

Quest® Security Explorer® 9.9

Release Notes

July 2020

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

Topics:

- [About this release](#)
- [Supported platforms](#)
- [New features](#)
- [Enhancements](#)
- [Resolved issues](#)
- [Known issues](#)
- [System requirements](#)
- [Product licensing](#)
- [Upgrade and installation instructions](#)
- [More resources](#)
- [Globalization](#)
- [About us](#)

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 9.9 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	Windows 8.1
Share Security	Windows 10
Registry Security	Windows Server 2012
Printer Security	Windows Server 2012 R2
Service Security	Windows Server 2016
Task Management	Windows Server 2019
Group & User Management	
NTFS Security	Dell™ Fluid File System (FluidFS)
Share Security	EMC® Isilon®
Group & User Management	EMC Celerra®
	EMC VNX®
	NetApp® 8.2 (7-Mode and Clustered Mode)
	NetApp 8.3, 9.0, 9.1, 9.2, 9.3, and 9.4 Clusters
	NOTE: If Security Explorer is installed on a device with 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:
	<code>sc config lanmanworkstation depend=</code> <code>browser/mrxsmb10/ntsi</code>
	<code>sc config mrxsmb20 start= disabled</code>
	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, 9.2, 9.3 and 9.4.
	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® 2019 SQL Server 2019 Reporting Services SQL Server 2017 SQL Server 2017 Reporting Services SQL Server 2016 SQL Server 2014 SQL Server 2012
SharePoint Security	SharePoint® 2019 SharePoint 2016 SharePoint 2013 SharePoint 2010 SharePoint Foundation
Exchange Security	Exchange 2019 Exchange 2016 Exchange 2013 Exchange 2010
Active Directory Security	Windows Server® 2019 Functional Level Windows Server 2016 Functional Level Windows Server 2012 R2 Functional Level Windows Server 2012 Functional Level

New features

New features in Security Explorer 9.9:

- **Search for permissions using SxpSearch.exe.** Introduced a new command line program that allows you to search for permissions from the command line with the following arguments:
 - `<module name>`: Specifies a module.
 - `<search definition file path>`: Specifies an XML file that defines the search scope and criteria.
 - `<report file name>`: Specifies the path to save the search report and status file.See the user guide for more information about SxpSearch.exe.
- **Schedule a permission export or search.** You can now schedule a permission export or search, and choose to automatically send the report by email or to a specified shared folder.
 - Introduced the Search Scheduler to the NTFS Security, Share Security, Registry Security, Printer Security, Group And User Security, SharePoint Security, SQL Security, Exchange Security, and Active Directory modules.
 - More modules now support the Export Scheduler: Share Security, Task Management, Service Security, Group and User Management, SQL Server Security, Exchange Security, SharePoint Security, and Active Directory Security.
- **Compare security.** In the NTFS Security module, you can now select **Security | Compare Security** to compare permissions of two folders. The feature offers a side-by-side comparison view and uses color cues to highlight the differences.

- **Set auto-pause time for a scheduled backup.** In the NTFS Security module, you can now configure a scheduled backup to automatically pause at a specified time. The paused backup will automatically resume when the task runs again.
- **Support for Managed Service Accounts.** The Group and User Management module now supports for Managed Service Accounts. You can perform the following actions to manage your Managed Service Accounts:
 - Creating a new Managed Service Account
 - Modifying properties of a Managed Service Account
 - Modifying Active Directory properties of a Managed Service Account
 - Viewing memberships of a Managed Service Account
 - Deleting a Managed Service Account
- **Additional supported platforms:**
 - SQL Server 2019 Reporting Service (for SQL Server Security module)

See also:

- [Enhancements](#)
- [Resolved issues](#)

Enhancements

The following is a list of enhancements implemented in Security Explorer® 9.9.

Table 2. General enhancements

Enhancement	Issue ID
Added support for Federal Information Processing Standard (FIPS) Publication 140-2 by using the Data Protection API (DPAPI) from Microsoft.	170692
Introduced a new command “SxpSearch.exe” to search for permissions from the command line.	28880
Added the ability to automatically send report by email or to a shared folder when a scheduled search or export completes.	28880
Added the ability to change the icon size in the Tool Bar (View Tool Bar Size).	20135
Added the ability to select multiple target accounts when cloning groups and users.	22797

Table 3. Share Security module enhancements

Enhancement	Issue ID
Added the ability to export NTFS permissions in the Share Security module directly.	12506

Table 4. NTFS Security module enhancements

Enhancement	Issue ID
Added the ability to export NTFS permissions to a SQLite database.	15460
Added the ability to compare permissions of two folders.	19180
Added new arguments in SxpClone.exe to clone protected objects and ownership.	20833
Added the ability to automatically pause a scheduled backup at a specified time.	17370

Table 5. Group and User Management module enhancements

Enhancement	Issue ID
Added support for Managed Service Accounts.	14153
Added the ability to create a user or group for multiple domains or computers.	14980

