE changes right-sided
□ List resolved groups

Export Report Options for DACL Differences

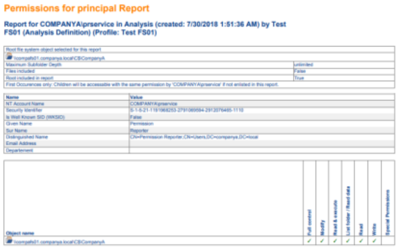
4.1 Show Only First Occurrences

By enabling this option the report will only list securable objects, for whom the effective permission granted to the selected security principal differs from the effective permission granted on the current parent object.

This means effectively that if analyzed sub-objects are not listed in the exported file, these objects grant the same permission to the security principal as the current parent object.

Affected report types:

- Permissions for Principal



Permissions for principal Report

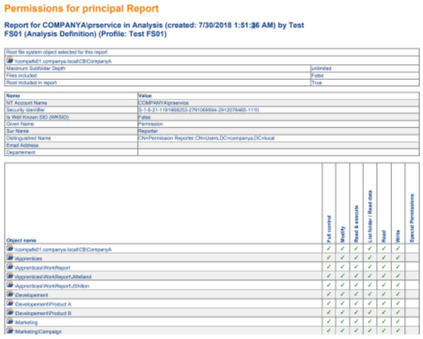
Report for COMPANYA\prservice in Analysis (created: 7/30/2018 1:51:36 AM) by Test FS01 (Analysis Definition) (Profile: Test FS01)

Root file system object selected for this report	
\\compafs01.companya.local\C$\CompanyA	
Maximum Subfolder Depth	unlimited
Files included	False
Root included in report	True
First Occurences only: Children will be accessable with the same permission by 'COMPANYA\prservice' if not enlisted in this report.	

Name	Value
NT Account Name	COMPANYA\prservice
Security Identifier	S-1-5-21-1191968253-2791069594-2912076465-1110
Is Well Known SID (WKSID)	False
Given Name	Permission
Sur Name	Reporter
Distinguished Name	CN=Permission Reporter,CN=Users,DC=companya,DC=local
Email Address	
Departement	

Object name	Full control	Modify	Read & execute	List folder / Read data	Read	Write	Special Permissions
\\compafs01.companya.local\C$\CompanyA	✓	✓	✓	✓	✓	✓	

Show Only First Occurences enabled



Permissions for principal Report

Report for COMPANYA\prservice in Analysis (created: 7/30/2018 1:51:36 AM) by Test FS01 (Analysis Definition) (Profile: Test FS01)

Root file system object selected for this report	
\\compafs01.companya.local\C$\CompanyA	
Maximum Subfolder Depth	unlimited
Files included	False
Root included in report	True

Name	Value
NT Account Name	COMPANYA\prservice
Security Identifier	S-1-5-21-1191968253-2791069594-2912076465-1110
Is Well Known SID (WKSID)	False
Given Name	Permission
Sur Name	Reporter
Distinguished Name	CN=Permission Reporter,CN=Users,DC=companya,DC=local
Email Address	
Departement	

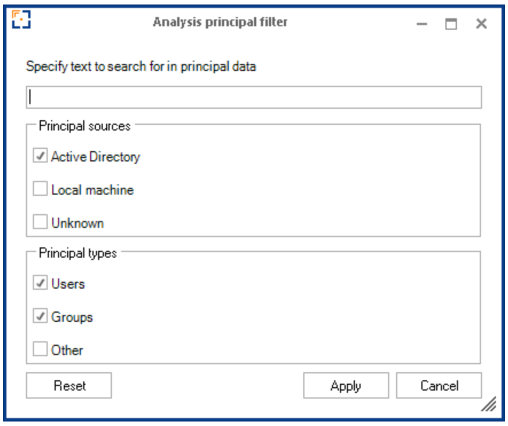
Object name	Full control	Modify	Read & execute	List folder / Read data	Read	Write	Special Permissions
\\compafs01.companya.local\C$\CompanyA	✓	✓	✓	✓	✓	✓	
\Apprentices	✓	✓	✓	✓	✓	✓	
\Apprentices\WorkReport	✓	✓	✓	✓	✓	✓	
\Apprentices\WorkReport\JMelland	✓	✓	✓	✓	✓	✓	
\Apprentices\WorkReport\JShilton	✓	✓	✓	✓	✓	✓	
\Developement	✓	✓	✓	✓	✓	✓	
\Developement\Product A	✓	✓	✓	✓	✓	✓	
\Developement\Product B	✓	✓	✓	✓	✓	✓	
\Marketing	✓	✓	✓	✓	✓	✓	
\Marketing\Campaign	✓	✓	✓	✓	✓	✓	

