

Rapid Recovery 6.4 Release Notes

December 2019

These release notes provide information about the Rapid Recovery release, build 6.4.0.718.

Topics include:

- [About this release](#)
- [Rapid Recovery release designations](#)
- [Quest Support policy](#)
- [Rapid Recovery service levels](#)
- [New features](#)
- [Enhancements](#)
- [Deprecated features](#)
- [Resolved issues](#)
- [Known issues](#)
- [Where to find Rapid Recovery system requirements](#)
- [Product licensing](#)
- [Getting started with Rapid Recovery](#)
- [Globalization](#)
- [About us](#)

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 6.4 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:

- [Replication conflicts with agentlessly protected virtual machines on SMB shares](#)
- [Content differences between context-sensitive help and technical documentation](#)

Replication conflicts with agentlessly protected virtual machines on SMB shares

In specific cases, users cannot set up replication between 6.1.3 and 6.3 Cores. Users attempting to establish replication from a source Core running Rapid Recovery Core 6.1.3 to a target Core running version 6.2.0 or higher will fail if the target Core has recovery points from an agentlessly protected machine that had shared VHDX disks placed on a network shared volume using the Server Message Block (SMB) protocol.

If using such a configuration, all attempts to set up replication will fail (not only protection of agentless VMs). At this time, Quest does not expect to backport a fix. To resolve, upgrade your source Core to release 6.2.0 or later.

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 6.4 User Guide*. To view help topics in a web browser, from the Rapid Recovery Core Console, click [Help](#) ▾ or [?](#), and from the resulting drop-down menu, select [?](#) **Help**.

Due to publication schedules, sometimes there are content differences between content in the in-product help and in the *User Guide*, with the latter document being the most recent. In such cases, these differences are typically documented in the [Documentation](#) section of the [Known issues](#) topic.

Since Rapid Recovery release 6.2, the "REST APIs" appendix appears only in the HTML and PDF versions of the *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 [iAbout](#) menu. This topic does not appear in HTML or PDF versions of the *User Guide*.

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. Maintenance releases may also reflect changes (additions and deprecations) in supported operating system or application platforms.
- **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 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 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.
 - Difference in build numbers does not affect replication when the target Core has the same or a more recent build installed than the source Core.

The release designation for this release, 6.4.0.718, therefore represents the following: The first digit shows this version as part of the 6.x major release. The digit after the first point (4) shows this release as the fourth minor version in 6.x. The 0 after the second point shows this is the first generally available release within 6.4 (a 1 or higher would signify a maintenance release). Finally, the build number identifies the release down to the lowest level and is generally only referenced in release notes.

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. For more information, see "Rapid Recovery support levels" in the *Rapid Recovery 6.4 Release Notes*.

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.

Rapid Recovery service levels

Quest Data Protection Support is committed to providing customers that have a current maintenance contract with assistance and advice for supported releases.

Quest strives to put resources behind the most recent product releases so that we can continually improve and enhance the value of our solutions. As new versions are released, interoperability testing is conducted only


between those new versions and the releases that will be in full or limited support when the new version becomes generally available. Other versions are no longer tested, even if they are expected to be interoperable. At a minimum, Quest commits company-wide to supporting the current software version (N) and the prior version (N-1). Some products—including Rapid Recovery—offer higher support levels and commitments.

Rapid Recovery customers with an active maintenance agreement are entitled to Quest Data Protection Support under the following terms:

- Rapid Recovery software versions supported follow the **N-2 policy**.
 - **N** represents the major and minor release numbers (for example, 6.4, 6.3, 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 6.4, N-1 refers to release 6.3.
 - **N - 2** refers to the penultimate major/minor release. For example, in release 6.4, N-2 refers to release 6.2.
- 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 (6.2), the latest maintenance release (6.2.1) 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. Support for earlier maintenance releases is discontinued because viable, easy-to-upgrade alternatives are available. For example, users of release 6.2.0 can upgrade directly to release 6.2.1, which is fully supported.
- Limited support can be offered to other versions by exception. As of the date of publication, no Rapid Recovery releases currently are supported by exception.

If you are using a release that is in limited support and you request assistance from Quest Data Protection Support, you may be asked to upgrade. If you are using a release in discontinued support, you will first be asked to upgrade.

For each product on the Quest Support website, in the Product Life Cycle section, you can view a chart showing recent software versions, and the service levels and dates applicable to those service levels. For example, to see Rapid Recovery- specific product life cycle support information, do the following:

1. Navigate to <https://support.quest.com/rapid-recovery/>.
2. Click  **Product Life Cycle & Policies**.
The resulting matrix shows the product-specific list of supported releases. For example, dates are included for each Rapid Recovery release to specify the support status (full, limited, or discontinued) for each release shown.
3. Scroll down to the **Product Support Policies** heading and expand the link **Product Support Life Cycle Policy**.
This content details the Quest-wide N-1 product support life cycle policy. It describes aspects of full, limited, and discontinued support levels and describes an option for continuing support.

