Quest® Security Explorer® 9.8

What's New

July 2018

Quest® Security Explorer® provides a single console for managing access controls, permissions and security across Microsoft® platforms that span multiple servers. The product provides a broad array of security enhancements including the ability to identify who has rights to resources across the entire organization. It also provides the ability to grant, revoke, clone, modify and overwrite permissions quickly and from a central location.

Unlike native tools, Security Explorer provides the ability to back up and restore permissions only, ensuring the integrity of data. To help meet auditing requirements, Security Explorer provides convenient reports that can be pulled on the fly. Lastly, the product's cleanup capabilities address common post-migration security issues.

This document highlights key features new in this release. For more information about these or any features, see the Security Explorer 9.8 Installation and User Guides.

Active Directory Security

The new Active Directory Security module gives you the ability to manage Active Directory® permissions. You can grant, revoke, clone, modify, delete, export, backup and restore permissions on Active Directory objects. You also can search for permissions, back up and restore permissions, and generate reports. If you are also using Quest® Enterprise Reporter®, you can launch Security Explorer® from within Enterprise Reporter and use the new Active Directory Security module.

View Active Directory permissions

When you open the Active Directory Security module, Active Directory loads the Active Directory objects for the specified domain. You can easily drill-down to view permissions on a specific object.

- In the Navigation pane, expand the Active Directory node to browse all Active Directory objects in the default naming contexts of the specified domains.
- In the Navigation pane, select an object. The Objects pane displays the LDAP path, the children of the selected object, the object name, and class.

- In the Objects pane, select a child object. The Permissions pane displays permissions for the selected object. The **Owner** box displays the user or group that owns the selected object.

Search Active Directory

Search Active Directory for the name of a principal, and choose from the following options to include in the results:

- all group memberships
- permission name
- allow permissions
- inherited permissions
- deny permissions
- explicit permissions
- deleted accounts
- disabled accounts

Once you finish the search, you can right-click and choose to manage the permissions. You can save the search scope, save the search results, or generate a report.

Manage permissions on Active Directory objects

You can grant, revoke, clone, modify, and delete permissions on Active Directory objects.

- You can grant permissions to domain users and groups without affecting the permissions of any other user. First, choose the permissions to grant, and select a domain user or group. You can grant different permissions for several domain users and groups with one operation.
- You can revoke access for domain users and groups.
- Use the Clone feature to copy one user/group's permissions to another user/group.
- Modify the permissions of groups or users on the selected Active Directory object. Use this feature for quick changes to accounts displayed in the permissions list. Use the Grant feature to give permissions to accounts that are not displayed in the permissions list.
- Easily delete permissions from selected objects.

Back up and restore permissions on Active Directory objects

As with all other Security Explorer modules, you can back up and restore permissions on Active Directory objects. The Security Explorer Active Directory Backup File has the .adb extension. You also can use the back up scheduler to schedule the backup.

Export permissions on Active Directory objects

By default, permissions are exported to a report, which you can save, print, or export. You can generate a report or export permissions to a delimited file for use with Microsoft® Excel®. This report is useful when you are asked to see which users have access to a specific Active Directory path.

NTFS Security module enhancements

- Added the ability to modify selected multiple permissions. Selected multiple permissions must be under the same path or object.
- Added the ability to purge backup files (**Security | Purge Backup Files**) and a Purge Backup Scheduler to manage scheduled purges of backup files (**Security | Purge Backup Scheduler**).
- Added the ability to exclude selected files and folders from an export.

- Added the ability to restore security to multiple paths that have identical file structures.
- Added the ability to use wild cards when restoring security to a different path.
- Added the ability to back up a root folder (01) and its subfolders, and restore it to all other root folders (02, 03, 04, and so on).
- Added the ability to back up permissions on one folder, and then import a list of up to 1000 or more target folders to which the permissions may be restored.
- Added the ability to manage permissions at the drive root level.

User and Groups module enhancements

- Added the ability to set alternate credentials for workgroup computers. Select to show workgroups in the navigation pane in **Tools | Options | View**, and then use the **Workgroup** tab to set alternate credentials (**Tools | Options | Workgroup**).
- Added the ability to select multiple accounts from the list in the **Select Accounts** dialog.
- Added the ability to select multiple accounts from the list in the **Group Contents** dialog.
- Added the ability to edit the Managed By attribute for a domain group.

