

SE SECURITY EXPLORER®

The Permissions Management Platform.

Security Explorer is a powerful, graphical solution for real-time management of access controls and security on files and folders, SharePoint, SQL Servers, Exchange and workstations across the enterprise. This broad, real-time solution offers administrators the ability to manage, search, clone, backup, and recover permissions across the network.

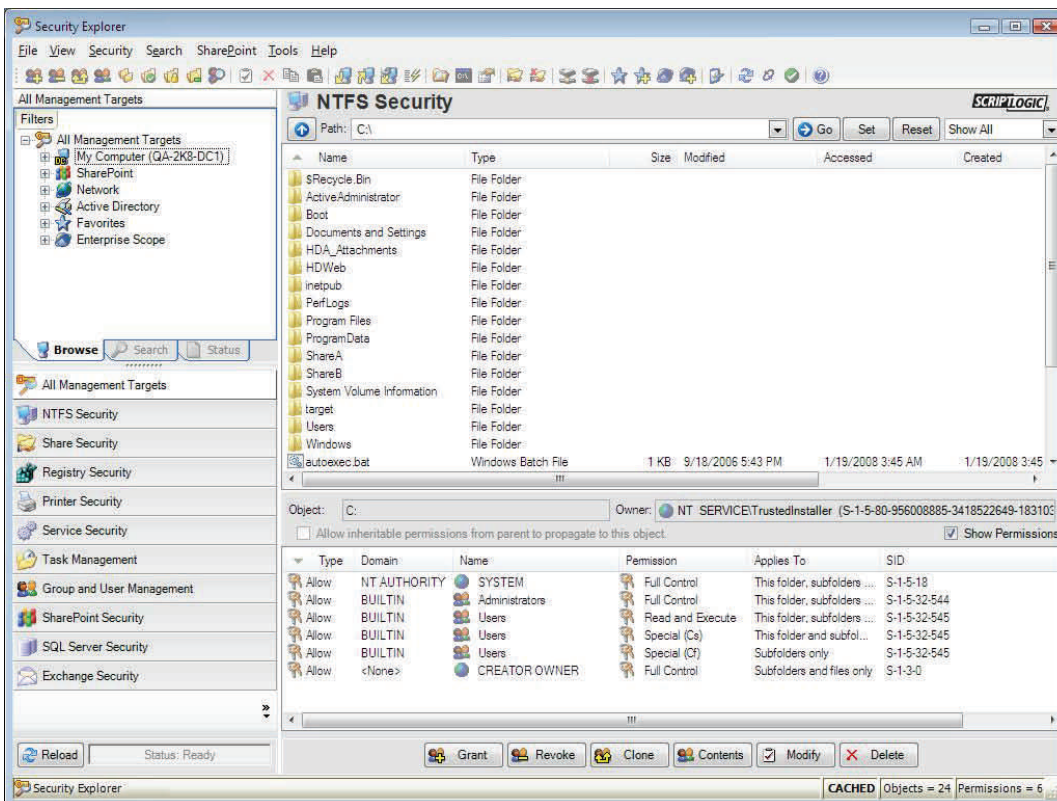
The Access Control Challenge

Organizations need a comprehensive approach to centralize and simplify the management of Windows security to ensure that access to privileged information is restricted.

This information can reside on file servers, SharePoint sites, SQL databases, or in Exchange mailboxes across the organization. Maintaining this access across the network is burdensome due to the different interfaces required to manage each platform and the difficulty involved with command line utilities to perform some of the more complex tasks.

Additionally, meeting compliance requirements to discover, manage, and restore the access to resources by specific users and groups is time consuming and often impossible.

Security Explorer makes the complicated task of security management simple with a single, intuitive and high performance interface for managing security on file servers, SharePoint sites, SQL Servers and Exchange.



KEY FEATURES/BENEFITS

Standardized Platform

Eliminates the need to learn and rely on the various built in tools and command line utilities required to secure resources. Easily find and secure sensitive data wherever it resides on the network.

Instant Access

The rich, interactive UI allows for easy navigation of objects on file servers, SharePoint servers, SQL servers, and Exchange and instantly shows both assigned and inherited permissions.

Performance

Local caching of permissions, combined with a multi-threaded architecture means less time waiting for results, improved browsing performance, and more time to get critical tasks done.

Search

Find security weaknesses and over-privileged users with the ability to search for specific assignments to all types of users and groups, including permissions received via group memberships.

Manage

Easily make targeted or bulk changes to servers with the ability to grant, revoke or modify permissions. Optionally force permissions onto protected objects and overcome access denied errors with Security Explorer's Administrative Override functionality. View and manage group membership settings directly from within the access control list for the resource.

Clone

Find all resources to which a user or group has been granted access on file servers, workstations, SharePoint, SQL, and Exchange and transfer the access to another user with the same needs. Append or replace existing access and optionally replace the ownership settings on the resource.

Recover

The ability to backup & restore permissions, without having to restore data, means you can baseline access controls and revert to that baseline at any time. Easily recover from accidental or malicious changes, and ensure that compliance requirements are enforced.