New features

The following new features have been added to Rapid Recovery in release 6.4, or were not previously documented in earlier releases.

- [Virtual Machine-only licensing](#)
- [Support for Oracle 18c RDBMS](#)
- [VM configuration backup and restore on Hyper-V](#)
- [Support for backup and restore of Linux LVM cache volumes](#)
- [BMR for disk-level agentless backups on Linux](#)
- [Support for many disk-level volumes for Linux BMR](#)

Virtual Machine-only licensing

As of release 6.4, Quest Rapid Recovery supports VM-only licensing.

Rapid Recovery customers who protect a substantial number of virtual machines can opt to use this new licensing model. The more virtual machines you protect, the more economically advantageous this licensing model is for users.

As in the past, you can only use a single licensing model per Core. Therefore, plan your Core configurations accordingly to take maximum advantage of possible licensing discounts. For example, if you configure one Core to protect primarily virtual machines, you can use VM-only licensing. Other Core configurations with primarily physical protected machine can use standard licensing.

Discounts for VM-only licenses are tiered, starting with as few as 10 licenses. On average, you can save between 10 and 65 percent on the cost of per-machine licenses. For more information, contact your Quest Sales representative and ask about Rapid Recovery Backup and Protection licenses per protected virtual server.

Support for Oracle 18c RDBMS

In Rapid Recovery release 6.4, our application support is expanded to include Oracle 18c relational database management system (RDBMS). This new RDBMS version reaches end of standard support with Oracle in March of 2023, and reaches end of extended support in March of 2026.

Rapid Recovery supports Agent-based protection of Oracle 12c and 18c relational database servers. When using ARCHIVELOG mode, you can protect an Oracle database server and all of its databases, you can restore, perform virtual export, truncate Oracle logs, and perform DBVERIFY database integrity checks.

As described in [Support for backup and restore of Linux LVM cache volumes](#), you can even back up and restore of Linux LVM cache volumes.

VM configuration backup and restore on Hyper-V

Rapid Recovery Core release 6.4 introduces a new feature, the ability to back up and restore virtual machine (VM) configurations on Hyper-V, including the option to include VM configurations during virtual export to Hyper-V virtual machines. This feature was introduced for VMware/ESXi in release 6.3.

Backup. Rapid Recovery Core release 6.4 and later automatically saves agentlessly protected Hyper-V and ESXi virtual machine configurations in each volume image when snapshots are captured. Hyper-V virtual machine configurations are stored in .vmcx files, whereas VMware virtual machine configurations are stored in

.vmx files (and related BIOS settings are stored in .nvram files). The relevant files are saved in the custom metadata for each relevant VM volume, and includes hypervisor version information to ensure compatibility.

Restore. Optionally, when restoring data from a recovery point of an agentlessly protected Hyper-V or ESXi machine, you can choose whether to include in the VM all VM configurations and data, or only the data. This choice is presented in the UI through the **Restore configuration data** check box. This option appears only for Hyper-V or VMware machines protected agentlessly (replacing the **Show advanced options** check box that is relevant only for machines protected by Rapid Recovery Agent). When the option is selected, all VM configurations for volumes being recovered are restored. When the option is cleared, only data (and not VM configurations) are restored for those volumes.

Virtual export. Optionally, when performing virtual export from a recovery point of an agentlessly protected Hyper-V or ESXi machine, you can choose whether to export all VM configurations and data, or export only the data. This choice is presented in the UI through the **Restore configuration data** check box. This option appears only for agentlessly protected Hyper-V or ESXi machines. When the option is selected, all VM configurations for volumes being exported to a VM are included in the exported VM. When the option is cleared, only data (and not VM configurations) are included in the exported VM.

Based on the restore or virtual export type, the **Restore configuration data** option is selected by default in the following situations:

- When restoring data or performing virtual export from a recovery point to the same agentless virtual machine.
- When performing virtual export to a different server of the same hypervisor type. For example, when exporting from a vCenter/ESXi recovery point to a different ESXi VM, or from a Hyper-V recover point a different Hyper-V VM. For both ESXi and Hyper-V, there is no backward compatibility between hypervisor versions.

Otherwise, the **Restore configuration data** option is not selected by default, although you can change the default option by selecting or clearing this setting.

Support for backup and restore of Linux LVM cache volumes

Rapid Recovery continues to enhance its support of Linux by offering backup and restore of Linux LVM cache volumes.

With Logical Volume Management (LVM) caching, the performance of larger and slower logical volumes is improved by using smaller, faster block devices such as SSD drives to store frequently used blocks.

