Quest®

Rapid Recovery 6.5 Release Notes

October 2020

These release notes provide information about the Rapid Recovery release, build 6.5.0.724.

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, 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 6.5 is a minor release, with new features and functionality. See New features and Enhancements for details.

> **i**   **NOTE:** For more information about how major, minor, and maintenance releases are differentiated, see Rapid Recovery release designations.

Some features, previously integrated software tools, or platforms are no longer supported. For more information on these items, see Deprecated features.

As a minor release, defect fixes and known issues listed in this document are not cumulative.

For information relevant for any other release, please see the edition of release notes specific to that release on the Quest technical documentation website.

Topics in this section include:

Quest Support policy

Full support: For customers with a current maintenance contract, Quest Data Protection Support provides call-in or email support for the current major and minor release, when patched to the latest maintenance release. That release is known as N. Quest also fully supports N - 1. For Rapid Recovery, Quest also provides limited support for N - 2.

Limited support: Quest Data Protection Support may attempt to answer questions on other versions of our products, provided resources are available. However, if you are using an unsupported or discontinued version, no new patches or code fixes will be created for those versions. In such cases, we encourage you to upgrade to a currently supported version of the product.

Product support life cycle: Quest describes its product life cycle (PLC) support policy on its Support website (visit https://support.quest.com/rapid-recovery/, click **Product Life Cycle & Policies,** and then expand the topic **Product Support Life Cycle Policy**). To understand full support, limited support, and discontinued support, consult the detailed policy on the website referenced above.

New features

The following new features have been added to Rapid Recovery in release 6.5, or were not previously documented in earlier releases.

- Azure Storage repository - Azure specific backup storage that is more cost-efficient than running DVM repositories in the cloud. See Azure Repository

- Synthetic incrementals - Optimized backups that take less space in repositories compared to full base images. Synthetic incremental backups can be configured to automatically occur when Rapid Recovery cannot find the changed blocks.

    i | **NOTE:** Both the Rapid Recovery Core and the Rapid Recovery Agent need to be upgraded to the lasted version to use this feature.

Azure Repository

Rapid Recovery 6.5 adds support for a new repository type (Native Azure Storage) that enables direct repository connections to Microsoft Azure Blob storage.

Consider the following details when implementing this feature:

- This feature has been released in **Beta** status to allow for evaluation and testing. In some circumstances, performance is not suitable for production environments.

- This feature is intended for use as a replication target repository. Using an Azure repository for backup storage on a primary or source core is not recommended.

- Metadata files must be stored locally.

- Only one Azure repository is supported per Rapid Recovery Core

Complete the following steps to create an Azure Repository.

1. Navigate to the Rapid Recovery Core Console.

2. On the icon bar, click ••• (More), and then select 🗄**Repositories**.

3. At the top of the page, under the *Repositories* page title, click **+ Create**.

4. Select **Azure Repository**.

5. On the *Configuration* page, enter the information as described below:

   - **Name** - Enter the display name of the repository.
     By default, this text box consists of the word Repository and a number, which corresponds to the number of repositories for this Core. For example, if this is the first repository, the default name is Repository 1. Change the name as needed. Repository names must contain between 1 and 40 alphanumeric characters, including spaces. Do not use prohibited characters or prohibited phrases.

   - **Comments** - Optionally, enter a descriptive note about this repository. You can enter up to 254 characters.

6. Click **Next**.

7. On the *Storage Location* page, enter the following information:

   - **Location** - Specify the path to a storage location on Azure blob storage. Use only alphanumeric characters, hyphen, or period, with no spaces or special characters.

   - **Dedupe cache location** - Select **Azure blobs** or **Local file system.**

   - **Index files location** - Select **Azure blobs** or **Local file system.**

   - **Data Storage account** -Select the appropriate Azure Storage account. Refer to **Cloud Accounts** in the *Rapid Recovery User Guide* for more information.

     > ℹ **NOTE:** If you have configured a Microsoft Azure Resource Management (for Virtual Export) account for use with VM export, that account cannot be used for the Azure repository.

   - **Account name** - Enter the name of your Microsoft Azure storage account. The name must match the storage account name in Azure precisely. It must contain lower case letters and numbers only, and be between 3 and 24 characters in length.

