Rapid Recovery 6.2 Release Notes

April 2018

These release notes provide information about the Rapid Recovery release, build 6.2.0.17839.

Topics include:

About this release

Rapid Recovery software delivers fast backups with verified recovery for your VMs and physical servers, on-premises or remote. Rapid Recovery is software built for IT professionals who need a powerful, affordable, and easy-to-use backup, replication, and recovery solution that provides protection for servers and business-critical applications like Microsoft SQL Server, Oracle Database 12c, Microsoft Exchange, and Microsoft SharePoint. Using Rapid Recovery, you can continuously back up and protect all your critical data and applications from a single web-based management console.

Rapid Recovery release 6.2 is a minor release, with new features and enhancements. Support for some features, items, or related components have changed; see deprecations. As a minor release, defect fixes and known issues listed in this document are cumulative.

For information specific to other releases, see the release notes edition specific to the relevant release.

NOTE: The default view of the technical documentation website shows documentation for the most recent generally available version of the Rapid Recovery software. Using the filters at the top of the page, you can view documentation for a different software release or for a Quest DL series backup and recovery appliance. You can also filter the view by guide category.

Repository upgrade advisory

Upgrading the Core software to release 6.2 from any earlier version (for example, Rapid Recovery 6.1.x, 6.0x, or AppAssure 5.x) changes the structure of your DVM repository. The updates let you use new features in the latest release, such as application support for Oracle Database 12c, agentless protection, and so on.

After you change the structure of your DVM repository through an upgrade, you cannot downgrade the version of Core. Should you determine in the future that you want to use an earlier version of Core after upgrade to this release, you will need to archive the data in your repository. You could then uninstall the new version, re-install the older version, and then re-import the information manually from the archive, which can be a substantial effort.

Automatic Update advisory

Due to parameters introduced as part of GDPR compliance changes, customers using previous versions of Rapid Recovery will not be able to use the Automatic Update feature to upgrade to Rapid Recovery release 6.2. Customers can still manually upgrade to Rapid Recovery release 6.2. Once you have upgraded Core to release 6.2, future automatic updates will be unaffected.

Linux Agent advisory for release 6.2

At this time, the Rapid Recovery Agent version for release 6.2 is not yet available for Linux. If protecting Linux machines using Rapid Recovery 6.2 Core, please use Rapid Recovery Agent release 6.1.3.

For more information, see knowledge base article 251154, "Quest Rapid Recovery 6.2 Linux Agent Delayed."

When the 6.2 release for Linux Agent is issued, release notes will be updated, and the software will be made available on the Support website, Data Protection Portal, and the Rapid Recovery License Portal. Check for the latest version of release notes.

New system requirements documentation

For each software release, we review and update the system requirements for Rapid Recovery software and components. As of release 6.2, this information is now exclusively accessible in the new *Rapid Recovery System Requirements Guide*. Always refer to this document for the most current system requirements.

New commands and scripting documentation

Rapid Recovery lets administrators automate the administration and management of certain resources through the execution of commands and scripts. Two command line tools are included when you install Rapid Recovery Core: the Rapid Recovery Command Line Management utility (cmdutil.exe), and the Rapid Recovery PowerShell Module.

Administrators can also use PowerShell, Bourne shell or Bash scripting to extend or automate Rapid Recovery functionality. Supporting this capability, a small collection of sample scripts is included when you install Rapid Recovery Core.

In Rapid Recovery release 6.0 and 6.1, information about command line management tools and scripting appeared as appendices in the *Rapid Recovery User Guide.* For release 6.2, this information has been moved to a separate document, the *Rapid Recovery Commands and Scripting Reference Guide.* This document is available in English only.

Content differences between context-sensitive help and technical documentation

Rapid Recovery Core includes in-product context-sensitive help. Help topics are derived from the *Rapid Recovery User Guide.* To view help topics in a web browser, from the Rapid Recovery Core Console, click 

or  , and from the resulting drop-down menu, select **Help**.

In *Rapid Recovery release 6.2*, the "REST APIs" appendix appears only in the HTML and PDF versions of the *Rapid Recovery User Guide*. This topic, which describes how to download and work with Rapid Recovery REST APIs, does not appear in context-sensitive help.

Likewise, as in previous releases, the help topic "Third-party contributions" appears only in context-sensitive help, or from the **About** menu. This topic does not appear in HTML or PDF versions of the *Rapid Recovery User Guide.*

Compatibility between Kaseya VSA and Rapid Recovery Core

Kaseya Virtual System Administrator (VSA) is remote monitoring and management software used by IT professionals, including managed service providers. Quest provides a plug-in for Kaseya VSA users to help manage Rapid Recovery Cores from the Kaseya interface.

This release includes a new Rapid Recovery Add-on for Kaseya. If using Kaseya to manage your release 6.2 Core, you should upgrade to the 6.2 version of the Add-on. The Add-on is backward compatible (you can run the 6.2 Add-on with older versions of Rapid Recovery Core). The reverse is not true. The version of Core must not be later than the Add-on for Kaseya version.

For instructions on installing the Add-on, see the *Rapid Recovery Third-Party Integration Guide* for release 6.1.3. Other than structural changes to reference system requirements in their new location, that guide has not been updated for release 6.2.

Rapid Recovery release designations

Rapid Recovery release designations consist of up to four parts. Each part consists of a set of numerals separated by a decimal point.

- **Major releases** are specified by the first numeral. These releases include dramatic changes to UI, the repository, or application behavior.
- **Minor releases** are specified by the numeral following the first decimal point. If this number is greater than 0, it is part of a minor release. Minor releases introduce new functionality that is smaller in scope than the types of changes included in major releases.
- **Maintenance releases** are specified by the numeral following the second decimal point. If this number is greater than 0, it is a maintenance release. Maintenance releases correct previously identified defects or behaviors.
- **Build numbers** (typically between 3 and 5 digits) are specified by the fourth set of numerals. This part is used to differentiate versions of the software program generated during the development process.
    - For the Rapid Recovery Agent software, build numbers may differ between Windows and Linux versions. If the first three parts of the release number are identical, interoperability between the Core and Agent with different build numbers is not affected.
    - Updated builds of the same software release may be made available on to the Rapid Recovery License Portal within a release cycle. Therefore, if your Core is set to automatically update the Agent version on protected machines, you may see differences in build numbers for a single release. These differences will not negatively influence functionality.
    - Build numbers may also differ between software-only versions of the Core and the versions used on the Quest DL series backup and recovery appliances.
    - Build numbers will differ between the Core and the Add-on for Kaseya component.
    - Difference in build numbers does not affect replication when the Core has the same or a more recent build installed than the replicated target machine.

For release 6.2.0.17839, the first digit (6) is the major release. The second digit, if greater than 0, represents a minor release. The third digit, if greater than 0, indicates a maintenance release. The build number (17839) is last and is generally only referenced in release notes. The build number for this release is identical between Core and Windows Agents, and components such as the Local Mount Utility.

The Linux Agent for 6.2, when released, will have a higher build number. For more information, see Linux Agent advisory for release 6.2.

Support policy

The Rapid Recovery support policy is to provide technical support to customers with an active Support agreement for specific software versions under the following terms:

- Rapid Recovery software versions supported follow the **N-2 policy**.
  - **N** represents the major and minor release numbers (for example, 6.2, 6.1, 6.0, 5.4) of the most recent generally available software release. For more information about parsing a Rapid Recovery release number, see Rapid Recovery release designations,
  - **N - 1** refers to the most recent prior release, considering major and minor versions only. For example, in release 6.2, N-1 refers to release 6.1.
  - **N - 2** refers to the penultimate major/minor release. For example, in release 6.2, N-2 refers to release 6.0.
- For each release, some versions are eligible for full support; some for limited support; and for some versions, support is discontinued.
  - The current version (N) and the most recent maintenance release (N-1) are fully supported.
  - For N-2 (6.0), the latest maintenance release (6.0.2) is in limited support. Patches or fixes are not written for releases in limited support; however, once identified and confirmed, software defects can be expected to be corrected in the most recent version of the software.
  - Support for all other versions is discontinued.

    Quest Software strives to put resources behind the most recent product releases in order to continually improve and enhance the value of our products. Support for earlier maintenance releases is discontinued because viable, easy-to-upgrade alternatives are available. For example, users of release 6.1.0 can upgrade directly to release 6.1.3, which is fully supported. Users of 6.0.1 can upgrade to 6.0.2 (in limited support) or to 6.1.3 (in full support).
- Limited support can be offered to other versions by exception. As of the date of publication, no releases currently are supported by exception.

NOTE: To see definitions of full, limited and discontinued support, see our **Product Life Cycle** (PLC) page on the Support website as follows:

1. Navigate to https://support.quest.com/rapid-recovery/.
2. Click **Product Life Cycle & Policies**.
3. Scroll down to Product Support Policies and expand the link **Software Product Support Life Cycle Policy**.

New features

This section includes new features in Rapid Recovery release 6.2 (or features not previously described in technical product documentation).

Topics include:

- Core integration with the Quest Data Protection Portal
- General Data Protection Regulation compliance
- Oracle Database 12c application support
- Graceful shutdown and restart of Core services
- Support for shared Hyper-V virtual hard disks (VHDX)
- Support for Microsoft Scale-Out File Server with Hyper-V
- Application support for agentless protection
- Encrypting data in transport over a network
- Network resiliency improvements
- Restoring Exchange mail items from the Rapid Recovery Core Console

Core integration with the Quest Data Protection Portal

The new https://dataprotection.quest.com/dashboard lets you monitor and manage machines that use a selection of Quest software products, including Rapid Recovery, from any location with internet access. The web-based portal serves many functions and is currently accessible to Rapid Recovery users with a current maintenance agreement.