Rapid Recovery release 6.4 can now back up and restore these smaller, faster volumes.

BMR for disk-level agentless backups on Linux

Rapid Recovery continues to enhance its Linux support by adding the ability to perform bare metal restore at the disk level of recovery points from agentlessly protected Hyper-V backups.

When using the Rapid Recovery Core console to perform the BMR, you can connect to the Linux Live DVD, and choose and map disks to restore.

Support for many disk-level volumes for Linux BMR

Previously, when performing bare metal restore from the `local_mount` command line utility, volumes were identified by the drive letter, using alphabetic English characters.

In Rapid Recovery release 6.4, disk-level volumes are now numbered. Instead of using a lettered designation to specify a disk volume, you can specify the numbered disk volume. This change enables you to exceed 26 volumes (a restriction based on 26 alphabetic English characters).

The former command line syntax to restore using `local_mount` was:

```
mount <machine_line_item_number> <base_image_recovery_point_line_number> <volume_letter> <path>, where
```

- `<machine_line_item_number>` is derived from running `lm` output
- the recovery point line number and volume letter are derived from the lettered list of volumes within the recovery point
- `path` is the file descriptor for the actual volume.

When variables are replaced with sample values, this command appears as: `mount 36 5 a /dev/sda1`

Now in the command line you should specify the volume *number*, not letter. Thus the proper command to restore is now: `r 36 5 1 /dev/sda1`

Enhancements

The following enhancements have been added to Rapid Recovery 6.4, or were not previously documented in earlier releases.

- [VMware Workstation 15 now supported](#)
- [Oracle VirtualBox 6.0 now supported](#)
- [VM configuration backup and restore improvements on ESXi](#)
- [Protection of shared VHDX disks for standalone Hyper-V](#)
- [Debian 10 Linux now supported](#)

VMware Workstation 15 now supported

Rapid Recovery Core supports specific versions of VMware Workstation as a target for one-time or continual virtual export.

VMware Workstation version 15 was released on September 24, 2018. Rapid Recovery Core release 6.4 has been fully tested with VMware Workstation version 15 and is fully supported for the near future.

In this release of Rapid Recovery, other support changes for VMware Workstation are applicable. For details, please see [VMware Workstation support changes](#).

Oracle VirtualBox 6.0 now supported

Rapid Recovery Core supports virtual export of recovery points to supported versions of Oracle VM VirtualBox. As of release 6.4, version 6.0 is supported.

VM configuration backup and restore improvements on ESXi

In release 6.3, Rapid Recovery introduced the ability to back up and restore configurations on ESXi.

In release 6.4, this ability is expanded. When restoring from a backed-up configuration file, you now have the option to duplicate the source machine's MAC address, or to use a new one. Similarly, the VM you are exporting can duplicate the source machine's unique Rapid Recovery machine ID, or can generate a new ID.

If replacing the prior VM with the new one, using the same MAC address and RRID are useful features. If creating a new VM that you plan to co-exist with the original, you should assign new MAC address and RRID.

i | **NOTE:** This feature only works when the VM being exported was from ESXi and is again being exported to ESXi.

Protection of shared VHDX disks for standalone Hyper-V

VHDX is the newer Hyper-V storage disk type. Whereas VHD files have a 2 TB capacity, VHDX has a capacity of 64 TB.

A shared VHDX (for example, on a scaleout file server or SOFS) can have more than one owner. Shared VHDX were not visible for protection when only a standalone Hyper-V server was protected with agentless protection in release 6.3.

In release 6.4, Rapid Recovery expands its support of Hyper-V VHDX so that you can protect shared VHDX when protecting a standalone Hyper-V host and the SOFS cluster using agentless protection.

This is an Agent-based feature. When you protect the Hyper-V VM, install Rapid Recovery Agent on the Hyper-V host and SOFS cluster nodes. When viewing the protected Hyper-V host in the Rapid Recovery Core Console, the host and all nodes of the SOFS cluster are visible in the Virtual Machines pane.

Debian 10 Linux now supported

Debian Linux support has been enhanced in this release.

Rapid Recovery Agent now supports Debian Linux 10 in addition to releases 7, 8, and 9.

Deprecated features

The following is a list of features that are no longer supported starting with Rapid Recovery 6.4.

[Upcoming end of support for Rapid Recovery version 6.1.3](#)

[Rapid Recovery support for Microsoft Windows Server 2008 R2 SP1 is deprecated](#)

[VMware Workstation support changes](#)

[vCenter/ESXi support changes](#)

[Hypervisor support changes](#)

[End of support for version 6.3 of Red Hat, CentOS and Oracle Linux](#)

Upcoming end of support for Rapid Recovery version 6.1.3

This notification is for customers who continue to run Rapid Recovery release 6.1.3 or older.

Rapid Recovery version 6.1.3 is in limited support until it is officially discontinued on May 22, 2020.

