



Security Explorer[®]

What's New Guide

Security Explorer 8.0



www.scriptlogic.com 1.800.424.9411 EMEA: +44 (0)1628 518410 APAC: +61 (0)3 8352 6600

© 2011 ScriptLogic Corporation and its licensors. All rights reserved. ScriptLogic and the ScriptLogic log are registered trademarks of ScriptLogic Corporation in the United State and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

© 2011 ScriptLogic Corporation ALL RIGHTS RESERVED.

ScriptLogic, the ScriptLogic logo and Point, Click, Done! are trademarks and registered trademarks of ScriptLogic Corporation in the United States of America and other countries. All other trademarks and registered trademarks are property of their respective owners.



Security Explorer provides IT administrators with one platform to completely manage access controls and security across a Windows network environment. The robust functionality of Security Explorer allows IT administrators to manage, backup/recover, search, migrate and report on access controls for Windows Server, Exchange, SharePoint, and SQL Server from a common, easy to use graphical interface. Security Explorer enables IT administrators to meet today's strict regulatory compliance requirements and increase IT department productivity by reducing the number of management products required to maintain a secure environment.

New Feature Highlights for Version 8.0

Summary

Security Explorer 8.0 introduces a number of enhancements that significantly improve the usability of the product.

New Tasks View

The new **Tasks** view exposes the numerous Security Explorer features from each of the product modules in a simple wizard-driven task-based view. This new view gives users a task driven workflow when performing permissions related operations making it easy for both new and experienced users to perform basic or advanced permissions management tasks as well as generating permissions reports.





New Control Pane

The classic Security Explorer Browse View which provides an instant view of permission information when browsing the network now includes the new **Control Pane**. The **Control Pane** exposes all of the product actions available for the selected object when browsing resources on the network. The tasks available through the Control Pane are the same as those found on the Task Pane but will automatically run in the context of the selected resource.





Formatted Reporting

Security Explorer 8.0 adds numerous pre-defined formatted reports that allow users to report on permissions, users and group membership information and other security related details on file servers, SharePoint, SQL Server and Exchange. In most modules, you can choose to create either an export-type report or a search-type report.





Executing a Simple Export

File Yiew Background									
3 A 🗁 📓 🗳 🗅 🖓 🔍 🔍 100% 🕑 🔍 4 4 🕨 🕅 🕒 🖗 🔯 🖓 😪 🛛									
	700	n Out							
	200								
		NI	FS Security Export Report						
C:\Program Files\									
Summary Mode: Yes Export folder permissions: Yes Export file permissions: Yes File Wildcard: *.* Subfolders: Recurse all subfolders									
	Allow /					iner	sted	ted	
Path	Deny	Permission	Account	Owner	Applies to	Container	Protected	Inherited	
1									
C:\Program Files\	Allow	Read and Execute LfRaRxTfRp	NT AUTHORITY\Authenticated Users S-1-5-11	BUILTINVAdministrators	This folder subfolders and files	Yes	Yes	No	
C:\Program Files\ C:\Program Files\	Allow			BUILTINVAdministrators BUILTINVAdministrators		Yes Yes	Yes Yes	No No	
-	Allow	LfRaR×TfRp Modify	S-1-5-11 BUILTIN\Server Operators		and files This folder subfolders				

Searching for Permissions





Disabled Account Management

Search for, report on, and manage access granted to **disabled accounts** on file servers, (including NTFS, Shares, Services, and Tasks), SharePoint, SQL Server, and Exchange.

The **Tasks** tab provides quick access.

Adv	anced Ta	asks	-					
	ind Find	Revoke Unknown	Eind Disabled	Revoke Disabled	Auto Clone	G Browse SID History	Find SID History	Revoke SID History
7			577	20				
	Set hership	Repair Security	Copy Security	Reduce to Read Only	Home Directory			

When using the Browse tab, you can select to search for disabled accounts, and then easily create a report.