Features of the Data Protection Portal include the following:

- **Multiple Core management.** This portal lets you manage multiple Rapid Recovery Cores from a central location. You can organize these Cores into organizations and sub-organizations for easier management.

  NOTE: This portal replaces the functionality of the now-deprecated Central Management Console.

- **Machine monitoring.** You can also monitor the health, functionality, and connections of multiple Cores and their protected machines through a dashboard of widgets and a topology map. The map and its view of machine-level details uses animation to depict the communication happening between machines.
- **Reporting.** This portal offers an ever-evolving selection of reports that you can run on any and all of the connected machines. Options include a Backups report and a Utilization report .
- **Protection and replication management.** The Data Protection Portal also includes functionality that lets you pause and restart protection, start and stop the Rapid Recovery service, add repositories, and set up replication.
- **Quest product integration.** From this portal, you can also manage and access other Quest products used on your machines, such as Foglight.

Rapid Recovery Core includes optional integration between your Core (including its protected machines) and the Data Protection Portal. This integration is enabled by default, but can be disabled in Core general settings.

General Data Protection Regulation compliance

The General Data Protection Regulation (GDPR) is legislation crafted to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU, which makes it relevant to software manufacture in the US and other countries. It updates rules governing the handling of individuals' personal data. GDPR is being widely adopted throughout the software industry.

To comply with the GDPR, the collection of any personally identifiable information (PII) by Rapid Recovery has been carefully considered. Data collection has been streamlined, and the information collected and how it is used is clearly documented.

When installing the Rapid Recovery Core or running the Info Gathering Tool, you are provided a description of the information Rapid Recovery collects and our purposes for collecting the information.

If you accept the stated use of personal data, you can then associate a license (running in standard "phone-home" mode) with your Core. If you choose to decline the use of personal data described in the privacy policy, you must request a special "non-phone-home" license. After you receive that license and associate it with your Core, your PII will not be used, and certain functions (auto update, and enabling integration between the Core and the Data Protection Portal) are disabled.

Regardless of the privacy option you selected during installation, from the Core General setting **Agree to use of personal data**, you can change this setting. To switch between phone-home and non-phone-home modes in either direction, you must have access to the appropriate license.

For more information about the GDPR, see the EU General Data Protection Regulation website at http://www.eugdpr.org/eugdpr.org.html.

For more information about managing your privacy, see the following topics in the *Rapid Recovery User Guide*:

- Certain business rules apply when changing between phone-home and non-phone-home mode using the **Agree to use of personal data** General setting. For more information, see the topic "Configuring Core general settings."
- To see what information Rapid Recovery collects, in which circumstances, and why the information is collected, see "How Rapid Recovery uses personal information."
- To see what functions you cannot perform when using a non-phone-home license, see the topic "Non-phone-home license restrictions."
- To download a phone-home license, log into the Rapid Recovery License Portal. From the navigation menu, click **Licensing**, and from the drop-down menu on the top right, select **License Key.**
- To learn how to obtain a license in non-phone-home mode, see the topic "Obtaining and using non-phone-home keys."

Oracle Database 12c application support

Rapid Recovery release 6.2 expands application support to include Agent-based protection of Oracle 12c relational database servers. You can protect an Oracle database server and all of its databases, and perform related tasks.

In this release, the following restrictions apply:

- Oracle 12c is the only tested and supported version for protection on the Rapid Recovery Core. Use any other Oracle versions at your own risk.
- Protected Oracle database servers must run Windows Server 2012 R2 or later.
- You must install the Rapid Recovery Agent software (release 6.2 or later) on your Oracle server. Agentless protection is not supported for Oracle application support.
- Protection of Oracle12c databases is limited to using Volume Snapshot Service (VSS) in the ARCHIVELOG mode.

  NOTE: Oracle databases with ARCHIVELOG mode enabled must also be set to archive all online redo logs using the ARCH (archive) process. A database administrator (DBA) can change the mode and set archiving of redo logs using Oracle SQL*Plus or Oracle Enterprise Manager. For more information about enabling ARCHIVELOG mode and archiving, see Oracle documentation or consult a qualified Oracle 12c DBA.

  When an Oracle database is set to archive log mode, the logs can accumulate and consume substantial disk space. For this reason, you are able to truncate Oracle logs to reclaim disk space.

Setup includes protection of the database server, entering credentials for each database in the Core Console, enabling archive log mode in the Core Console, and verifying or enabling the Oracle VSS writer. For more information about adding an Oracle server to protection and properly configuring it, see the *Rapid Recovery User Guide* section "About protecting Oracle database servers."

Once you install the Agent, protect the machine in your Core, and configure settings properly, you can do the following:

- **View metadata.** From the protected machine **Summary** page, you can view metadata about each database on your Oracle server, including connection and status for each child log and transaction file.
- **Check database integrity.** You can perform integrity checks from the Core Console using the DBVERIFY utility.
- **Truncate archive logs**, using one of three deletion policies.
- **Restore databases.** Restore entire volumes, all databases or select databases. Once you enable Archive log mode, snapshots of the Oracle database are crash-consistent from the point of view of the Oracle service.
- **Perform virtual export.** You can make a one-time export, or set up a virtual standby VM that continually updates a VM with new information as backups on your protected database are captured.

  If you boot up a VM of an Oracle database, you may have to manually start the database services.

Graceful shutdown and restart of Core services

Invariably, a machine on which Rapid Recovery Core is running shuts down or must be rebooted. In release 6.2, Rapid Recovery Core is enhanced to improve its ability to gracefully shut down and restart Core services.

When an administrative user explicitly requests a soft reboot or shutdown of the Core server, Rapid Recovery Core delays the shutdown. During this pause, the user is notified of running Rapid Recovery tasks and can delay or cancel the shutdown. The user has the option to let specific application tasks complete, or explicitly pause or cancel tasks. If the user specified no action, Rapid Recovery automatically pauses running backup, replication, or archive tasks and terminates recovery or rollup tasks. All Core and related services are then gracefully terminated before the operating system shutdown or reboot completes.

In cases when planned maintenance of the Core server (including rebooting or restarting) is required, the Core UI now offers UI features to either restart or shut down the Core service with one click. Users receive notification when corresponding services are completely shut down. These features are accessed from the top of the Core Settings page. For more information about suspending or resuming the scheduler, see the *Rapid Recovery User Guide* topic "Restarting or shutting down the Core service."

On the **Tasks** page (reached from the Events icon), users can postpone all scheduled tasks on the Core that have not already started by clicking the **Suspend Scheduler** option. Only when the scheduler is suspended, you can resume task scheduling by clicking the **Resume Scheduler** option. You can choose to cancel running tasks, or just suspend new tasks. This feature suspends new tasks from scheduling on the Core until you explicitly resume the scheduler. For more information about suspending or resuming the scheduler, see the *Rapid Recovery User Guide* topic "Suspending or resuming scheduled tasks."

Supporting graceful shutdown and restart changes, threads and processes have been separated or grouped intentionally with performance in mind. Speed of recovery has been improved, in some cases dramatically. Improper Core shutdowns due to system crash, reboot, or sudden power loss are now substantially less disruptive to Core functionality.

Support for shared Hyper-V virtual hard disks (VHDX)

A Hyper-V virtual hard disk (VHDX) is a disk image file format used to create a virtual hard disk on Windows Server 2012 R2-based virtualization environments.

With this release, Rapid Recovery now supports shared VHDX on protected Hyper-V hosts running Windows Server 2012 R2 or Windows Server 2016.

Support for Microsoft Scale-Out File Server with Hyper-V

Scale-Out File Server (SOFS) is a Microsoft feature that, when enabled, provides scale-out file shares that are readily accessible for file-based server application storage. With this feature, multiple nodes from the same cluster can share one folder.

Rapid Recovery can now agentlesly protect VMs on a Hyper-V cluster with disks located on a SOFS. The Rapid Recovery Agent must be installed on each of the physical cluster nodes.

Rapid Recovery support for SOFS begins with Windows Server 2012 R2.

Application support for agentless protection

With this release, Rapid Recovery introduces the ability to protect and restore Microsoft Exchange and Microsoft SQL Server data agentlessly. Agentless protection applies to VMware ESXi and Microsoft Hyper-V virtual machines installed on Windows operating systems.

To protect a VM agentlessly, Rapid Recovery performs the following actions:

- Backs up metadata
- Performs Exchange mountability checks
- Performs Core-side SQL attachability checks
- Performs Exchange checksum checks
- Enables log truncation for SQL and for Exchange

  NOTE: Log truncation is supported starting on ESXi 6.5. Rapid Recovery performs log truncation as a single job, and does not truncate Exchange and SQL logs separately when both applications are installed on the same machine.

- Drive letter identification for the protected volume

CAUTION: For application protection, the VM must be powered on, and the Core server must have direct network access to the VM guest.

Encrypting data in transport over a network

Rapid Recovery Core release 6.2 includes a new encryption feature: you can now encrypt all data in transport over a network. Quest recommends enabling this encryption setting when data between your Core and protected

machines (or between two Cores such as for replication) must flow over the public or untrusted networks such as the internet.

The option is enabled by default when protecting a machine. While there is only a small performance cost involved in enabling this encryption, if your Cores and protected machines are within the confines of a private local area network, you can disable this option with confidence.

Network resiliency improvements

When network communication is lost briefly, queued or in-process Core jobs previously failed. Resiliency improvements in Rapid Recovery Core release 6.2 include re-try logic that adds resiliency to network operations. Backups, VM exports, and other jobs that cannot execute due to small temporary network outages are now re-tried for a five-minute period. If the network is available in that period, the operation commences, creating only a slight delay instead of a job failure and skipped operation.