Other than helping users to upgrade, Quest Data Protection Support is not obligated to assist with discontinued versions. Any issue found with discontinued software is not patched; instead, engineering efforts are focused on supported versions and building new features. If you have a perpetual license, you are welcome to continue using older versions of Rapid Recovery without support.

Users of Rapid Recovery version 6.1.3 or earlier are encouraged to upgrade to fully supported versions, for which enhancements and defect fixes are considered. Please review your requirements and check all systems for compatibility. Supported versions of our software can be found on the [Downloads](#) page of the [Support website](#).

For more information about versions that are fully supported, limited in support, or discontinued, please see the policy detailed on our website. From the Support page, click [Product Life Cycle & Policies](#). Under "Product Support Policies," click to expand the Product Support Life Cycle Policy.

For details on compatibility, please review the latest edition of the *Rapid Recovery System Requirements Guide*, accessible from the [Technical Documentation website](#).

Rapid Recovery support for Microsoft Windows Server 2008 R2 SP1 is deprecated

On January 20, 2020, Microsoft Windows Server 2008 R2 Service Pack 1 reaches end of extended support. As of this date, Microsoft no longer supports any version or service pack (SP) of that Windows Server operating system.

Accordingly, Rapid Recovery support of Windows Server 2008 R2 SP1 is deprecated for Rapid Recovery Core and Agent.

While SP 1 of this OS has been tested and is supported in Rapid Recovery release 6.4, users are advised that future releases of Rapid Recovery will only include limited support for Cores and protected machines running Windows Server 2008 R2 SP1. At that time, 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 Windows Server 2008 R2 SP1 in relation to our software.

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

VMware Workstation support changes

Rapid Recovery customers are advised of the following changes in support for VMware Workstation.

- [Support for VMware Workstation version 11 is discontinued](#)
- [Limited Support for VMware Workstation versions 12 and 14](#)
- [VMware Workstation version 15 now supported](#)

Support for VMware Workstation version 11 is discontinued

VMware Workstation version 11 reached end of general support in June of 2016. Because VMware no longer supports this version, Rapid Recovery support changes from limited support to discontinued support in this release.

Limited Support for VMware Workstation versions 12 and 14

VMware Workstation version 12 reached end of general support in February of 2018. Accordingly, support of this version with Rapid Recovery release 6.4 is deprecated. As of this release, only limited support is available. VMware Workstation version 14 reached end of general support in March of 2019. Accordingly, support of this version with Rapid Recovery release 6.4 is deprecated.

As of Rapid Recovery release 6.4, only limited support is available for these versions of VMware Workstation. users are advised to make plans to migrate to a supported version of VMware Workstation such as version 15.x, which is supported by VMware through March of 2020.

VMware Workstation version 15 now supported

As described in [VMware Workstation 15 now supported](#), VMware version 15 has been tested with Rapid Recovery release 6.4 and is fully supported for the near future.

vCenter/ESXi support changes

VMware vCenter version 5.5 reached end of general support by its manufacturer in September 2018. In Rapid Recovery release 6.3, Quest offered limited support of ESXi 5.5 as an export target and for agentless protection using Rapid Snap for Virtual.

In Rapid Recovery release 6.4, ESXi 5.5 is no longer supported as an export target. Limited support for agentless protection continues in this release.

General support by VMware for ESXi 6.0 is expected to end in March 2020. VMware recommends that its customers upgrade to vSphere 6.5 or vSphere 6.7. Rapid Recovery users are advised to migrate to fully supported versions and be aware of the support dates.

Full support by Quest is provided only until a related product reaches end of general support by its manufacturer; thereafter, its support within Rapid Recovery is limited in that release, and its status is deprecated—it will not be supported in future releases.

For a full list of supported versions for vCenter/ESXi and all other products that Rapid Recovery works with in release 6.4, see the *Rapid Recovery 6.4 System Requirements Guide*.

Hypervisor support changes

Rapid Recovery customers are advised of the following changes for supported hypervisors.

- [Oracle VM VirtualBox](#)
- [VMware Workstation support changes](#)
- [VMware vSphere on ESXi support changes](#)

Oracle VM VirtualBox

Rapid Recovery supports Oracle VM VirtualBox as an export target for virtual machines.

Recent VirtualBox support changes

New in release 6.4 is support for VirtualBox version 6.0.

VirtualBox support matrix

The following matrix shows Quest Data Protection Support status for VirtualBox versions:

Table 1: Oracle VM VirtualBox version support in release 6.4

VirtualBox Version	End of General Support	Support Status in 6.4
5.1	July 2020	Limited support
5.2	July 2020	Supported
6.0	December 2023	Supported

See the [Oracle Lifetime Support Policy](#) on the Oracle website.