Show Only First Occurences disabled

4.2 Filter Principals

If a filter is applied for security principals the resulting report will only list security principals which match the defined filter conditions. During the creation of the report however a given filter will not prevent security groups to be resolved, even if these groups do not match the given filter conditions.

You can filter by only selecting specific type e.g. *Active Directory users and groups* without the need of filtering by name.



Analysis principal filter

Specify text to search for in principal data

Principal sources
☑ Active Directory
□ Local machine
□ Unknown

Principal types
☑ Users
☑ Groups
□ Other

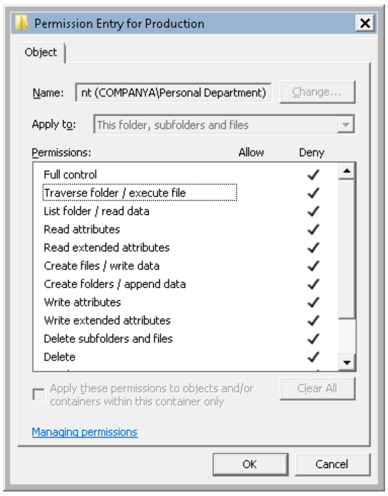
Affected report types:

- Effective Permissions
- Permissions for Tree
- DACL Differences

4.3 Show Special Permissions

Enabling this option will cause Permission Reporter to export the access mask of permissions in the form of advanced permissions similar to the advanced permissions listed in the Advanced Permission Dialog of Microsoft’s Windows Explorer.

If this option is disabled, Permission Reporter will display the access mask similar to the permissions listed in the “Security”-Tab of the Property-Dialog of Microsoft’s Windows Explorer.


Permission Entry for Production

Name: nt (COMPANYA\Personal Department)

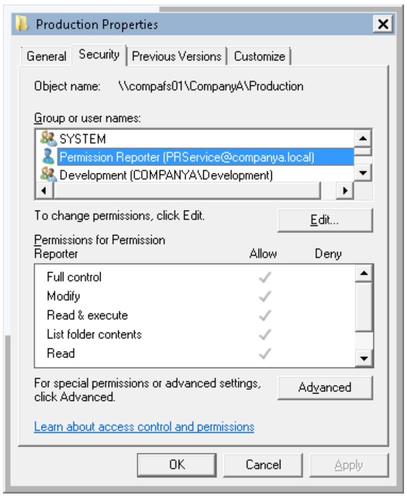
Apply to: This folder, subfolders and files

Permissions: Allow Deny

- 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 ✓

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

Special permissions


Production Properties

Object name: \\compafs01\CompanyA\Production

Group or user names:

- SYSTEM
- Permission Reporter (PRService@companya.local)
- Development (COMPANYA\Development)

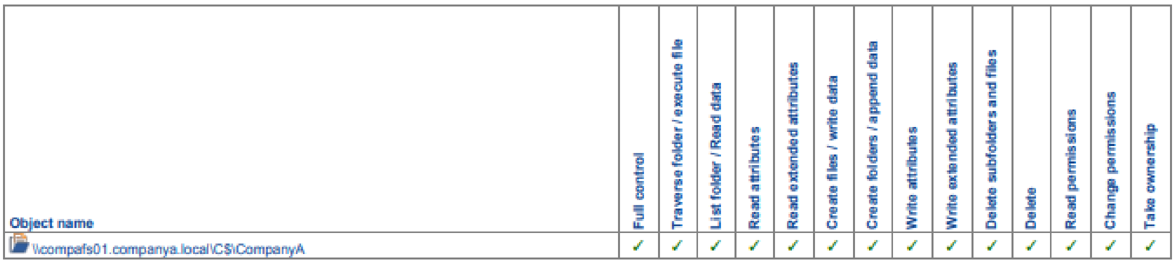
To change permissions, click Edit.