Restoring Exchange mail items from the Rapid Recovery Core Console

Rapid Recovery now lets you recover Microsoft Exchange mail items, such as emails, calendar appointments, and contacts, directly from the Rapid Recovery Core Console. When an Exchange server is backed up in a recovery point, you no longer need to use a second application to retrieve its contents.

To begin an Exchange recovery, you must first open the location of the Exchange items using the Open Exchange Database wizard on the Mail Restore page, which is accessible from the More menu of the Core Console. The wizard lets you select the recovery point that contains the backup of the Exchange server.

After the database is open and connected to Rapid Recovery, you can go to the Mail Restore page of the Core Console, select the item that you want to recover, and then open the Email Restore Wizard. This wizard lets you select a destination for the recovered item, such as a recovery folder, the original location, or a PST file. From there, you can also select advanced options, including the ability to restore deleted items from Exchange 2007 (deprecated), 2010, 2013, and 2016 databases.

The new Mail Restore feature in Rapid Recovery is in addition to the mail restore capabilities of Mailbox Restore for Exchange.

Enhancements

This section lists enhancements implemented in Rapid Recovery release 6.2 (or enhancements not previously described in technical product documentation).

Topics include:

Improved reporting

From the Core Console, you can now generate a summary report, currently known as the Core Nostalgia Report.This report is available on demand, or based on a schedule, and provides a classic summary of information about your Core, using pie and trend charts and tables. This report provides a summary view of job statistics success, repository summaries by GB, snapshots success, repository usage trends, and a summary of protected machines on your Core.

For more information about report settings, see the *Rapid Recovery User Guide* topic "About Rapid Recovery reports." In that section, this report is described as the Classic summary report.

Additionally, new features are available in Core settings supporting the generation of reports. In addition to setting a default font for your reports, you can now establish a default paper size and page orientation. A wide range of paper sizes is supported.

The ability to specify larger paper sizes and page orientation increases flexibility and legibility of your report outputs. The default page orientation is landscape, since most reports are designed with several columns of output in mind.

For more information about report settings, see the *Rapid Recovery User Guide* topic "Managing report settings."

Enhanced support for vSphere/ESXi 6.5

Beginning with release 6.1, Rapid Recovery provided limited support for vSphere/ESXi 6.5, including the following functions:

- Protection of virtual machines on ESXi 6.5
- Replication of recovery points from ESXi 6.5
- Virtual export of recovery points to ESXi 6.5

Additionally, as of release 6.2, support for vSphere/ESXi 6.5 has been enhanced as described in the following points:

- In release 6.2, you can now export a virtual machine to vCenter/ESXi 6.5 even if the source machine uses the Secure Boot option. To use Secure Boot, the source Virtual Machine must have an Extensible Firmware Interface (EFI) system partition, and the target exported VM must be ESXi 6.5 or later.
- When protecting virtual machines agentlessly on ESXi 6.5, you can now protect encrypted VMs. Rapid Recovery release 6.2 now leverages the Virtual Disk Development Kit (VDDK) for vSphere 6.5, which supports encrypted VMs.
- When protecting virtual machines agentlessly on ESXi 6.5, transfer now works as intended even when the transport mode is set to SAN (storage area network).

Changes in SQL Server versions supported

New version supported.

Microsoft released SQL Server 2017 for general availability on October 2, 2017.

Rapid Recovery supports protection of machines with SQL Server 2017, including agent-based and agentless protection. This includes application support for SQL Server. Backup snapshots are application-aware, and SQL attachability is supported. DocRetriever for SharePoint release 6.2 also supports this version of SQL Server.

Old version deprecated.

End of life for SQL Server 2008 and 2008 R2 is July 9, 2019. Users are advised to move to a current version of SQL Server that is supported by both Microsoft and Quest in advance of that date.

Expanded archiving to Amazon S3, Amazon Glacier, and Google Cloud

As of release 6.2, Rapid Recovery has expanded its archiving capabilities to include three new cloud destinations: Amazon S3 storage classes, Amazon Glacier storage class, and Google Cloud.

An Amazon S3 storage account offers a variety of storage classes, with different costs, benefits, and access restrictions. The Standard class is intended for data that you plan to access frequently or quickly, and is the default storage option. The Standard Infrequent Access (IA) class is intended for data that you plan to access less often. The Reduced Redundancy Storage (RRS) storage class offers lower costs and is intended for noncritical reproducible data.

Also available for Amazon S3 accounts is the Glacier storage class, which is intended for long-term storage that does not require real-time access. There is no ability to select Glacier storage from your cloud accounts. Instead, to archive to a Glacier account, select your Amazon S3 cloud account, and then select **Use Glacier storage** as the Location option.

For more information about archiving to Amazon S3 storage accounts, see "Amazon storage options and archiving" in the *Rapid Recovery 6.2 User Guide*.

In addition to the Amazon S3 options, Rapid Recovery has also added Google Cloud as a supported cloud account.

As with archiving to any cloud account, you must first add the account to Rapid Recovery on the Cloud Accounts page in the Core Console. Only then will the account be available as a destination when you create or schedule an archive.

Simplified licensing model

Rapid Recovery has simplified the way it organizes licenses by consolidating multiple license pools into one pool. For more information, see "Managing licenses" in the *Rapid Recovery 6.2 User Guide*.

Changes in non-phone-home license format

The format of non-phone-home licenses was changed in Rapid Recovery release 6.2. Non-phone-home licenses issued in earlier releases are not compatible with release 6.2 and need to be replaced. The Rapid Recovery Core 6.2 installer detects this case, and prompts the user to obtain a new license key.

Contact the Quest licensing team to obtain a non-phone-home license. Details on filling out the Licensing Assistance web form are included in the *Rapid Recovery User Guide* topic "Obtaining and using non-phone-home licenses."

User interface enhancements

Rapid Recovery Core release 6.2 includes the following UI enhancements:

New color themes for Core Console

The familiar color scheme used in previous versions comprises the Hybrid theme, and is the default theme setting for new installations or upgrades. Newer themes feature color elements that follow UI color standards for Quest Software applications.

Supported color themes are described as follows:

- **Dark**. This theme features a solid dark gray background throughout the interface (left navigation menu, top button bar, and primary pane). Text elements and text buttons not in focus appear in off-white, or white when in focus. Clickable links appear in a medium blue. Occasional buttons have white text over a medium blue background.
- **Hybrid**. This theme features the familiar dark gray background for the left navigation menu and button bar at the top of the Core Console. Text elements in these areas are white. The primary pane has a white background with off-white highlights, with text elements and text buttons in black. Clickable links appear in a dark blue. Occasional buttons have white text over a blue background.
- **Light**. This theme features a clean white background throughout the interface (left navigation menu, top button bar, and primary pane). The Quest logo and some design elements are orange. Text elements are dark gray, with titles in black. Clickable links appear medium blue on hover. Occasional buttons have white text over a medium blue background.

To select and apply a color theme on the **Settings** page of the Core Console, from the **Theme** drop-down, select a theme, and confirm by selecting the ✔ check mark. For more information, see the topic "Configuring Core general settings" in the *Rapid Recovery User Guide*.

Filter recovery points by date range

When viewing recovery points for a protected machine, virtual machine, or VM host, you can now filter recovery points by date range. This ability also applies to recovery points-only machines.

When you select a protected machine in the Core Console, the **Summary** page appears. Click **Recovery Points** to view the existing recovery points for the selected machine. In the Recovery Points table, underneath the titles, there are new **From** and **To** text fields, with associated calendar widgets. If you want to filter the view of recovery points appearing in the table, enter start and end dates in these fields. To clear the filter, click the **X** in the relevant filter text field.

Protect Cluster Wizard connection improvement

In the past, when you selected **Protect Cluster** from the button bar's Protect Machine drop-down menu, a **Connect to Cluster** dialog box appeared. After defining connection information and clicking **Connect**, the Protect Cluster Wizard opened. Using that wizard, you could then protect a supported DAG cluster or Windows Server 2008 R2 CSV.

The Protect Cluster Wizard now includes connection information, and is launched when you select **Protect Cluster**. This UI improvement brings consistency to the machine, cluster, and cluster node protection experience. This updated wizard also incorporates new options such as encryption over the network.

For more information or specific details, see the topic "Protecting a cluster" in the *Rapid Recovery User Guide*.

Replication Target available in Azure Government Marketplace

Beginning with release 6.1.2, Rapid Recovery Replication Target is available to users of the Azure Government cloud computing platform. Azure Government users who have an on-premises installation of Rapid Recovery Core can now select the "Rapid Recovery Replication Target" from the Azure Government marketplace. Using this VM, Azure compute services, and storage that you add to the VM for your repository, users can quickly and easily set up a target Core that replicates your on-premises backup data in the Azure Government cloud. This lets you take advantage of the simplicity, security, and redundancy offered by Microsoft's cloud computing platform.

This is the identical product available to public users of the Azure platform.

The VM uses a fully patched Windows Server 2016 OS and comes with simple-to-use scripts that set up your VM in minutes. For information about replicating to Azure, see the *Rapid Recovery Replication Target for Microsoft Azure Setup Guide*.

Support for archiving to AWS GovCloud US and other S3-compatible cloud accounts

Amazon Web Services offers a service called AWS GovCloud (US). This is an isolated AWS region designed to meet specific regulatory and compliance requirements, thus letting United States government agencies and customers join private businesses in leveraging cloud accounts.

Beginning with release 6.1.2, Rapid Recovery fully supports archive of recovery points to Simple Storage Service (S3) cloud accounts on AWS GovCloud. Quest also provides limited support for other S3-compatible cloud storage accounts for archiving.

When defining cloud accounts in the Rapid Recovery Core Console, for **Cloud type**, select **Amazon S3**, and enter a fully qualified URL into the **Service endpoint** field to define and cache your account credentials.

