Quest® Security Explorer® 9.8

Release Notes

July 2018

These release notes provide information about the Quest® Security Explorer® release.

Topics:

About this release

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 generated at your convenience. Lastly, the product's cleanup capabilities address common post-migration security issues.

Security Explorer 9.8 is a minor release, with enhanced features and functionality. See New features and Enhancements.

Supported platforms

Table 1. Supported platforms for Security Explorer®

Security Explorer Module	Supported Platform
NTFS Security Share Security Registry Security Printer Security Service Security Task Management Group & User Management	Windows XP Windows Vista® Windows 7 Windows 8 Windows 8.1 Windows 10 Windows Server® 2003 Windows Server 2008 Windows Server 2008 R2 Windows Server 2012 Windows Server 2012 R2 Windows Server 2016

NTFS Security
Share Security
Group & User Management
	Dell™ Fluid File System (FluidFS)
	EMC® Isilon®
	EMC Celerra®
	EMC VNX®
	NetApp® 8.2 (7-Mode and Clustered Mode)
	NetApp 8.3, 9.0, 9.1 Clusters
	NOTE: If Security Explorer is installed on a device with Windows 8 or Windows Server 2012 or higher, EMC Celerra is not supported. The workaround is to disable Server Message Block version 2 (SMBv2) and enable Server Message Block version 1 (SMBv1).
	To disable SMBv2 and enable SMBv1
	1 Use the following commands:
	`sc config lanmanworkstation depend= bowser/mrxsmb10/nsi`
	`sc config mrxsmb20 start= disabled`
	2 Restart the computer.
	For more information, see https://support.microsoft.com/kb/2696547?wa=wsignin1.0
	NOTE: **vsadmin** must be entered in NAS credentials dlg for full management of NetApp Clusters 8.2, 8.3, 9.0, 9.1.
	NOTE: NetApp 8.2.7-Mode is not supported on Windows 10.
	NOTE: For NetApp Clustered Mode, to see changes after a permission action, such as Grant, Revoke, or Modify, on folders and shares, you must refresh the tree in the Navigation pane.
	NOTE: Security Explorer supports only default NetApp vFiler units. Additional vFiler units are not supported.
	NOTE: Security Explorer supports CIFS volumes. Mixed CIFS/UNIX volumes are supported if the volume root owner is a Windows account.
	NOTE: If Security Explorer is running as a user who is not Domain Administrator, that user must be added to local Administrators group on NAS devices.

Table 1. Supported platforms for Security Explorer®

Security Explorer Module	Supported Platform
SQL Security	SQL Server® 2017
	SQL Server 2017 Reporting Services
	SQL Server 2016
	SQL Server 2014
	SQL Server 2012
	SQL Server 2008 R2
	SQL Server 2008
	SQL Server 2005
SharePoint Security	SharePoint® 2016
	SharePoint 2013
	SharePoint 2010
	SharePoint Foundation
	SharePoint 2007
	SharePoint Services 3.0
Exchange Security	Exchange 2016
	Exchange 2013
	Exchange 2010
	Exchange 2007
Active Directory Security	Windows Server® 2016 Functional Level
	Windows Server 2012 R2 Functional Level
	Windows Server 2012 Functional Level
	Windows Server 2008 R2 Functional Level
	Windows Server 2008 Functional Level
	Windows Server 2003 Functional Level

New features

New features in Security Explorer 9.8:

- ***New* Active Directory Security module**: 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.

See also:

- Enhancements
- Resolved issues

Enhancements

The following is a list of enhancements implemented in Security Explorer® 9.8.

