Quest® NetVault® Backup Plug-in *for Standard Encryption* 11.4

User’s Guide

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

Legend

■ **WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.**

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

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

NetVault Backup Plug-in *for Standard Encryption* User's Guide
Updated - September 2017
Software Version - 11.4
NVG-122-11.4-EN-01

Contents

1

Introducing NetVault Backup Plug-in *for Standard Encryption*

About NetVault Backup Plug-in *for Standard Encryption*

NetVault Backup offers two encryption products:

- **NetVault Backup Plug-in *for Standard Encryption* (Plug-in *for Standard Encryption*):** The Plug-in *for Standard Encryption* supports CAST-128 algorithm to protect your data and meet the regulatory requirements.

  CAST-128 is a 12- or 16-round Feistel network with a 64-bit block size and a key size of between 40 to 128 bits, but only in 8-bit increments.

- **NetVault Backup Plug-in *for Advanced Encryption* (Plug-in *for Advanced Encryption*):** The Plug-in *for Advanced Encryption* supports AES-256 and CAST-256 algorithms to protect your data and meet the regulatory requirements.

  - **CAST-256:** CAST-256 uses the same elements as CAST-128, but it is adapted for a block size of 128 bits — twice the size of its 64-bit predecessor. Acceptable key sizes are 128, 160, 192, 224 and 256 bits. CAST-256 is composed of 48 rounds, sometimes described as 12 “quad-rounds”, arranged in a generalized Feistel network.
  - **AES-256:** Advanced Encryption Standard (AES) is an encryption standard adopted by the U.S. government. The standard consists of three block ciphers, AES-128, AES-192, and AES-256. Each AES cipher has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively.

> **NOTE:** The CAST-128 and CAST-256 encryption algorithms do not comply with the requirements of the United States Federal Information Processing Standard (FIPS). These algorithms are provided for the restoration of legacy data. For FIPS compliance, use the AES-256 algorithm.

When installed on the NetVault Backup Client, these plug-ins encrypt and transfer data across the network to the backup device, where the data remains encrypted until restored to the client. If encryption is only required for secondary storage, job-level encryption offers the choice of encrypting only the secondary copy while the primary backup remains unencrypted to shrink the backup window. When using disk-based storage devices, job-level deduplication allows you to separate deduplicated from nondeduplicated unencrypted data for optimal deduplication ratios and performance.

For a list of NetVault Backup Plug-ins that are incompatible with the Plug-in *for Standard Encryption* and Plug-in *for Advanced Encryption*, see the respective release notes.

ℹ **NOTE:** The NetVault Backup encryption architecture only supports the Electronic Code Book (ECB) mode of operation. This support means that every data block is encrypted individually. If two or more consecutive blocks contain identical data, the encrypted forms of these blocks are also identical.

Target audience

This guide is intended for Backup Administrators and other technical personnel who are responsible for designing and implementing a backup strategy for the organization. Familiarity with encryption solutions is assumed.

Recommended additional reading

The following documentation is also available:

- *Quest NetVault Backup Installation Guide*: This guide provides details on installing the NetVault Backup Server and Client software.
- *Quest NetVault Backup Administrator's Guide*: This guide explains how to use NetVault Backup and describes the functionality common to all plug-ins.
- *Quest NetVault Backup CLI Reference Guide*: This guide provides a description of the command-line utilities.

You can download these guides from https://support.quest.com/technical-documents.

Defining a backup strategy

Encryption strategy overview

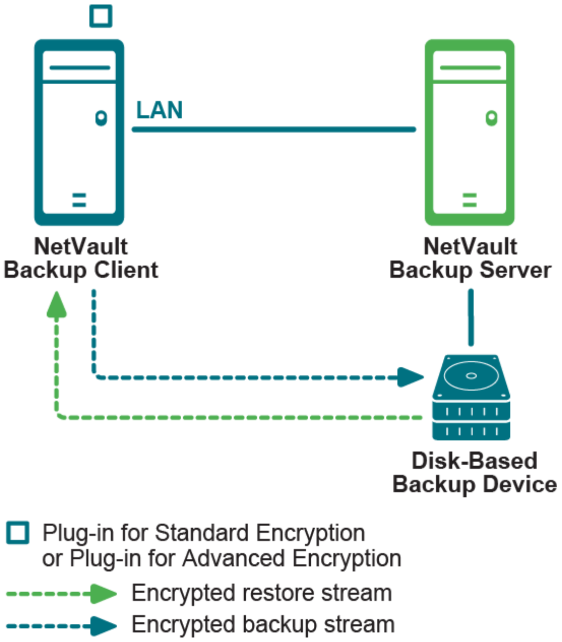
When defining an encryption strategy, you must determine the following:

- Which backups are encrypted.
- Which encryption algorithm is required.
- Whether encryption is required for primary backups or secondary backups.
- Whether encryption is enabled for all backups or on a per-job basis.

