Quest® Security Explorer® 9.7

Release Notes

August 2017

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 9.7 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® 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

New features

New features in Security Explorer 9.7:

- **Additional supported platforms**:
  - Windows® 10
  - Windows Server® 2016
  - SharePoint® 2016
  - SQL Server® 2016
  - Exchange 2016
  - NetApp 9.0 and NetApp 9.1
- **Enhanced Access Explorer functionality** - In previous versions of Security Explorer, the Access Explorer Permission Wizard helped you manipulate explicit permissions and/or group memberships for accounts, computers, and/or resource groups managed by Access Explorer, but the Access Explorer service was installed and set up in other Quest products. Now in version 9.7, the Access Explorer module is enhanced with the full installation and management of the Access Explorer service, database, and agents, available right in Security Explorer. Once you install the agents and set up the database, the Access Explorer service scans and indexes security access information on files, folders, and shares on managed computers in managed domains. The data is stored in the Access Explorer database. Use the Access Explorer Permission wizard to change, clone, delete, export, and back up permissions. Currently supported resources include Windows® computers, Windows clusters, and certain network attached storage (NAS) devices.
- **Enhanced Exchange Security functionality** - You can now manage Active Directory® permissions for Exchange object properties. If Exchange mail servers are installed in parent and child domains, and Security Explorer is installed in the same forest, you can manage Exchange object permissions for domain accounts in both parent and child domains. Also, the performance of loading Exchange object permissions and the connection way to the Exchange organization are improved.

- **Start Security Explorer without local Administrator rights** - In previous versions, users could not start Security Explorer unless they were a local administrator on the computer where Security Explorer was installed. In version 9.7, a user who is not a local administrator can start Security Explorer, but the functionality is limited to actions that require local administrator rights.
- **Access in a cross forest environment** - *NTFS Security only.* If you select a network share for which you have no rights to read any resource in that network share, you are presented with a dialog to enter custom credentials. You can save the custom credentials to Windows Credentials, which are stored in your roaming profile. If you do not save the custom credentials, Security Explorer uses them until you log off.
- **Ability to purge backup files** - You can now choose to purge NTFS backup files. When setting general option in **Tools | Options**, you can select to purge backup files from a selected folder and set the number of days that determines what files to purge. Backup files older than the specified number of days are purged every day at midnight.
- **Additional group membership options** - When exporting permissions in the NTFS Security module (**Security | Export**), you can choose to include group members, nested groups, and Domain Users group members. The feature is available when generating reports or saving to a Microsoft® Excel® spreadsheet.

  When searching, you can now include BUILTIN\Users and Domain Users memberships in the search. If the account you are searching is a member of the BUILTIN\Users or Domain Users groups, those permissions are included in the search results.
- **Support for Security Explorer on 32-bit and 64-bit operating systems** - During installation, you can choose to install either a 32-bit or 64-bit version of Security Explorer. Security Explorer (32 bit) can be installed to 32-bit and 64-bit operating systems. Security Explorer (64 bit) can be installed to 64-bit operating systems only. You cannot install both versions of Security Explorer on the same computer.

See also:

- Enhancements
- Resolved issues

Enhancements

The following is a list of enhancements implemented in Security Explorer 9.7.

Table 2. General enhancements

Enhancement	Issue ID (TFS)	Issue ID (VSTS)
Improved performance of loading domain users and groups.	489237	13506
Added the ability to purge previously created *.sec backup files.	491608	12689
Improved performance of Restore Permissions.	594604	12625
Added support for the Security Explorer network tree in a cross forest environment.	608328	12613
Added the support for context menus in Windows® 10.	613036	12706
Enabled the **New** and **Edit** buttons on the **Export Scheduler Task List** dialog.	613295	12615
Added ability for users to be able to start Security Explorer without having to be a member of the local Administrators group.	631684	12598
Added the ability to suppress the NAS credentials dialog boxes.	638959	12595
Added the ability to grant the deny permission on a folder.	644459	12638
Ability to modify Exchange object permissions if Exchange mail servers are installed in parent and child domains.	649987	12687
Ability to install/uninstall PowerShell.	657787	12602
Added a count of the number of objects scanned by Access Explorer Agents.	666503	12593

