

Security Explorer®

The complete Windows permissions management solution

Organizations keep data in many places, including Microsoft SQL Server databases, Exchange mailboxes, SharePoint sites and file servers. Managing access to these resources is critical to ensuring their security and complying with internal policies and government regulations. Yet permissions are virtually impossible to manage consistently and effectively when they are stored and managed directly on each resource or in parent containers.

Relying on native management interfaces and complex command-line utilities to manage access across various technologies is time consuming and error prone — and may even be impossible in many environments.

Security Explorer® delivers a unified solution for complete access control and security management across your entire Windows network. You can back up, recover, manage, search, migrate and report on permissions

for Windows Server, Exchange Server, SharePoint Server and SQL Server — all from a common graphical user interface. Moreover, Security Explorer enhances the management of Windows Server 2012 Dynamic Access Control by enabling you to add, remove, modify, back up, restore, copy and paste permissions that include conditional expressions.

FEATURES

Manage — Don't open a dozen Windows Explorer windows to manage permissions. Security Explorer enables you to grant, revoke, modify and clone permissions, including those applied with Dynamic Access Control — all from a single, easy-to-use console. You don't have to worry about changing permissions for individual resources because you can modify permissions at the server level from a single solution. You can also force permissions onto protected objects in order to overcome "access denied" errors.

Protect your Windows network



File/Print



Tasks/Services



SharePoint



Exchange



SQL Server

Manage

Search

Clone/Migrate

Back up and recover

Report

Security Explorer centralizes and simplifies permissions management, eliminating the need to use different native tools and command-line utilities to secure online resources.

"Having Security Explorer in place immediately saved our staff over 40 hours worth of manual digging to find information ... It was a must-have for us!"

Pamela Andringa, service support manager, WCI

BENEFITS:

- Centralizes permissions management to a single console
- Simplifies permissions management by eliminating the need to use multiple tools and utilities
- Improves visibility into users and permissions
- Enables you to achieve and maintain compliance

Search — Quickly find who has access to what. With Security Explorer, you can easily locate overprivileged users and identify users who should have access but don't. You can search for permissions by group membership, resources and claim types. You can even search for permissions that were created with Dynamic Access Control.

Recover — Back up and recover permissions, including those applied with Dynamic Access Control, without affecting the data those permissions apply to. Data remains available, servers remain online and users remain productive. You can create access control baselines and reinvent them at any time, as well as easily roll back accidental or malicious changes to ensure that you remain compliant. You can even restore permissions to the same resources on another server or location.

Report — Create ad hoc security reports to facilitate auditing or troubleshooting. Security Explorer enables you to export search results (such as a list of permissions on items anywhere in the Windows server) to a database or spreadsheet, so you can meet almost any requirement. Security Explorer also includes a variety of built-in reports that enable you to easily review permissions assignments, group memberships, permissions applied with Dynamic Access Control and more. For example, you can produce a complete list of everything a user has permission to — even through group membership — or show only permissions that differ from a parent folder.

Migrate — Keep security permissions intact by migrating permissions whenever you move resources. With Security Explorer, you can compare migrated passwords to a backup baseline to ensure accuracy after a migration. You can find all resources to which a user or group has permissions, and transfer that access to another user with the same needs. And you can update account settings and passwords for services and tasks across the network.

KEY CAPABILITIES

File servers

- Replace 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 memberships.
- Browse SharePoint permissions more quickly.

Exchange

- Access all mailbox, mailbox folder and directory permissions from one console.
- Eliminate the need for extra consoles, including Exchange Management Console and Shell, Active Directory Users and Computers, Outlook and the Public Folder Management Console.

SQL Server

- Manage SQL Server logins, users, schemas and database roles from one console.
- Highlight and resolve SQL Server user accounts with blank or insecure passwords.

Services and tasks

- Centrally reset service and task passwords.
- Manage service properties, including logon account and startup mode.
- Schedule password changes for service logon accounts.

Local users and groups

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

ABOUT QUEST

Quest helps our customers reduce tedious administration tasks so they can focus on the innovation necessary for their businesses to grow. Quest® solutions are scalable, affordable and simple to use, and they deliver unmatched efficiency and productivity. Combined with Quest's invitation to the global community to be a part of its innovation, as well as our firm commitment to ensuring customer satisfaction, Quest will continue to accelerate the delivery of the most comprehensive solutions for Azure cloud management, SaaS, security, workforce mobility and data-driven insight.

SYSTEM REQUIREMENTS

For a complete list of system requirements, visit quest.com/products/security-explorer.