Selecting which backups to encrypt

NetVault Backup performs software-based encryption. The backup stream is encrypted using the selected algorithm by the NetVault Backup Server or Client where the plug-in is installed. The encrypted data stream is transferred over the network to the backup device where it remains encrypted. During restore, the encrypted backup is transferred from the backup device to the targeted NetVault Backup client, where the plug-in installed on the client completes the decryption.

Figure 1. Encrypted backup and restore path



ℹ **NOTE:** Installing the Plug-in *for Standard Encryption* or Plug-in *for Advanced Encryption* on the NetVault Backup Server is only required to encrypt the backups that originate from the server, such as NetVault Database backups. It is not required to encrypt backups that originate on a client running any built-in or licensed plug-in.

The backup encryption and decryption processes are performed by the plug-in installed on the NetVault Backup Server or Client. These processes use resources on the machine. The encryption process lengthens the time it takes to perform backups, while the decryption process lengthens the time it takes to perform restores. The impact to the performance of the client, backup window, and restore time should be considered when deciding which backups must be encrypted. In summary, backups should only be encrypted when security requirements outweigh the impact to performance, backup windows, and restore times.

Selecting the encryption algorithm

NetVault Backup provides multiple algorithms that can be used to encrypt and decrypt backups. While each NetVault Backup client can use a different encryption algorithm, all backups from a particular client must use the same algorithm.

The same encryption algorithm that was used during backup must be used during restores. It is possible to use a different algorithm from this point forward than was previously used. However, when restoring backups that used the previous algorithm, the NetVault Backup Server or Client must be configured to specify the algorithm used by the backup to restore data successfully. For example, if previous backups used the CAST-128 algorithm while current backups are using the AES-256 algorithm, the plug-in must be configured on the server or client to use the CAST-128 algorithm when restoring a backup that was taken using that algorithm; otherwise, restore fails.

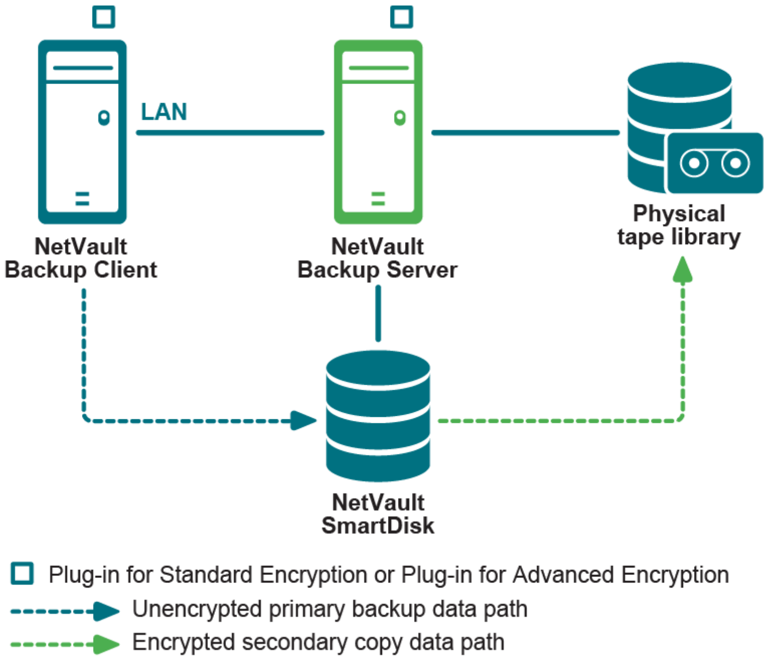
Encrypting primary or secondary backups

A backup job consists of one or optionally two phases—Primary Backup and Secondary Copy. The primary backup is the backup of data stream to the selected backup device. These backups are performed to local storage devices to enable faster restores. The Secondary Copy is a Duplicate or Data Copy of the primary backup to a different backup device. These backups are targeted to remote disk-based storage devices or physical tape libraries whose tapes are stored offsite for disaster recovery purposes.

Your security requirements dictate whether you require encryption for both the primary backups and the secondary copies. For example, if the security requirements dictate that only the backups that leave the corporate network require encryption (such as those backups stored on physical tapes in a remote location), encrypt the secondary copy backups that target the physical tape libraries. However, if the security requirements dictate that data must be encrypted while it transfers across the network or while it is stored on a disk-based backup device—even if the disk-based backup device is located within the corporate network—encrypt both the primary backup and secondary copy.