Table 2. General enhancements

Enhancement	Issue ID (TFS)	Issue ID (VSTS)
Added ability to change the account used to connect to the Access Explorer database.	666762	12594
Ability to manage Active Directory® permissions for Exchange object properties.	669554	12637
Improved performance of loading Exchange object permissions.	671600	13507
Improved connection way to Exchange organization.	695060	13508
The **Generate Report** check box has been enabled in Export dialog for Access Explorer objects.	702299	12627

Resolved issues

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

Table 3. General resolved issues

Resolved issue	Issue ID (TFS)	Issue ID (VSTS)
Cannot grant/revoke some Built-In and Well-Known accounts on localized non-English Windows® operating systems.	463452	13525
If the Include Everyone Group, Include Authenticated Users Group, Include Network Group, or the Include Interactive User check boxes on Group/User Search Criteria tab are selected for the search, an error occurs when you click **Report** to print the results.	480639	13526
Security Explorer fails to restore large backups due to system running out of memory.	484735	13527
When trying to remove permissions for deleted accounts a Claims-based Authentication error occurs.	492217	13528
Receive an invalid pointer error for NetApp shares if the proper credentials are entered in **Tools | Options | NAS Devices** and the account that runs Security Explorer does not have access.	503533	13529
Incorrect domain name for accounts that were migrated.	544232	13530
Security Explorer network tree in a cross forest environment.	596712	13532
The Yes and Now buttons work incorrectly for the export scheduler task deletion.	612960	13531
User accounts cannot be added to the security of NTFS items if a computer with the same name as the user exists in the domain.	613776	13533
Security Explorer cannot resolve a domain name if PDC is off.	615464	13534
Security Explorer cannot open an SQL Server® instance if multiple computer management WMI scopes exist.	615469	13535
When trying to do a Run As using a smart card, the **No Valid certificates found** error is displayed.	640390	13536
Command line utility and PowerShell cmdlet incorrectly grant NTFS List folder contents permission.	640956	13537
NTFS: Error in Restore dlg after trying to Restore permissions for many files (2000 folders with 1000 files in each folder).	641891	13538
Granting a deny delete on a folder using Security Explorer results in no users having access on a NETAPP 8.2 mode 7 computer.	642053	13539

Table 3. General resolved issues

Resolved issue	Issue ID (TFS)	Issue ID (VSTS)
Redundant NAS credential requests for NetApp shares.	643801	13540
The scheduled backup will not properly back up a folder with special character in the name.	691207	13541

Table 4. Group and User Management module resolved issues

Resolved issue	Issue ID (TFS)	Issue ID (VSTS)
Receive an error when trying to load a domain users list with greater than 15000 users.	488597	13542
Receive an error when trying to view Group Memberships for global groups.	488598	13543
Receive an error if a pre-Windows 2000 group name is changed, but the Security Explorer list is not refreshed.	488645	13544
Receive an Out of Range error when selecting **Domain Users** in the Security Explorer tree.	494915	13545

Table 5. Exchange Security module resolved issues

Resolved issue	Issue ID (TFS)	Issue ID (VSTS)
It is impossible to grant mailbox folder permissions for accounts if the logon name differs from the display name.	648968	13546
It is impossible to revoke public folder permissions and mailbox folder permissions for disabled accounts.	648977	13547

Table 6. Access Explorer module resolved issues

Resolved issue	Issue ID (TFS)	Issue ID (VSTS)
Access Explorer loses connectivity to its database.	666751	13548

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 7. General known issues

Known issue	Issue ID (TFS)	Issue ID (VSTS)
If you back up permissions for Exchange objects in Security Explorer 9.6 and earlier, it is impossible to restore permissions from the backup file in Security Explorer 9.7. Permissions must be backed up in Security Explorer 9.7 to restore them in Security Explorer 9.7. **Workaround**: After installing Security Explorer 9.7, perform a back up of Exchange permissions.	701554	13550

System requirements

Before installing or upgrading Security Explorer 9.7, 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 8. Hardware requirements

Requirement	Details
Processor	Pentium® 600MHz or faster
Memory	1 GB
Hard disk space	150 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 9. 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.
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.