Table 2. General enhancements

Enhancement	Issue ID
Added the ability to view EMC Isilon devices through a load balancer.	12233
Added the ability to run multiple instances of Security Explorer on the same system with the same user.	12244
Added the ability to search all computers for a certain registry key and to view the value.	12264
Added a license dashboard to show licensed users, enabled users, and license information.	12266
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**.	12268
Added the ability to use alternate credentials for shares.	12493
Added the ability to use an OU in the search scope.	12502
Added an exclusion option for SXPExport.exe.	12503
Allowed SXPGrant.exe to incorporate variables such as %USERNAME% to allow multiple folders to be sequenced for use in assigning permissions and ownership.	12505
Added recursion depth to SXPBackup.exe.	12507
Added a retry option for resetting passwords	12511

Table 2. General enhancements

Enhancement	Issue ID
Sped up the process when browsing NetApp® 7-mode shares.	12512
When using SXPExport.exe, added the ability to select summary mode and to specify that specific columns be exported.	12513
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**. **NOTE:** 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.	12514
Added a setting that allows each user to change where their settings are stored, such as a home folder or drive.	12519
Added the ability to change bulk permissions based on criteria, such as the folder name.	14512
Added the **Select all children for current item** and **De-select all children for current item** to the **Add Search Scope** dialog box for all modules.	14533
Added the Favorites node to the **Add Search Scope** dialog box for the NTFS, Share, Printer, Service, Task, and Exchange modules. Added the Active Directory node to the **Add Search Scope** dialog box to the Share, Registry, Printer, Group and User Management, SharePoint, and SQL Server modules.	14533
Allowed SXPExport.exe to export security group information for directories to Microsoft® Excel®.	14892
Improved query account performance.	17108
Allowed more than a 260 character file path length.	21255
Added support for the Access Explorer PowerShell® snap-in in Security Explorer.	21342
Added the ability to add Active Directory alternate credentials for multiple domains to Security Explorer Favorites.	24206

Table 3. NTFS Security module enhancements

Enhancement	Issue ID
Added the ability to schedule exports with options.	12491
Added the ability to use wild cards when restoring security to a different path.	12492
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).	12494
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.	12495
Added the ability to manage permissions at the drive root level.	12497
Added the ability to modify selected multiple permissions. Selected multiple permissions must be under the same path or object.	12498
Added the ability to restore security to multiple paths that have identical file structures.	12500
Added the ability to create a schedule to temporarily grant or revoke a permission.	12508
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**).	12575
Added the ability to exclude selected files and folders from an export.	14532

Table 4. Group and User Management module enhancements

Enhancement	Issue ID
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**).	12517

Table 5. Exchange Security module enhancements

Enhancement	Issue ID
Inactive Room mailbox in exchange does not display folders.	12230

Resolved issues

The following is a list of issues addressed in this release.

Table 6. General resolved issues

Resolved issue	Issue ID
In some cases, there is no reaction after clicking **OK** in the License dialog.	12937 14138
Cannot remove a disabled account from Active Directory® groups.	13316
Added the domain name to account names in the Revoke Disabled Accounts log file.	13458 14092
The **Not a valid Win32 FileTime** error occurs when performing an NTFS search on an EMC® Isilon® NAS device.	14096 14097
When modifying security for a user with two ACEs on an object editing on ACE will remove the other if they overlap.	14098 14099
An error occurs when creating a user account that spans multiple computers and the cache is on.	14810
SXPExport.exe is not working as expected and produces the error **Object reference not set to an instance**.	15244
Issue in permission comparison with backup.	15632 16252 16253
The Enterprise Reporter Suite license is not valid in Security Explorer® 9.7.	15947 15948
When recovering security from a backup, existing security setting are overwritten when **Append security** is selected.	17943
When adding or modifying permissions, Security Explorer removes some permissions.	18820
Navigation menu in Security Explorer is not being populated.	19591
Receive an error when attempting to manage root drive permissions from Windows Explorer.	20458
When removing deleted accounts from a site, the scope is enlarges to the site collection.	21198
Closing the main Security Explorer window when modifying permissions causes Security Explorer to lock up.	21201
Memory leak issues and all memory used on a file server after four days.	24362