Encrypted data does not deduplicate well. Therefore, encrypting only the secondary copy backup is beneficial when the primary backups are performed to storage devices that support deduplication. This approach lets you take advantage of both encryption and deduplication by deduplicating the primary backup and encrypting the secondary copy.

Figure 2. Unencrypted primary backups and encrypted secondary copy backups


LAN
NetVault Backup Client
NetVault Backup Server
Physical tape library
NetVault SmartDisk
Plug-in for Standard Encryption or Plug-in for Advanced Encryption
Unencrypted primary backup data path
Encrypted secondary copy data path

Encrypting all or specific backups

After the Plug-in *for Standard Encryption* or Plug-in *for Advanced Encryption* is installed, you can enable encryption for all backups on the NetVault Backup Server or Client where the plug-in is installed, or enable encryption only for specific jobs. Encryption can also be enabled only for the primary backup or the secondary copies. This approach lets you take advantage of both encryption and deduplication. For example, you can deduplicate the primary backup and encrypt the secondary copy.

The job-level encryption option can be used in the following situations:

- When any plug-in installed on the server or client is incompatible with the Plug-in *for Standard Encryption* or Plug-in *for Advanced Encryption*.
- Only specific backups on the server or client require encryption.
- Primary backups do not require encryption while secondary backups for offsite protection require encryption.
- Primary backups are targeted to storage devices that support deduplication.

The NetVault Backup Server and Client should only be configured to encrypt all its backups in the following situations:

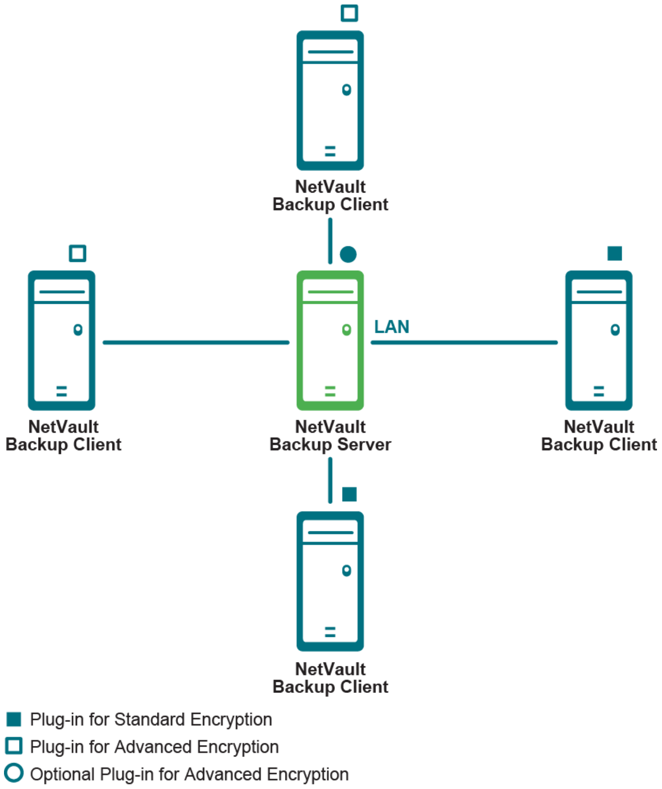
- All plug-ins installed on the server or client are compatible with the Plug-in *for Standard Encryption* or Plug-in *for Advanced Encryption*.
- All backups from the server or client require encryption.
- Both primary and secondary backups require encryption.
- Backups are not selected for deduplication.

3

Installing the plug-in

Deployment overview

Figure 3. Deployment overview



The Plug-in *for Standard Encryption* or Plug-in *for Advanced Encryption* must be installed on all NetVault Backup clients on which the backups should be encrypted. For each client, you must obtain a separate permanent license key. The server and clients can be configured to use different encryption algorithms, except when using the server or client to create encrypted secondary copies.

For example, if a client is configured to use the AES-256 algorithm, and the server is used to create the encrypted secondary copy, the server must also be configured to use the AES-256 algorithm to ensure that the secondary copy backups can be restored by the client.

Installing the plug-in

You can install the plug-in simultaneously on multiple machines by using the configuration wizard. Alternatively, you can install a plug-in on a single client from the **Manage Clients** page.