Minimum permissions for Access Explorer

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

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

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

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

Exchange 2007

Table 10. Required software for Microsoft® Exchange 2007

Client type	Required software
Windows® XP Windows Server® 2003	• IIS Services Manager from Windows Components • NET Framework 2.0 or 3.5 • Windows PowerShell® 1.0 or 2.0
Windows Vista® Windows Server 2008	• IIS 6.0 Management Compatibility from Windows Features • Windows PowerShell 1.0 from Windows Features, or 2.0, or 3.0 (Windows Server 2008 only; requires NET Framework 4.5.x)
Windows 7 Windows Server 2008 R2	• IIS 6.0 Management Compatibility from Windows Features • Windows PowerShell 2.0 from Windows Features or 3.0 (requires NET Framework 4.5.x)
Windows 8 Windows 8.1 Windows Server 2012 Windows Server 2012 R2	• 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 2010, 2013, Mixed Mode (Exchange 2010–2013)

Table 11. Supported versions of Microsoft® Exchange 2010 and 2013

Client type	Required software
Windows® XP Windows Vista® Windows Server® 2003 Windows Server 2008	• NET Framework 2.0 or 3.5 • Windows PowerShell® 2.0

Table 11. Supported versions of Microsoft® Exchange 2010 and 2013

Client type	Required software
Windows 7 Windows Server 2008 R2	• Windows PowerShell 2.0 from Windows Features or 3.0 (requires NET Framework 4.5.x)
Windows 8 Windows 8.1 Windows Server 2012 Windows Server 2012 R2	• Windows PowerShell 2.0 or 3.0 from Windows Features

Mixed Mode (Exchange 2007–2010 and 2007–2013)

Table 12. Required software for Microsoft® Exchange 2007-2010 and 2007-2013 mixed modes

Client type	Required software
Windows® XP Windows Server® 2003	• IIS Services Manager from Windows Components • NET Framework 2.0 or 3.5 • Windows PowerShell® 2.0
Windows Vista Windows Server 2008	• IIS 6.0 Management Compatibility from Windows Features • Windows PowerShell 2.0 or 3.0 (Windows 2008 only; requires NET Framework 4.5.x)
Windows 7 Windows Server 2008 R2	• IIS 6.0 Management Compatibility from Windows Features • Windows PowerShell 2.0 from Windows Features or 3.0 (requires NET Framework 4.5.x)
Windows 8 Windows 8.1 Windows 2012 Windows 2012 R2	• 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

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
- Mixed Mode (Exchange 2007–2010)
- Mixed Mode (Exchange 2007–2013)
- Mixed Mode (Exchange 2010–2013)

Exchange 2007

Table 13. 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 14. 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

Table 15. Restrictions with mailbox management in Security Explorer with Microsoft® Exchange 2013

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 16. 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 17. 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)

Table 18. Restrictions with mailbox management in Security Explorer with Microsoft® Exchange 2010–2013 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.
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 9.7 side-by-side with all of these previous versions.

Product licensing

You must have a Quest® license file (.dlv) to use version 9.7. Your previous licenses will not be recognized by version 9.7.

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 9.7 What's New Guide
- Security Explorer 9.7 Installation Guide
- Security Explorer 9.7 Upgrade Guide
- Security Explorer 9.7 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 19. List of third-party contributions

Component	License or acknowledgment
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.

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.