Table 7. SharePoint Security module resolved issues

Resolved issue	Issue ID
It is impossible to add two different domain accounts to a SharePoint® group.	13320 14093
Updated an error message that occurs when restoring a backup of SharePoint 2013 if the user does not provide credentials.	14531

Table 7. SharePoint Security module resolved issues

Resolved issue	Issue ID
Issue getting orphaned user accounts out of SharePoint.	16250 16251
Unable to find a user in SharePoint and the sites to which they have access from another domain.	18226

Table 8. Access Explorer module resolved issues

Resolved issue	Issue ID
Access Explorer agents always show Update Available.	14072
On the **Managed Computers** tab in the Access Explorer module, **Upgrade Available** displays for agents after an Upgrade is performed.	14270 14286
Access Explorer agents unregister when a new agent is installed on the same agent host.	14287
Unavailable to see user's shares.	16404

Known issues

The following is a list of issues, including those issues attributed to third-party products, known to exist at the time of release.

Table 9. General known issues

Known issue	Issue ID
PowerShell CmdLets & CmdUtils: impossible to Grant/Revoke/Clone for short names of accounts in another domain.	12162
Cannot grant/modify deny permissions when the user has no permissions and is not an owner.	12171
The Security Explorer context menu does not allow managing multiple folders and files.	12180
Modifying one permission for a user with two ACEs sometimes incorrectly removes the other.	12183

Table 10. Exchange Security module known issues

Known issue	Issue ID
It is impossible to create a mailbox as a new user if Exchange 2013 in mode: Active Directory split permission security model to the Exchange organization.	12141
It is impossible to restore Exchange permissions if they were backed up in previous versions of Security Explorer.	13550

Table 11. Access Explorer known issues

Known issue	Issue ID
Impossible to use SQL credentials when setting up the database.	12122

System requirements

Before installing or upgrading Security Explorer 9.8, ensure that your system meets the following minimum hardware and software requirements.

IMPORTANT: The minimum system requirements listed are for the computer on which Security Explorer® is installed.

- Hardware requirements
- Software requirements
- User privilege requirements
- Minimum permissions for Access Explorer
- Minimum requirements for Microsoft Exchange for Security Explorer
- Permission requirements to manage Microsoft Exchange in Security Explorer
- Upgrade and compatibility

Hardware requirements

Table 12. Hardware requirements

Requirement	Details
Processor	Pentium® 600MHz or faster
Memory	1 GB
Hard disk space	550 MB
Operating system	• Windows® 7 • Windows 8 • Windows 8.1 • Windows 10 • Windows Server® 2003 • Windows Server 2008 • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016

Software requirements

- .Net Framework v.4.0 or later

  NOTE: Install either the Full or Standalone version. Do not install just the Client Profile.

User privilege requirements

It is recommended to be a member of the local Administrators group to use all the features in Security Explorer®. However, it is possible to run Security Explorer without being a member of the local Administrators group.

Table 13. Requirements to enable permission management

Module	Requirement
NTFS Security	To manage permissions on folders and files on remote computers, the file and printer sharing option must be enabled on the firewall on the computer with Security Explorer installed and on the remote computer.
Share Security	To manage permissions on shares on remote computers, the file and printer sharing option must be enabled on the firewall on the computer with Security Explorer installed and on the remote computer.
Registry Security	To manage permissions on registry keys on remote computers, the file and print sharing option must be enabled on the firewall on the computer with Security Explorer installed and on the remote computer.
Printer Security	To manage permissions on printers on remote computers: • The Printer Spooler service must be running on the target computer. • The file and printer sharing option must be enabled on the firewall on the computer with Security Explorer installed.
Service Security	To manage permissions on services on remote computers, the file and printer sharing option must be enabled on the firewall on the computer with Security Explorer installed and on the remote computer.
Task Management	To manage tasks on remote computers, the file and printer sharing option must be enabled on the firewall on the computer with Security Explorer installed and on the remote computer.
Group and User Management	To manage groups and users on remote computers, the file and printer sharing option must be enabled on the firewall on the computer with Security Explorer installed and on the remote computer.
SharePoint® Security	To manage permissions on servers running SharePoint, the SharePoint site must be on the same network as the computer on which Security Explorer is installed. To manage SharePoint sites exposed over SSL (https://), add the certificate of the server running SharePoint to the Trusted Root Certification Authorities store on the computer with Security Explorer installed. To deploy and remove Security Explorer Web Services, and to search for SharePoint sites automatically, the current user must be a member of the Administrators local group on the servers.
SQL Server® Security	To manage permissions on servers running SQL Server: • Current user must be a member of the Administrators local group on the server. • Windows® Firewall on the server must be configured to allow SQL and WMI. For more information please refer to: *Configure the Windows Firewall to Allow SQL Server Access* at http://msdn.microsoft.com/en-us/library/cc646023.aspx.