Bulk removal of permissions

NTFS Security module only. You can now use the Search module to easily delete both explicit and inherited permissions on a specific user on specified folders.

For example, Peter has explicit access permission on the Customer folder, and all subfolders have inherited permissions. You want to remove Peter's permission on all folders with Internal in the folder name.

- C:\Customer\ Internal1\
- C:\Customer\ Internal1\Internal2
- C:\Customer\ Mixed\Internal3
- C:\Customer\ External1\

Using the **Search** tab, set the search scope to **C:\Customer**, browse to find Peter's account, select to search for both **Inherited Permissions** and **Explicit Permissions**, add ***Internal*** as a folder search criteria, and click **Search.** All permissions that belong to Peter on all folders with Internal in the name display. From the search results, delete selected permissions.

Additional supported platforms

- SQL Server® 2017
- SQL Server 2017 Reporting Services

Retry options for resetting password

To help you manage password resets, several features were added to the Group and User Management module.

- To help you quickly change the passwords on local administrator accounts, a new check box was added to the **Group/User Search Criteria** tab. Select **Search for local administrator accounts**, and run the search. From the search results, right-click the results, and choose **Change Password**.

- If any password resets failed, you can select to save failed computers to a search scope to repeat the search with only the failed computers. Select **Save Failed Computers to Scope**, and repeat the search. Right-click the results, and choose **Change Password**.
- A new column was added to the **Object** and **Search Result** panes that shows the date the password was last set so you can easily see which passwords were reset versus those that may have failed.
- When changing passwords, you can select to create a new log file (ChangedPasswordResult.log) that lists the accounts with their changed passwords.

Modify registry values

In the Registry Security module, you can now add, modify, and delete values in a selected registry key. You also can save the list of values to a .TXT file. Open the **Registry Security** module, open the **Browse** tab, select a registry key, and select **Tools | Display Registry Values.** Use the buttons to modify the values in the registry key.

To quickly find a registry key, use the new **Registry Key Search Criteria** tab in the Search module. Just type in a string using the * or ? wildcards to locate a registry key. From the results list, right-click a registry key, and choose **Display Registry Values** to modify values or **Delete Registry Key** to delete the key.

Enhancements to SXPExport.exe

Several options were added to the command line program.

- `/columns` allows you to indicate which columns to include in the exported spreadsheet or report.
- `/exclusion` allows you to indicate paths to folders and files to exclude from the export.
- `/showgroupmembers` allows you to exclude or include nested groups and Domain Users group members from the exported spreadsheet or report.

General product enhancements

- Added a license dashboard to show licensed users, enabled users, and license information.
- Added the ability to log exceptions when running scheduled tasks. If a task runs normally. it is not logged. The log file name format is **{*call_exe_name*}_{*datetime*}.log**. Logs are located at **C:\Program Files\Quest\Security Explorer\v9\Logs**.
- Added the ability to use alternate credentials for shares.
- Added support for the Access Explorer PowerShell® snap-in.
- Added the ability to use an OU in the search scope.
- Allowed SXPGrant.exe to incorporate variables such as %USERNAME% to allow multiple folders to be sequenced for use in assigning permissions and ownership.
- Added recursion depth to SXPBackup.exe.
- Sped up the process when browsing NetApp® 7-mode shares.
- Added the ability to export the search scope and settings to an XML file for later import into another module. Saved searches appear under **Saved Searched | User Searches**.

  You can only import an XML file that was exported from the same module with the exception of the NTFS Security and Share security modules. In these modules, you can import an XML file that was exported by the other module.
- Added a setting that allows each user to change where their settings are stored, such as a home folder or drive.

About us

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece—you—to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit www.quest.com/contact.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request.
- View Knowledge Base articles.
- Sign up for product notifications.
- Download software and technical documentation.
- View how-to-videos.
- Engage in community discussions.
- Chat with support engineers online.
- View services to assist you with your product.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept.
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our website (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

Quest, the Quest logo, Security Explorer, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are property of their respective owners.

Legend

! | **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

i | **IMPORTANT NOTE**, **NOTE**, **TIP**, **MOBILE**, or **VIDEO:** An information icon indicates supporting information.