Permissions for Permission Reporter Allow Deny

- Full control ✓
- Modify ✓
- Read & execute ✓
- List folder contents ✓
- Read ✓

For special permissions or advanced settings, click Advanced.

Permissions



Object name	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
\\compafs01.companya.local\C$\CompanyA	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

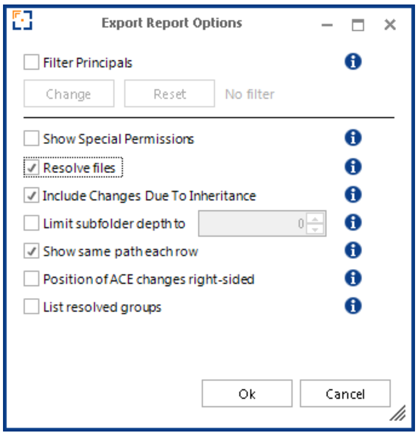
Special Permissions in report

4.4 Resolve Files

Enable the option *Resolve Files* if you to include files in the report. Please note that including files will likely lead to a significant increase of the amount of results in the report.

Consequently the time needed for the export to be generated will also increase.

Note: This option can only be applied if the analysis has “include Files” enabled.



Export Report Options

□ Filter Principals

No filter

□ Show Special Permissions

☑ Resolve files

☑ Include Changes Due To Inheritance

□ Limit subfolder depth to 0

☑ Show same path each row

□ Position of ACE changes right-sided

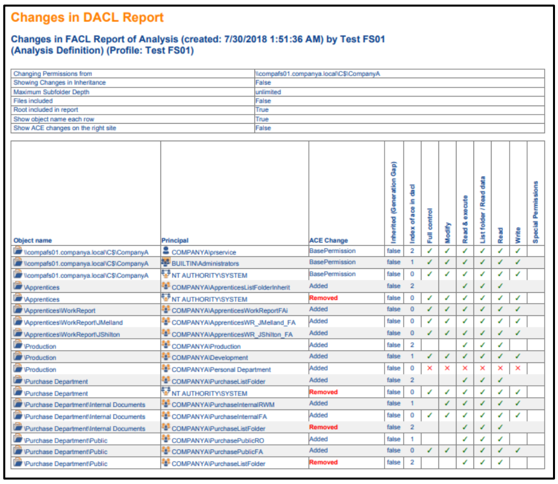
□ List resolved groups

Affected report types:

- Permissions for Principal
- Permissions for Tree
- DACL Differences

4.5 Include Changes Due To Inheritance

Disabling the option *Include Changes Due To Inheritance* will cause Permission Reporter not to list ACEs which are going to be flagged with the “InheritanceChanged” disparity.



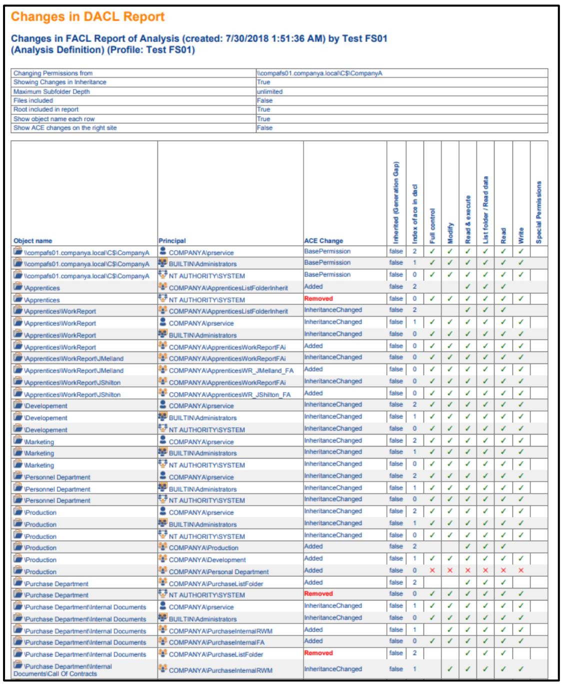
Changes in DACL Report

Changes in FACL Report of Analysis (created: 7/30/2018 1:51:36 AM) by Test FS01 (Analysis Definition) (Profile: Test FS01)