DocRetriever for SharePoint enhancements

DocRetriever for SharePoint is a separately installed component that accompanies Rapid Recovery Core. If you protect one or more SharePoint front end web servers in your Core, DocRetriever provides additional recovery options. Using the DocRetriever Console, DocRetriever for SharePoint lets SharePoint administrators recover SharePoint objects from the site collection level down to the component level.

The following enhancements have been added to DocRetriever release 6.2.

- **Restore job history**. You can view the history of previous restores performed of SharePoint data using DocRetriever Console. Once you select a restore job in the "Jobs list" tab, you can drill down to its details

in the "Job restore actions" and "Job restore parameters" tabs. This previously existing feature is now documented in the *DocRetriever for SharePoint User Guide*.

- **Restore improvements**. DR Console now has the ability to display and restore system items, including web part templates, site themes, master pages, views, forms, list items, and files in the DR "Associated Files" folder that are not associated with a list. Also, more properties for a SharePoint object can now be restored—for example, a site's welcome page link.
- **Additional metadata**. The DR Console offers the ability to display more properties. For example, in Settings, you can control display of system items. If set to display, then from the tree view or the list, when viewing attributes, you can see if an item is a system item. The same function is available for hidden items when they are set to display. Title bars for the DocRetriever Console now display additional information such as the SQL database instance being used. The status bar at the bottom of the DR console now shows item counts or other attributes of selected items, and the SharePoint version being used.
- **Updated settings**. Restore settings for the DocRetriever Console have been moved from the Settings dialog box to the Windows registry. Restore settings (such as duplicate actions, container actions, object types to be included in the restore, and restore direction) from any restore are now cached to be the default settings for the subsequent restore. For any restore of SharePoint data, the default settings can be customized to serve your needs. Other settings are also stored in the Windows registry, such as SQL Server settings that include command timeouts (in seconds), and recent recovery sources.
- **Code optimizations**. Code optimizations improve performance, letting some restore operations occur concurrently. Error handling has also been improved.

For more information about this component, see the *DocRetriever for SharePoint User Guide*.

Additional Linux operating systems supported

The following Linux operating system distributions are now supported:

- Version 6.9 is supported for CentOS Linux, Red Hat Enterprise Linux, and Oracle Linux.
- Version 9 is now supported for Debian Linux.
- Version 17.04 LTS is now supported for Ubuntu Linux.
- Versions 12 SP1 and 12 SP2 of SUSE Linux Enterprise Server (SLES) are now supported.

Deprecated in this release

This section includes a list of features, items, or related components that are deprecated in Rapid Recovery release 6.2.

Topics include:

Central Management Console deprecated

Rapid Recovery release 6.2 includes the production rollout of the Data Protection Portal. This feature, particularly useful for managed service providers, lets you manage multiple Cores; access a dashboard where you can monitor tasks and events, view repository status, and check system health; generate reports; and perform a growing list of other functions from a single web-based user interface. This new web-based portal is currently accessible to Rapid Recovery users with a current maintenance agreement. Its ability to manage multiple Rapid Recovery Cores from a central location replaces the functionality of the now-deprecated Central Management Console.

If you manage two or more Cores in release 6.2, Quest recommends that you migrate to the Data Protection Portal. Only the new portal is supported for management of release 6.2 Cores.

As of release 6.2, the Central Management Console is now in limited support only. Topics related to the Central Management Console have been removed from technical documentation. If you are no longer using this component, as a best practice, Quest recommends uninstalling the Central Management Console.

In Rapid Recovery Core release 6.2, the **Data Protection Portal** Core setting lets you enable or disable connection with the portal.

Integration between the Rapid Recovery Core Console and the Data Protection Portal is enabled by default. To view the current connection setting, disable, or enable the connection for any Core, navigate to Settings in the Core Console and view or change the **Data Protection Portal** configuration.

If using a Core version older than release 6.2, you must download a plug-in that lets your Core connect to the portal. When you log in to the Data Protection Portal from any Core server, you can download and install the appropriate plug-in for your Core version. The plug-in lets you manage multiple Cores, and is backward compatible with currently supported versions of Rapid Recovery Core.

For more information about the Data Protection Portal, see in-product help for the Data Protection Portal.

Synchronous replication no longer supported

Earlier versions of this product (prior to AppAssure 5.4.1) supported only synchronous replication, in which there was a single retention policy between source and target Cores. Asynchronous replication mode—the capability to support disparate retention policies—was introduced in release 5.4.3, and has been the standard for every release since. The old mode was deprecated.

As of Rapid Recovery release 6.2, support for the old synchronous replication mode is discontinued. When upgrading earlier releases, the Core installer checks a registry key to verify if a DVM repository integrity check is required. If so, you are notified that you must perform an integrity check. This check is only required if your DVM repository was created prior to release 5.4.1, if you used replication at that time, and if the integrity check was not previously performed.

NOTE: If you are prompted to run an integrity check, be aware that this job is expected to take an extended period of time. The amount of time differs based on the amount and type of data in your repository, and on the underlying storage system. While the job is running, no other transactions can be performed in that repository, including transfers (snapshot and base image backups, and replication), nightly jobs, and so on. You can perform other operations in other repositories while this job is running.

For more information, see the *Rapid Recovery User Guide* topic "About checking the integrity of DVM Repositories." For details on manually performing the integrity check, see the procedure for "Performing an integrity check on a legacy DVM repository."

Operating system support changes

Rapid Recovery release 6.2 includes upgrades of the .NET framework from version 4.5.2 to version 4.6.2. Additionally, support has been added in release 6.2 for Secure Hash Algorithm 2 (SHA2). This certificate security protocol is stronger and generates a longer hash, and is used for Rapid Recovery drivers. Because of these incremental improvements, and because of required libraries and binary limitations, older Windows versions that do not fully support these requirements are no longer supported as of Rapid Recovery release 6.2.

The changes in OS support are documented below. For a full list of operating systems and the Rapid Recovery components supported for each, refer to the *Rapid Recovery System Requirements Guide* topic "Rapid Recovery release 6.2 operating system installation and compatibility matrix."

If you currently protect machines with an operating system that is no longer supported, you have two options:

1. You can upgrade the OS on the machines you want to protect to a supported OS, then upgrade Rapid Recovery Agent to release 6.2 and continue to protect the machine on your release 6.2 Core.
2. You can protect the machine on a release 6.2 Core using an older but supported version of Rapid Recovery Agent (such as 6.1.3). Of course, in such cases, new release 6.2 features are not available for that protected machine and are not supported.

The following Windows operating system support changes apply to Rapid Recovery release 6.2:

- **Windows XP.** As in release 6.1.3, Core and Agent are not supported for machines running this OS. Rapid Recovery now no longer supports agentless protection or URC restore for machines with this OS.
- **Windows Vista.** As in release 6.1.3, Core and Agent are not supported for machines running this OS. Rapid Recovery now no longer supports agentless protection or URC restore for machines with this OS. This OS is not supported.
- **Windows Vista SP2.** As in release 6.1.3, Core is not supported for machines running this OS. Rapid Recovery now no longer supports protection for machines with this OS using Agent or agentless. LMU, Mailbox Restore, and DocRetriever for SharePoint are no longer supported on this OS.
- **Windows 7.** As in release 6.1.3, Core and Agent are not supported for machines running this OS. Support for this operating system is discontinued. Rapid Recovery no longer supports agentless protection, URC restore or URC driver injection for machines with this OS.
- **Windows 7 SP1.** Core and Agent are no longer supported for machines running this OS with Service Pack 1. LMU, Mailbox Restore, and DocRetriever for SharePoint are no longer supported on this OS. Limited

support is provided only for agentless protection, URC restore, and VM export to Azure, which works only for 64-bit installations.

- **Windows 8.** Core and Agent are no longer supported for this OS. Limited support is provided only for agentless protection, URC restore, and VM export to Azure (which works only for 64-bit installations).
- **Windows 8.1.** Core is supported for this OS . Agent and agentless protection support continues. VM export to Azure works only for 64-bit installations.
- **Windows 10.** Core is supported for this OS . Agent and agentless protection support continues. The previous incompatibility with virtual exported to VirtualBox (in which SCSI controller drivers were missing for Windows 10) has been corrected. VM export to Azure works only for 64-bit installations.
- **Windows Server 2003.** As in release 6.1.3, Core and Agent are not supported for machines running this OS. Support for agentless protection for VMs with this operating system is limited, as is URC restore. No other aspects of this OS are supported.
- **Windows Server 2008.** As in release 6.1.3, Core and Agent are not supported for machines running this OS. Support for agentless protection for VMs with this operating system is limited, as is URC restore. VM export to Azure works only for 64-bit installations.
- **Windows Server 2008 SP2.** Core and Agent are no longer supported for machines running this OS. Support for agentless protection for VMs with this operating system is now limited, as is URC restore. VM export to Azure works only for 64-bit installations.
- **Windows Server 2008 R2.** As in release 6.1.3, Core and Agent are not supported for machines running this OS. Support for agentless protection for VMs with this operating system is now limited, as is URC restore. URC driver injection is no longer supported. VM export to Azure works only for 64-bit installations.
- **Windows Server 2008 R2 SP1.** Core is supported for this OS, provided you follow guidance in Microsoft KB 3033929. Silent installation of Core is not supported. Agent and agentless protection are supported on this OS. VM export to Azure works only for 64-bit installations.
- **Windows Server 2012.** Core, Agent, and agentless protection are supported on this OS . VM export to Azure works only for 64-bit installations.
- **Windows Server 2012 R2.** Core, Agent, and agentless protection are supported on this OS. VM export to Azure works only for 64-bit installations.
- **Windows Server 2016.** Core, Agent, and agentless protection are supported on this OS. VM export to Azure works only for 64-bit installations.