   - **Access key** - Enter the access key for your account. You can enter the primary or secondary key. Your access key can be found under the **Settings > Access Keys** section of your Azure Storage account.

   - **Account type** - Choose your Azure account type; for example Azure, Azure Germany, Azure China, or (US) Government.

   - **Use https protocol** - Select this option to use the secure https protocol instead of the standard http protocol.

8. Click **Next**.

9. On the *Space Allocation* page, specify the following :

   a. Azure repostory size in GB

   b. Deduplication cache size in GB

   c. When you have completed your repository configuration, click **Finish**.
    The *Create Repository Wizard* closes, and Rapid Recovery applies the settings to your Core. If Toast alerts are enabled, you see messages indicating that repository creation has started, and the repository is mounted. Alternatively, you can monitor the progress of the repository creation by viewing alerts on the *Events* page.
   After a brief pause, on the *Repositories* page, in the Repositories summary table, your new repository is listed

Enhancements

The following enhancements have been added to Rapid Recovery 6.5, or were not previously documented in earlier releases

- Multiple platform and application support updates:
  - Support for SharePoint 2019
  - Support for Ubuntu 19.10
  - Support for Ubuntu 20.04
  - Support for RHEL/CentOS/Oracle Linux 8
- Improved performance of SQLmetadata checks
- Added the ability to configure deletion of recovery points on a per volume basis
- Added the ability to enable/disable SQL Metadata Checking for protected machines via the UI

Resolved issues

This topic contains the issues resolved in this release:

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

Table 1: Issues resolved in this release

Issue ID	Resolved Issue Description
110503	Live restore should be occurring simultaneously for all volumes and can access the files during the restore
110450	Incremental ESXi export fails with * An unexpected error occurred: An argument was unexpectedly null in code located in or called by 'EsxServer.SetCachedValue'
110365	Restore of linked Agent failed with error: The volume restore failed because it is in use
110332	Azure Cloud account (for export) Secret Key is written in plain text in Core registry
110325	Specific Windows Server 2019 BIOS (ESXi 6.5 version) is not booting after BMR

Issue ID	Resolved Issue Description
110147	PowerShell scripts failing with a dependency error
110102	Inbox folder is empty after opening an Exchange 2019 CU4 database
110090	Archive to Amazon S3 (Wasabi endpoint) job fails with "The remote server returned an error: (500) Internal Server Error." if chain contains volume image with size 0 MB
110076	VMs goes offline after changing HyperV cluster credentials
110073	Archiving to Amazon Government Cloud with Glacier option fails "The specified bucket is not valid" and "400 Bad Request"
110070	Export fails with "Replay.Common.Contracts.Win32Api.Win32ApiFailedException: Failed to open 'C:\Mount...\FatVolumeMetadata.xml' for writing - The file or directory is corrupted and unreadable"
110020	Incorrect description of transfer queue option "Maximum concurrent transfers from a single Hyper-V host" for cluster agentless protection
109999	Installer crashes while upgrading Rapid Recovery to version 6.4 on a SQL Server with Analysis Services Configuration in Tabular Mode
109967	Linux agent's service crash on the passive node of oracle cluster with shared device
109951	Core do not parsed Linux volumes with specific ID (more then 255)
109902	Rapid Recovery Linux driver attached to new block device without protection by Core
109862	There is no ability to protect Cluster using account/credentials saved in Credentials Vault
109842	Oracle metadata cannot be collected if the Oracle database has specific configuration and customized db registry key name
109835	Archive to Amazon S3 (Wasabi endpoint) job fails with "The remote server returned an error: (500) Internal Server Error."
109790	Agentless VM is in trial after re-protect with NPH front-end capacity license with large enough license pool applied
109770	Archive to Google job fails after 7 days
109740	Oracle metadata will not be obtained if the Oracle DB listener has non-default (customized) name
109691	Device does not detach or attach from the Rapid Recovery driver without refreshing metadata
109615	Transfer fails with "Length cannot be less than zero. Parameter name: length" error for specific ESXI agentless VM
109600	Transfer fails due to exception ' '.vmx' download failed with status 'NotFound' ' for ESXI if datacenter located in folder
109188	24 hour interval not able to be saved correctly in Transfer Schedule Templates and leads to inoperative transfers
108299	Replicated data is calculated as Protected data with NPH capacity license applied on target Core
104393	Agentless backup fails with "Invalid URI: The hostname could not be parsed" error when the shadow copy has specific path (\\?\Volume{fb3687e7-57b5-11e7-80c4-f48e38cee0fd}\diskc.vhdx)
102756	Deploy to Azure fail if specify cloud service name in FQDN format