Changing Permissions from	\\compafs01.companya.local\C$\CompanyA
Showing Changes in Inheritance	False
Maximum Subfolder Depth	unlimited
Files included	False
Root included in report	True
Show object name each row	True
Show ACE changes on the right site	False

Object name	Principal	ACE Change	Inherited (Generation Gap)	Index of ace in dacl	Full control	Modify	Read & execute	List folder / Read data	Read	Write	Special Permissions
\\compafs01.companya.local\C$\CompanyA	COMPANYA\prservice	BasePermission	false	2	✓	✓	✓	✓	✓	✓	
\\compafs01.companya.local\C$\CompanyA	BUILTIN\Administrators	BasePermission	false	1	✓	✓	✓	✓	✓	✓	
\\compafs01.companya.local\C$\CompanyA	NT AUTHORITY\SYSTEM	BasePermission	false	0	✓	✓	✓	✓	✓	✓	
\Apprentices	COMPANYA\ApprenticesListFolderInherit	Added	false	2			✓	✓	✓		
\Apprentices	NT AUTHORITY\SYSTEM	Removed	false	0	✓	✓	✓	✓	✓	✓	
\Apprentices\WorkReport	COMPANYA\ApprenticesWorkReportFAi	Added	false	0	✓	✓	✓	✓	✓	✓	
\Apprentices\WorkReport\JMelland	COMPANYA\ApprenticesWR_JMelland_FA	Added	false	0	✓	✓	✓	✓	✓	✓	
\Apprentices\WorkReport\JShilton	COMPANYA\ApprenticesWR_JShilton_FA	Added	false	0	✓	✓	✓	✓	✓	✓	
\Production	COMPANYA\Production	Added	false	2			✓	✓	✓		
\Production	COMPANYA\Development	Added	false	1	✓	✓	✓	✓	✓	✓	
\Production	COMPANYA\Personal Department	Added	false	0	✗	✗	✗	✗	✗	✗	
\Purchase Department	COMPANYA\PurchaseListFolder	Added	false	2			✓	✓	✓		
\Purchase Department	NT AUTHORITY\SYSTEM	Removed	false	0	✓	✓	✓	✓	✓	✓	
\Purchase Department\Internal Documents	COMPANYA\PurchaseInternalRWM	Added	false	1		✓	✓	✓	✓	✓	
\Purchase Department\Internal Documents	COMPANYA\PurchaseInternalFA	Added	false	0	✓	✓	✓	✓	✓	✓	
\Purchase Department\Internal Documents	COMPANYA\PurchaseListFolder	Removed	false	2			✓	✓	✓		
\Purchase Department\Public	COMPANYA\PurchasePublicRO	Added	false	1			✓	✓	✓		
\Purchase Department\Public	COMPANYA\PurchasePublicFA	Added	false	0	✓	✓	✓	✓	✓	✓	
\Purchase Department\Public	COMPANYA\PurchaseListFolder	Removed	false	2			✓	✓	✓		

disabled option with resulting report



Changes in DACL Report

Changes in FACL Report of Analysis (created: 7/30/2018 1:51:36 AM) by Test FS01 (Analysis Definition) (Profile: Test FS01)

Changing Permissions from	\\compafs01.companya.local\C$\CompanyA
Showing Changes in Inheritance	True
Maximum Subfolder Depth	unlimited
Files included	False
Root included in report	True
Show object name each row	True
Show ACE changes on the right site	False