The following Linux operating system support changes apply to Rapid Recovery release 6.2:

- **Ubuntu Linux 12.04 LTS, 12.10, 13.04, 13.10, 14.10, 15.04, 15.10.** These OS distributions have reached end of life, and are therefore no longer tested. Agent, Agentless, and Live DVD support for these OS is therefore limited.

Hypervisor support changes

For interoperability with Rapid Recovery, users are advised that Quest support for hypervisors, operating systems, and other software generally ends for a specific version when its publisher determines it has reached end of life (EOL).

Microsoft .NET Framework 4.6.2 cannot be installed on Windows Server 2008 SP2. As a result, virtual export to Windows Server 2008 SP2 is no longer supported. The table in the System Requirements Guide listing Hypervisor requirements supporting virtual export has been updated accordingly.

Oracle no longer supports VirtualBox versions 4.x or version 5.0. Accordingly, in release 6.2, Rapid Recovery support for VirtualBox begins with version 5.1. If trying to perform virtual export to this hypervisor target, upgrade to VirtualBox version 5.1 or later.

Rapid Recovery now supports virtual export to vCenter/ESXi 6.5 if the source machine uses the Secure Boot option.

Exchange Server 2007 deprecated

In April of 2017, Microsoft Exchange Server 2007 reached end of life. Microsoft no longer supports that version of Exchange Server.

Accordingly, Rapid Recovery support of Exchange 2007 is deprecated. In Rapid Recovery release 6.2, only limited support is provided for Exchange 2007. If customers encounter issues, Quest Data Protection Support will apply their best effort to provide known work-arounds or fixes. However, no coding effort will be applied to issues discovered in Exchange 2007 in relation to our software.

Quest recommends migrating to newer, supported versions of Exchange if you want to continue protecting your data using Rapid Recovery.

Application support changes

The following application support changes apply to Rapid Recovery release 6.2:

- SharePoint Server 2007 reached end of life on October 10, 2017, and is therefore no longer tested or supported with our product. While Rapid Recovery may work with 64-bit versions of SharePoint 2007, that version of SharePoint is no longer supported. Accordingly, references to this SharePoint version have been removed from the *DocRetriever for SharePoint User Guide*.
- As indicated in Exchange Server 2007 deprecated, support for Exchange Server 2007 is deprecated. Only limited support is provided for Exchange 2007 (x64). 32-bit versions are not supported.
- Rapid Recovery no longer supports VMware vSphere on ESXi 5.0 and 5.1. Support continues for ESXi 5.5, 6.0, and 6.5.
- As indicated in Oracle Database 12c application support, Rapid Recovery now includes application support for Oracle 12c database servers with Rapid Recovery Agent installed. Agentless application support is planned for a future release.
- As noted in Hypervisor support changes, due to EOL, Rapid Recovery no longer supports virtual export with VirtualBox versions 4.x or version 5.0. Use version 5.1 or later.

Tiering repository feature deprecated

A tiering repository is a secondary repository defined on your Core into which recovery points can be relocated from a primary DVM repository. Once they are moved, recovery points are deleted from your primary DVM repository. The Core continues to manage the relocated recovery points until they are eventually rolled up and deleted.

In release 6.2, tiering is only supported on DR Series deduplication appliances running OS 4.0. The repository requires RDS services native to the DR appliance.

The tiering feature, supported in releases 6.1 and 6.2 only, is deprecated. This feature is not expected to be included in future releases.

Resolved issues

Customer-facing issues resolved in this release are listed below.

Table 1. Core and Windows resolved issues

Resolved Issue Description	Issue ID	Functional Area
Sometimes the Core failed to restore the configuration for some services during the remount volumes job that occurred after a factory reset, but the remount volumes job showed as successfully completed.	104043	Core
	103813	RRT
In the Spanish UI, agentless virtual machines did not appear on the virtual machines tab in the Spanish interface.	103782	Localization
In the Korean UI, there was no ability to boot from a RASR USB flash drive due to invalid information in the BCD file (0xc0000098).	103775	Localization
The Agent service crashes when trying to collect cluster SQL metadata of a database with the FileAttributes.ReparsePoint attribute.	103740	Agent
The status of a virtual machine exported to ESXi appears as "Disabled" or "Stopped" after editing the export configuration, which is expected.	103704	ESXi
Replication started outside of the scheduled time if the job was added to the queue.	103702	Replication
Restoring ReFS volumes did not work on Windows Server 2016.	103698	Restore
There was no ability to add a cloud account for Azure Government.	103683	Azure
Core performance got worse and used a lot of system resources while mounting a recovery point from an attached Azure archive.	103670	Azure
A connection to the MongoDB reporting database cannot be established due to insufficient free ports, which is expected.	103664	Reports
Restoring a Core configuration with a configuration backup file of a previous Core was not restricted.	103632	Core
A machine with a root on a RAID volume didn't boot after a successful export.	103558	Export
	103556	RRT
The limitation for the maximum concurrent exports did not work correctly after specific steps.	103515	Core
The error "Placeholder mismatch with format string [Checking volume images by read {0} on {1} recovery point {2}] and arguments ..." appeared while performing an integrity check on a DVM repository, even though the check was successful.	103492	Repository
Resizing the Dedup Cache failed with the error "cache_io_engine: windows error 87" if the Dedup Cache was located on a disk with a sector size of 4 KB.	103469	Repository

Resolved Issue Description	Issue ID	Functional Area
When protecting a vCenter virtual machine, agentless protections fails with the error "An item with the same key has already been added."	103426	Agentless protection
A Core localized in Brazilian Portuguese failed to communicate with the License Portal, because the string was not recognized as a valid DateTime.	103371	Localization
While protecting a machine agentlessly, if the maximum number of permitted snapshots was exceeded, an incorrect error message displayed.	103334	Agentless protection
A transfer failed because there are no retries present on the CleanupSnapshotInternal stage, which is as designed.	103310	Transfers
There was a logic issue with the option "Include only the recovery in the date range..." when this option was used for a scheduled archive.	103283	Archiving
Sometimes the export postprocessing step took a lot of time, because there was incorrect dismount logic in the driver.	102742	Export
Sometimes there was no ability to protect a second cluster that had the same hostname as the first cluster, even though it was from a different domain.	102702	Protection
Incremental and Virtual Standby Hyper-V exports failed if the location or name for the exported virtual machine contained Chinese symbols.	102589	Localization
The warning "VSS full snapshot was taken with excluded VSS writers 'Microsoft Exchange Writer has state'" appeared about a non-existing writer on a protected machine (SQL or Exchange, depending on the instance installed) during log truncation.	102567	Protection
Incremental snapshots were slow for volumes with specific write activity.	102493	Protection
Deferred delete canceled after a rollup job on French operating systems.	102436	Localization
After an upgrade to 6.1.2, repository maintenance failed after restoring the provisioning configuration.	102340	Upgrade
After several days, the AAFileFilter driver caused a blue screen to appear on a Hyper-V cluster running Windows Server 2012 R2 or Windows Server 2016.	102232	Agentless protection, server cluster, driver
A seed drive job automatically canceled due to a NullReferenceException.	101617	Seed drive
On Windows 2016, some drivers were blocked during an installation of the Agent software with the "Secure boot" option enabled.	101573	Agent installation
The VMwareProxy service crashed due to TCP/IP port exhaustion.	101485	VMware proxy
A remount job did not restore the locale of a Core.	101316	Localization

Resolved Issue Description	Issue ID	Functional Area
If a letter was assigned to a Recovery partition, the status of the volume displayed as "Not valid."	101224	
On a system test environment, ESXi virtual standby failed with the error "An entry with the same key already exists."	100868	ESXi
The VMM actions were available while the ESXi host was in maintenance mode.	35740	ESXi
There was an incorrect validation for the "Maximimum connection pooling size" and the "Minimum connection pooling size" fields for the MongoDB connection.	35607	Reports
A base image was taken when the NTFS Boot Sector copy changed.	34981	NTFS
Virtual disk provisioning failed with Return Code 4 if the storage pool did not consistently have empty space, which is as designed.	34937	Virtual machines
Unexpected base images were taken of the ESX(i) virtual machines that had snapshots with quiescing enabled.	34916	ESXi
The Virtual Standby tab performance was slow.	34434	Exporting
The warning message "Information about allocated space for some volumes is unavailable..." appeared on the Summary tab for a protected virtual machine (VM) if that VM was located on an NFS datastore.	33551	Virtual machines
All running archive jobs failed with the error "There is not enough space on the disk" if more than one archive job was in progress at the moment when the target network storage ran out of space.	31827	Archiving
Rollback or export using SAN transport mode failed because one of the parameters had an invalid error in ESXi.	29508	Agentless

Table 2. DL appliance resolved issues

Resolved Issue Description	Issue ID	Functional Area
On a DL1000, sometimes launching FTBU would hang on the splash screen after a required reboot of the server during a configuration using the first wizard.	105114	FTBU
Some ESXi export jobs failed with the error "VddkApiException: You do not have access rights to this file."	105029	ESXi
If one of the physical disks on a DL1300 or DL1000 was offline, the FTBU would hang after the first wizard on the "Applying Settings ..." window.	103699	FTBU
On a DL1300 or DL4300 with FI#3.2.55, the ApplianceProvisioningConfiguration.xml file was present on the RECOVERY partition after configuring FTBU.	103389	FTBU
Sometimes the message "Internal Server Error" appeared on the Backup tab.	102379	RASR