VMware Workstation

Rapid Recovery supports VMware Workstation as an export target for virtual machines.

Recent VMware Workstation support changes

- Support for VMware Workstation version 11 is discontinued.
- Support for VMware Workstation versions 12 and 14 is now limited.
- VMware Workstation version 15 is now supported.

VMware Workstation support matrix

The following matrix shows Quest Data Protection Support status for VMware Workstation versions:

Table 2: VMware Workstation version support in release 6.4

Workstation Version	End of General Support	Support Status in 6.4
11.x	June 2016	Limited support
12.x	February 2018	Limited support
14.x	March 2019	Supported

Quest recommends that Rapid Recovery customers using versions of VMware Workstation that are no longer supported or are in limited support upgrade to VMware Workstation 14 (or a later version when supported).

VMware vSphere on ESXi

Rapid Recovery supports VMware vSphere/vCenter on ESXi, both as an export target for virtual machines, and for agentless protection.

Recent ESXi support changes

In September of 2018, vSphere Hypervisor ESXi 5.5 reached end of general support. VMware no longer supports that version of ESXi. Accordingly, only limited support is extended to Quest Data Protection Support customers using ESXi 5.5 in this release.

Additionally, ESXi 6.0 reaches end of general support in March of 2020.

This support applies to ESXi as a target for virtual export, as well as for agentless protection. Support for these versions is deprecated and is expected to be discontinued in an imminent release.

Quest recommends that Rapid Recovery customers using ESXi 5.5 and 6.0 upgrade to vSphere 6.5 or vSphere 6.7.

VMware ESXi support matrix

The following matrix shows Quest Data Protection Support status for VMware vCenter/ESXi versions as a target for virtual export:

Table 3: VMware vCenter/ESXi version support in release 6.4

vCenter/ESXi Version	End of General Support	Support for Virtual Export in 6.4	Support for Agentless Protection in 6.4
ESXi 5.5	September 19, 2018	Not supported	Limited support
ESXi 6.0	March 12, 2020	Supported	Supported
ESXi 6.5	November 15, 2021	Supported	Supported
ESXi 6.7	November 15, 2021	Supported	Supported

See the [VMware Lifecycle Product Matrix](#) on the VMware website.

Microsoft Hyper-V

Rapid Recovery supports Hyper-V both as an export target for virtual machines, and for agentless protection.

Recent Hyper-V support changes

- Windows 8 reached end of support in January 2018. For this release, Quest offers limited support for virtual export to a VM running Windows 8 (64-bit), as well as agentless protection.
- Windows Server 2008 (SP2) and Windows Server 2008 R2 (SP1) were both previously included in the *Rapid Recovery 6.2.1 System Requirements Guide* as being supported for virtual export. These operating systems are no longer supported in release 6.4 for virtual export or agentless support.
- Windows Server 2012 reached end of support in January 2018. Rapid Recovery offers limited support for agentless protection on Hyper-V servers running this operating system. Virtual export to Hyper-V targets running Server 2012 is supported for this release.

- Windows Server 2012 R2 reached end of support in January 2018. Rapid Recovery offers support for agentless protection on Hyper-V servers running this operating system, as well as virtual export to Hyper-V targets running Server 2012 R2. This support is likely to change in future releases.
- Hyper-V running on Microsoft Windows Server versions 2008 R2 SP1, 2012, 2012 R2, 2016, 2019 (limited).
- Limited support is available for Windows Server 2019 as a VM export target in release 6.4. Full support of this hypervisor is expected in future releases.

i **NOTE:** Regarding limited support, Quest Data Protection Support accepts support calls for these features by customers with a current maintenance agreement. Support representatives may offer suggestions and work-arounds when available. Quest does not commit to software patches or revisions related to products or operating systems that have reached end of life. Users are advised that any support provided by Quest for EOL software is deprecated and likely to be discontinued soon.

For information on end-of-life dates, see [Hyper-V Server lifecycle](#) on the Microsoft website.

End of support for version 6.3 of Red Hat, CentOS and Oracle Linux

Quest strives to put resources behind the most recent product releases in order to continually improve and enhance the value of our solutions. In some cases, that means we can no longer support older software versions that interact with our products.

Rapid Recovery release 6.4 no longer supports Red Hat Enterprise Linux version 6.3, or its companion distributions, CentOS 6.3 and Oracle Linux 6.3.

Quest recommends that users upgrade to the most recent Linux version compatible with your needs; for example, upgrade to release 6.6 or 7.x. For an updated list of operating systems supported, always refer to the topic "Rapid Recovery Agent software requirements" in the relevant version of the *Rapid Recovery System Requirements Guide*.

Customers who wish to continue backing up Linux machines using release 6.3 of those Linux distributions can choose to remain on Rapid Recovery Core release 6.3.0, which is the last release to support the specified 6.3 Linux distributions.