The following sections describe the different procedures that you can use to install the plug-in:

- Installing the plug-in using the push installation method (Windows)
- Installing the plug-in using the configuration wizard (Linux/UNIX)
- Installing the plug-in from the Manage Clients page

Installing the plug-in using the push installation method (Windows)

On Windows-based machines, you can use the push installation method to install the plug-ins on several machines at the same time. You can perform push installations from the NetVault Backup WebUI.

Before you start the push installation procedure, verify that the following requirements are met:

- **Copy the packages to a shared location:** Copy the client and plug-in packages to a shared location. Only CIFS shares are currently supported as package stores. The path must be accessible to the NetVault Backup Server and all target machines where you want to install the packages.

  Make sure that you use the original names of the installation packages. Renamed packages cannot be selected for push installations.

- **Configure a package store in NetVault Backup:** After copying the installation packages, configure the shared location details in NetVault Backup. For more information, see the *Quest NetVault Backup Administrator's Guide*.

To install the plug-in on Windows-based clients:

1. In the Navigation pane, click **Guided Configuration**, and then on the **NetVault Configuration Wizard** page, click **Install Software/Add Clients**.
2. On the **Select Software/Add Clients** page, select **Install NetVault software on remote machines**.
3. In the **Package Store** list, select the repository that contains the installation packages that you want to deploy.
4. To add plug-in packages, click **Add NetVault plug-in package**.

   In the **Select Packages for Deployment** dialog box, select the check boxes corresponding to the **".npk"** binary files that you want to use. The files names are listed in the following table (where **x-x-x-x** represents the version, build, and platform numbers).

Encryption algorithm	Binary filename
CAST-128	cst-x-x-x-x.npk
CAST-256	cst2-x-x-x-x.npk
AES-256	aes-x-x-x-x.npk

   Click **OK**, and then click **Next**.
5. On the **Machines to Have NetVault Software Installed** page, click **Choose Machines**, and select **From available machines**.
6. On the **NetVault Machine Details** tab, select the client that you want to add, and click **OK**.
7. To add more machines, repeat Step 5 and Step 6.
8. To submit the task, click **Install Software/Add Clients**.

You can monitor the progress and status of the task from the **Deployment Task Status** page. For more information, see the *Quest NetVault Backup Administrator's Guide*.

Installing the plug-in using the configuration wizard (Linux/UNIX)

On Linux-based machines, you can use the configuration wizard to install the plug-in on multiple clients at the same time.

> **NOTE:** When you use this procedure, make sure that the plug-in binary file is compatible with the client OS and platform.

To install the plug-in on Linux- and UNIX-based clients:

1. In the Navigation pane, click **Guided Configuration**, and then on the **NetVault Configuration Wizard** page, click **Install Plugins**.
2. In the **NetVault Backup Clients** table, select the clients on which you want to install the plug-in.
3. Click **Choose Plug-in File**, and in the browse window, navigate to the location of the **".npk"** installation file for the plug-in (on the installation CD or the directory to which the file was downloaded from the website).
4. Select the platform-specific binary file for the plug-in.

   The files names are listed in the following table, where **x-x-x-x** represents the version, build, and platform numbers.

Encryption algorithm	Binary filename
CAST-128	cst-x-x-x-x.npk
CAST-256	cst2-x-x-x-x.npk
AES-256	aes-x-x-x-x.npk

5. To begin installation, click **Next**.

   After the plug-in is installed successfully, a message is displayed.

Installing the plug-in from the Manage Clients page

From the **Manage Clients** page, you can install a plug-in on a single client.

1. In the Navigation pane, click **Manage Clients**.
2. In the **NetVault Backup Clients** table, select the client, and click **Manage**.
3. At the lower-right corner of the Installed Plug-ins table, click the Install Plugin button (⊕).
4. Click **Choose Plug-in File**, and in the browse window, navigate to the location of the **".npk"** installation file for the plug-in (on the installation CD or the directory to which the file was downloaded from the website).
5. Select the platform-specific binary file for the plug-in. The files names are listed in the following table (where **x-x-x-x** represents the version, build, and platform numbers).

Encryption algorithm	Binary filename
CAST-128	cst-x-x-x-x.npk
CAST-256	cst2-x-x-x-x.npk
AES-256	aes-x-x-x-x.npk

6 To begin installation, click **Install Plugin**.

After the plug-in is installed successfully, a message is displayed.