Resolved Issue Description	Issue ID	Functional Area
Jobs failed with the error "System.OutofMemoryException" on DL appliances after running for a period of time, which is as designed.	101246	Jobs
If a letter was assigned to a Recovery partition, the status of the volume displayed as "Not valid."	101224	Provisioning
Windows Backup could not be created because the necessary volume items for a backup could not be determined if the volume letters were changed.	100985	Windows Backup
If Windows Backup was forced on a server with old Winbackups of a 75 GB volume with no free space on the internal controller, the main appliance status was red and could not be resolved.	100887	Windows Backup
A restore of the provisioning configuration job failed with the uninformative error "Cannot mount volume to the folder 'I:\' because it contains files or folders," if the virtual disk has a letter that was already used before the remount.	35805	Provisioning
The behavior of the logic used to determine the provisioning size was incorrect.	35770	Provisioning
The GUI was not disabled immediately after confirming the remount process.	35579	Provisioning
The Start VM and Start Network Adapters buttons were not disabled when an ESXi or Hyper-V export of a machine was launched.	30989	Exporting

Table 3. DocRetriever resolved issues

Resolved Issue Description	Issue ID	Functional Area
DocRetriever failed to retrieve SharePoint hierarchy if a web application's port contained an extra space character.	105749	Restore
An incorrect username was displayed in the "Modified by" and "Modified" columns after restore of a file uploaded by another user. The file now shows the original username after restore.	105101	Restore
DocRetriever failed to open a SharePoint 2016 database with several sites that had similar IDs.	103710	SharePoint
DocRetriever did not restore "Content Editor" web parts in SharePoint 2013.	103241	Restore
The DocRetriever Agent did not work (all restore operations failed) on a machine with MOSS 2007 32-bit installed. Corrected for 6.1.2 and 6.1.3. 32-bit versions are no longer supported.	102522	Restore

Table 4. Documentation resolved issues

Known Issue Description	Issue ID	Functional Area
The components ANTLR 3.3.3 and ANTLR 4.0.2 previously appeared in the "Third-party contributions" topic found only within in-product help. These	104031	Context-sensitive help

Known Issue Description	Issue ID	Functional Area
versions were not used in Rapid Recovery 6.1.3 and have been removed. The 6.2 version references ANTLR 3.4 and 4.0.2.		
The component MongoDB 2.6 previously appeared in the "Third-party contributions" topic, even though it was not used in Rapid Recovery 6.1.3. For 6.2, the listing is updated to reference MongoDB 2.6.11.	104030	Context-sensitive help
The component Microsoft Windows Azure Storage 7.2.1 did not appear in the 6.1.3 third-party contributions topic. 6.2 uses version 8.2.0, which is included in the list.	102504	Context-sensitive help
The component DataGridViewImageAnimator 1.0 appeared in the 6.1.3 third-party contributions topic, even though it was not used in Rapid Recovery 6.1.3 and is no longer used. It has been removed in the current list.	102503	Context-sensitive help
The component SimpleRestServices 1.3.0.3 did not appear in the list of third-party contributions, whereas an outdated version had appeared. This version is included in the current list.	102502	Context-sensitive help
The component OpenStack.NET 1.4.0.2 did not appear in the list of third-party contributions, whereas an outdated version of the component appeared in its place. This version is included in the current list.	102501	Context-sensitive help
The component NLog 3.2.1 did not appear in the list of third-party contributions, whereas an outdated version of the component appeared in its place. The current list references version 4.4.1.2, which is used in release 6.2.	102500	Context-sensitive help
The component AWS SDK for .NET 3.3.1.2 did not appear in the list of third-party contributions, whereas an outdated version of the component appeared in its place. The current list references this version.	102499	Context-sensitive help

Table 5. Linux resolved issues in release 6.1.3.527

Resolved Issue Description	Issue ID	Functional Area
There was no ability to support LVM-based storage pools.	103488	LVM
Transfers from a Core failed on SLES 11.4 x32 with the following error: "The partition size is incorrect, please shrink the volume."	103300	SLES
There was an ability to select Linux system folders for a rollback restore, even though restoring to a system folder is not supported.	103178	Restore
The Agent service could not be started if it was installed on a machine that did not use the default init system, which is as designed.	35818	Agent
Specific volumes could not be mounted after the export of a Linux machine.	35288	Export

Table 6. Mailbox Restore resolved issues

Resolved Issue Description	Issue ID	Functional Area
MailboxRestore failed to perform restore to original location on specific environment due to wrong flags passed into OpenMsgStore MAPI method.	105755	Restore
Public folder permissions were not restored for empty folders.	105267	Restore
After opening an Exchange 2016 CU5 database in Mailbox restore, the Inbox folder was missing in some mailboxes.	104334	Restore
A security alert dialog did not display during a restore when the Exchange server used a self-signed certificate.	102765	Restore
A non-informative error message appears if the user was not found in GAL during a restore of permissions for a public folder.	102018	Restore

Known issues

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

Table 7. Core and Windows known issues

Known Issue Description	Issue ID	Functional Area
Unexpected base images occur for cloned disks during Hyper-V agentless transfers. **Workaround:** None.	106296	Hyper-V
The New License and Privacy Policy parameters are not rewritten during a Core installation if the Core was previously uninstalled without configurations. **Workaround:** In the Settings of the Core Console, set the Privacy Policy and License settings.	106243	Configuration
An export to Amazon EC2 fails if the Amazon account has few subnets. **Workaround:** None.	106107	Exporting
The custom retention policy for a virtual machine on a Hyper-V cluster is not saved and rollup does not perform. **Workaround:** Add the retention policy to the Nightly Jobs in the Core settings.	106088	Retention policy
There is no ability to deploy and protect the machines if an older version of the Agent (release 5.4.3, 6.0.1, or 6.0.2) is installed on the Hyper-V server and you raise an error: "Unexpected end of file." **Workaround:** Manually upgrade the Agent on the Hyper-V server to release 6.2.	105500	Hyper-V agentless
The Trustedinstaller process is called during every metadata request.	105445	Metadata

Known Issue Description	Issue ID	Functional Area
Workaround: None.		
The RapidRecoveryCore service is deleted during an upgrade of the Core if any Microsoft Management Console (MMC) windows are open. **Workaround:** Close all MMC windows before you begin upgrading the Core.	105282	Upgrade
In a specific case, replication fails to start with an "incorrect RPFS file size" error. **Workaround:** None.	105048	Replication
Agentless backups fail with the error "Invalid URI: The hostname could not be parsed" when the shadow copy has the path "\\?\Volume{fb3687e7-57b5-11e7-80c4-f48e38cee0fd}\diskc.vhdx."	104393	Agentless
After an upgrade from release 5.4.3 to release 6.1, all task events convert to service events. **Workaround:** None.	103945	Upgrading
On specific environments, the Core GUI launch after an upgrade from release 6.1.1 to release 6.1.2. **Workaround:** Complete the following steps: 1. Stop the Core service. 2. Go to C:\Program Files\AppRecovery\Core\CoreService\coreadmin and open the Web.config file in Notepad. 3. In the file, change the value localhost <add key="CoreHostName" value="localhost" /> to the hostname (<add key="CoreHostName" value="charon" />). 4. In the same file, turn inmemory hosting on by finding <add key="InMemoryHosting" value="false" /> and changing the value to "true" (<add key="InMemoryHosting" value="true" />). **NOTE:** In release 6.1.1, inmemory hosting was turned on by default, but beginning with release 6.1.2, it is turned off. 5. Restart the Core service.	103783	Upgrading
If the Quest NetVault Backup with BMR plugin is installed on the same server as the Rapid Recovery Core, then ESXi exports fail. **Workaround:** Copy the following DLLs from Coreservice\vddk\bin to the Coreservice folder: • glib-2.0 • gobject-2.0 • gvmomi • iconv • intl • libcurl • libxml2 • vixDiskLibVim	103477	Virtual exports

Known Issue Description	Issue ID	Functional Area
Restart the Core service.		
If the Core has more than 100 virtual machines under protection, it is not possible to protect an ESXi virtual machine agentlessly due to a timeout error in the wizard. **Workaround:** Increase the .\CoreVMwarePRoxyService\ConnectionTimeout to 10 minutes.	102893	Agentless
A deploy to Azure fails if the cloud service name is specified in FQDN format. **Workaround:** Specify the service name in the format - just hostname.	102756	Azure
Drive letters are not assigned on an exported machine that is identical to the original machine. **Workaround:** Contact Support for a script to run on the exported machine that solves the issue.	102390	Virtual exports
An unclear error message appears for an ESXi export with auto disk mapping. **Workaround:** None.	27309	Virtual export

Table 8. DL Appliance known issues

Known Issue Description	Issue ID	Functional Area
The wrong translation appears in the German version of the Items Backed Up table on the **Backup** page. Future versions will be corrected. **Workaround:** In the first column, the intended label is "der Zustand" instead of "Bundesland."	35031	Localization

Table 9. Documentation known issues

Known Issue Description	Issue ID	Functional Area
The license/copyright for the third-party component python minimal 2.7.7 does not appear in the list of third-party contributions in the product. **Workaround:** The python minimal 2.7.7 component uses the Python 2.7 license, which is available at http://www.quest.com/legal/license-agreements.aspx. The component includes the following copyrights: • Copyright 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2014 Python Software Foundation; All Rights Reserved • Copyright 1995-2001 Corporation for National Research Initiatives; All Rights Reserved • Copyright 1991 - 1995, Stichting Mathematisch Centrum Amsterdam, The Netherlands. All rights reserved.	106842	3PC
The license/copyright for the third-party component openssh-server 1.7.2 does not appear in the list of third-party contributions in the product.	106841	3PC