Table 13. Requirements to enable permission management

Module	Requirement
Exchange Security	To manage permissions on the Exchange organization, the Exchange organization must be on the same Active Directory® forest as the computer on which Security Explorer is installed.
Active Directory Security	To manage permissions on the domain, the domain must have a trusted relationship with the current domain on which the user is logged on. See *Setting Options for Active Directory Security* In the *Security Explorer 9.8 User Guide*.

Minimum permissions for Access Explorer

Table 14. Minimum permissions for Access Explorer

Account	Requirement
Logged in user	• To install the Access Explorer agent, the user must have administrator access on the local computer. • To create the Access Explorer database, the logged in user (Windows® Authentication) or SQL account must have rights to create databases, logins, and groups on the computer running SQL Server®. • Must have rights to create groups in Active Directory®. • Must be able to enumerate the targets during scope selection.
Security Explorer service account	• Must have Login as service right on the computer on which it is being installed. • Will be automatically granted Read and Write permissions on the Security Explorer database (Windows Auth.) • If the server is configured to use SQL authentication, the SQL credentials will be used to access the database instead of the service account. • Must be able to write to the Admin$ share to deploy the node (local admin rights)
Service accounts for managed computers	• Local Administrator rights for managed computers is recommended. • To create the database, Sysadmin rights on the computer running SQL Server are required. Once the database is created, the service account can be granted dbowner rights on the database alone. • The database has to be created using the wizard in Security Explorer. • Full Administrator rights are required on the Netapp filer / EMC • Must be able to do group expansion and SID resolution for managed accounts and their membership (Domain Admin recommended).

Minimum requirements for Microsoft Exchange for Security Explorer

Topics:

Client access server configuration

1. Check that all Exchange Windows services that have Automatic startup type are started.
2. Check that IIS Admin Service and World Wide Web Publishing Service IIS Services are started.
3. Check that the Exchange Web Application is configured correctly in IIS:
   - Authentication: Windows Authentication is Enabled
   - SSL Settings: Require SSL is switched on
4. Exchange Server 2010 and 2013 only: Enable Windows PowerShell® Remoting on the Exchange Server by running the Windows PowerShell command: **Enable-PSRemoting –force**.

Client Configuration

1. Open port 443 on the firewall.
2. Install an Exchange Server SSL certificate.

Required software for Microsoft Exchange for Security Explorer

The following versions of Microsoft® Exchange are supported for Security Explorer®. This section contains the required software for each version.