Known issues

This topic contains known issues in the following categories:

- Core and Windows known issues
- Documentation known issues
- Linux known issues
- Local Mount Utility issues

Table 2: Core and Windows known issues

Issue ID	Known Issue Description	Workaround	Functional Area
27309 93141	ESXi virtual export with automatic disk mapping using default configuration for the VM configuration location fails with unclear error. The Failure Reason is "Task 'ReconfigVM_Task' failed: Invalid configuration for device '0'."	Reduce the number of concurrent exports.	Virtual exports, ESXi
110523	Exchange log truncation not working for ESXi agentless VMs if one database is dismounted	Mount all of the databases on the Exchange Server side.	**Agentless protection, Exchange**
110479	Newly created virtual machines don't automatically show up in the Core GUI Virtual Machines list of ESXi host.	Restart Core services to update Virtual Machines list.	
110473	Exchange log truncation not working for HyperV agentless VMs	Available workarounds are: - Perform a manual log truncation - Install the Windows agent on the VM - Use a post backup script to call Exchange	**Agentless protection, Exchange**
109236	Transfer job for VM with SharedVHDX on SOFS appears to fail with errors "Session with the id has not been found: fileTransmitSessionId" and "The process cannot access the file because it is being used by another process: " but recovery points actually are created.		

Issue ID	Known Issue Description	Workaround	Functional Area
108972	Trying to perform an "Open Exchange Database" job from a recovery point fails with error "Multiple concurrent writable mounts of a single volume are not supported."	Use the Local Mount Utility, or manually mount the recovery point and open the database.	
108764	When performing a virtual export or a virtual standby and you choose 'Specific' network adapters, the virtual standby is created with an additional e1000 NIC on top of the one you specified	No workaround at this time.	Virtual export
109828	When Core services are restarted, a "Virtual environment component 'Hypervisor Storage' changed status to 'Warning" alert is displayed.	No workaround at this time.	
109682	When attempting to archive to an existing Azure Government cloud account, error 'Initialization of new instance of type...' appears and archive is unsuccessful.	No workaround at this time.	Archive, cloud, Azure Government
109575	On a specific environment, Core Console UI does not load, with the error "Attempted to read or write protected memory. This is often an indication that other memory is corrupt."	No workaround at this time.	Core Console UI
107978	When deploying the Rapid Recovery Agent from the Core server, the Microsoft Store Install Service disappears from the list of services visible on the protected machine.	No workaround at this time.	Agent installation
107947	On a specific environment, virtual export fails to start, with error: 'Cannot connect to a remote machine '{0}' ' sometimes on unstable environment.	Contact Quest Support for a patch to resolve this issue.	Virtual export
107855	On a specific Dell PowerEdge Windows server environment, protected machine hangs briefly (up to 1 minute) every hour when the Rapid Recovery Agent service starts, seemingly due to a 20-30 BCD query.	Perform BCD queries one at a time, sequentially, to avoid this issue. For diagnostic steps, see Quest Knowledge Base article 259558.	Agent hang
107784	**When protecting a cluster, there is no ability to add cluster nodes to Virtual Standby**	**No workaround at this time.**	**Virtual export**
107755	When creating an archive using the Archive Wizard, if you return from the *Options* wizard page back to the *Machines* page, there is no ability to edit	Close the wizard without saving the archive, and run through the wizard	Archiving, usability