Known Issue Description	Issue ID	Functional Area
Workaround: The openssh-server 1.7.2 component uses the OpenBSD 1.19 license, which is available at http://www.quest.com/legal/license-agreements.aspx. The component includes the following copyrights: • Copyright 1995 Tatu Ylonen , Espoo, Finland • Copyright 1998 CORE SDI S.A., Buenos Aires, Argentina • Copyright 1996 David Mazieres • Copyright 1995 The Regents of the University of California. • Copyright Markus Friedl, Theo de Raadt, Niels Provos, Dug Song, Aaron Campbell, Damien Miller,Kevin Steves, Daniel Kouril, Wesley Griffin, Per Allansson, Nils Nordman, Simon Wilkinson. All rights reserved.		
A change was introduced in Rapid Recovery Core after documentation was published and translated related to log truncation for Oracle databases. The "Log truncation for Oracle" nightly job is now disabled by default, to keep parity with default behavior of log truncation for other supported applications. Future editions of the User Guide will update topics "About protecting Oracle database servers" and "About truncating Oracle logs" to note that the nightly job is disabled by default. **Workaround:** Users are advised that log truncation for Oracle is disabled by default. You can enable this nightly job to automatically truncate logs on a daily basis, or you can manually truncate logs on demand.	106264	Technical documentation, nightly jobs, log truncation
System requirements for Rapid Recovery now appear only in the *Rapid Recovery System Requirements Guide.* References to system requirements in other technical documents now reference that guide instead. This includes the *Rapid Recovery Installation and Upgrade Guide* and the *Rapid Recovery Third-Party Integration Guide*. No other content changed in the latter document. Information that previously appeared as appendices in the *Rapid Recovery User Guide* have been removed. These chapters will be published as the *Rapid Recovery Commands and Scripting Reference Guide*.	104973	Technical documentation
The *Rapid Recovery User Guide* procedure "Deploying a virtual machine in Azure" for release 6.2 contains unnecessary steps 4 through 8. Future versions of documentation are to be modified accordingly. **Workaround:** When following this procedure, disregard steps 4 through 8. After performing step 3, skip to step 9. This step is performed on the **Destination** page of the Deploy to Azure Wizard.	101859	Azure export
The *Rapid Recovery User Guide* procedure "Setting up continual export to Azure" for release 6.1.x contains unnecessary steps 4 and 5. Future versions of documentation are to be modified accordingly. **Workaround:** When following this procedure, disregard steps 4 and 5. Since you are defining ongoing continual export, you are not prompted to select a recovery point. After performing step 3, skip to step 6. Likewise, there is no Summary page at the end of the wizard. On the Volumes page of the wizard, click Finish (instead of Next).	101858	Azure export
Containers created in Azure are used to store virtual machines exported from the Rapid Recovery Core to your associated Azure account. If you create a specific container prior to performing virtual export, the Virtual Machine Export Wizard typically displays that container as one of the choices in the Container	101853	Azure export

Known Issue Description	Issue ID	Functional Area
name field of the Destination window. If you create the container by typing a valid container name into the Container name field as part of the process of defining a virtual export, the container may not be immediately visible in the wizard. This behavior is not reflected in the appropriate procedures in the *Rapid Recovery User Guide*. **Workaround:** If you create a container from the Virtual Machine Export Wizard, and that container is not accessible in the wizard UI, simply close the wizard, and launch it again, and you should then be able to access the newly created container. Future versions of documentation are to be modified accordingly.		
When performing virtual export to Azure, the Rapid Recovery Core uses Azure storage and containers created using the Classic management model. Containers created in Azure using the newer Resource Manager deployment model are not recognized by the Core. The *Rapid Recovery User Guide* procedure "Creating a container in an Azure storage account" for release 6.1.x does not specify that the Classic management model is required. Future versions of documentation are to be modified accordingly. **Workaround:** Use the Classic management model to create storage accounts and containers for virtual export. If you already have a storage account created using the Classic model, any new containers created for it will automatically use the correct model (Classic).	101837	Azure export

The issues listed in the Linux table below apply to release 6.1.3.527.

Table 10. Linux protection known issues

Known Issue Description	Issue ID	Functional Area
Snapshots and jobs for taking metadata fail for some Linux servers with RAID5 hardware. **Workaround:** This defect was resolved in Linux Agent 6.1.3.527. Upgrade to this build if experiencing this issue.	104919	Protecting
Protection of volumes created with LVM-based storage pools fails. LVM functionality will be included in a future release. **Workaround:** Contact Support to request a patch that addresses this issue.	103488	Protection
Unable to use TLS 1.2 with Linux Agent. This is related to the version of Mono in release 6.1.3. Upgrade to Linux Agent 6.2 when available, which includes TLS 1.1 and 1.2 support. **Workaround:** None.	101279	TLS
An ESXi agentless RedHat machine is not bootable after a VirtualBox export. **Workaround:** None.	31277	Virtual export
Agentlessly protected Linux machines are not bootable after BMR. **Workaround 1:** Use the Rapid Recovery Agent on all supported Linux distributions instead of using agentless protection if BMR is required. **Workaround 2:** To fix boot issues, engage a knowledgeable Linux administrator to update the volume, reinstalling grub and editing the content of /etc/fstab. Other steps may be required for individual distributions.	31206	BMR bootability

System requirements reference

System requirements for Rapid Recovery and all related components are now located in the *Rapid Recovery System Requirements Guide*. Please refer to this document on the technical documentation website.

Licensing Rapid Recovery software and appliances

Before you use and manage any version of Rapid Recovery, AppAssure, or Quest DL series backup and recovery appliance, you must first obtain a software license. To purchase licenses, contact the Quest Sales team by completing the web form at https://www.quest.com/register/95291/. A Sales representative will contact you and arrange for the license purchase.

After each license purchase, you must activate the license on the Rapid Recovery License Portal. From this portal, you can then download your Rapid Recovery license files.

When you initially install Rapid Recovery Core, you are prompted to upload these license files the first time you open the Rapid Recovery Core Console.

Some users start with a trial license, which has limited capabilities. Once a trial period expires, the Rapid Recovery Core stops taking snapshots. For uninterrupted backups, upgrade to a long-term subscription or perpetual license before the trial period expires. If you purchase a license after backups are interrupted, performing this procedure resumes your backup schedule.

When using a software license in standard phone-home mode, the Rapid Recovery Core Console frequently contacts the Rapid Recovery License Portal server to remain current with any changes made in the license portal. This communication is attempted once every hour. If the Core cannot reach the license portal after a grace period (typically 10 days), the Core stops taking snapshots for non-trial licenses.

If a Core does not contact the license portal for 20 days after the grace period, it is removed from the license pool automatically. If the Core subsequently connects to the license portal, the Core is automatically restored on the license portal.

Use of phone-home licenses requires Rapid Recovery users to accept a limited use of personal information, as described in the privacy policy shown when you install Core software. For more information, see General Data Protection Regulation compliance.

NOTE: When registering or logging into the license portal, use the email address that is on file with your Quest Sales representative. If upgrading from a trial version, use the email address associated with the trial version. If you need to use a different email address, contact your Sales representative for assistance.

Complete the following steps to license your Rapid Recovery software.

1. **Open your registration email.** When you first purchase a license from Quest, you receive an email from the Quest licensing system. The email includes your license entitlements, expiration date (if relevant), registered email address, and 9-digit Quest license number (in format 123-456-789).
2. **New users: Register for the Rapid Recovery License Portal.** If you have not previously created an account on the Rapid Recovery License Portal, then do the following:
    a. **Sign up for an account.** In a web browser, access the license portal registration URL, https://rapidrecovery.licenseportal.com/User/Register.

    The **Sign Up** page appears.

    b. **Complete the form.** Enter the information requested, review and accept the privacy policy and terms of use, and click **Sign Up**.

The **Confirm Email** page appears.

c. **Verify your account information.** Check your email and verify your account information by clicking **Verify email address**.

The **Add License Numbers** page appears.

d. **Proceed to** step 4 .

3. **Existing users: Log into the Rapid Recovery License Portal.** If you previously registered a license portal account to use with AppAssure or Rapid Recovery, then do the following:
   a. **Use existing credentials.** Log into the Rapid Recovery License Portal.
   b. **Open the License Numbers dialog box.** On the **Licensing** page, underneath your license pool information, click the **License Numbers** link.

   The **License Numbers** dialog box appears.

   c. **Proceed to** step 4 .
4. **Enter your license numbers.** For each nine-digit Quest license number included in your welcome email, click in the **License Number** field and enter or paste your license number. Then click **+ Add License Numbers**. When satisfied, click **Close**.

   The **License Number** dialog box closes.
5. **Review updated license information.** Review license type and license pool information displayed on the **Licensing** page.

Getting started with Rapid Recovery

These topics provide information you can use to begin protecting your data with Rapid Recovery.

Topics include:

- Rapid Recovery Core and Agent compatibility
- Upgrade and installation instructions
- Additional resources
- Obtaining Rapid Recovery software

Rapid Recovery Core and Agent compatibility

The following table provides a visual guide of the interoperability between Core and Agent software versions. This table lists versions tested for release 6.2.

Table 11. Interoperability between Core and Agent versions

This table explicitly lists compatibility between specific Agent and Core software versions.

	AppAssure 5.4.3 Core[1]	Rapid Recovery 6.0.2 Core	Rapid Recovery 6.1.3[3] Core	Rapid Recovery 6.2 Core
AppAssure 5.4.3 Agent[1, 2]	Fully compatible	Fully compatible[3]	Fully compatible[3]	Fully compatible[3]
Rapid Recovery 6.0.2 Agent	Not compatible	Fully compatible	Fully compatible[3]	Fully compatible[3]

	AppAssure 5.4.3 Core[1]	Rapid Recovery 6.0.2 Core	Rapid Recovery 6.1.3[3] Core	Rapid Recovery 6.2 Core
Rapid Recovery 6.1.3[4] Agent	Not compatible	Not compatible	Fully compatible	Fully compatible[3]
Rapid Recovery 6.2 Agent	Not compatible	Not compatible	Not compatible	Fully compatible

[1]While not supported for release 6.2 and later, AppAssure 5.4.3 is shown in this chart to convey interoperability. See note [4].