Resolved issues

This topic contains resolved issues in the following categories:

- [Core and Windows resolved issues](#)
- [DL appliance resolved issues](#)
- [Documentation resolved issues](#)
- [Linux resolved issues](#)
- [Local Mount Utility resolved issues](#)
- [QorePortal resolved issues](#)

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

Table 4: Core and Windows resolved issues

Issue ID	Resolved Issue Description	Functional Area
109436	On a specific environment, the Agent software on protected Linux machine crashed due to the inability to obtain MBR disk metadata sectors.	Linux, MBR disks
109740	Could not obtain Oracle metadata if the Oracle DB listener had non-default (customized) name.	Oracle protection
109615	Transfer failed for specific ESXi agentless VM with error: "Length cannot be less than zero. Parameter name: length."	Agentless protection, ESXi
109600	Transfer failed for ESXi agentless VM status: 'NotFound' if VM was hosted on vCenter in datacenter sub-folder.	Agentless protection, ESXi
109552	In specific environment with standard phone-home licensing, the Core could not automatically contact the license portal if connection to QorePortal was disabled.	License portal
109513	Rollup failed with error: "Can not find the recovery point with the id [ID]" after specific steps related to the mountability check job.	Rollup, Mounts
109442	On Recovery Points page for ESXi agentless VM, the "Allocated Space" metadata value in the Recovery Points summary table displayed incorrect values for large volumes.	Agentless protection, ESXi, Core Console
109418	Prior to optimizations in registry serialization, in a specific environment, VM export hung at 95% progress and eventually failed with timeout exception "The operation has timed out."	VM export, Core Console
109380	License type of Agent changed from Virtual to Physical after re-protecting an ESXi VM.	Licensing, Agentless protection
109231	Transfer failed due to exception: 'System.NullReferenceException' if ESXi VM was located in a child vApp.	Agentless protection, ESXi
109178	Damaged recovery points were captured for ESXi Agentless VMs using SAN transport mode.	Agentless protection, ESXi, transfer mode
109147	When machines protected with Rapid Recovery Agent 6.1.3 or earlier with high change rates were upgraded to Agent releases 6.2.0, 6.2.1, or 6.3.0, portions of the change log over 1MB were discarded. This resulted in damaged recovery points, which required capture of a new base image to ensure full restore options. For more information, see Quest Knowledge Base article 301910 . Since this defect was corrected in release 6.4, Quest strongly encourages users of Rapid Recovery Agent versions 6.1.3 and older to upgrade directly to release 6.4.x.	Agent upgrade, recovery points
109140	There was no ability to select Hyper-V Generation 2 export for a Windows 2019	Hyper-V, UEFI

Issue ID	Resolved Issue Description	Functional Area
	UEFI agent.	
109129	The Core could not contact the Rapid Recovery License Portal using the "Contact Now" button in Core Settings even when connection to QorePortal was enabled.	Licensing, Core Settings
109059	In a specific environment with a non-typical configuration, mounts failed with Error "TevoMountReplay failed with error -2147024873 (0x80070017 - Data error (cyclic redundancy check))."	Mounts
109044	Damaged recovery points were captured for ESXi agentless VMs if transfer was performed with non-default Outstanding Reads per Stream setting (anything other than 0).	Agentless, Protected machine settings, Transfer
108879	Transfer for ESXi agentless VM fails if name contains Chinese characters	Transfer, agentless protection, localization
108825	For agentlessly protected cluster on ESXi or Hyper-V, there was no ability to associate the cluster to the hypervisor host to decrease license usage.	Hypervisors, clusters, protection, licensing
108782	Transfer failed with error: "Value cannot be null. Parameter name: list" for specific protected windows machine running Rapid Recovery Agent 6.2.1.	Transfer; Agent
108625	VMs agentlessly protected on vCenter Linked agents switch to trial once NPH key with large enough license pool is applied	Licensing, Agentless protection
108611	Incorrect validation message appeared in 'User Name' field when creating Rackspace Cloud Files account.	Cloud accounts
108385	For Cores with protected server clusters, paused protection for clusters (not nodes) resumed without explicit command after Core contacted the License Portal.	Protection, Pause/Resume, server clusters
108313	Upgrade, Deploy and other web-installer depended jobs failed with error code: 3002, "The certificate for MSI issued to Quest Software Inc is invalid."	Web installer, certificates
108174	For a replicated SQL Server cluster running Windows 2008 R2 Systems Configuration Checker (SCC), the error: "public action method 'SqlGrid' was not found on controller Replay.Core.Web.Controllers. ReplicatedClustersController" appeared when trying to open the Summary page for the target Core.	Replication, SQL Server cluster, Agent, Windows 2008 R2
100569	EC2 Export job fails with exception: 'Amazon.EC2.AmazonEC2Exception: The key pair '{key_name}' does not exist.' for replicated Agent from another region	Virtual exports, Amazon E2C

Go to the [top of the Resolved issues topic](#).