Exchange 2007

Table 15. Required software for Microsoft® Exchange 2007

Client type	Required software
Windows Vista® Windows Server® 2008	• IIS 6.0 Management Compatibility from Windows Features • Windows PowerShell 1.0 or 2.0 from Windows Features
Windows® 7 Windows Server 2008 R2	• IIS 6.0 Management Compatibility from Windows Features • Windows PowerShell 2.0 or later from Windows Features
Windows 8 Windows 8.1 Windows 10 Windows Server 2012 Windows Server 2012 R2 Windows Server 2016	• IIS 6.0 Management Compatibility from Windows Features • NET Framework 3.5 from Windows Features
All Operating Systems	• Management Tools from Exchange Server 2007 Installation Package

Exchange mixed modes: 2007–2010 and 2007–2013

Table 16. Required software for Microsoft® Exchange mixed modes: 2007-2010 and 2007-2013

Client type	Required software
Windows Vista® Windows Server® 2008	• IIS 6.0 Management Compatibility from Windows Features • Windows PowerShell 2.0
Windows® 7 Windows Server 2008 R2	• IIS 6.0 Management Compatibility from Windows Features • Windows PowerShell 2.0 or later from Windows Features
Windows 8 Windows 8.1 Windows 10 Windows 2012 Windows 2012 R2 Windows Server 2016	• IIS 6.0 Management Compatibility from Windows Features • NET Framework 3.5 from Windows Features
For all operating systems	• Management Tools from Exchange Server 2007 Installation Package

Exchange 2010, 2013, 2016

Table 17. Supported versions of Microsoft® Exchange 2010, 2013, 2016

Client type	Required software
Windows Vista® Windows Server® 2008	• Windows PowerShell® 2.0

Table 17. Supported versions of Microsoft® Exchange 2010, 2013, 2016

Client type	Required software
Windows 7 Windows Server 2008 R2	• Windows PowerShell 2.0 or later from Windows Features
Windows 8 Windows 8.1 Windows 10 Windows Server 2012 Windows Server 2012 R2 Windows Server 2016	• Windows PowerShell from Windows Features

Exchange mixed modes: 2010–2013, 2010–2016, 2013–2016

Table 18. Supported versions of Microsoft® Exchange mixed modes: 2010–2013, 2010–2016, 2013–2016

Client type	Required software
Windows Vista® Windows Server® 2008	• Windows PowerShell® 2.0
Windows 7 Windows Server 2008 R2	• Windows PowerShell 2.0 or later from Windows Features
Windows 8 Windows 8.1 Windows 10 Windows Server 2012 Windows Server 2012 R2 Windows Server 2016	• Windows PowerShell from Windows Features

Permission requirements to manage Microsoft Exchange in Security Explorer

- To connect to an Exchange 2007 Organization, a user must be a domain user, have a mailbox on one of the Exchange Servers, be a member of the Exchange Organization Management group, and have impersonation rights on the Exchange 2007 client access server(s) and mailbox database(s).

  For more details on configuring user impersonation, see Configuring Exchange Impersonation (Exchange Web Services).

- To connect to an Exchange 2010 Organization, a user must be a domain user, have a mailbox on one of the Exchange Servers, be a member of the Organization Management group, and have impersonation rights.

  For more details on configuring user impersonation, see Configuring Exchange Impersonation in Exchange 2010.

- To connect to an Exchange 2007–2010 Organization (Mixed Mode), a user must be a domain user, have a mailbox on the Exchange 2010 Server, be a member of the Exchange Organization Administrators group, and have impersonation rights on all versions of Exchange servers.

For more details on configuring user impersonation, see Configuring Exchange Impersonation (Exchange Web Services) and Configuring Exchange Impersonation in Exchange 2010.

- To connect to an Exchange 2013 or 2016 Organization, a user must be a domain user, have a mailbox on one of the Exchange Servers, be a member of the Organization Management domain group, and have impersonation rights.

To configure impersonation in Security Explorer

1. In the Navigation pane, expand **Role Based Access Control | Roles | ApplicationImpersonation | Assignments**.
2. Select **Assignments**, and select **File | New**.
3. Enter the name and user.
4. Select **RecipientRelativeWriteScope** and choose **Organization** from the list.
5. Click **OK** and restart Security Explorer.
    - To connect to an Exchange 2007–2013 Organization (Mixed Mode), a user must be a domain user, have a mailbox on one of the 2013 Exchange Servers, be a member of the Organization Management domain group, and have impersonation rights on the Exchange 2007 and 2013 client access servers.
    - To connect to an Exchange 2010–2013 Organization (Mixed Mode), a user must be a domain user, have a mailbox on one of the 2013 Exchange Servers, be a member of the Organization Management domain group, and have impersonation rights on the Exchange 2010 and 2013 client access servers.