[2] Protected machines with EFI partitions must be upgraded to Rapid Recovery Agent release 6.0.x or later to successfully restore data, perform bare metal restore, or perform virtual export.

[3] Users can protect machines using older versions of the Agent software in a newer Core. Logically, newer features provided in more recent versions of Rapid Recovery Agent are not available for machines protected with older versions of Agent installed.

[4] As shown in this chart, Rapid Recovery supports the current version, and the latest maintenance release of the last two major/minor versions (6.1.x and 6.0.x). Thus, if Rapid Recovery 6.2.1 is released, it becomes fully supported (along with versions 6.1.3 and 6.0.2), and release 6.2 goes into limited support. For detailed information, see the "Product Life Cycle and Policies" section of the Rapid Recovery support website at https://support.quest.com/rapid-recovery/ .

The matrix shows releases that have been fully tested with this release, and represent fully supported releases. Other software versions in limited support status (such as releases 6.0.1, 6.1, 6.1.1, and 6.1.2) have not been tested for interoperability, but are also expected to work.

Other factors affect interoperability. For example, the Rapid Snap for Virtual feature was first introduced in Rapid Recovery Core version 6.0, letting you protect VMware ESXi VMs agentlessly. Rapid Recovery Core release 6.1.0 expanded this support to host-based protection for Hyper-V VMs. Release 6.2 introduces agentless application support for protected machines running Exchange Server and SQL Server. Logically, users of Core version 5.4.3 cannot agentlessly protect any VMs. Users of Core version 6.0 cannot protect VMs on Hyper-V without installing the Agent software. And Cores earlier than release 6.2 have limited agentless support for Exchange and SQL Server, as detailed in the user guide topic "Understanding Rapid Snap for Virtual agentless protection" or "Understanding agentless protection" for each relevant release.

Upgrade and installation instructions

Quest recommends users carefully read and understand the *Rapid Recovery Installation and Upgrade Guide* before installing or upgrading. See the section "Installing Rapid Recovery" for minimum software requirements and general installation approach. This section lists requirements for a software license, an account on the license portal, installing a Core, creating a repository, and protecting machines with the Agent software or agentlessly.

All existing users should read the section "Upgrading to Rapid Recovery." This content describes upgrading factors, provides an overview of upgrading, and includes procedures upgrading Core, and upgrading Agent on Windows and Linux machines. Linux procedures have been optimized and simplified.

Additionally, Quest requires users to carefully review the release notes for each release, and the Rapid Recovery system requirements for that release, prior to upgrading. This process helps to identify and preclude potential issues. As of release 6.2, system requirements are found exclusively in the *Rapid Recovery System Requirements Guide*.

When planning an implementation of Rapid Recovery, for guidance with sizing your hardware, software, memory, storage, and network requirements, see knowledge base article 185962, “Sizing Rapid Recovery Deployments".

If upgrading from AppAssure Core release 5.4.3, or Rapid Recovery Core release 6.0.x or 6.1.x, then run the latest Core installer software on your Core server. If using replication, always upgrade the target Core before the source Core.

To protect machines running supported operating systems with the latest features, upgrade or install Rapid Recovery Agent on each.

CAUTION: Ensure that you check system requirements for compatibility before upgrading. For protected machines with operating systems that are no longer supported, you can continue to run older supported versions of Agent. In some cases, you can protect those machines agentlessly.

You can use the same installer executable program (standard, or web installer) to perform a clean installation or to upgrade an existing version of Rapid Recovery Core, Agent, or the Local Mount Utility. If upgrading from versions earlier than release 5.4.3, you must first upgrade to 5.4.3 and then run the release 6.2 installer on the same machine. For more information, see the *Rapid Recovery Installation and Upgrade Guide*.

When upgrading a protected Linux machine from AppAssure Agent to Rapid Recovery Agent version 6.x, you must first uninstall AppAssure Agent. For more information and specific instructions, see the topic "Installing or upgrading Rapid Recovery Agent on a Linux machine" in the *Rapid Recovery Installation and Upgrade Guide*.

You can also use the Rapid Snap for Virtual feature to protect virtual machines on supported hypervisor platforms agentlessly. Important restrictions apply. For more information on benefits or restrictions for agentless protection, see the topic "Understanding Rapid Snap for Virtual" in the *Rapid Recovery User Guide*.

For information on downloading Rapid Recovery software, see Obtaining Rapid Recovery software.

License requirements

New Core users must purchase a long-term subscription or perpetual license to use Rapid Recovery.

Some Rapid Recovery Core users start with a trial license, which uses a temporary license key for the duration of the trial. After the trial period expires, you can continue to restore from existing backups, but cannot perform new backups or replication until you purchase a long-term subscription or perpetual license. You must then activate the license on the Rapid Recovery License Portal, download Rapid Recovery license files, and associate them with your Core.

For more information about licensing, see the following resources:

- For information about activating your new license and obtaining Rapid Recovery license files for your Core, see Licensing Rapid Recovery software and appliances in these release notes.
- For information about managing licenses from the Rapid Recovery Core, including uploading license files to associate them with the Core, see the topic "Managing licenses" in the *Rapid Recovery User Guide* or the *Rapid Recovery Installation and Upgrade Guide*.
- For information about managing license subscriptions and license groups on the license portal, see the *Rapid Recovery License Portal User Guide*.

Obtaining Rapid Recovery software

You can obtain Rapid Recovery software using the following methods:

- **Download from the License Portal.** If you have already registered Rapid Recovery in the Rapid Recovery License Portal, you can log into that portal at https://licenseportal.com. From the left navigation menu, click **Downloads**. and download the appropriate software.
- **Download from the Data Protection Portal.** If you have an active maintenance agreement, you can log into the Data Protection Portal portal at https://dataprotection.quest.com/dashboard. From the top menu, click **Settings**, and from the left navigation menu, select **Downloads** . Here you will have access to installers for various Rapid Recover components, including Core, Agent, LMU, DR, and more.
- **Download trial software from the Rapid Recovery Support website.** To download trial software, navigate to the Rapid Recovery Support website at https://support.quest.com/rapid-recovery and from the left navigation menu, click **Software Downloads**. Here you can access trial versions of Rapid Recovery Core, Agent (for Windows or Linux), tools and utilities, and more. Trial versions function for 14 days, after which time you must purchase and register a subscription or perpetual license to continue using Rapid

Recovery. To purchase a license, fill out the web form at https://support.quest.com/contact-us/licensing and select **Obtain a license for my product**.

You can also obtain the Rapid Recovery Agent software from within the Rapid Recovery Core Console using the following methods:

- **Protecting machines with the wizard.** If the Rapid Recovery Core is installed, you can deploy the Agent software to the machine you want to protect from the Protect Machine Wizard or the Protect Multiple Machines Wizard. Using these wizards, you can also choose to add machines to protection using an older installed version of Agent. For more information about these wizards, see the topics "Protecting a Machine" and "About protecting multiple machines" in the *Rapid Recovery User Guide*.
- **Use the Deploy Agent Software feature.** If the Rapid Recovery Core is installed, you can deploy the Agent software from the Core to one or multiple machines. This is useful for upgrading Agent to one or more machines simultaneously. From the **Protect** drop-down menu on the Rapid Recovery Core Console, select **Deploy Agent Software** and complete details in the resulting wizard. For more information about using this feature, see the topic "Deploying Agent to multiple machines simultaneously from the Core Console" in the *Rapid Recovery User Guide*.
- **Download Agent or LMU from the Rapid Recovery Core Console.** From a network-accessible Windows machine you want to protect, you can log into the Rapid Recovery Core Console and download the Agent software. From the icon bar, click **More** and then select **Downloads.** From the **Downloads** page, you can download the web installer to install Agent or the Local Mount Utility on Windows machines.

Additional resources

Additional information is available from the following:

- Technical documentation
- Videos and tutorials
- Knowledge base
- Technical support forum
- Training and certification
- Rapid Recovery License Portal
- Quest Data Protection Portal

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 in the *Rapid Recovery System Requirements Guide.*

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. It supports bidirectional writing (Arabic and Hebrew). The release supports Complex Script (Central Asia – India, Thailand).

The release is localized to the following languages: Chinese (Simplified), French, German, Japanese, Korean, Portuguese (Brazil), Spanish.

This release has the following known capabilities or limitations:

- Quest Data Protection Portal is in English only.
- Rapid Recovery release 6.2 requires the Microsoft .NET Framework version 4.6.2. Earlier releases of Rapid Recovery used different versions of the .NET Framework. There is no downgrade option available. If you upgrade versions of Rapid Recovery to a release using a more recent version of the .NET Framework, and then subsequently decide to return to a prior version, you must perform a new installation of the appropriate Core and Agent software.
- Logs and KB articles for Rapid Recovery are in English only.
- Certain technical documentation is available in English only for this release. These documents include:
  - *Rapid Recovery Third-Party Integration Guide*.
  - *Rapid Recovery Commands and Scripting Reference Guide*. This document contains information previously included as appendices to the *Rapid Recovery User Guide.*
  - *Mailbox Restore for Exchange User Guide.*
  - *Rapid Recovery License Portal User Guide.*
  - *DocRetriever for SharePoint User Guide.*
  - *Rapid Recovery Replication Target for Microsoft Azure Setup Guide*

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 https://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 our product

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.

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