Table 5: DL appliance resolved issues

Issue ID	Resolved Issue Description	Functional Area
100569	EC2 Export job fails with exception: 'Amazon.EC2.AmazonEC2Exception: The key pair '{key_name}' does not exist.' for replicated Agent from another region.	Virtual exports, Amazon E2C

Go to the [top of the Resolved issues topic](#).

Table 6: Documentation resolved issues

Issue ID	Resolved Issue Description	Functional Area
108288	In-product help is now available for agentlessly protected ESXi and Hyper-V virtual machines (not just hypervisors) when viewing Active Block Mapping (ABM) settings at the machine level.	Agentless protection, ABM, machine-level settings, In-product help
108327	An incorrect web help link has been removed from the <i>System Information</i> page for protected virtual machines.	Agentless protection, In-product help
108934	Errors that were corrected in the 6.3 User Guide but had not been updated in the in-product help for that release are now also updated in the in-product help content. See the 6.3 release notes for details.	In-product help
N/A	License and copyright information for the components listed in <i>Rapid Recovery release 6.3.0 Release Notes</i> have been added to third-party components visible within in-product help if they are still appropriate. Additionally, the third-party components section contains substantial updates in release 6.4 to ensure all third-party components are identified as required.	Third-party components, licensing, copyright

Go to the [top of the Resolved issues topic](#).

Table 7: Linux resolved issues

Issue ID	Resolved Issue Description	Functional Area
109453	Protected Linux machine captured base image instead of empty incremental when no changes occurred on the protected device.	Base image, backup, Linux
108750	BMR of Linux machine failed to start with error code: ERROR_REG_PARTS while mapping device with size greater than 3 TB.	BMR, Linux Restore, Live DVD

Issue ID	Resolved Issue Description	Functional Area
108395	There was no ability to protect a Linux machine with more than 2000 disk devices attached.	Linux protection
108290	Linux Live DVD did not recognize disks on a specific environment.	Linux, Live DVD
97017	Exported CentOS7 wasn't bootable on the ESX(i) when it had more than 6 system volumes and root volume with the 'xfs' filesystem.	Virtual exports, Linux, XFS


Go to the [top of the Resolved issues topic](#).

Table 8: Local Mount Utility resolved issues

Issue ID	Resolved Issue Description	Functional Area
109087	There was no ability to open Exchange database using Mailbox restore from LMU.	LMU, Exchange protection, Mailbox Restore

Go to the [top of the Resolved issues topic](#).

Table 9: QorePortal resolved issues

QorePortal features a *What's new* article that is refreshed with each deployment to list new features, enhancements, and resolved issues. To access the article, from the QorePortal header, click  **Help Center**. From the *Help Center* header, click **What's new**.

Go to the [top of the Resolved issues topic](#).

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 10: 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	Reduce the number of concurrent exports.	Virtual exports, ESXi

Issue ID	Known Issue Description	Workaround	Functional Area
	the VM configuration location fails with unclear error. The Failure Reason is "Task 'ReconfigVM_Task' failed: Invalid configuration for device '0'."		
109790	This issue applies only to agentlessly protected VMs successfully using a non-phone-home (NPH) front-end capacity license. If the VM is removed from protection and re-protected using the same license, the license status appears as "Trial" instead of "Active."	Completely delete the registry (licenseinfo) hive and apply the NPH key again.	Licensing, agentless protection
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
109188	When setting the protection schedule for an interval of 24:00 (24 hours exactly) and saving as a template, the Core does not apply this template properly. No transfers occur when based on a saved template using this interval. This affects Core releases 6.3.0 and 6.4.0.	Until this defect is addressed, do not use an interval of 24:00. For example, you can use 23:59 .	Protection schedules
108299	Replicated data is incorrectly calculated as protected data when a non-phone-home capacity license is applied on the target Core. "Used by this Core" statistic on the target Core should read "0" or unlimited, since replication data transfer is not counted towards limitations for licensing.	1. Increase license pool size (purchasing additional licenses if necessary). 2. Use another type of license (for example, a standard phone home capacity license).	Replication, licensing
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.	No workaround at this time.	Virtual export
107855	On a specific Dell PowerEdge	Perform BCD queries one at a	Agent hang

Issue ID	Known Issue Description	Workaround	Functional Area
	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.	time, sequentially, to avoid this issue. For diagnostic steps, see Quest Knowledge Base article 259558 .	
107755	When creating an archive using the Archive Wizard, if you return from the <i>Options</i> wizard page back to the <i>Machines</i> page, there is no ability to edit the date range.	Close the wizard without saving the archive, and run through the wizard again.	Archiving, usability
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 <i>Appliance</i> page.	No workaround at this time.	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 <i>Appliance Health</i> page.	No workaround at this time.	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 <i>Compatibility</i> 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.	None available.	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
104393	In a specific environment, when a shadow copy has a specific path, agentless backup fails with "Invalid URI: The hostname could not be parsed" error.	Contact for a patch to address this issue.	Agentless