        IMPORTANT: Only a user who is a Domain Administrator and Exchange Administrator has no restrictions for mailbox management in Security Explorer. There are possible restrictions in Security Explorer for mailbox management. See Restrictions with mailbox management.

Restrictions with mailbox management

Only a user who is a Domain Administrator and Exchange Administrator has no restrictions for mailbox management in Security Explorer. If a user uses **Run As** to start Security Explorer and that user does not have enough privileges and enters valid Alternative Credentials (Domain User, Exchange Administrator, Local Administrator, Has Mailbox, Has Impersonation), there are some restrictions with mailbox management in Security Explorer.

- Exchange 2007
- Exchange 2010
- Exchange 2013 and 2016
- Mixed Mode (Exchange 2007–2010)
- Mixed Mode (Exchange 2007–2013)
- Mixed Mode (Exchange 2010–2013, 2010–2016, 2013–2016)

Exchange 2007

Table 19. Restrictions with mailbox management in Security Explorer with Microsoft® Exchange 2007

If the user entered in the Run as window has these privileges:	And these privileges are used to connect to Exchange Server:	Then these restrictions are possible in Security Explorer:
Domain Administrator Exchange Organization Administrator	Windows® Authentication Valid Alternative Credential	No restrictions
Domain User Exchange Organization Administrator	Windows Authentication Valid Alternative Credential	Cannot create, delete, and manage distribution groups. Cannot manage Active Directory® permissions for mailboxes and public folders (View-only mode).
Domain User	Windows Authentication	Cannot connect to Exchange.
Domain User	Valid Alternative Credential	Cannot create, delete, and manage security and distribution groups (except dynamic distribution groups). Cannot manage Active Directory permissions for mailboxes and public folders (View-only mode).

NOTE: Valid Alternative Credential: Domain User, Exchange Admin, Local Admin, Has Mailbox

Exchange 2010

Table 20. Restrictions with mailbox management in Security Explorer with Microsoft® Exchange 2010

If the user entered in the Run as window has these privileges:	And these privileges are used to connect to Exchange Server:	Then these restrictions are possible in Security Explorer:
Domain Administrator Member of Organization Management	Windows® Authentication Valid Alternative Credential	No restrictions
Domain User Member of Organization Management	Windows Authentication Valid Alternative Credential	Cannot create, delete and manage distribution groups. Cannot manage Active Directory® permissions for mailboxes and public folders (View-only mode).
Domain User	Windows Authentication	Cannot connect to Exchange.
Domain User	Valid Alternative Credential	Cannot create, delete, and manage security and distribution groups (except dynamic distribution groups). Cannot create mail-enabled public folders. Cannot manage Active Directory permissions for mailboxes and public folders (View-only mode).

NOTE: Valid Alternative Credential: Domain User, Exchange Admin, Local Admin, Has Mailbox

Exchange 2013 and 2016

Table 21. Restrictions with mailbox management in Security Explorer with Microsoft® Exchange 2013 and 2016

If the user entered in the Run as window has these privileges:	And these privileges are used to connect to Exchange Server:	Then these restrictions are possible in Security Explorer:
Domain Administrator	Windows® Authentication	No restrictions
Domain Administrator	Valid Alternative Credential	Cannot manage Active Directory® permissions for all objects. Cannot delete mail contacts.
Domain User is member of Organization Management domain group	Windows Authentication Valid Alternative Credential	Cannot manage Active Directory permissions for all objects. Cannot delete mail contacts.
Domain User	Windows Authentication	Cannot connect to Exchange.
Domain User	Valid Alternative Credential	Cannot manage Active Directory permissions for all objects. Cannot delete mail contacts.