Issue ID	Known Issue Description	Workaround	Functional Area
	the date range.	again.	
107346	When restoring or performing virtual export of a volume with 512-bytes per sector to a volume with 4096-bytes per sector, a warning message does not appear.	For workaround, please see Quest Knowledge Base article 144232.	Virtual export, notifications
107304	On a specific appliance environment, the error message "GetResponse Timed Out" appears when trying to open the *Appliance* page.	Contact Quest Support for a patch to resolve this issue.	Appliance, Core Console UI
107182	Encryption key does not apply to cluster nodes during cluster protection.	Select encryption key for nodes manually in Settings.	Encryption
106938	On a specific appliance environment, the "Storage Hardware" information is not available on the *Appliance Health* page.	Contact Quest Support for a patch to resolve this issue.	Appliance, Core Console UI
106545	When upgrading a Core (in languages other than English) that protects machines with Agent version earlier than 5.4.3.106, the *Compatibility* page of the Rapid Recovery Core Installer wizard incorrectly shows Agent version 7 in the message instead of Agent 6.2 or Agent 6.3 (based on the installer being used).	None available. Disregard the version number. Protected machines with supported operating systems will be upgraded to Rapid Recovery Agent version 6.3.	Installer, localization
105830	Rollup job does not merge replicated recovery points according to the retention policy if seed drive for older recovery points was not consumed.	Consume the seed drive on the target core.	Rollup jobs, replication, seed drive
105445	Trustedinstaller process called during every metadata request from Agent, consuming about 100MB of additional RAM.	Contact for a patch to address this issue.	Metadata
103477	If the Quest NetVault Backup with BMR plugin is installed on the same server as the Rapid Recovery Core, then ESXi exports fail.	Copy the following DLLs from Coreservice\vddk\bin to the Coreservice folder, and then restart the Core service: • glib-2.0 • gobject-2.0 • gvmomi • iconv • intl	Virtual exports

Issue ID	Known Issue Description	Workaround	Functional Area
		• libcurl	
		• libxml2	
		• vixDiskLibVim	
102390	Drive letters are not assigned on an exported machine that is identical to the original machine.	Assign drive letters manually, or contact Support for a script to run on the exported machine that solves the issue.	Virtual exports
97451	Volume letters are not assigned after BMR for GPT partitions of ESXi Agentless VM.	Assign drive letters manually.	BMR, ESXi agentless

Go to the top of the *Known issues* topic.

Table 3: Documentation known issues

Issue ID	Known Issue Description	Workaround	Functional Area
109897	The following corrections were made to the Rapid Recovery 6.4 User Guide but not in the in-product help:	Please refer to the PDF or HTML-based User Guide on the Quest technical documentation website to see the latest content in the topics specified. When reviewing these topics within in-product help, disregard the minor discrepancies, and take heed of the updated information regarding deduplication cache which is flushed and re-created if the deduplication cache size is reduced.	In-product help, technical product documentation

Issue ID	Known Issue Description	Workaround	Functional Area
	1. References to former topic name "Managing licenses" in the *Rapid Recovery Installation and Upgrade Guide*have been updated to "Understanding Rapid Recovery licenses." The topics in in-product help that use the older topic name are listed below: • Factors when choosing agent-based or agentless protection (first paragraph of subtopic "release 6.4 license consumption concepts") • Rapid Recovery Core settings (the table row that reads "Licensing") • How Rapid Recovery ses personal information (first sentence, and later in a bulleted list of resources) • Obtaining and using non-phone-home licenses (fourth paragraph)		

Issue ID	Known Issue Description	Workaround	Functional Area

2. In the Core settings chapter of the *User Guide*, some updates were made to topics related to the DVM deduplication cache that do not appear in the 6.4 version of in-product help.

- In topic "Understanding deduplication cache and storage locations," formatting changes only appear. Specifically, the alphabetic case has been changed from title case to sentence case in the table showing default storage location settings. When those steps refer to UI elements, they now appear in bold, following UI conventions for click steps.

- In topic "Configuring DVM deduplication cache settings," in the table under step 5, the same formatting changes were applied to the same settings.

- Additionally, in the row showing Deduplication cache size, the description has been changed to correctly show the current text box label (also set in boldface), and to include a note. The updated text reads:

  "If you want to change the deduplication cache size for DVM repositories, then in the **Deduplication cache size** (GB) text box, enter a new amount in gigabytes.

