

Rapid Recovery 6.2

Installation and Upgrade Guide



Table of Contents

Rapid Recovery overview and system requirements.....	5
Introduction to Rapid Recovery.....	5
Where to find Rapid Recovery system requirements.....	6
Installing Rapid Recovery.....	7
Understanding Rapid Recovery components and related products.....	9
About installing the Rapid Recovery Core.....	10
Installing the Rapid Recovery Core.....	12
Installing the Rapid Recovery Agent software.....	16
Obtaining Rapid Recovery software.....	17
Installing the Rapid Recovery Agent software on Windows machines.....	18
Installing the Agent software on Windows Server Core Edition machines.....	20
About installing the Agent software on Linux machines.....	20
Downloading the Linux distribution.....	23
About security.....	23
Location of Linux Agent files.....	23
Agent dependencies.....	24
Linux scripting information.....	25
Installing or upgrading Rapid Recovery Agent on a Linux machine.....	25
Linux commands by package manager.....	27
Installing the Agent software on offline Linux machines.....	28
Configuring the Rapid Recovery Agent on a Linux machine.....	30
Starting and stopping the Linux Agent Daemon.....	31
Automatically installing updates.....	32
About the Quest Data Protection Portal.....	32
Uninstalling the Rapid Recovery Core.....	33
Uninstalling the Rapid Recovery Agent software from a Windows machine.....	34
Uninstalling the Rapid Recovery Agent software from a Linux machine.....	35
Uninstalling the AppAssure Agent software from a Linux machine.....	37
Backing up and restoring the AppAssure agent ID.....	38
Uninstalling the Rapid Recovery Central Management Console.....	39
About the Local Mount Utility.....	39
Downloading the Local Mount Utility.....	40
Installing the Local Mount Utility.....	40
Uninstalling the Local Mount Utility.....	42
Upgrading to Rapid Recovery.....	43
Rapid Recovery Core and Agent compatibility.....	44

Upgrading factors to consider.....	45
Consider localization before upgrading.....	46
Rapid Recovery beta program considerations.....	46
Upgrading AppAssure 5.x Core to Rapid Recovery Core.....	47
Upgrading steps overview.....	48
Preparing the Core server to upgrade.....	50
Upgrading the Rapid Recovery Core.....	50
Upgrading the Rapid Recovery Agent software.....	51
Upgrading Rapid Recovery Agent on a Linux machine.....	52
Managing licenses.....	53
Updating or changing a license.....	55
Adding a license.....	56
Contacting the Rapid Recovery License Portal server.....	57
Viewing license information on a machine.....	57
About us.....	58

Copyright © 2018 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 website (<https://www.quest.com>) for regional and international office information




Patents

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

Trademarks

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

Legend

-  **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.
-  **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.
-  **IMPORTANT, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

Rapid Recovery overview and system requirements

This section includes an introduction to Rapid Recovery and where you can find its system requirements.

Topics include:

- [Introduction to Rapid Recovery](#)
- [Where to find Rapid Recovery system requirements](#)

Introduction to Rapid Recovery

Rapid Recovery is a backup, replication, and recovery solution that offers near-zero recovery time objectives and recovery point objectives. Rapid Recovery offers data protection, disaster recovery, data migration and data management. You have the flexibility of performing bare-metal restore (to similar or dissimilar hardware), and you can restore backups to physical or virtual machines, regardless of origin. Rapid Recovery can also archive to the cloud, to a DL series backup and recovery appliance, or to a supported system of your choice. With Rapid Recovery, you can replicate to one or more targets for added redundancy and security.

Rapid Recovery offers:

- **Flexibility.** You can perform universal recovery to multiple platforms, including restoring from physical to virtual, virtual to physical, virtual to virtual, and physical to physical.
- **Cloud integration.** You can export a VM, archive and replicate to the cloud, and perform bare metal restore from archives in the cloud. Compatible cloud services include Microsoft Azure, Amazon Web Services (AWS), any OpenStack-based provider (including Rackspace), and Google Cloud. US government-specific platforms include AWS GovCloud (US) and Azure Government.
- **Intelligent deduplication.** You can reduce storage requirements by storing data once, and referencing it thereafter (once per repository or encryption domain).
- **Instant recovery.** Our Live Recovery feature allows you to access critical data first, while remaining restore operations complete in parallel.
- **File-level recovery.** You can recover data at the file level on-premises, from a remote location, or from the cloud.
- **File-level search.** Using criteria you specify, you can search a range of recovery points for one or more files. From the search results, you can then select and restore the files you want to the local Core machine directly from the Core Console.
- **Virtual support.** Rapid Recovery supports one-time virtual export, letting you generate a bootable VM from a recovery point; and virtual standby, in which the bootable VM you generate is continually updated after each backup. You can even perform virtual export to Microsoft Hyper-V cluster-shared volumes.
- **Rapid Snap for Virtual support.** Enhanced support for virtualization includes agentless protection for vCenter/ESXi VMs and for Hyper-V VMs. Rapid Snap for Virtual includes protection and autodiscovery for VMware ESXi 5.5 and higher with no agent software installed. Host-based protection supports installing Rapid Recovery Agent on a Microsoft Hyper-V host only, letting you agentlessly protect all its guest VMs.
- **Application support.** Rapid Recovery Agent is built with application support for Microsoft Exchange, SQL Server, and Oracle. When you protect these application servers in your Core, the backup snapshots are automatically application-aware; open transactions and rolling transaction logs are completed and caches

are flushed to disk before creating snapshots. Specific application features are supported, including SQL attachability (for SQL Server) and database integrity DBVERIFY checks (for Oracle). Application awareness also extends to agentless protection for SQL Server and Exchange Server.

See the following resources for more information about Rapid Recovery.

- The Rapid Recovery product support website at <https://support.quest.com/rapid-recovery/>.
- The documentation website at <https://support.quest.com/rapid-recovery/technical-documents/>.

Where to find Rapid Recovery system requirements

As of Rapid Recovery release 6.2, system requirements are documented in the *Rapid Recovery System Requirements Guide*. Use this document as your single authoritative source for system requirements, which are always release-specific.

System requirements and all other documentation is found at the technical documentation website at <https://support.quest.com/rapid-recovery/technical-documents/>.



NOTE: The default view of the [technical documentation](https://support.quest.com/rapid-recovery/technical-documents/) website shows documentation for the most recent generally available version of the Rapid Recovery software. Using the filters at the top of the page, you can view documentation for a different software release or for a Quest DL series backup and recovery appliance. You can also filter the view by guide category.