NOTE: Valid Alternative Credential: Domain User, Exchange Admin, Local Admin, Has Mailbox

Mixed Mode (Exchange 2007–2010)

Table 22. Restrictions with mailbox management in Security Explorer with Microsoft® Exchange 2007–2010 mixed mode

If the user entered in the Run as window has these privileges:	And these privileges are used to connect to Exchange Server:	Then these restrictions are possible in Security Explorer:
Domain Administrator Exchange Organization Administrator (2007) Member of Organization Management	Windows® Authentication Valid Alternative Credential	No restrictions
Domain User Exchange Organization Administrator (2007) Member of Organization Management	Windows Authentication Valid Alternative Credential	Cannot create, delete, and manage distribution groups. Cannot manage Active Directory® permissions for mailboxes and public folders (View-only mode).
Domain User	Windows Authentication	Cannot connect to Exchange.
Domain User	Valid Alternative Credential	Cannot create, delete, and manage security and distribution groups (except dynamic distribution groups). Cannot manage Active Directory permissions for mailboxes and public folders (View-only mode).

NOTE: Valid Alternative Credential: Domain User, Exchange Admin, Local Admin, Has Mailbox

Mixed Mode (Exchange 2007–2013)

Table 23. Restrictions with mailbox management in Security Explorer with Microsoft® Exchange 2007–2013 mixed mode

If the user entered in the Run as window has these privileges:	And these privileges are used to connect to Exchange Server:	Then these restrictions are possible in Security Explorer:
Domain Administrator	Windows® Authentication	No restrictions
Domain Administrator	Valid Alternative Credential	Cannot manage Directory permissions for all objects. Cannot delete mail contacts. Cannot create mailboxes on Exchange 2007.
Domain User is member of Organization Management and Exchange Organization Administrators domain groups	Windows Authentication Valid Alternative Credential	Cannot manage Directory permissions for all objects. Cannot delete mail contacts. Cannot create mailboxes on Exchange 2007.
Domain User	Windows Authentication	Cannot connect to Exchange
Domain User	Valid Alternative Credential	Cannot manage Directory permissions for all objects. Cannot delete mail contacts. Cannot create mailboxes on Exchange 2007.

NOTE: Valid Alternative Credential: Domain User, Exchange Admin, Local Admin, Has Mailbox

Mixed Mode (Exchange 2010–2013, 2010–2016, 2013–2016)

Table 24. Restrictions with mailbox management in Security Explorer with Microsoft® Exchange 2010–2013, 2010–2016, and 2013–2016 mixed mode

If the user entered in the Run as window has these privileges:	And these privileges are used to connect to Exchange Server:	Then these restrictions are possible in Security Explorer:
Domain Administrator	Windows® Authentication	No restrictions
Domain Administrator	Valid Alternative Credential	Cannot manage Directory permissions for all objects. Cannot delete mail contacts.
Domain User is member of Organization Management domain group	Windows Authentication Valid Alternative Credential	Cannot manage Directory permissions for all objects. Cannot delete mail contacts.
Domain User	Windows Authentication	Cannot connect to Exchange
Domain User	Valid Alternative Credential	Cannot manage Directory permissions for all objects. Cannot delete mail contacts.

NOTE: Valid Alternative Credential: Domain User, Exchange Admin, Local Admin, Has Mailbox

Upgrade and compatibility

Security Explorer 9 does not require that you uninstall version 5, version 6, version 7, or version 8. You can install Security Explorer 9.8 side-by-side with all of these previous versions.

Product licensing

You must have a Quest® license file (.dlv) to use version 9.8.

To activate a trial or purchased commercial license

1. Start Security Explorer.

   When you start Security Explorer, a license check is performed. If you are installing Security Explorer for the first time, you are asked to update the license.