Security Explorer 8 [LICENSED TO SCRI	PTLOGIC CORPORATION]						
ile <u>Vi</u> ew <u>S</u> ecurity S <u>e</u> arch <u>A</u> ccess Manager <u>T</u> ools	: <u>H</u> elp						
🕹 🕹 🦉 🖉 🗇 🌝 🖓 🗏 🕅	i) 📋 🗳 🗳 😪 🧳	🔯 🖬 😭	🧕 🙀 🎯	🏂 🙀 🌾 🥥 🚱 🛛	2 🛛		
Security Explorer	🛒 NTFS Secu	rity Sea	rch		SCRIPT		
Tasks Browse Search Status	Sroup/User Search Co	riteria 🗌	Permission Search	Criteria 🔂 Folder a	and File Search Criteria		
THES Search Progress Complete VM-2K3-DC1 Gomplete VM-2K3-DC1 Gomplete XX-3DC1\C\$\ (19091 items se X Errors	Group/User: Include all group members Include "Everyone" Group	ships	Include gr	Advanced User Se Search Acc oup results	election ess Manager group memberships Include SID history		
Permissions Found: 313	Include "Authenticated Us Include "Network" Group Include "Interactive" User		 Include us Dearch for Search for 	disabled accounts	Show only SID history permissi	ons	
	Start Search 🗙 Clear F	Results 📀	Defaults	Save Results 🛐 Rep	iort 💥 Auto-update result:	5	
🏸 All Management Targets	A Path	Path Type	Туре	Domain Name	Permis		
NTFS Security	\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	Folder Folder File	R Allow Allow R Allow	MOSSFARM & jspe MOSSFARM & swill MOSSFARM & jspe	is 🛉 Ful	I Control	
Share Security	\VM-2K3-DC1\C\$\1dbfecc-5.			MOSSFARM		l Control	
Registry Sect 🦻 Preview							
🗊 🎡 🍖 Eile View Background							
	🕹 🔓 🛃 🖑 🍳 🍳 1	.00% 🔽 🤄	↓ ●	🛛 🛛 🔁 🐴 🔯	• 🖂 • 🔞 •		
Stop							
			NTI	S Security Search Repo Scope: WVM-2K3-DC1	rt		
			Gr	oup/User Search Criteri	a		
Group/User: include all group me Search Access Mar include SID history	mberships nager group memberships		ryone" Group nenticated Users" (nknown acco unt s	· —		nclude "Network" Group nclude "Interactive" User Show only SID history permi	ssions
		Permissi	ion Search Crite	ria		Folder and File	Search criteria
File permission: Search	ons (DACL) Search for irch for any permission, Allow or De of or any permission, Allow or Deny rmissions or better Search for	eny, All Scope Ty v, All Scope Type	s	nvert results set (applie nherited Permissions Explicit Permissions	is to DACL only) Protected Folders/Files Show duplicated permit	()	sions
	Path	Path Type	Туре	A	ccount	Permission	Applies to
WVM-2K3-DC11C\$\		Folder	Allow	MOSSFARMijspencer S-1-5-21-2659425245-3644	4453046-721493414-1138	Full Control	This folder, subfolders and files
WVM-2K3-DC11C\$\		Folder	Allow	MOSSFARM\swillis S-1-5-21-2659425245-3644	4453046-721493414-1149	Full Control	This folder, subfolders and files
WYM-2K3-DC1 VC\$11dbfecc-5020-416 i	6f-b6bf-42d7c0ebfac3 RegFile.ph	File	Allow ()	MOSSFARMijspencer S-1-5-21-2659425245-364	4453046-721493414-1138	Full Control	This file only
WVM-2K3-DC1 VC\$\9e5bc143-081b-4	10d-94f5-d6affe51093d RegFile.	File	Allow ()	MOSSFARMijspencer S.1.5.21.2659425245.364	4453046.721493414.1138	Full Control	This file only
Page 1 of 27							Zoom Factor: 100



When you find disabled accounts, simply right-click the accounts, and then choose **Revoke** from the shortcut menu. The **Revoke** feature opens with the accounts populated and you can easily choose to revoke the selected disabled accounts or revoke all disabled accounts.

PNTFS Security		
🛒 Revoke Folder Permissions		
Set Reset	(WM-2K3-DC1\C\$\	*
■ Some Security ■ B Computer (VM-2K3-DC1)	List Names From: Current object permissions	
🕀 🎱 Domains	▲ Type Domain Name Permission Applies To ၛ Allow MOSSFARM & ispencer ၛ Full Control This folder, subfolders	
	Allow MOSSFARM & swillis R Full Control This folder, subfolders	
	Group/User MOSSFARM\ispencer Advanced User Selection	
	Permission Eul Control Allow Advanced Permission Selection	
	Revoke all permissions (Allow and Deny) for the selected user	
	Include SID history search when adding permissions for revoking	
	List of users Type Domain Name Permission	
	revoke: RAllow MOSSFARM & ispencer R Full Control	
	Add>	
	Advanced Revoke Options Revoke all unknown and deleted accounts	
	Log Actions Revoke all disabled accounts	
Reload Status: Ready	Include protected objects (objects with 'Inherit Permissions from Parent' disabled)	
Help	<u> </u>	

Select Advanced Revoke Options to revoke all disabled accounts.