Installing Rapid Recovery

Install software as a user with administrative privileges. This recommendation applies to all Rapid Recovery software and is not repeated.

Before you install Rapid Recovery, consider which components are necessary for your implementation, as not all components are required. For more information about these components, see [Understanding Rapid Recovery components and related products](#).

Minimum software requirements

At minimum, plan to install the following for your Rapid Recovery environment:

- **Rapid Recovery Core.** You must install Core on a dedicated Windows server that is properly sized for your environment. The server can be a physical or virtual machine, including a Quest DL series backup and recovery appliance. For guidance on sizing your hardware, software, memory, storage, and network requirements, see knowledge base article 185962, "[Sizing Rapid Recovery Deployments](#)".
- **Hypervisor tools.** If your environment includes virtual machines (VMs) hosted on VMware vCenter/ESXi or Hyper-V hypervisors, you can protect VM guests agentlessly using the Rapid Snap for Virtual feature. In such cases, Quest strongly recommends installing VMware Tools or Hyper-V Integration Services utilities on VMs you want to protect. If you want application-consistent agentless backups, this step is required. Otherwise, your backups on VMs running SQL Server or Exchange Server will be crash-consistent only. For more information about the difference between these two states, see "Understanding crash-consistent and application-consistent backups" in the *Rapid Recovery User Guide*.
- **Rapid Recovery Agent.** You must install the Rapid Recovery Agent software on each physical machine you want to protect in your Core. To protect Hyper-V guests agentlessly, install the Rapid Recovery Agent software on the Hyper-V host. To protect nodes in a Hyper-V cluster, install the Agent software on each node. Finally, install Agent on all VMs you want to protect using standard protection instead of Rapid Snap for Virtual agentless protection.
- **Microsoft .NET Framework and ASP .NET role or feature.** Windows operating systems running Rapid Recovery Core or Agent release 6.2 require the Microsoft .NET Framework version 4.6.2. For Core, some operating systems require the corresponding ASP .NET 4.6.2 role or feature. When installing or upgrading Rapid Recovery, the installer checks the system for required .NET components; if needed, the user is prompted to install or activate the components, which requires a reboot of the machine.

Other components may be required for additional functionality.

General installation approach

The steps you must follow to install Rapid Recovery are as follows:

- **Step 1:** Obtain a software license for Rapid Recovery Core. Some users start with a trial version of Rapid Recovery Core. To continue using the Core after the initial trial period, or to use non-trial versions of the Core, a software license is required. If using a trial version and you want to purchase a software license, complete the form at <https://www.quest.com/register/95291/> to be contacted by a Sales representative.
- **Step 2:** Ensure you have an account on the Rapid Recovery License Portal. This portal is used to register and manage software licenses and license groups. Existing AppAssure or Rapid Recovery customers can continue to use their existing license portal accounts. New customers must register on the Rapid Recovery License Portal at <https://licenseportal.com>, activate their software licenses, download the license files from the license portal, and from the Rapid Recovery Core Console, upload license files. For detailed steps, see the *Rapid Recovery Release Notes* topic "Licensing Rapid Recovery software and appliances." For information about managing licenses from the Rapid Recovery Core, including uploading license files to

associate them with the Core, see the topic [Managing licenses](#). For information about managing license subscriptions and license groups on the license portal, see the *Rapid Recovery License Portal User Guide*.

- **Step 3:** Review and ensure that the system requirements have been met for the servers and machines on which you plan to install Rapid Recovery components. For more information, see the *Rapid Recovery System Requirements Guide*.
- **Step 4:** Install the Rapid Recovery Core software on each Windows machine you plan to use as a Core. For more information, see [Installing the Rapid Recovery Core](#).
- **Step 5:** The Core stores backup data in a repository. Before you use the Core to protect machines, if not yet defined, you must specify a storage location and configure a primary repository. You can create a DVM or tiering (secondary) repository as a separate process. You can also create a DVM repository as part of the workflow when using the Protect Machine or Protect Multiple Machines wizards. For detailed information, see "Understanding repositories" in the *Rapid Recovery User Guide*
- **Step 6:** Install the Rapid Recovery Agent software on all physical Windows or Linux machines you plan to protect. Also install Agent on all Hyper-V hosts; on Hyper-V cluster nodes; and on VMs you want to protect without using agentless protection. For more information, see [Installing the Rapid Recovery Agent software on Windows machines](#) and [About installing the Agent software on Linux machines](#).
- **Step 7:** If using Rapid Snap for Virtual to provide agentless protection, install the appropriate hypervisor tool on each VM. For more information, see the topic "Understanding Rapid Snap for Virtual" and subtopics "Benefits of installing hypervisor tools for agentless protection" and "Understanding crash-consistent and application-consistent backups" in the *Rapid Recovery User Guide*.
- **Step 8:** Consider using the Data Protection Portal. If you have a valid Quest Data Protection Support maintenance agreement, you are entitled to use the Data Protection Portal. This portal is automatically integrated with Rapid Recovery as of release 6.2, and replaces the Rapid Recovery Central Management Console in this release. This feature, particularly useful for managed service providers, lets you manage multiple Cores; access a dashboard where you can monitor tasks and events, view repository status, and check system health; generate reports; and perform a growing list of other functions from a single web-based user interface.

i **NOTE:** If you choose not to share personally identifiable information with Quest, you must request a non-phone home license, which will disable connection with the Data Protection Portal and disable automatic update for Core software. Coincidentally, the automatic update feature of Rapid Recovery Core is effectively disabled for release 6.2 (but will be enabled for future releases). For more information, see the subtopic "Automatic update advisory" in the "About this release" section of *Rapid Recovery Release Notes*. For more information about the Data Protection Portal, see [About the Quest Data Protection Portal](#). For information on managing privacy from the Rapid Recovery Core Console, see the topic "Managing privacy" in the *Rapid Recovery User Guide*.

Optionally, you may want to perform other configuration tasks, such as setting encryption keys, configuring event notification, or replicating recovery points from a source Core to a target Core. Each of these configuration tasks is included in the Quick Start Guide feature of Rapid Recovery Core. You can read more information about the Quick Start Guide or performing these tasks independently in the *Rapid Recovery User Guide*. That document also contains information about tasks such as configuring an SMTP server for notification messages, changing the data retention policy, or configuring SQL attachability.

