Quest

Quest® Security Explorer® 9.7
Install Guide

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

Legend

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

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

Quest Security Explorer Install Guide
Updated - June 2017
Software Version - 9.7

Contents

1

Installation Considerations for Security Explorer

Minimum requirements

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

Hardware

Table 1. Hardware requirements

Requirement	Details
Processor	Pentium® 600MHz or faster
Disk space	150 MB
Memory	1 GB

Supported operating systems

- Windows® 7
- Windows 8
- Windows 8.1
- Windows 10
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

- Windows Server 2016

Required software

- .Net Framework v.4.0 or later

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

Supported platforms for Security Explorer

Table 2. 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

Table 2. Supported platforms for Security Explorer®

Security Explorer Module	Supported Platform

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.

SQL Security	SQL Server® 2016 SQL Server 2014 SQL Server 2012 SQL Server 2008 R2 SQL Server 2008 SQL Server 2005 **NOTE:** The SQL Server Browse service must be started on the SQL Server to enumerate all SQL Instances.
SharePoint Security	SharePoint® 2016 SharePoint 2013 SharePoint 2010 SharePoint Foundation SharePoint 2007 SharePoint Services 3.0

Table 2. Supported platforms for Security Explorer®

Security Explorer Module	Supported Platform
Exchange Security	Exchange 2016
	Exchange 2013
	Exchange 2010
	Exchange 2007

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 3. 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.

Table 3. Requirements to enable permission management

Module	Requirement
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).

Port requirements for Access Explorer

On the server where the Access Explorer agent is installed, configure the firewall to allow outgoing traffic on TCP port 8721, as well as incoming traffic on TCP port 18530. Also, ensure that the Access Explorer service firewall has the following exceptions configured: incoming TCP 8721, 8722, and outgoing 18530.

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 - 2016: 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 mixed modes: 2007–2010 and 2007–2013
- Exchange 2010, 2013, 2016
- Exchange mixed modes: 2010–2013, 2010–2016, 2013–2016

Exchange 2007

Table 4. 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 5. 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 6. Supported versions of Microsoft® Exchange 2010, 2013, 2016

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

Table 6. 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 7. 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 Modes (Exchange 2010–2013, 2010-2016, 2013-2016)

Exchange 2007

Table 8. 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 9. 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 10. 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 11. 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 12. 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 Modes (Exchange 2010–2013, 2010-2016, 2013-2016)

Table 13. Restrictions with mailbox management in Security Explorer with Microsoft® Exchange 2010–2013, 2010-2016, and 2013-2016 mixed modes

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

2

Installing Security Explorer

Upgrading Security Explorer

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.

Back up your files

As with all software installations, it is recommended that you back up your files before installing the new software. The simplest way to back up your files is to navigate to the directory on the server where Security Explorer is installed. Press CTRL-A to select all files in this folder. Press CTRL-C to copy the files to the clipboard. Create a new folder and press CTRL-V to paste these files into this new backup folder.

Licenses

For Security Explorer 9.7, you must have a Quest® license file (.dlv) or a Site Administrator QLL license file (*asc). Your previous licenses will not be recognized by version 9.7.

Access Explorer

The User Centric Security Management features provided by Security Explorer appear as an Access Explorer node in the navigation tree on the Browse tab if the Access Explorer feature is installed and the license is enabled for Access Explorer. If installed, the Access Explorer menu options are present regardless of whether the license is enabled for Access Explorer.

If you are currently using the Access Explorer feature installed with Enterprise Reporter 2.6, you need to upgrade the Access Explorer service and any installed Access Explorer agents after you install Security Explorer 9.7. See Upgrading Access Explorer.

Installing Security Explorer

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.

IMPORTANT: 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. Upon installation of Security Explorer 9.7, perform a back up of Exchange permissions.

IMPORTANT: Security Explorer uses NetBios names to resolve domains and computers, so you must add the DNS suffixes of domains to the Domain Group Policy or to the Network properties of the computer where Security Explorer is installed.

- **Default domain policy | Computer Configuration | Policies | Administrative Templates: Policy definitions | Network | DNS Client | DNS Suffix Search List**

  -OR-

- On the computer where Security Explorer is installed: **Network Properties | Advanced TCP/IP Settings | DNS tab | Append DNS suffixes**

NOTE: The SQL Server Browse service must be started on the SQL Server to enumerate all SQL Instances.

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**.

Starting Security Explorer

The first time you start Security Explorer you must apply a license file.

Applying a license file

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.

To apply a license file

- Click **Update License** and locate the license file. The license file is approximately 1 KB in size and has a .dlv file extension or .asc file extension for a Site license.

Upgrading Access Explorer

If you are currently using the Access Explorer feature installed with Enterprise Reporter 2.6, you need to upgrade the Access Explorer service. See Upgrading the Access Explorer service. You also should upgrade any installed Access Explorer agents. See Upgrading agents.

Upgrading the Access Explorer service

If you are currently using the Access Explorer feature installed with Enterprise Reporter 2.6, you need to upgrade the Access Explorer service. You also should upgrade any installed Access Explorer agents. See Upgrading agents.

To upgrade the Access Explorer service

1 Select **Tools | Access Explorer Configuration**.

2 Click **Configure Access Explorer**.

A message indicates that an older version of the Access Explorer service was installed through Enterprise Reporter and asks if you want to upgrade.

3 Click **Yes** to upgrade the Access Explorer service.

NOTE: If you choose **No**, the message will display continue to display when you click **Configure Access Explorer** until you choose **Yes** to upgrade the service.

Upgrading agents

If you are upgrading from Enterprise Reporter 2.6, you should upgrade any installed Access Explorer agents. Once upgraded, the Security Explorer version number will display for the managed computer.

To upgrade installed Access Explorer agents

1. Select **Tools | Access Explorer Configuration**.
2. Click **Configure Access Explorer**.
3. Open the **Manage Computers** tab.

   If an upgrade is available for an installed agent, **Upgrade Available** displays in the **Version** column next to the version number.
4. Select the managed computers to upgrade, and click **Upgrade**.
5. Click **Yes** to rescan the selected managed computers.

   The Access Explorer agents are reinstalled and the managed computers are rescanned. When the process is complete, **Data available** displays in the **Data State** column and the new version number displays in the **Version** column.

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.