List of users and groups to revoke: Add> < Remove	🔺 Type Domain Name	Permission
	Advanced Revoke Options Log Actions Include protected objects (objects with 'In	Revoke all unknown and deleted accounts Revoke all disabled accounts herit Permissions from Parent' disabled)



Post-migration Permission Comparison

View backed up permissions in comparison to the live environment when restoring permissions to an alternate location. Permissions are backed up before data is migrated and then compared and optionally restored to the destination location. This feature provides verification that security is consistent when data is migrated from one server to another (*NTFS module only*).

Backup File	Current Permis	sions (C:\Program	n Files'	\NetMeeting\)				
\\vmware-host\\program files backup.sec	Object: Neth	leeting			Owner:	BUILTIN\Administrate	ors	
🖃 🔲 👧 Backup (\\vmware-host\Shared Folders	🔺 Туре	Domain	Na	ame	P	ermissions	Applies To	SID
🖻 🔲 🛗 C:\Program Files\	R Allow	MOSSEARM		bsmith	23	Full Control	This folder, subfolders	S-1-5
🗉 🔲 🚞 Adobe	RAllow	MOSSFARM	_	ispencer	, a	Full Control	This folder, subfolders	
🕀 🔲 🚰 Common Files	Allow (1)	NT AUTHO	- C	Authenticated Users	Ś.	Read and Execute	This folder, subfolders	
🗉 🔲 🤖 ComPlus Applications	Allow (I)	BUILTIN	-	Server Operators	, R	Modify	This folder, subfolders	
🗈 🔲 🚰 GPMC	Allow (I)	BUILTIN	_	Administrators	Ŕ	Full Control	This folder, subfolders	
🗈 🔲 🚰 Internet Explorer	Allow (I)	NT AUTHO		SYSTEM	Ř	Full Control	This folder, subfolders	
i∎- □ 🚰 Microsoft.NET II- □ III MSBuild	Allow (I)	<none></none>	-	CREATOR OWNER	R R	Full Control	Subfolders and files only	
- -	<)		
Composition	Backed-up Per	rmissions (C:\Pro	gram F	Files/NetMeeting/)				
Support Tools TechSmith	Object: Neth	feeting			Owner:	BUILTIN\Administrate	ors	
🖬 🔲 🚰 VMware	🔺 Туре	Domain	Na	ame	P	ermissions	Applies To	SID
🖶 🗌 🛗 Windows Media Player 🕀 🔲 🌁 Windows NT	R Allow (I)	NT AUTHO	0	Authenticated Users	R	List Folder Contents	This folder only	S-1-5-
■ □ Control Windows NT ■ □ Control WindowsUpdate	Allow (I)	NT AUTHO	0	Authenticated Users	Ŕ	Read and Execute	Subfolders and files only	S-1-5
	Allow (I)	BUILTIN	22	Server Operators	Ŕ	Modify	This folder only	S-1-5
<	Allow (I)	BUILTIN	92	Server Operators	Ŕ	Modify	Subfolders and files only	S-1-5
Select all children De-select all children	Allow (I)	BUILTIN	82	Administrators	Ŕ	Full Control	This folder only	S-1-5
	Allow (I)	BUILTIN	92	Administrators	Ŕ	Full Control	Subfolders and files only	S-1-5-
	Allow (I)	NT AUTHO	0	SYSTEM	Ŕ	Full Control	This folder only	S-1-5
			ā	SYSTEM	Ŕ	Full Control	Subfolders and files only	S-1-5
Show differences (folders and files only) Include files when previewing backup Restore permissions Restore owner	Allow (I)	NT AUTHO						



Clone Group Membership Settings Between Accounts

The clone feature in Security Explorer allows users to duplicate access control settings from one account to another when setting up a new user's access. In Version 8.0, this feature has been expanded to optionally clone the user's group membership settings in addition to the directly assigned permissions. This ensures the same level of access is granted to the new user whether the access was granted directly to the user, or indirectly through group membership settings. This feature applies to the NTFS, Share, SharePoint, SQL Server, and Exchange modules.