Object name	Principal	ACE Change	Inherited (Generation Gap)	Index of ace in dacl	Full control	Modify	Read & execute	List folder / Read data	Read	Write	Special Permissions
\\compafs01.companya.local\C$\CompanyA	COMPANYA\prservice	BasePermission	false	2	✓	✓	✓	✓	✓	✓	
\\compafs01.companya.local\C$\CompanyA	BUILTIN\Administrators	BasePermission	false	1	✓	✓	✓	✓	✓	✓	
\\compafs01.companya.local\C$\CompanyA	NT AUTHORITY\SYSTEM	BasePermission	false	0	✓	✓	✓	✓	✓	✓	
\Apprentices	COMPANYA\ApprenticesListFolderInherit	Added	false	2			✓	✓	✓		
\Apprentices	NT AUTHORITY\SYSTEM	Removed	false	0	✓	✓	✓	✓	✓	✓	
\Apprentices\WorkReport	COMPANYA\ApprenticesListFolderInherit	InheritanceChanged	false	2			✓	✓	✓		
\Apprentices\WorkReport	COMPANYA\prservice	InheritanceChanged	false	1	✓	✓	✓	✓	✓	✓	
\Apprentices\WorkReport	BUILTIN\Administrators	InheritanceChanged	false	0	✓	✓	✓	✓	✓	✓	
\Apprentices\WorkReport	COMPANYA\ApprenticesWorkReportFAi	Added	false	0	✓	✓	✓	✓	✓	✓	
\Apprentices\WorkReport\JMelland	COMPANYA\ApprenticesWorkReportFAi	InheritanceChanged	false	0	✓	✓	✓	✓	✓	✓	
\Apprentices\WorkReport\JMelland	COMPANYA\ApprenticesWR_JMelland_FA	Added	false	0	✓	✓	✓	✓	✓	✓	
\Apprentices\WorkReport\JShilton	COMPANYA\ApprenticesWorkReportFAi	InheritanceChanged	false	0	✓	✓	✓	✓	✓	✓	
\Apprentices\WorkReport\JShilton	COMPANYA\ApprenticesWR_JShilton_FA	Added	false	0	✓	✓	✓	✓	✓	✓	
\Developement	COMPANYA\prservice	InheritanceChanged	false	2	✓	✓	✓	✓	✓	✓	
\Developement	BUILTIN\Administrators	InheritanceChanged	false	1	✓	✓	✓	✓	✓	✓	
\Developement	NT AUTHORITY\SYSTEM	InheritanceChanged	false	0	✓	✓	✓	✓	✓	✓	
\Marketing	COMPANYA\prservice	InheritanceChanged	false	2	✓	✓	✓	✓	✓	✓	
\Marketing	BUILTIN\Administrators	InheritanceChanged	false	1	✓	✓	✓	✓	✓	✓	
\Marketing	NT AUTHORITY\SYSTEM	InheritanceChanged	false	0	✓	✓	✓	✓	✓	✓	
\Personnel Department	COMPANYA\prservice	InheritanceChanged	false	2	✓	✓	✓	✓	✓	✓	
\Personnel Department	BUILTIN\Administrators	InheritanceChanged	false	1	✓	✓	✓	✓	✓	✓	
\Personnel Department	NT AUTHORITY\SYSTEM	InheritanceChanged	false	0	✓	✓	✓	✓	✓	✓	
\Production	COMPANYA\prservice	InheritanceChanged	false	2	✓	✓	✓	✓	✓	✓	
\Production	BUILTIN\Administrators	InheritanceChanged	false	1	✓	✓	✓	✓	✓	✓	
\Production	NT AUTHORITY\SYSTEM	InheritanceChanged	false	0	✓	✓	✓	✓	✓	✓	
\Production	COMPANYA\Production	Added	false	2			✓	✓	✓		
\Production	COMPANYA\Development	Added	false	1	✓	✓	✓	✓	✓	✓	
\Production	COMPANYA\Personal Department	Added	false	0	✗	✗	✗	✗	✗	✗	
\Purchase Department	COMPANYA\PurchaseListFolder	Added	false	2			✓	✓	✓		
\Purchase Department	NT AUTHORITY\SYSTEM	Removed	false	0	✓	✓	✓	✓	✓	✓	
\Purchase Department\Internal Documents	COMPANYA\prservice	InheritanceChanged	false	1	✓	✓	✓	✓	✓	✓	
\Purchase Department\Internal Documents	BUILTIN\Administrators	InheritanceChanged	false	0	✓	✓	✓	✓	✓	✓	
\Purchase Department\Internal Documents	COMPANYA\PurchaseInternalRWM	Added	false	1		✓	✓	✓	✓	✓	
\Purchase Department\Internal Documents	COMPANYA\PurchaseInternalFA	Added	false	0	✓	✓	✓	✓	✓	✓	
\Purchase Department\Internal Documents	COMPANYA\PurchaseListFolder	Removed	false	2			✓	✓	✓		
\Purchase Department\Internal Documents\Call Of Contracts	COMPANYA\PurchaseInternalRWM	InheritanceChanged	false	1		✓	✓	✓	✓	✓	