To learn about using scripts or sending commands to manage your Core from the command line, see the *Rapid Recovery Commands and Scripting Reference Guide*. If you want to use other Rapid Recovery components such as Mailbox Restore for Exchange or DocRetriever for SharePoint, see the *Mailbox Restore for Exchange User Guide* or *DocRetriever for SharePoint User Guide*, respectively. If you want to replicate your on-premises installation of Rapid Recovery Core using Microsoft's Azure platform, see the *Rapid Recovery Replication Target for Microsoft Azure Setup Guide*.

Understanding Rapid Recovery components and related products

This section describes the Rapid Recovery components and related products available for your backup, replication, and recovery needs. The purpose of this section is to help you gain an understanding of the components that you may install in your Rapid Recovery environment and how they work together to help protect your data.

- **Rapid Recovery Core.** The central component of the Rapid Recovery architecture, the Core provides the essential services for backup, recovery, retention, replication, archiving, and management. The Core manages the repositories that store your backup data. It contains the settings that change behavior, manages schedules for backups, replication and archives, provides security, and enforces your data retention policy. After the Core is installed, you access it using the web-based interface called the Rapid Recovery Core Console. The Rapid Recovery Core must be installed on a dedicated Windows server. Depending on your license and your environment requirements, you may need to install multiple Cores.
- **Rapid Recovery Agent.** This component is the primary provider of the services and software that let you protect your data. You install Rapid Recovery Agent software on the Windows and Linux machines in your environment (for example, on an Exchange server, SQL Server, Oracle server, on Windows and Linux desktop and laptop machines, and so on). After you add a machine with the Agent software as a protected machine in the Rapid Recovery Core, the Agent software tracks changed data blocks on the disk volume of the machine and creates snapshot images of the data which it sends to the Core, based on the backup schedule. You manage protected machines using the Core Console of the associated Core, including establishing or changing the frequency of backups.



NOTE: If your Core and the machines you want to protect are all ESXi virtual machines on a VMware vSphere host, and if all of the VMs use a supported Windows operating system, then you do not need to install the Agent software. Likewise, if the machines that you want to protect are all Hyper-V virtual machines, you need only install the Agent software on the Hyper-V host server or cluster node host. This agentless protection feature for VMs is called Rapid Snap for Virtual.

- **Data Protection Portal.** This new web-based portal is currently accessible to Rapid Recovery users with a current maintenance agreement. The Data Protection Portal lets you manage your Cores, generate and view reports, manage protection and replication, and perform many other functions from a single modern user interface. This portal replaces the functionality of the now-deprecated Rapid Recovery Central Management Console. This feature is intended to be particularly useful for managed service providers.
- **Rapid Recovery Portal plugin.** The Portal Plugin gives Cores the ability to connect and transfer information to the Data Protection Portal to manage multiple Cores and their protected machines. This plugin for the Core server is required only if you want Rapid Recovery Cores version 6.1.3 and older to communicate with the Data Protection Portal.
- **Rapid Recovery License Portal.** This web-based portal lets you manage licenses for Rapid Recovery Cores. It lets you create and manage groups of licenses, manage license pools, and view machines with licenses registered on the portal. You can generate license-related reports, and download Rapid Recovery software, tools, and components. The Rapid Recovery License Portal integrates with the Data Protection Portal. See [Managing licenses](#) for information about managing licenses from the Rapid Recovery Core Console. For information about managing license subscriptions and license groups on the license portal, see the *Rapid Recovery License Portal User Guide*.
- **Local Mount Utility (LMU).** The Local Mount Utility is a Windows-based application that lets you mount a Rapid Recovery recovery point in any of the three available modes on any compatible Windows machine. The lightweight utility can be installed on the same 32-bit and 64-bit Windows operating systems as the Rapid Recovery Agent software, but it does not have to be installed on the same machine as the Agent.

The LMU includes the rapidrecovery-vdisk (formerly aavdisk) and aavstor drivers, but it does not run as a service. For more information, see the topic "The Local Mount Utility" in the *Rapid Recovery User Guide*.

- **Local_mount Utility.** The local_mount utility is a Linux-based command line utility application that lets you query the Core for protected machines and their corresponding recovery points. It lets users remotely mount a recovery point volume; lets users explore the volume contents at the file levels; and lets users restore individual files or an entire volume from the recovery point, including BMR of the system volume.
- **Rapid Recovery Command Line Management utility.** The Rapid Recovery Command Line Management utility, cmdutil.exe, provides third-party access to manage system functionality. This tool permits scripting of the Rapid Recovery Core management functions. In earlier versions of the Core, this tool was called AACMD. For more information about using this component, see the *Rapid Recovery Commands and Scripting Reference Guide*.
- **Rapid Recovery PowerShell Module.** The Rapid Recovery PowerShell Module is a collection of Windows PowerShell scripts that lets users interact directly with the Core server. This module offers some of the same functionality that the Rapid Recovery Core Console graphic user interface (GUI) provides. For example, the Rapid Recovery PowerShell Module can mount recovery points or force a snapshot of a protected machine. For more information about using this component, see the *Rapid Recovery Commands and Scripting Reference Guide*.
- **Mailbox Restore for Exchange.** This comprehensive email recovery program works with Rapid Recovery and the LMU to simplify the recovery of Exchange items, from a full data store to a single email message. The installer is bundled as an optional feature with Core and the LMU installers. For more information about this component, see the *Mailbox Restore for Exchange User Guide*.
- **DocRetriever for SharePoint.** DocRetriever for SharePoint lets SharePoint administrators recover SharePoint objects from the site collection level down to the component level. This product simplifies recovery of SharePoint data when the Rapid Recovery Agent and DocRetriever Agent are installed on your SharePoint servers. For more information about this component, see the *DocRetriever for SharePoint User Guide*.
- **Azure replication target.** Microsoft Azure users who want to replicate on-premise Rapid Recovery backups from a version 6.x Core to the cloud can use the *Rapid Recovery Replication Target* VM in Azure. The VM is free for licensed Rapid Recovery customers; users are responsible for storage costs associated with storing their replicated backups in the Azure cloud. For more information about this component, see the *Rapid Recovery Replication Target for Microsoft Azure Setup Guide*.

About installing the Rapid Recovery Core

Because the Rapid Recovery Core manages the backups of all protected machines in your environment, you should install the Core software on a dedicated server.

Depending on your license and your environment requirements, you may need to install multiple Cores. If running two or more Cores, consider the following:

- The tools for managing multiple Rapid Recovery Cores have changed in release 6.2. The Central Management Console is now in limited support only. If you manage two or more Cores, Quest recommends that you migrate to the Quest Data Protection Portal. Only the new portal is supported for management of release 6.2 Cores.