Table 6. SQL Server Security module enhancements

Enhancement	Issue ID
Added support for SQL Server 2019 Reporting Service.	170700

Table 7. Active Directory Security module enhancements

Enhancement	Issue ID
Added the option Search for inheritance-disabled objects in the Permission Search Criteria form.	155741

Resolved issues

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

Table 8. General resolved issues

Resolved issue	Issue ID
Cannot connect to Exchange with an edge server connection error.	200304
Security Explorer crashes when switching path on Tools Show Open Files Choose Server / Base Path .	184417
The summary mode for the NTFS Security report does not work well.	161731
Errors occur when Security Explorer is launched by a user who is not a member of the Local Administrators group.	158388
Cannot display SID history when revoking permissions.	129533
Users load slowly in the Grant Permissions window.	21851

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

Table 9. General known issues

Known issue	Issue ID
Modifying one permission for a user with two ACEs sometimes incorrectly removes the other.	12183
Cannot grant NTFS permissions to a user or group from a one-way trusted domain with selective authentication enabled.	201337
Workaround: Add user credentials to Windows Credential Manager for all domain controllers in the trusted domain.	

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 9.9, ensure that your system meets the following minimum hardware and software requirements.

i | **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

Table 12. Hardware requirements

Requirement	Details
Hard disk space	550 MB
Operating system	<ul style="list-style-type: none">• Windows 8.1• Windows 10• Windows Server 2012• Windows Server 2012 R2• Windows Server 2016• Windows Server 2019

Software requirements

- .Net Framework v.4.0 or later

i | **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: <ul style="list-style-type: none">• 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.

Table 13. Requirements to enable permission management

Module	Requirement
SharePoint® Security	<p>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.</p> <p>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.</p> <p>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.</p>
SQL Server® Security	<p>To manage permissions on servers running SQL Server:</p> <ul style="list-style-type: none">• 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. <p>For more information please refer to: <i>Configure the Windows Firewall to Allow SQL Server Access</i> at http://msdn.microsoft.com/en-us/library/cc646023.aspx.</p>
Exchange Security	<p>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.</p>
Active Directory Security	<p>To manage permissions on the domain, the domain must have a trusted relationship with the current domain on which the user is logged on.</p> <p>See <i>Setting Options for Active Directory Security</i> in the <i>Security Explorer 9.9 User Guide</i>.</p>

Minimum permissions for Access Explorer

Table 14. Minimum permissions for Access Explorer

Account	Requirement
Logged in user	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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](#)
- [Client Configuration](#)

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.

Permission requirements to manage Microsoft Exchange in Security Explorer

- 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 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 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.

i | **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 2010](#)
- [Exchange 2013, 2016, and 2019](#)
- [Mixed Mode \(Exchange 2010–2013, 2010–2016, 2010-2019, 2013–2016, 2013-2019, 2016-2019\)](#)

Exchange 2010

Table 15. 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, 2016, and 2019

Table 16. Restrictions with mailbox management in Security Explorer with Microsoft® Exchange 2013, 2016, and 2019

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.

Table 16. Restrictions with mailbox management in Security Explorer with Microsoft® Exchange 2013, 2016, and 2019

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 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 2010–2013, 2010–2016, 2010-2019, 2013–2016, 2013-2019, 2016-2019)

Table 17. Restrictions with mailbox management in Security Explorer with Microsoft® Exchange mixed modes (2010–2013, 2010–2016, 2010-2019, 2013–2016, 2013-2019, 2016-2019)

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 9.9 side-by-side with all of these previous versions.

Product licensing

You must have a Quest® license file (.dlv) to use version 9.9.

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.

i | **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.

i | **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 9.9 What's New Guide
- Security Explorer 9.9 Installation Guide
- Security Explorer 9.9 Upgrade Guide
- Security Explorer 9.9 User Guide
- Security Explorer 9.9 Deployment in FIPS Environments

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

Quest provides software solutions for the rapidly-changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid datacenters, security threats, and regulatory requirements. We are a global provider to 130,000 companies across 100 countries, including 95% of the Fortune 500 and 90% of the Global 1000. Since 1987, we have built a portfolio of solutions that now includes database management, data protection, identity and access management, Microsoft platform management, and unified endpoint management. With Quest, organizations spend less time on IT administration and more time on business innovation. For more information, visit www.quest.com.

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 18. 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	<p>Copyright (c) 2010, RENCi All rights reserved.</p> <p>Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:</p> <p>* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.</p> <p>* 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.</p> <p>* 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.</p> <p>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.</p>
Windows Installer XML Toolset (aka WIX) 3.11	<p>Copyright (c) .NET Foundation and contributors. Microsoft Reciprocal License (MS-RL)</p>

© 2020 Quest Software Inc.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

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, Security Explorer, and the Quest logo 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.

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