enabled option with resulting report

Affected report types:

- DACL Differences

4.6 Limit Subfolder Depth To …

In order to avoid excessive memory consumption, a report may be limited to a maximum level of sub-folder. If this level is reached, no further sub-folder will be included in the report.

If no limitation is set, the report will include every securable object starting from the selected entry point (e.g. folder or share).

E.g. C:\ is analyzed and the limit is set to 2, the folder C:\Root\Sub1\ will be included to the report, but C:\Root\Sub1\Sub2\ will not be included.

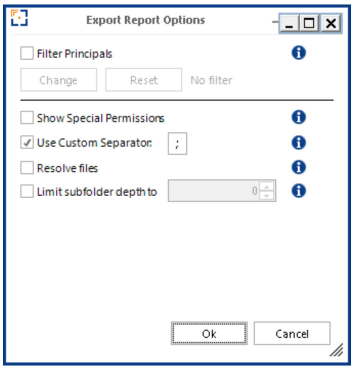
Affected report types:

- Permissions for Tree
- Permissions for Principal
- DACL Differences

4.7 Use Custom Separator (CSV only)

Normally there is no need to change the separator for a CSV Report.

But if you want Permission Reporter to use a separator other than the default separator (“;”) to divide cells inside a CSV Report, you can use this option to select a separator.



Export Report Options

☐ Filter Principals

Change Reset No filter

☐ Show Special Permissions

☑ Use Custom Separator: ;

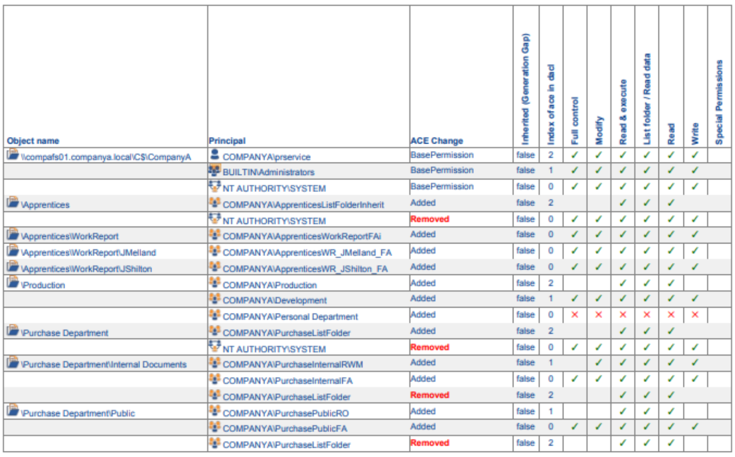
☐ Resolve files

☐ Limit subfolder depth to 0

Ok Cancel

4.8 Show same path each row

On huge reports it will be confusing to see the folder-name displayed for each permission. By de-selecting this option you will see the folder only once.