If using two or more pre-release 6.2 Cores, you can continue to use the Central Management Console. However, since that component is deprecated, you should plan to migrate to the new Data Protection Portal in the near future. As of release 6.2, you do not need any additional software to manage Cores using the Data Protection Portal.

- Licensing requirements apply to all Core installations, as follows.

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

To use Rapid Recovery Core, you must register it with the Rapid Recovery License Portal. If you do not already have one, you must create a license portal account at <https://rapidrecovery.licenseportal.com/User/Register>. The email address you use to register your license portal account is used in the future for important communication.

i **NOTE:** This license portal was recently rebranded. If you previously registered a license portal account to use with AppAssure or Rapid Recovery, then use that account information. You can log in at <https://licenseportal.com>. Previous license portal users do not need to register a new account for Rapid Recovery.

The license portal identifies a Rapid Recovery Core by its Core ID. For this reason, to avoid a conflict between managing Core IDs, Quest recommends not cloning machines with Rapid Recovery Core installed. In the event you have already done so, then remove the Rapid Recovery Core software on the cloned machine, and then reinstall it. This results in a new Core ID being assigned to the cloned machine.

Rapid Recovery Core users with a valid maintenance agreement can access the Data Protection Portal. This feature, particularly useful for managed service providers, lets you manage multiple Cores; access a dashboard where you can monitor tasks and events, view repository status, and check system health; generate reports; and perform a growing list of other functions from a single web-based user interface.

When installing the Rapid Recovery Core, you can choose to automatically update the Rapid Recovery Core software. You can also choose to be notified about or to ignore updates. Once installation is complete, these settings can be changed at any time. For more information on changing automatic update settings, see the topic "Configuring update settings" in the *Rapid Recovery User Guide*.

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

i **NOTE:** For optimal performance, it is recommended that you install the Rapid Recovery Core on more recent operating systems such as Windows 8.1 or later, or Windows Server 2012 R2 or later.

The Rapid Recovery Core requires a 64-bit Windows platform; 32-bit systems and Linux systems are not supported. For more information, see "Rapid Recovery Core installation requirements" in the *Rapid Recovery System Requirements Guide*. In addition, on Windows 8.1, Windows 10, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 operating systems, you must have the ASP .NET 4.6.2 role or feature installed on the server. If you do not have the feature installed, the Core installer will install it automatically.

After you install the Rapid Recovery Core, you can download the Rapid Recovery Agent installer from the Core or the Rapid Recovery License Portal for each machine that you want to protect using the Rapid Recovery Agent software.

See also: [Installing the Rapid Recovery Core](#)

See also: [Installing the Rapid Recovery Agent software on Windows machines](#)

See also: [About installing the Agent software on Linux machines](#)

Installing the Rapid Recovery Core

Before you begin, see [About installing the Rapid Recovery Core](#).

If upgrading an existing Core, you must first pause any existing protection and replication, and cancel or finish any running jobs. You can accomplish this by temporarily stopping the Core service. For details, see "Restarting or shutting down the Core service" in the *Rapid Recovery User Guide*.

When upgrading an existing Core, protected machines are paused. To resume protection in your upgraded release 6.2 Core, your protected machines must be upgraded to Rapid Recovery Agent version 6.x or later. While no longer supported, you can also protect a machine with AppAssure Agent with version 5.4.3 installed.

To see which operating systems are supported for Rapid Recovery Core release 6.2, see the topic "Rapid Recovery release 6.2 operating system installation and compatibility matrix" in the *Rapid Recovery System Requirements Guide*.

Complete the procedure below to install or upgrade the Rapid Recovery Core.



NOTE: Quest recommends retaining the binary installer file for any currently installed Rapid Recovery software product. You can use this file in the future to reinstall, repair, or remove the software.

1. Download the Rapid Recovery Core installer file from the **Downloads** page of the Data Protection Portal or the Rapid Recovery License Portal; for example:

Core-X64-6.2.x.xxxxx.exe

2. Double-click on the executable Rapid Recovery Core installer file to run the installer.

Depending on the configuration of your machine, the **User Account Control** window or the **Open File - Security Warning** window may appear.

3. If prompted for permission, confirm that you want to run the installer file and make changes to the system.

For more information, see "Rapid Recovery Core installation requirements" in the *Rapid Recovery System Requirements Guide*.

4. If .NET components are missing or need to be upgraded, accept the prompts to download and install the framework. This may require a reboot.
5. In the **Setup** dialog box, from the language field, select the appropriate language and then click **OK**.

The Setup dialog shows progress while the installer is prepared, and then closes.

6. If this machine has an earlier version of the AppAssure Core or Rapid Recovery Core software installed, the **Rapid Recovery Core** dialog box displays a confirmation message. Click **Yes** to confirm that you want to upgrade to the current version. When upgrading, you only see a limited number of steps in the installation wizard.

The dialog box closes, and the Rapid Recovery Core Installation Wizard appears. If this Core is a source or target Core, or if your Core protects machines with Agent versions prior to release 5.4.3, the **Compatibility** page is displayed. Proceed to [step 8](#). If prerequisites must be installed, the **Prerequisites** page is displayed. Proceed to [step 11](#). If neither of these situations applies, the **Progress** page appears and includes a status bar that lets you monitor the progress of the installation. Skip to [step 19](#).

7. If this is the first time the Rapid Recovery Core software is being installed on this machine, the installer prepares the installation, and then the Rapid Recovery Core Installation wizard displays the **Welcome** page. Proceed to [step 9](#).
8. On the **Compatibility** page, if using replication, you may see a relevant informational message. Do one of the following:
 - If the Core you are upgrading is the source Core for replicating to a target Core, you see a message advising you to upgrade the target Core first. Click **Cancel**, and upgrade the target Core first following these instructions. When completed, on the source Core, return to this procedure and begin again.
 - If the Core you are upgrading is the target Core for replicating from a source Core, you see a message informing you that replication will be disabled until you update the source Core. If you want

to upgrade the source Core afterward, repeat this process afterward on the source Core. For now, click **Next**.

The **Privacy Policy** page appears. Skip to [step 15](#).

9. In the Rapid Recovery Core Installation Wizard, on the **Welcome** page, click **Next** to continue with the installation.

The **License Agreement** page appears.

10. On the **License Agreement** page, select **I accept the terms in the license agreement**, and then click **Next**.

The **Prerequisites** page appears. Proceed to the next step.