Report

Export a database or spreadsheet listing the permissions on items anywhere in the directory tree. Filter results to show only permissions that differ from the parent folder when exporting permissions. Perform targeted searches for all locations that a particular group or user has access across the network and export this data to create ad-hoc security reports.

Managed Technologies

The Security Explorer permissions management platform provides a single interface for managing access controls on file servers and workstations, SharePoint sites, SQL Servers, and Exchange.

SE SECURITY EXPLORER®

The Permissions Management Platform.

Effectively Managing permissions can be time consuming and error prone, requiring the use of many different management consoles and command line tools. Security Explorer provides an intuitive, security focused interface that performs all permissions management tasks, improving administrator productivity and reducing the potential for errors that can lead to security leaks or compliance issues.

File Servers

- Replaces the need to use Windows Explorer and complex command line tools like icacls, xcacls, and subinacl
- Manage access on Windows Servers & desktops as well as on NAS/SAN devices
- Manage permissions on NTFS, Shares, Registry, Printers, Services, and Tasks

SharePoint

- Identify SharePoint sites on your network and manage all security & group membership for entire SharePoint environment
- Easily find who has access to SharePoint resources, and how they were granted
- Eliminate need to wait for web pages to load when browsing SharePoint permissions

SQL

- SQL security model is complex with multiple levels of nesting; Security Explorer instantly exposes the permissions of all securable SQL objects
- Create and Manage new SQL logins, users, schemas, and DB roles from one console
- Highlight and address SQL user accounts with blank or insecure passwords

Exchange

- Exchange houses critical corporate data; permissions are stored both in AD and in the mailbox store
- Security Explorer exposes all mailbox and directory permissions from one console
- Eliminates the need to use Exchange Management console, Exchange Management Shell, ADUC, Outlook, and Public Folder Management console

Local Users & Groups

- Easily find users with local admin rights
- Change local account passwords
- Centrally manage local account properties such as changing account name and modifying group membership

Services & Tasks

- Centrally reset service and task passwords
- Search for services and tasks based on numerous criteria
- Manage service properties such as logon account name or startup type

F.A.Q.

How does Security Explorer help with migrations?

Security Explorer provides the ability to migrate access controls, and to clean up access post migration.

Because Security Explorer can back and restore security settings to an alternate location, you can be sure that necessary access is in place on the new server(s) post migration.

Search for, report on, and revoke access assigned to orphaned SIDs from accounts not migrated or no longer in existence.

Update SID history when cloning permissions by finding all permissions assigned to a user's legacy SID and swapping it out with the SID from the new domain.

Pair up accounts from one domain to another when cloning permissions. Match up accounts with the same name between two different domains and clone all permissions on one or more servers after the migration is complete.

Security Explorer saves man-hours on every migration, and helps to ensure a smooth post-migration user experience.

SYSTEM REQUIREMENTS

Management Console

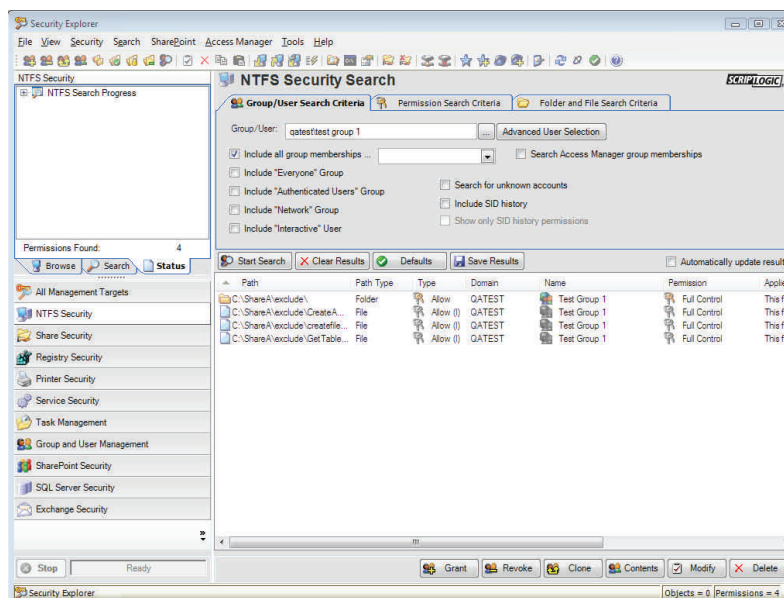
- Windows 7, Vista, XP
- 2008 R2, 2008, 2003
- .Net Framework—3.5 or higher

Managed Targets

- File Servers: 2008 R2, 2008, 2003, 2000
- Workstations: Windows 7, Vista, XP, 2000
- Exchange: 2007, 2003, 2000
- SQL: 2008, 2005, 2000—Server and Express editions
- SharePoint: 2007 and Windows SharePoint Services 3.0

LICENSING

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



Easily search to find all resources to which a particular account has access, both directly assigned and/or access granted via group membership.