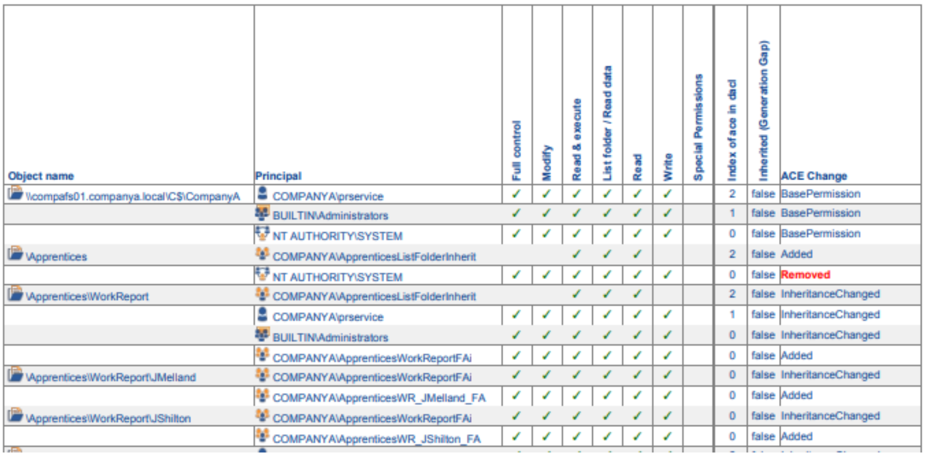
Object name	Principal	ACE Change	Inherited (Generation Gap)	Index of ace in dacl	Full control	Modify	Read & execute	List folder / Read data	Read	Write	Special Permissions
\\compafs01.companya.local\C$\CompanyA	COMPANYA\prservice	BasePermission	false	2	✓	✓	✓	✓	✓	✓	
	BUILTIN\Administrators	BasePermission	false	1	✓	✓	✓	✓	✓	✓	
	NT AUTHORITY\SYSTEM	BasePermission	false	0	✓	✓	✓	✓	✓	✓	
\Apprentices	COMPANYA\ApprenticesListFolderInherit	Added	false	2			✓	✓	✓		
	NT AUTHORITY\SYSTEM	Removed	false	0	✓	✓	✓	✓	✓	✓	
\Apprentices\WorkReport	COMPANYA\ApprenticesWorkReportFAi	Added	false	0	✓	✓	✓	✓	✓	✓	
\Apprentices\WorkReport\JMelland	COMPANYA\ApprenticesWR_JMelland_FA	Added	false	0	✓	✓	✓	✓	✓	✓	
\Apprentices\WorkReport\JShilton	COMPANYA\ApprenticesWR_JShilton_FA	Added	false	0	✓	✓	✓	✓	✓	✓	
\Production	COMPANYA\Production	Added	false	2			✓	✓	✓		
	COMPANYA\Development	Added	false	1	✓	✓	✓	✓	✓	✓	
	COMPANYA\Personal Department	Added	false	0	✗	✗	✗	✗	✗	✗	
\Purchase Department	COMPANYA\PurchaseListFolder	Added	false	2			✓	✓	✓		
	NT AUTHORITY\SYSTEM	Removed	false	0	✓	✓	✓	✓	✓	✓	
\Purchase Department\Internal Documents	COMPANYA\PurchaseInternalRWM	Added	false	1		✓	✓	✓	✓	✓	
	COMPANYA\PurchaseInternalFA	Added	false	0	✓	✓	✓	✓	✓	✓	
	COMPANYA\PurchaseListFolder	Removed	false	2			✓	✓	✓		
\Purchase Department\Public	COMPANYA\PurchasePublicRO	Added	false	1			✓	✓	✓		
	COMPANYA\PurchasePublicFA	Added	false	0	✓	✓	✓	✓	✓	✓	
	COMPANYA\PurchaseListFolder	Removed	false	2			✓	✓	✓		

Affected report types:

- DACL Differences (PDF only)

4.9 Position of ACE changed right-sided

Here you can set the ACE change information to be positioned right sided instead of the middle. This makes the reading of reports easier for non-technicians.