11. On the **Prerequisites** page, the Rapid Recovery Core installer verifies the existence of prerequisite files.
 - If the prerequisite files do not exist on this machine, the installer identifies which files are needed and displays the results accordingly. Click **Install Prerequisites** or **Click to install**, as appropriate.
 - If the prerequisite files exist, a message appears indicating that all prerequisites are installed on the machine.
12. Once the installation of prerequisite files is completed, click **Next**. Then, do the following:
 - If installing for the first time, the **Installation Options** page appears. Proceed to the next step.
 - If upgrading, the **Progress** page appears and includes a status bar that lets you monitor the progress of the installation. Skip to [step 19](#).
13. On the **Installation Options** page, review the installation options. If necessary, modify them as described below.

- In the **Destination Folder** text field, review the destination folder for the installation. If you want to change the location, do the following:
 - Click the folder icon.
 - In the **Browse to Destination Folder** dialog box, select a new location.
 - Click **OK**.
- In the **Core port number** text field, enter a port number to use for communication between the Rapid Recovery Core and its protected machines.
 - **NOTE:** The default value is 8006. If you change the port number, be sure to make note of it in the event that you need to adjust configuration settings at a later time.
- In the **MongoDB port number** text field, enter a port number to use for communication between Rapid Recovery and the MongoDB service database in which transactional information is stored.
 - **NOTE:** The default value is 27017. If you change the port number, be sure to make note of it in the event that you need to adjust configuration settings at a later time.
- Optionally, in the **Select optional components** area, if you want to install Mailbox Restore, select **Mailbox Restore for Exchange**.

Mailbox Restore for Microsoft Exchange is a comprehensive email recovery program that works with Rapid Recovery and the Rapid Recovery Local Mount Utility (LMU) to recover Exchange items from a full data store to a single email message. For more information about Mailbox Restore, see the *Mailbox Restore for Exchange User Guide*.

14. Once you are satisfied with the installation options, click **Next**.

The **Privacy Policy** page appears.

15. For General Data Protection Regulation (GDPR) compliance, Quest offers users control of their personally identifiable information (PII). Select from one of the options below, and then click **Next** or **Install**, as appropriate.

Option	Description
I accept this use of personal data.	<p>Select this option if you want to take advantage of automatic updates or use the Data Protection Portal to manage multiple Cores, generate reports, and more.</p> <p>i NOTE: The automatic update feature of Rapid Recovery Core is effectively disabled for release 6.2 (but will be enabled for future releases). For more information, see the subtopic "Automatic update advisory" in the "About this release" section of <i>Rapid Recovery Release Notes</i>.</p>

I do not accept this use of personal data.	<p>Use this option if you do not want to share the limited set of PII collected by Rapid Recovery Core. If you select this option you cannot use automatic updates or view information about any Cores or protected machines on the Data Protection Portal. Unless using a trial version, if you continue with installation using this option, you cannot use the Core until you obtain and register a non-phone-home license from the Rapid Recovery licensing team.</p>
--	---

For more information about managing your PII, the GDPR, the functions you cannot perform if you do not accept the use of personal data, and how to obtain a non-phone-home license, see the topic "Managing privacy" in the *Rapid Recovery User Guide*.

16. Choose from one of the following:

- If you accepted the use of personal data, and are installing Core on this machine for the first time, the **Update Options** page appears. Proceed to the next step.
- If you accepted the use of personal data and are upgrading from a previous version of Core, and if the machine being upgraded has not met all prerequisites, the **Prerequisites** page appears. Proceed to [step 11](#).
- If you accepted the use of personal data, are upgrading from a previous version of Core, and the machine being upgraded has met all prerequisites, the **Progress** page appears and includes a status bar that lets you monitor the progress of the installation. Skip to [step 19](#).
- If you declined the use of personal data, the **Progress** page appears and includes a status bar that lets you monitor the progress of the installation. Skip to [step 19](#).

i **NOTE:** If you choose not to share personally identifiable information with Quest, you must request a non-phone home license, which will disable connection with the Data Protection Portal and disable auto update for Core software. For more information about this portal, see [About the Quest Data Protection Portal](#). For information on managing privacy from the Rapid Recovery Core Console, see the topic "Managing privacy" in the *Rapid Recovery User Guide*

17. On the **Update Options** page, choose from one of the options described in the following table.

Option	Description
Automatically install updates (recommended)	<p>If you select this option, the Rapid Recovery Core will automatically compare your version of the Core with the latest version available in the manifest, once weekly. If a minor update is available (for example, upgrade to 6.2 from 6.1.3), the updated version is installed automatically after the nightly</p>

Option	Description
	<p>jobs have completed. If a major upgrade is available (for example, upgrade to 6.1 from 5.4.3), you will see an alert at the top of the Rapid Recovery Core Console when a newer version is available, including a link to download the update.)</p> <p>i NOTE: Until users upgrade to Core release 6.2, automatic update has been intentionally disabled, and you will not be notified of its availability by alert at the top of the Core Console. You must upgrade to this release manually.</p> <p>When using replication, configuring your system to install updates automatically could result in upgrading the source Core before the target Core. Updating Cores in this sequence may result in replication failure or the inability to set up new replication between Cores.</p> <p>For replication users, Quest recommends administrators apply automatic upgrades only to the target Core, and then manually upgrade the source Core, and lastly upgrade the protected machines.</p>
Notify me about updates, but do not install them automatically	If you select this option, you will see an alert at the top of the Rapid Recovery Core Console when a newer version is available, including a link that will download the update.
Never check for updates	If you select this option, you will not be notified when a newer version is available.

18. Click **Install**.

The **Progress** page appears and includes a status bar that lets you monitor the progress of the installation.

19. When the installation has finished, the **Completed** page appears.

20. On the **Completed** page, if a reboot of the Core server is required, you see a message displayed. In such cases, Quest recommends rebooting the Core server after installation. Do one of the following:

- To reboot immediately, select **Yes, I want to restart my computer now** and then click **Finish** to close the installer and reboot immediately.
- If you plan to reboot at a later time, click **Finish** to close the installer.

The installer closes and, if you selected the option, the Core server restarts.

i **NOTE:** Unless you installed a trial version, the first time you open the Rapid Recovery Core, you will need to enter your license information. If you declined to share PII with Quest, you must obtain and register a non-phone home key before using your Core. For more information about managing your PII, the GDPR, the functions you cannot perform if you do not accept the use of personal data, and how to obtain a non-phone-home license, see the topic "Managing privacy" in the *Rapid Recovery User Guide*. For more information about registering a phone-home or non-phone-home license with your Core, see [Updating or changing a license](#).