2. Click **Update License,** and locate the license file. The license file is approximately 1 KB in size and has a .dlv file extension.

To update a license

1. Start Security Explorer.
2. Select **Help | About Security Explorer**.
   - To view the applied licenses, click **Licenses**.
   - To update a selected license, click **Update License**.

Upgrade and installation instructions

During the install process, you can choose to install Access Explorer and the Security Explorer cmdlets for use with Windows PowerShell®.

The Access Explorer service scans and indexes security access information on files, folders, and shares on managed computers in managed domains. The Access Explorer Permission Wizard helps you manipulate explicit permissions and/or group memberships for Access Explorer accounts, computers, and/or resource groups. For more information, see chapter 9, Working with Access Explorer, in the Security Explorer User Guide.

The Security Explorer cmdlets perform common functions, such as Backup, Clone, Export, Grant, Restore, and Revoke, from the command line. For more information, see chapter 11, Using the command line, in the Security Explorer User Guide.

IMPORTANT: If you are running Active Administrator on the same computer as Security Explorer, exit Active Administrator and stop all Active Administrator services before upgrading to Security Explorer.

To install Security Explorer

1. Launch the autorun.
2. Select **Install Security Explorer.**
3. Select the version of Security Explorer to install, and click **Open**.

- **Security Explorer (32 bit)** can be installed to 32-bit and 64-bit operating systems. The installation folder is **Program Files** for 32-bit operating systems and **Program Files (x86)** for 64-bit operating systems.
- **Security Explorer (64 bit)** can be installed to 64-bit operating systems only. The installation folder is Program Files.

NOTE: You cannot install both versions of Security Explorer on the same computer.

4 On the Welcome screen of the Install Wizard, click **Next**.

5 Click **View License Agreement**.

6 Scroll to the end of the license agreement.

7 Click **I accept these terms**, and click **OK**.

8 Click **Next**.

9 On the **Custom Setup** page, you can change the location of the program files, install Access Explorer, install the Security Explorer cmdlets for use with Windows PowerShell®, and check disk usage.

- To install Access Explorer, click the icon next to **Access Explorer** and choose to install the feature.
- To install PowerShell®, click the icon next to PowerShell Snap-Ins, and choose to install the feature.
- To change the location of the program files, select the feature, and click **Browse**.
- To check disk usage, click **Disk Usage**.
- To reset selections, click **Reset**.

10 Click **Next**.

11 Click **Install**.

12 Click **Finish**.

More resources

Additional information is available from the following:

- Online product documentation (http://documents.quest.com/security-explorer/)
- Security Explorer 9.8 What's New Guide
- Security Explorer 9.8 Installation Guide
- Security Explorer 9.8 Upgrade Guide
- Security Explorer 9.8 User Guide

Globalization

This section contains information about installing and operating this product in non-English configurations, such as those needed by customers outside of North America. This section does not replace the materials about supported platforms and configurations found elsewhere in the product documentation.

This release is Unicode-enabled and supports any character set. In this release, all product components should be configured to use the same or compatible character encodings and should be installed to use the same locale and regional options. This release is targeted to support operations in the following regions: North America, Western Europe and Latin America, Central and Eastern Europe, Far-East Asia, Japan.

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.

Third-party contributions

This product contains the following third-party components. For third-party license information, go to https://www.quest.com/legal/license-agreements.aspx. Source code for components marked with an asterisk (*) is available at https://opensource.quest.com.

Table 25. List of third-party contributions

Component	License or acknowledgment
7-ZIP 9.20*	**NOTE:** This code cannot be used to create a RAR / WinRAR compatible archiver.
Renci SSH.NET Library Beta	Copyright (c) 2010, RENCI All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. * Neither the name of RENCI nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
Windows Installer XML Toolset (aka WIX) 3.11	Copyright (c) .NET Foundation and contributors. Microsoft Reciprocal License (MS-RL)

Legend

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

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