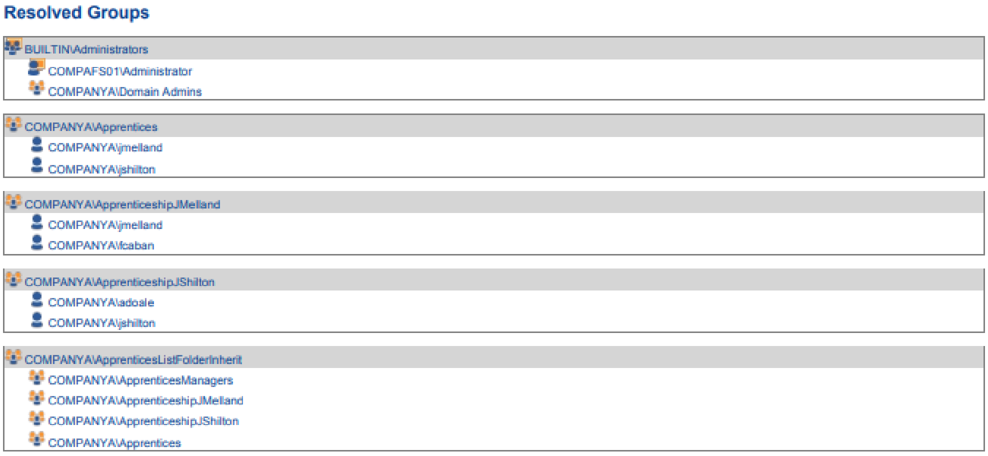
Object name	Principal	Full control	Modify	Read & execute	List folder / Read data	Read	Write	Special Permissions	Index of ace in dacl	Inherited (Generation Gap)	ACE Change
\\compafs01.companya.local\C$\CompanyA	COMPANYA\prservice	✓	✓	✓	✓	✓	✓		2	false	BasePermission
	BUILTIN\Administrators	✓	✓	✓	✓	✓	✓		1	false	BasePermission
	NT AUTHORITY\SYSTEM	✓	✓	✓	✓	✓	✓		0	false	BasePermission
\Apprentices	COMPANYA\ApprenticesListFolderInherit			✓	✓	✓			2	false	Added
	NT AUTHORITY\SYSTEM	✓	✓	✓	✓	✓	✓		0	false	Removed
\Apprentices\WorkReport	COMPANYA\ApprenticesListFolderInherit			✓	✓	✓			2	false	InheritanceChanged
	COMPANYA\prservice	✓	✓	✓	✓	✓	✓		1	false	InheritanceChanged
	BUILTIN\Administrators	✓	✓	✓	✓	✓	✓		0	false	InheritanceChanged
	COMPANYA\ApprenticesWorkReportFAi	✓	✓	✓	✓	✓	✓		0	false	Added
\Apprentices\WorkReport\JMelland	COMPANYA\ApprenticesWorkReportFAi	✓	✓	✓	✓	✓	✓		0	false	InheritanceChanged
	COMPANYA\ApprenticesWR_JMelland_FA	✓	✓	✓	✓	✓	✓		0	false	Added
\Apprentices\WorkReport\JShilton	COMPANYA\ApprenticesWorkReportFAi	✓	✓	✓	✓	✓	✓		0	false	InheritanceChanged
	COMPANYA\ApprenticesWR_JShilton_FA	✓	✓	✓	✓	✓	✓		0	false	Added

Affected report types:

- DACL Differences (PDF only)

4.10 List resolved groups (PDF only)

You can show all groups affected in this report with their membership resolved.



Resolved Groups

BUILTIN\Administrators
- COMPAFS01\Administrator
- COMPANYA\Domain Admins

COMPANYA\Apprentices
- COMPANYA\jmelland
- COMPANYA\jshilton

COMPANYA\ApprenticeshipJMelland
- COMPANYA\jmelland
- COMPANYA\fcaban

COMPANYA\ApprenticeshipJShilton
- COMPANYA\adoale
- COMPANYA\jshilton

COMPANYA\ApprenticesListFolderInherit
- COMPANYA\ApprenticesManagers
- COMPANYA\ApprenticeshipJMelland
- COMPANYA\ApprenticeshipJShilton
- COMPANYA\Apprentices

5 Explanation of Terms

5.1 DACL (Discretionary Access Control List)

The DACL is part of the security descriptor of a securable object like a file, a folder of the file system or even a shared folder.

As a part of the security descriptor of a securable object, a DACL is the list which describes the permissions granted for security principals (like users or security groups) on the securable object.

5.2 ACE (Access Control Entry)

An ACE is an entry inside an ACL (Access Control List). In the case of the DACL an ACE defines the permission granted for a security principal (like a user or a security group) on a securable object, to whose security descriptor the DACL belongs.