For new Core installations:

- You must create a repository in a storage location designated for your Core. For information about repositories, see the "Repositories" section of the *Rapid Recovery User Guide*.
- You can protect virtual machines agentlessly, or install the Agent software on physical or virtual machines, and then add those machines to protection on your Core. For more information about protecting machines in your Core, see the section "Protecting machines" in the *Rapid Recovery User Guide*. For more information about agentless protection, including some important exclusions, see the topic "Understanding Rapid Snap for Virtual" in the *Rapid Recovery User Guide*.

For upgrades of the Core software:

- Backups and replication are paused during the upgrade process. Do not forget to resume protection or replication to continue protecting your data.
- When upgrading your Core, if you declined to share PII with Quest, you must obtain and register a non-phone home key before using your Core. For more information, see the topic "Managing privacy" in the *Rapid Recovery User Guide*.

For information about configuring the Rapid Recovery Core and protecting and managing your data, see the *Rapid Recovery User Guide*.

Installing the Rapid Recovery Agent software

i **NOTE:** As of release 6.2, unless using capacity-based licensing, a Rapid Recovery software license is consumed from your Enterprise license pool for each installation of Rapid Recovery Agent installed and protected on your Core. If protecting virtual machines on ESXi and Hyper-V hosts, Quest recommends uninstalling the Agent software and protecting those machines using Rapid Snap for Virtual agentless protection. Agentless protection offers several advantages and some restrictions, as described in the topic "Understanding Rapid Snap for Virtual." If interested in reducing the amount of licenses consumed, see the topic "Choosing Agent-based or agentless VM protection." Finally, if your VMs are running server applications such as Microsoft Exchange and Microsoft SQL Server, you must enable application support to protect them agentlessly. This process is described in "Enabling application support." These topics all appear in the *Rapid Recovery User Guide*.

For agent-based protection, install the Rapid Recovery Agent software on machines that you want to protect with Rapid Recovery Core, using the criteria specified below.

If upgrading a Linux machine from AppAssure Agent to Rapid Recovery Agent, perform these basic steps:

1. Optionally, back up the agent ID information associated with that protected machine.
For more information, see [Backing up and restoring the AppAssure agent ID](#).
2. Completely remove the AppAssure Agent software from the machine using a shell script.
For more information, see [Uninstalling the AppAssure Agent software from a Linux machine](#).
3. Install Rapid Recovery Agent.
For more information, see [About installing the Agent software on Linux machines](#).
4. Configure the Agent software on the upgraded machine.
For more information, see [Configuring the Rapid Recovery Agent on a Linux machine](#).
5. Restore the agent ID.

This process is also described in the topic [Backing up and restoring the AppAssure agent ID](#).

i **NOTE:** After updating Rapid Recovery Agent, the first snapshot will result in a base image, creating a new recovery point chain.

For new installations, or if the drivers have changed in the version of the Rapid Recovery Agent software to which you are upgrading, you are prompted to restart your system.

Install the Rapid Recovery Agent software on machines that you want to protect using the following criteria:

- Install Rapid Recovery Agent software on every physical machine in your environment.
- Install Rapid Recovery Agent software on every hypervisor host you want to protect.



NOTE: Optionally, you can protect supported versions of ESXi hosts agentlessly in the Core. Its guest machines can also be protected agentlessly. For more information about agentless protection, see the previously mentioned topics in the *Rapid Recovery User Guide*. For information on supported hypervisors and versions, see "Hypervisor requirements" in the *Rapid Recovery System Requirements Guide*.

- If protecting Hyper-V guest virtual machines agentlessly, install Rapid Recovery Agent software on the Hyper-V host.
- Install Rapid Recovery Agent software on every Hyper-V or ESXi VM you explicitly want to protect with the Agent (regardless of license consumption) instead of agentlessly.



NOTE: For specific information relevant to your decision, see the previously mentioned topics in the *Rapid Recovery User Guide*.

- Install Rapid Recovery Agent software on every XenServer VM or VMs hosted on Amazon Web Services or Azure hosted machines that you want to protect in your Rapid Recovery Core.
- Install Rapid Recovery Agent software on each VM (node) hosted on a Hyper-V cluster that you want to protect with the Agent, instead of agentlessly.

Review the methods to obtain the Rapid Recovery Agent software and determine which method you will use. Then obtain the software, and install on the machines you want to protect on the Rapid Recovery Core. Finally, add the machines to protection on your Core.



NOTE: Quest recommends retaining the binary installer file for any currently installed Rapid Recovery software product. You can use this file in the future to reinstall, repair, or remove the software.

Related tasks

See also: [Installing the Rapid Recovery Agent software on Windows machines](#)

See also: [Installing the Agent software on Windows Server Core Edition machines](#)

Related reference

See also: [Obtaining the Rapid Recovery Agent software](#)

See also: [Installing the Agent software on Linux machines](#)

Obtaining Rapid Recovery software

You can obtain Rapid Recovery software using the following methods:

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

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

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

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

Installing the Rapid Recovery Agent software on Windows machines

Deploy the Rapid Recovery Agent installer file to the machine you want to protect using one of the methods described in [Installing the Rapid Recovery Agent software](#). Then launch the installer program as described below to install or upgrade the software on each Windows machine you want to protect in the Rapid Recovery Core.



NOTE: You must run the installer with local administrator privileges.

The procedure for installing on Windows Server Core editions differs than other versions of Windows, since that version describes how to install from the command line. For more information, see [Installing the Agent software on Windows Server Core Edition machines](#).

1. From the machine you want to protect, double-click on the executable Rapid Recovery Agent installer file to start the installer.

Depending on the configuration of your machine, the **User Account Control** window or the **Open File - Security Warning** window may appear.


2. If prompted for permission, confirm that you want to run the installer and make changes to the system.
3. If .NET components are missing or need to be upgraded, accept the prompts to download and install the framework. This may require a reboot.
4. In the **Setup** dialog box, from the language field, select the appropriate language and then click **OK**.
5. Choose from one of the following:

- If this is the first time the Rapid Recovery Agent software is being installed on this machine, the installer prepares the installation, and then the Rapid Recovery Agent Installation Wizard appears. Proceed to [Step 6](#).
- If this machine has an earlier version of the AppAssure Agent or Rapid Recovery Agent software installed, you will see a message asking if you want to upgrade to the current version.