🥦 NTFS Security	
S Clone Folder Permissions	
È C∧	~
Manual User/Group Selection Automatic User/Group Selection SID History Import User/Group Selection	
Source Group or User: Destination Group or User:	
List Names Current object permissions Show Users Refresh List Names Current object permissions Show Users Refresh]
🔺 Name Description 🔼 🔺 Name Description 🤇	
28 BUILTIN\Administrators Full Control 28 BUILTIN\Administrators Full Control	
28 BUILTIN\Users Read and Execute 28 BUILTIN\Users Read and Execute 28 BUILTIN\Users Special (Cs)	
24 BUILTIN/Users Special (Cf) 24 BUILTIN/Users Special (Cf)	
CREATOR DWNER Full Control CREATOR DWNER Full Control	
Everyone List Folder Contents Everyone List Folder Contents	
Search State	
Source: BUILTIN\Administrators Advanced User Selection Destination: MOSSFARM\bsmith Advanced User Selection	j
Source Group or User Destination Group or User	
List of users 22 BUILTIN \Administrators	ן ר
and groups to	รี
cione:	-
Add ->	
< Remove	
Clone permissions Clone ownership 🗹 Clone group memberships 1 Source/Destination Pair(s)	
Replace source permissions with destination permissions.	
Include protected objects when cloning (objects with 'Inherit Permissions from Parent' disabled)	
Help Browse SID History	



Bulk Group Membership Changes

Security Explorer provides the ability to centrally view and manage local group membership settings on servers and workstations across the network. Search for and then select the accounts you want to manage.



Display Group Contents to view the members for the selected groups that are common for these groups. You can add or remove members to all the groups selected.

 Group Name 	Domain	SID	Description
BUILTIN \Administrators MOSSFARM \Domain Admins MOSSFARM \Enterprise Adm	BUILTIN MOSSFARM MOSSFARM	S-1-5-32-544 S-1-5-21-2659425245-364 S-1-5-21-2659425245-364	(Administrators) Administrators have complet (Domain Admins) Designated administrators (Enterprise Admins) Designated administrator
iroups common members The selected groups contain the fo			1
	<i>llowing members</i> Domain	SID S-1-5-21-2659425245-364445	



Expanded PowerShell functionality

Twenty new PowerShell cmdlets have been created to allow for permissions management on NTFS, Shares, SharePoint, SQL Server, and Exchange. The PowerShell cmdlets provide the capability to Grant, Revoke, Clone, Backup, and Export permissions.

Deleted Account Cleanup in SharePoint

When an account is deleted from Active Directory, that account does not automatically get removed from SharePoint or SharePoint groups. Security Explorer now provides the capability to search and remove all access in SharePoint to deleted AD accounts and remove those accounts from all SharePoint groups.

🦻 Shi	arePoint Security
#	Remove Permissions for Deleted Accounts
	You have selected the option which will remove permissions for deleted accounts on the selected SharePoint site(s) (including all children: sites, lists and documents, etc).
	Permissions for deleted accounts can be retained in SharePoint because the SharePoint server is unaware that the parent AD account has been deleted. This special "Remove Permissions for Deleted Accounts" function will remove these unwanted permissions for you. You should ensure that you have backed up your permissions before executing this function.
	Please note: you may, if you wish, choose to produce a report only. This will not make any changes to your SharePoint site and will allow you to perform a review before deciding if you want to proceed.
	Remove deleted accounts from SharePoint groups
	Create report (will list changed items)
	File:
	Produce report only (i.e. no changes will be made)
	OK Cancel

Various Exchange Management Enhancements

- Grant permissions to manage group contents
- Mail enable/disable public folders
- Create new distribution group from existing AD group
- View and configure external contacts
- Various RBAC enhancements for Exchange 2010
- Manage permissions for multiple mailbox folders in one operation



Multiple Account Searching

Security Explorer provides the capability to search across multiple servers to highlight account access (both directly assigned and indirectly assigned through group membership). Version 8.0 adds the ability to search for permissions assigned to multiple accounts at one time.