Issue ID	Known Issue Description	Workaround	Functional Area
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\wddk\bin to the Coreservice folder, and then restart the Core service: <ul style="list-style-type: none"> • glib-2.0 • gobject-2.0 • gvmomi • iconv • intl • libcurl • libxml2 • vixDiskLibVim 	Virtual exports
102756	A deploy to Azure fails if the cloud service name is specified in FQDN format.	Specify only the hostname (without periods) in the Cloud service name text box. For example, instead of specifying companycloudhost.cloudapp.net, enter companycloudhost.	Azure
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
101736	Add menu for switching between pages with recovery points on the top of the Recovery Points page.	None available. This item is an enhancement request.	Recovery Points, GUI
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 11: 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	In-product help, technical product documentation

Issue ID	Known Issue Description	Workaround	Functional Area
1.	<p>References to former topic name "Managing licenses" in the <i>Rapid Recovery 6.4 Installation and Upgrade Guide</i> have been updated to "Understanding Rapid Recovery licenses." The topics in in-product help that use the older topic name are listed below:</p> <ul style="list-style-type: none"> • 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 sets personal information (first sentence, and later in a bulleted list of resources) • Obtaining and using non-phone-home licenses (fourth paragraph) 	<p>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.</p>	

Issue ID	Known Issue Description	Workaround	Functional Area
2.	<p>In the Core settings chapter of the <i>User Guide</i>, 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.</p>	<ul style="list-style-type: none"> • 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
	<p>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".</p>		
109793	<p>Within in-product help, on the <i>Settings</i> page of the Core Console, if you click the  Help icon for the License Details Core setting, a generic error message appears.</p>	<p>To read about licensing in release 6.4, see the Rapid Recovery 6.4 Installation and Upgrade Guide topic "Managing Rapid Recovery licenses."</p> <p>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.</p> <p>The  Help icon will not appear in future editions of in-product help.</p>	<p>In-product help, Rapid Recovery Core Console, Core Settings, License Details</p>
N/A	<p>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.</p>	<p>Consult these notifications in Release Notes for the latest updates to legal and copyright requirements.</p> <p>Component p7zip 16.0.2 uses the Mozilla Public License (MPL) 1.1. A copy of</p>	<p>In-product help, Third-party components, copyrights, legal requirements</p>
	<ul style="list-style-type: none"> Component p7zip 16.0.2 is not included in the list of third-party components available from in-product help for release 6.4. 		

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.	
	<ul style="list-style-type: none"> 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. <p>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.</p>	<p>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.</p> <p>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.</p>	

Go to the [top of the *Known issues* topic](#).

Table 12: Linux known issues

Issue ID	Known Issue Description	Workaround	Functional Area
109902	When a newly created block device is added to an already-protected Linux machine, the Linux driver attaches to the block device without it being explicitly added to protection.	Remove new volume from protection if you do not want to protect it in the Core.	Linux, Agent, protected volumes
109691	When a 6.4 Linux machine with multiple volumes mounted is protected in a 6.4 Core, if one or more volumes is not included in the protection schedule,	Refresh metadata for the affected machine from the Core Console.	Mounted devices, protection,

Issue ID	Known Issue Description	Workaround	Functional Area
	the volume or device remains attached to the Rapid Recovery driver until the data is refreshed for that machine from the Core.		Core Console
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 manually. 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 13: 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	In 6.2x, 6.3x versions of the LMU, there 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

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 6.4 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 6.4 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 14: Compatibility between supported Core and Agent versions

Version	6.2.1 Core	6.3.0 Core	6.4.0 Core
6.2.1 Agent	Fully compatible	Fully compatible	Fully compatible
6.3.0 Agent	Not compatible	Fully compatible	Fully compatible
6.4.0 Agent	Not compatible	Not compatible	Fully compatible

Upgrade and installation instructions

Quest recommends users carefully read and understand the *Rapid Recovery 6.4 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 6.4 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 6.4 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 6.4 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 6.4 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 6.4 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 .

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 6.4 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 6.4 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 6.4 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 .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

© 2019 Quest Software Inc. ALL RIGHTS RESERVED.

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

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS

PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (<https://www.quest.com>) for regional and international office information.



Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <https://www.quest.com/legal>.

Trademarks

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

Legend

-  **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.
-  **NOTE:** An information icon indicates supporting information.

Rapid Recovery Release Notes
Updated - December 2019
Version - 6.4