



Security Explorer[®]

The Complete Permissions Management Solution

OVERVIEW

THE ACCESS CONTROL CHALLENGE

Organizations keep data in a number of places: SQL Server databases, Exchange mailboxes, SharePoint sites, file servers, and more. Permissions are stored directly on each resource or on parent containers, making it nearly impossible to manually manage permissions consistently and effectively. Security Explorer centralizes this management into a single, unified console. Quickly search for permissions, centrally manage them, and produce reports for management, compliance audits, troubleshooting, and more.

SIMPLIFIED INTERFACE

The Security Explorer Tasks view puts common tasks right at administrators' fingertips, guiding them through complex procedures to reduce error and improve consistency. The Actions pane surfaces key features based on the administrator's current activity, helping them work faster, smarter, and more accurately.

NEW POWERSHELL INTEGRATION

Security Explorer provides 20 Windows PowerShell cmdlets, enabling administrators to automate permissions management on file servers, shares, SharePoint, SQL Server, and Exchange. Grant, revoke, clone, backup, and export permissions quickly and easily, integrating permissions management into other IT business processes and workflows.

NEW CLONING CAPABILITIES

Quickly replicate permissions and group memberships from one account to another, meeting the common demand to "give him the same permissions as this other account." Improve consistency and reduce user downtime by making sure everyone has the permissions they need.

Security Explorer[®] provides IT administrators with a unified solution for complete access control and security management across their entire Windows network. Administrators can back up, recover, manage, search, migrate, and report on permissions for Windows[®] Server, Exchange Server, SharePoint Server, and SQL Server, all from within a common, simplified graphical user interface. Administrators can even automate permissions management using Security Explorer's Windows PowerShell integration. With Security Explorer, IT administrators can bring consistency and efficiency to their organization's access controls, meeting and maintaining regulatory compliance as well as internal security policies. It's all done in a single product, using a single set of techniques and patterns.

KEY BENEFITS



MANY ACCESS CONTROLS – ONE STANDARDIZED SOLUTION

Eliminate the need to learn and rely on the different native tools and command-line utilities required to secure resources. Security Explorer provides a single console for managing access controls on file servers, workstations, SharePoint sites, SQL Server, and Exchange Server. The rich, simplified UI puts common tasks at your fingertips, using wizards to guide you through complex tasks. Security Explorer's multi-threaded architecture and advanced caching means less time waiting for results, getting you through your security management tasks faster.



REPORT, SEARCH, AND MANAGE

Built-in formatted reports and custom search capabilities let you see "who has access to what" across your entire environment, at any time. Report on permissions, user and group membership, and more on your file servers, SharePoint, SQL Server, and Exchange computers. You can even search, report, and manage the access permissions granted to disabled and deleted accounts across the entire network.



ACHIEVE AND MAINTAIN COMPLIANCE

Security Explorer performs targeted searches for all locations that a particular user or group has access to – including permissions granted through deeply-nested group memberships. Results can be exported to create ad-hoc security reports, making Security Explorer a dream come true for administrators and auditors. Quickly identify permissions that differ from their parent folder, and recover from situations where you were out of compliance.

USE CASE SCENARIOS

File Servers

- Replaces Windows Explorer and complex command-line tools such as Icacls, Xcacls, and Subinacl
- Manage permissions on NTFS, shares, registry, printers, services, and tasks

SharePoint

- Remove accounts that have been deleted from Active Directory
- Identify SharePoint sites on the network and manage all security and group membership
- Browse SharePoint permissions more quickly by eliminating the wait for web pages to load

Exchange

- Access all mailbox, mailbox folder, and directory permissions in one console
- Eliminate the need for extra consoles, including Exchange Management Console and Shell, ADUC, Outlook, and Public Folder Management Console

SQL Server

- Create and manage new SQL Server logins, users, schemas, and DB roles in one console
- Highlight and resolve SQL Server user accounts with blank or insecure passwords

Services & Tasks

- Centrally reset service and task passwords
- Manage service properties, including logon account and startup mode

Local Users & Groups

- Easily find users who have local admin rights
- Manage membership of local groups on multiple machines in a single operation

LICENSING

Security Explorer is licensed based on the total number of enabled user accounts in the domain(s) being managed.

KEY FEATURES



SEARCH

Quickly find “who has access to what.” Locate over-privileged users. Find security weaknesses. Identify directly-permissioned resources that aren’t inheriting from their parent container. It’s all possible through the ability to search for specific assignments, including permissions received via group membership.



REPORT

Export search results to a database or spreadsheet, creating ad-hoc security reports for almost any need. Or, use a variety of built-in, formatted reports to review permissions assignments, group memberships, and much more. Target reports to a specific user’s permissions, or show only those permissions that differ from a parent folder.



MANAGE

Quickly and easily make targeted or bulk changes to servers with the ability to grant, revoke, or modify permissions. Clone permissions and group memberships from one account to another. Force permissions onto protected objects and overcome “access denied” errors with the Administrative Override feature. View and manage group membership settings directly from within the access control list for the resource being managed.



RECOVER

Backup and recover permissions without modifying the data in the resources being managed. Create access control baselines and revert to them at any time. Easily roll back accidental or malicious changes, and ensure that you’re compliant at all times.



MIGRATE

Keep security permissions intact after a server migration with the ability to migrate permissions. Compare migrated permissions to a backup baseline to ensure accuracy after a migration. Find all resources to which a user or group has been given permissions, and transfer that access to another user who has the same needs.

Protect Your Windows Network



File/Print



Tasks/Services



SharePoint



Exchange



SQL Server

Manage

Search

Clone/Migrate

Backup & Recover

Report