Security Explorer 8 [LICENSED TO SCRI	TLOGIC CORPORATION]	
Eile View Security Search Access Manager Tools	Help	
🕹 🕹 🕸 🕾 🕾 🍕 🔊 🖉 🔊		
Security Explorer	📑 NTFS Security Search	SCRIPTIOGIC
Tasks Browse Search Status	🖉 Group/User Search Criteria 🖗 Permission Search Criteria 🍺 Folder and File Search	Criteria
NTFS Search Progress Complete VM-2K3-DC1	Group/User: MOSSFARM/bsmith;MOSSFARM/ispencer;MOSSFA Advanced User Selection	
ي //YM-2K3-DC1/C\$/ (19096 items se	Include all group memberships Search Access Manager g	roup memberships
	Include "Everyone" Group Include group results Include SID H	history
	□ Include "Authenticated Users" Group V Include user results □ Show only SI	ID history permissions
	Include "Network" Group Search for unknown accounts	
(Include "Interactive" User	
	Start Search X Clear Results O Defaults Save Results Report	uto-update results
	Path Path Type Domain Name	Permission 🔥
Permissions Found: 665	C)\\VM-2K3-DC1\C\$\ Folder 🖗 Allow MOSSFARM 🙎 bsmith	👫 Full Control
	Callow MOSSFARM a jspencer	Rull Control
🏸 All Management Targets 🔋 🔌	Holder Allow MOSSFARM swillis Holder NVM-2K3-DC1\C\$\ Folder NVM-2K3-DC1\C\$\ Folder NVM-2K3-DC1\C\$\ Folder Supervisors	R Full Control
NTFS Security	WM-2K3-DC1\C\$\1dbfecc-502 File Allow MOSSFARM Someth	R Full Control
	🛄 \\VM-2K3-DC1\C\$\1dbfecc-502 File 🕺 Allow MOSSFARM 🧔 jspencer	😤 Full Control
👾 Share Security	\\VM-2K3-DC1\C\$\1dbfecc-502 File \	R Full Control
Registry Security	(\VM-2K3-DC1\C\$\1dbfecc-502 File \vdots Allow MOSSFARM \vdots Supervisors \vdots VM-2K3-DC1\C\$\9e5bc143-08 File \vdots Allow MOSSFARM \vdots bsmith	R Full Control
	NVM-2K3-DC1\C\$\9e5bc143-08 File 🛛 👫 Allow MOSSFARM 🧸 jspencer	R Full Control
🍠 🏟 🧠 🐉 👗 🗊 🖂 🤅	🛄\\VM-2K3-DC1\C\$\9e5bc143-08 File 🛛 👰 Allow MOSSFARM 🗕 swillis	😤 Full Control
	(\VM-2K3-DC1\C\$\9e5bc143-08 File \vdots Allow MOSSFARM \vdots Supervisors \vdots VM-2K3-DC1\C\$\10.5Y5 File \vdots Allow MOSSFARM \vdots bsmith	Full Control
Stop Ready	WM-2K3-DC1\C\$\IO.SY5 File Allow MOSSFARM Smith	🕺 Full Control 🗸

Support for Managing Vista/Windows 2008 style tasks

In the Tasks Management module, support is expanded to include Windows Vista and Windows Server 2008.

Security Explorer 8 (LICENSED TO SCRIPTLOGIC CORPORA File View Search Tools Help ▷ ▶ ♦ ★ ☆ २ ♦ 0 0	
Security Explorer	Task Management
Tasks Browse Reports	Path Tasks Go Set Reset Show All
All Management Targets Gomputer (VM-2K8-E2010) Gmputer (VM-2K8-E2010) Gmputer (VM-2K8-E2010) Gmputer (VM-2K8-E2010) Gmputer (VM-2K8-E2010)	A Task Name Status Logon Account Name Applicator Run GoogleUpdateTaskUsers Pending MDSSFARM\Adminis new task C
Provintes Services Services Services Sources Sources	CoogleUpdateTaskUses Properties (Local Machine) General Triggers Actions Conditions Settings History Name: GoogleUpdateTaskUsers Author: Administrator Description: Security options: When running the task, use the following user account: MOSSFARMAdministrator Run whether user is logged on Run whether user is logged on rot Do not store password. The task will only have access to local computer resources. Run with histore trivileges
Reload Retus: Ready	Hidden Configure for: Windows Server [™] 2003, Windows® XP, or Windows® 2X, ▼ Windows Server [™] 2003, Windows® XP, or Windows® 2000 Windows Vota [™] , Windows Server [™] 2008 R2 Windows Server [™] 2008 R2
	OK Cancel

Back Up SACL on Files and Folders

Security Explorer 8.0 now provides the ability to backup and restore file and folder audit settings (known as the System Access Control List or SACL).