1. Click **Yes**.

The Rapid Recovery Agent Installation Wizard appears, showing the **Progress** page of the wizard. The application downloads to the destination folder, with progress displayed in the progress bar. When finished, the wizard automatically advances to the **Completed** page.

2. Skip to [Step 12](#).
6. In the Rapid Recovery Agent Installation Wizard, on the **Welcome** page, click **Next** to continue with the installation.
The **License Agreement** page appears.
7. On the **License Agreement** page, select **I accept the terms in the license agreement**, and then click **Next**.
The **Prerequisites** page appears.
8. The Rapid Recovery Agent Installer verifies the existence of the prerequisite files.
 - If the prerequisite files exist, a message appears indicating that all prerequisites are installed on the machine.
 - If the prerequisite files do not exist, the Rapid Recovery Agent Installer identifies which files are needed and displays the results accordingly. Click **Install Prerequisites**.
9. When the installation of the prerequisite files is completed, click **Next**.
The **Installation Options** page appears.
10. On the **Installation Options** page, review the installation options. If necessary, modify them as described below.
 - In the **Destination Folder** text field, review the destination folder for the installation. If you want to change the location, do the following:
 - Click the folder icon.
 - In the **Browse to Destination Folder** dialog box, select a new location.
 - Click **OK**.
 - In the **Port Number** text field, enter a port number to use for communication between the Agent software on the protected machine and the Rapid Recovery Core.

 **NOTE:** The default value is 8006. If you change the port number, be sure to make note of it in the event that you need to adjust configuration settings at a later time.
11. Once you are satisfied with the installation options, click **Install**.
The **Progress** page appears, and includes a status bar that lets you monitor the progress of the installation.
When the installation is complete, the **Completed** page appears. Skip to [Step 12](#).
12. On the **Completed** page, if you see a message indicating that the system must be restarted before the installation takes effect, perform one of the following steps:
 - To restart now, select **Yes, I want to restart my computer now**.
 - To restart later, clear the **Yes, I want to restart my computer now** option.
13. On the **Completed** page, click **Finish**.
The installer wizard closes, and the Agent installation is complete. If you designated this option, the machine may restart if necessary.

Related tasks

See also: [Installing the Agent software on Windows Server Core Edition machines](#)

Related reference

See also: [Installing the Rapid Recovery Agent software](#)

Related information

[Rapid Recovery system requirements](#)

Installing the Agent software on Windows Server Core Edition machines

Complete the steps in the following procedure to install the Rapid Recovery Agent software on a Windows Server Core machine.



NOTE: The following procedure installs the Agent software in console mode. To install in silent mode instead, append `/silent` to the installer file name on the command line. For example, `Agent-X64-6.2.X.xxxxx.exe /silent`.

After each

1. Download the Rapid Recovery Agent installer file from the Rapid Recovery License Portal or from the Rapid Recovery Core.
2. To begin the installation, type the path and name of the installer file.

For example, if the installer is located in path `C:\installers`, type the following command and then press **Enter**:

```
C:\installers\Agent-X64-6.2.x.xxxxx.exe
```

The installation program launches.

The **Setup** dialog box appears.

3. In the Setup dialog box, select a language and then click **OK**.

The dialog box closes, and the **Select installation progress** console displays, showing prompts for required input.

4. At the `destination folder` prompt, type the destination path to install the Rapid Recovery Agent files.

For example, type `C:\Program Files\AppRecovery\Agent` and then press **Enter**.

5. At the `port number` prompt, type the desired port for the Agent software.

For example, type `8006` and then press **Enter**.

6. If the installer identifies prerequisite files, each is listed in the console. To continue the installation at the prompt, type `1` to confirm and then press **Enter**.

The console refreshes and shows you installation progress.

7. After installation is complete, if you are prompted to restart the machine, type `1` to confirm and then press **Enter**.

If prompted, you must restart the newly protected machine to begin protecting your data using Rapid Recovery Core.

About installing the Agent software on Linux machines

For each new software release, Quest creates Agent repository packages for use on Linux machines. You must use an appropriate package manager (yum, zypper, or apt) to work with these packages. Download the appropriate package for the Linux distribution and version you want to protect.



NOTE: At the time of publication, the 6.2 version of Rapid Recovery Agent for Linux was not yet available. If upgrading your Core to release 6.2, continue protecting your Linux machines with Rapid Recovery Agent release 6.1.3.

NOTE: If upgrading your Linux Agent from an earlier release, the 6.1.3 Agent version is available for download on the Support website, , and the Rapid Recovery License Portal. The Linux repository packages for each distribution include the release number, for clarity.

NOTE: When a 6.2 release for Linux is generally available, the earlier versions of each download will be replaced with the corresponding 6.2 Agent repository package. Release Notes will also be updated to reference the updated Linux Agent versions.



NOTE: For more information about installing the Linux Agent software, see step 6 of the topic [Installing or upgrading Rapid Recovery Agent on a Linux machine](#).

Each repository package creates a local software repository on your Linux machine, which can retrieve the files necessary to install or remove Rapid Recovery Agent.

When installing the Rapid Recovery Agent software on Linux machines that you want to protect, use the following prerequisites and guidance.

Prerequisites for installation on Linux machines

If AppAssure Agent software is currently installed on a Linux machine and you want to upgrade it to Rapid Recovery Agent to take advantage of new features, then note the following:

- Consider backing up the agent ID for each Linux machine before removing AppAssure Agent. Without unique identifiers, you will be unable to connect to existing recovery points saved to the Core for that protected Linux machine. For more information, see [Backing up and restoring the AppAssure agent ID](#).
- Remove the AppAssure Agent from the machine using the AppAssure installation script. If you have not retained the installer script, you can manually uninstall the legacy version. For more information, see [Uninstalling the AppAssure Agent software from a Linux machine](#). [Check to see that this procedure addresses all distributions.]
- The operating system on the Linux machine must be a supported distribution, as listed in the topic "Rapid Recovery Agent software requirements" in the *Rapid Recovery System Requirements Guide*.

Deploying and installing the Agent software on Linux machines from the Core Console

The following items are prerequisites for deploying Agent to Linux machines when you select **Deploy Agent Software** from the Protect drop-down menu. This action pushes the repository package to the selected Linux machine.

- SSH Server must be running on the Linux machine you want to protect. You can confirm on the Linux machine from the root account by entering the command: `netstat -antp | grep ssh`.
- The firewall on the Linux machine you want to protect must be disabled, or not blocking port 22.
- The current Linux user must be a non-root user account with sudo privileges. To confirm, make sure that your user account is a member of the sudo, wheel, or root group by entering the command: `groups <username>`.
- The wget utility must be installed on the Linux machine you want to protect. To confirm, run the command: `which wget`.