  Note: If you decrease the size of the deduplication cache, the existing contents of the cache are flushed, and the cache is recreated."

Issue ID	Known Issue Description	Workaround	Functional Area
	3. In help, the Restoring data chapter topic "VMware VM configuration backup and restore" indicates that release 6.4 introduces the ability to back up VMware VM configurations. This capability was actually introduced to release 6.3; in release 6.4, you can also back up Hyper-V VM configurations, as described in Rapid Recovery 6.4 Release Notes topic "VM configuration backup and restore on Hyper-V." In the PDF/HTML version of the 6.4.0 User Guide, this topic is updated, and is now called "VM configuration backup and restore for VMware and Hyper-V".		
109793	Within in-product help, on the *Settings* page of the Core Console, if you click the ⑦ **Help** icon for the **License Details** Core setting, a generic error message appears.	To read about licensing in release 6.4, see the Rapid Recovery 6.4 Installation and Upgrade Guide topic "Managing Rapid Recovery licenses." In previous editions of in-product help, this Core setting included a link to information about licensing. That topic no longer appears in the User Guide or in-product help. The ⑦ **Help** icon will not appear in future editions of in-product help.	In-product help, Rapid Recovery Core Console, Core Settings, License Details
N/A	The information for the following third-party components has been added or updated in Rapid Recovery Core release 6.4 after in-product help was produced. The following notifications comprise supplemental updates to in-product help for third-party contributions. Their purpose is to provide proper attribution and meet legal and copyright requirements related to the use of the listed components.	Consult these notifications in Release Notes for the latest updates to legal and copyright requirements.	In-product help, Third-party components, copyrights, legal requirements
	• Component **p7zip 16.0.2** is not included in the list of third-party components available from in-product help for release 6.5.	Component **p7zip 16.0.2** uses the Mozilla Public License (MPL) 1.1. A copy of	

Issue ID	Known Issue Description	Workaround	Functional Area
		the MPL can be found as a linked license in Rapid Recovery's Third-Party Components link within in-product help.	
	• Component **NBD** is a Linux component which, when compiled into the kernel, lets Linux use remote servers as one of its network block devices. This software component is not used by Rapid Recovery Core but may be required by protected Linux agents. Quest is required to indicate where a copy of the source code for this GPL component is located. Component **NBD** is incorrectly noted within 6.4.0 in-product help as being available on the Linux DVD.	This component is not actually used by Rapid Recovery, but may be used by protected Linux machines. NBD is not available on the Linux DVD. Red Hat Enterprise Linux, CentOS and Oracle Linux installation packages download NBD source code from a publicly-accessible web location. Direct links differ based on distribution used; see the relevant Rapid Recovery Agent installation package. For assistance, please contact Quest Data Protection Support. Component **NBD** (various versions) uses the GNU General Public License 2.0, which can be found in Rapid Recovery's Third-Party Components link within in-product help. The copyright attributions there are accurate and complete.	

Go to the top of the *Known issues* topic.

Table 4: Linux known issues

Issue ID	Known Issue Description	Workaround	Functional Area
107984	When installing Rapid Recovery Agent on a Linux machine, minor misspellings appear on the command line for firewall settings.	No workaround at this time. The text "Configured manualy. May be reconfigured…" is expected to be changed to "Configured manually. This may be reconfigured...".	Linux, Agent installation

Go to the top of the *Known issues* topic.

Table 5: Local Mount Utility known issues

Issue ID	Known Issue Description	Workaround	Functional Area
108540	Toast pop-up notifications appear outside of the Local Mount Utility application window/frame.	No workaround at this time.	Notification
107756	Tthere is no ability to set Core Connection Timeout using the LMU UI.	You can set the Core Connection Timeout using the Windows registry using key CoreConnectionTimeout. For more information, see Quest Knowledge Base article 210006.	LMU, Connection timeout
110364	[LMU] There is no ability to open Exchange databases for ESXi agentless VMs due to error database does not exist		

Go to the top of the *Known issues* topic.