🦻 NTFS Security					
Backup Security					
Backup File Name:					
Add Add					
Clear					
Load					
Save					
New Path:					
You can manually enter a new backup path here (press [Enter] to add an item to the list) or you can click the "Add" button above to browse for the desired path(s).					
Recurse all subfolders and files for supplied paths (Depth)					
Perform a check/repair inheritance operation before executing backup					
✓ Include System Access Control List (SACL) in backup					
File Filter					
Wildcard: ** Provide Security					
Backup File	- Current Permissions (C:\P	ogram Files\NetMeeting\)			
\\vmware-host\\program files backup.sec Load	Object: NetMeeting		Owner: BUILTIN\Administrato	ns	
Comparison of the second	🔺 Type Domain	Name	Permissions	Applies To	SID
⊡-⊽C\Program Files\ ⊕-⊽ChProgram Files\	Allow (I) NT AUT		Read and Execute	This folder, subfolders	S-1-5-1
😟 🔽 🛅 Common Files	R Allow (I) BUILTIN R Allow (I) BUILTIN		👫 Modify 📆 Full Control	This folder, subfolders This folder, subfolders	
🖻 🔽 🛅 ComPlus Applications 😥 🖓 🧰		HO 🥘 SYSTEM	Full Control	This folder, subfolders	
trime trime trime trime trime trime	n (I) Rhow (I)	CREATOR OWNER	<table-of-contents> Full Control</table-of-contents>	Subfolders and files only	S-1-3-0
😥 🗹 🔂 🖬 🗹 🔁					
₩ V 📩 MSBuild ₩ V 📩 MSXML 6.0					
In the second s	<				>
🗷 🔽 🖂 ScriptLogic Corporation	Backed-up Permissions (0	:\Program Files\NetMeeting\)			
⊞ ⊽ 🧰 Support Tools ⊞ 🔽 🔂 TechSmith	Object: NetMeeting		Owner: BUILTIN\Administrato	ns	
🗷 🔽 🛅 VMware	🔺 Type 🛛 Domain	Name	Permissions	Applies To	SID
🖶 🔽 💼 Windows Media Player 🗷 🖓 🧰 Windows N T	😤 Allow (I) 🛛 NT AUT		<table-of-contents> List Folder Contents</table-of-contents>	This folder only	S-1-5-1
	Allow (I) NT AUT		Read and Execute	Subfolders and files only	S-1-5-1
<	R Allow (I) BUILTIN R Allow (I) BUILTIN		👫 Modify 😤 Modify	This folder only Subfolders and files only	S-1-5-3: S-1-5-3:
Select all children De-select all children	😤 Allow (I) 🛛 BUILTIN	🔜 Administrators	👫 Full Control	This folder only	S-1-5-3:
Show differences (folders and files only)	Allow (I) BUILTIN		Full Control	Subfolders and files only	
Include files when previewing backup		HO 🎱 SYSTEM HO 🎱 SYSTEM	👫 Full Control 📆 Full Control	This folder only Subfolders and files only	S-1-5-1) S-1-5-1)
Restore permissions	Allow (I) NT AUT	CREATOR OWNER	R Full Control	Subfolders and files only Subfolders and files only	
□ Restore missing folders □ ☑ Restore SACL □ Restore to a different pa.			4.		
	<				
Help Advanced Refresh				<u>R</u> estore	<u>C</u> ancel



Other New Features

- Additional logging provided to audit who made a security change along with recording the security changes made to the system (combined with the ability to backup permissions before a change is made, this feature can be tied in with a change management system to provide full audit details along with a rollback plan NTFS module only)
- Share application configuration settings between different users (saved searches, scheduled backups, scheduled exports, favorites, enterprise scopes, etc.)
- Option to "Force down tree" for inheritance changes (resets all permissions on an NTFS folder structure to inherit from the parent folder)

For more information, please visit http://www.scriptlogic.com/products/security-explorer/