Removing the plug-in

1 In the Navigation pane, click **Manage Clients**.

2 In the **NetVault Backup Clients** list, select the client, and click **Manage.**

3 In the Installed Plug-ins table, select the item that you want to remove:

- CAST-128 Encryption
- CAST-256 Encryption
- AES-256 Encryption

4 Click the **Remove Plugin** button (⊟).

5 In the confirmation dialog box, click **Remove**.

4

Configuring the plug-in

Configuring default settings

1 In the Navigation pane, click **Change Settings**.

2 On the **Configuration** page, click **Server** or **Client Settings**, as applicable.

3 Under **Plugins**, click **Encryption**.

4 Configure the following settings.

Setting	Description
Encrypt ALL Backups on this Client	After the Plug-in *for Standard Encryption* or Plug-in *for Advanced Encryption* is installed on a client, you can do either of the following: • Encrypt all backups performed for that client. • Encrypt specific backups performed for that client. To enable encryption for all backups, select this check box. When you enable encryption for all backups, you cannot change the setting on a per-job basis. For more information about enabling encryption for specific backups, see Performing job-level encryption. **NOTE:** To perform job-level encryption for backups originating from a NetVault Backup Server or Client, the plug-in should not be configured for encrypting all backups.
Encryption Key String	Type the string that serves as the encryption key for the NetVault Backup machine. Different platforms allow varying characters and password lengths. Quest recommends that you use passwords of 32 characters or less. You can use characters from the following set: “A–Z”, “a–z”, “0–9”, and “_”. Key strings that do not conform to these specifications may work on one platform but may be invalid in another environment.
Available Encryption Algorithms	Select the encryption algorithm that you want to use for backups and restores. Depending on the products that you have installed, the list includes the following options: CAST-128, CAST-256, and AES-256.

5 To apply the new settings and close the dialog box, click **Apply**.

NOTE: An encrypted backup can be restored to either its original location or to a new target machine. In either event, the plug-in must be installed on the target machine and it must be configured as it was when the backup was performed—using the same **Encryption Key String** and **Encryption Algorithm**.

5

Using the plug-in

Encrypting all backups

If encryption is enabled for all backups performed from a particular NetVault Backup Client, there are no additional requirements for encrypting backups. For more information about the backup and restore procedures, see the user's guide for the relevant plug-in.

Performing job-level encryption

The job-level encryption option can be used to encrypt the primary backup, secondary copy, or both. Encrypting both the primary backup and secondary copy is beneficial when security requirements dictate that the backup must be encrypted while it transfers across the network or while it is stored on a disk-based backup device even if the disk-based backup device is located within the corporate network.

The job-level encryption setting is specified in the Backup Advanced Options Set. For more information about creating an Advanced Options Set for a backup job, see the *Quest NetVault Backup Administrator's Guide*.

Encrypting primary backup

To enable job-level encryption for a primary backup:

1. Start the Backup Job Wizard, and open the **Advanced Options** page.

   For more information, see the *Quest NetVault Backup Administrator's Guide*.
2. Click **Additional Options**.
3. In the **Additional Options** dialog box, select the **Enable Encryption** check box.

Encrypting a Secondary Copy

NetVault Backup offers the following methods for creating Secondary Copies:

- **Duplicate:** The Duplicate method creates an exact copy which is linked to the original backup. This method breaks down the backup into segments and copies the segments to the storage device. During restore, the segments from the primary backup and secondary copy are interchangeable. As it is not possible to mix unencrypted segments with encrypted segments during restore, you cannot enable or disable encryption for the Duplicate. If the original saveset is encrypted, the Duplicate method creates an encrypted copy. If the original saveset is not encrypted, this method creates an unencrypted copy.

- **Data Copy:** The Data Copy method breaks down the backup into segments and copies the segments to the backup device. During restore, either the primary backup or the secondary copy is used to recover data; the segments from the primary backup and secondary copy are not interchangeable. Therefore, it is possible to enable encryption for the Data Copy when the primary copy is unencrypted. This option is useful when you want to use the deduplication option for primary backups.

To enable job-level encryption for a Secondary Copy:

1 Start the Backup Job Wizard, and open the **Advanced Options** page.

For more information, see the *Quest NetVault Backup Administrator's Guide*.

2 Click **Secondary Copy**.

3 In the **Secondary Copy** dialog box, select the **Create Secondary Copy** check box.

4 Select the **Encrypt Secondary Copy Only** check box.

This option can only be used with the Data Copy method.

i **IMPORTANT:**

- If the primary copy is encrypted, the Data Copy method automatically creates an encrypted saveset whether you select the **Encrypt Secondary Copy Only** check box or not. Therefore, this option is only useful when you want to create an encrypted secondary copy from an unencrypted primary copy.
- Encrypted primary backups are not encrypted again if you select the **Encrypt Secondary Copy Only** check box for a Data Copy.
- To restore data from an encrypted Data Copy, you must use the primary copy's Encryption Key.

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.

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.