Where to find Rapid Recovery system requirements

For every software release, Quest reviews and updates the system requirements for Rapid Recovery software and related components. This information is exclusively available in the release-specific *Rapid Recovery System Requirements Guide.* Use that document as your single authoritative source for system requirements for each release.

You can find system requirements and all other documentation at the technical documentation website at https://support.quest.com/rapid-recovery/technical-documents/.

> **i** **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 filter the view by document type.

Product licensing

Before you use and manage any version of Rapid Recovery, AppAssure, or DL series backup appliance, you must first obtain a software license. To purchase a license for the first time, contact the Quest Data Protection 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.

If you need to renew or purchase additional licenses, please contact the Quest Support Renewals team by completing the web form at https://support.quest.com/contact-us/renewals.

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, the Core stops taking snapshots for non-trial licenses. The grace period (10 days by default) is configurable (from 1 to 15 days) in the license group settings on the license portal.

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 the topic "General Data Protection Regulation compliance" in the *Rapid Recovery User Guide*.

> **i** | **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 Quest license number. The license number is typically 9 digits, in format 123-456-789. Other formats are supported, as described in the topic "Understanding Rapid Recovery licenses" in the *Rapid Recovery Installation and Upgrade Guide*.

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 Quest license number included in your welcome email, click in the **License Number** text box 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

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

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

Rapid Recovery Core and Agent compatibility

The following table provides a visual guide of the compatibility between supported versions of Rapid Recovery Core and Rapid Recovery Agent.

Table 6: Compatibility between supported Core and Agent versions

Version	6.3.0 Core	6.4.0 Core	6.5.0 Core
6.3.0 Agent	Fully compatible	Fully compatible	Limited support
6.4.0 Agent	Not compatible	Fully compatible	Fully compatible
6.5.0 Agent	Not compatible	Not compatible	Fully compatible

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 a step-by-step general installation approach. The approach includes requirements for a software license and for an account on the Rapid Recovery License Portal; adherence to the system requirements; installing a Core; creating a repository; and protecting machines with the Agent software or agentlessly. It also suggests use of the QorePortal.

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.

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. 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 Quest Knowledge Base article 185962, Sizing Rapid Recovery Deployments."

If upgrading from a currently supported major and minor version of Rapid Recovery Core (6.1x or 6.2x), then run the latest Core installer software on your Core server. If upgrading from a version of AppAssure or Rapid Recovery Core that is not currently supported, use a two-step upgrade process. First, upgrade using a supported Core installer such as 6.2.1; then run the latest Core installer software.

If using replication, always upgrade the target Core before the source Core.

To protect machines running supported operating systems with the latest Rapid Recovery Agent 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, Rapid Recovery 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 a more recent 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 Product licensing 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 Rapid Recovery licenses" in the *Rapid Recovery Installation and Upgrade Guide*.

- For information about managing license subscriptions and license groups on the license portal, see the latest edition of the *Rapid Recovery License Portal User Guide*.

More 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

- In-product help is available from the Rapid Recovery Core Console by clicking ⑦.

Obtaining Rapid Recovery software

You can obtain Rapid Recovery software using the following methods:

- **Download from the QorePortal.** If you have an active maintenance agreement, you can log into the QorePortal at https://qoreportal.quest.com. From the top menu, click **Settings**, and from the left navigation menu, select **Downloads**. Here you will have access to installers for various Rapid Recovery components, including Core, Agent, LMU, DR, and more.

- **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 trial software from the Support website.** To download trial software, navigate to the Rapid Recovery Rapid Recovery 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.

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).

Multi-language support is available for this product. The user interface for this release is localized to the following languages: Chinese (Simplified), French, German, Japanese, Korean, (Brazilian) Portuguese, Spanish.

This release has the following known capabilities or limitations:

- QorePortal is in English only.

- Reports are in English only.

- All currently supported versions of Rapid Recovery Core require 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.

- Technical product documentation for this release is in English only.

About us

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

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request

- View Knowledge Base articles

- Sign up for product notifications

- Download software and technical documentation

- View how-to-videos

- Engage in community discussions

- Chat with support engineers online

- View services to assist you with your product

i | **NOTE:** An information icon indicates supporting information.

Rapid Recovery Release Notes
Updated - October 2020
Version - 6.5