Guidelines for installation on Linux machines

AppAssure Agent software used installer shell scripts to install or remove the Agent software from Linux machines. Rapid Recovery Agent is installed or removed on Linux machines using a package manager utility (such as yum, zypper or apt). The following factors apply:

- You must use the package manager appropriate to your Linux distribution and version. For more information, see the table in [Installing or upgrading Rapid Recovery Agent on a Linux machine](#)
- Quest provides an Agent repository package for each supported Linux distribution. For each Linux machine you want to protect, you can download this Linux archive package from the Rapid Recovery License Portal.

Pay attention to details to ensure you download the version specific to the Linux distribution and version you want to protect.

- Each Linux archive (repository package) contains the files necessary to set up a software repository (`rapidrecovery-repo`) locally on the Linux machine you want to protect. The software repository is used for staging files for the relevant package managers.



NOTE: The local software repository is not related to the DVM repository associated with your Rapid Recovery Core, in which backup data is saved.

After you install the software repository on your Linux machine, the package manager is able to retrieve and install the packages needed for installation or removal of Rapid Recovery Agent software and related components, such as `local_mount`, `rapidrecovery-vdisk`, and `Mono`.

For each package manager, you can run the appropriate command at the command line to determine if it is configured to download Rapid Recovery packages. These commands are listed in the following table.

- Installations of Agent on a Linux machine with access to the internet are called online installations, and use the process described in the topic [Installing or upgrading Rapid Recovery Agent on a Linux machine](#).
- Each time you upgrade the Agent software on a Linux machine, you must remove the previous local repository and install its replacement. This process is represented by steps 3 and 4 in that topic.
- Installations of Agent on a Linux machine with no access to the Internet (such as air-gapped or secured standalone machines) are called offline installations. For offline installations, you must first download an installation package from a Linux machine with Internet access. Then, move those installation files to the secured computer for installation. For more information, see the topic [Installing the Agent software on offline Linux machines](#).

After configuring the newly installed Agent software on a Linux machine, you must restart the machine. Restarting ensures that the proper kernel module version is used to protect your machine.

Guidelines for upgrading on Linux machines

Previous versions of the AppAssure Agent software must be removed from a Linux machine before installing the Rapid Recovery Agent version and protecting the Linux machine using the Rapid Recovery Core. This requirement applies to both online and offline installations. For more information, see [Uninstalling the AppAssure Agent software from a Linux machine](#).

Thus, the installation process when upgrading from AppAssure to Rapid Recovery involves:

- Backing up the agent ID (optional, but recommended).
- Removing the AppAssure Agent software (not required for first-time installations).
- On each Linux machine, downloading the repository package relevant to that distribution and version.
- Follow the procedure for installing Rapid Recovery Agent using the package manager, which creates the local software repository.
- Run the configuration utility to set ports, configure users, add firewall exclusions, install the kernel module, and start the Agent service.
- Restart the Linux machine.

See the following important information before you begin installation of Agent software.

- [Downloading the Linux distribution](#)
- [About security](#)
- [Location of Linux Agent files](#)
- [Agent dependencies](#)
- [Linux scripting information](#)

Guidelines for upgrading from Rapid Recovery Agent to a newer Agent version

When you upgrade from one version of Rapid Recovery Agent to another, you must first remove the local software repository. During the installation process, a new local repository is created with the appropriate

installation files. Steps are included in the topic [Installing or upgrading Rapid Recovery Agent on a Linux machine](#) specific to upgrading.

Thus, the installation process when upgrading versions of Rapid Recovery involves:

- On each Linux machine, downloading the repository package relevant to that distribution and version.
- Follow the procedure for installing Rapid Recovery Agent using the package manager, including removing the existing local software repository for Rapid Recovery files.
- Run the configuration utility to set ports, configure users, add firewall exclusions, install the kernel module, and start the Agent service.
- Restart the Linux machine.

After installation on Linux machines

After installing Rapid Recovery Agent, configure the Agent software as described in the topic [Configuring the Rapid Recovery Agent on a Linux machine](#).

CAUTION: After configuring the newly installed Agent software on a Linux machine, restart the machine. Restarting ensures that the proper kernel module version is used to protect your machine.

Downloading the Linux distribution

You must download the distribution-specific 32-bit (x86) or 64-bit installer on every Linux machine that you want to protect. You can download the installers from the Rapid Recovery License Portal at <https://licenseportal.com>.

About security

Linux uses the Pluggable Authentication Module (PAM) to manage security. Once a user is authenticated through libpam, the user is only authorized to protect the machine if the user is in one of the following groups: sudo, admin, recovery, root, or wheel. For information on protecting a machine, see the section “Protecting a Machine” in the *Rapid Recovery User Guide*.

Location of Linux Agent files

There are several files required to support the Rapid Recovery Agent software on a Linux machine. For all supported Linux distributions, these files are located in the following directories:

- **mono:**
`/opt/apprecovery/mono`
- **agent:**
`/opt/apprecovery/agent`
- **local mount:**
`/opt/apprecovery/local_mount`
- **rapidrecovery-vdisk and aavdctl:**
`/usr/bin/aavdisk`
- **configuration files for rapidrecovery-vdisk:**
`/etc/apprecovery/aavdisk.conf`
- **wrappers for agent and local_mount**
`/usr/bin/agent`

```
/usr/bin/local_mount
```

- autorun scripts for agent and vdisk services:

```
/etc/init.d/rapidrecovery-agent  
/etc/init.d/rapidrecovery-vdisk
```

Agent dependencies

The following dependencies are required and are installed as part of the Agent installer package:

- For Debian 7 and Ubuntu 12.xx and 14.xx:
 - The rapidrecovery-agent requires:
lsscsi, libblkid1, e2fslibs, libpam0g, libc6, libpcre3, perl, make, e2fsprogs, xfsprogs, python-minimal, apprecoverly-dkms, rapidrecovery-mono, sysvinit-utils
 - The apprecoverly-dkms requires:
module-init-tools, gcc, build-essential, coreutils (>= 7.4), patch
- For Debian 8 and 9 and Ubuntu 15.xx, 16.xx, and 17.xx:
 - The rapidrecovery-agent requires:
lsscsi, libblkid1, e2fslibs, libpam0g, libc6, libpcre3, perl, make, e2fsprogs, xfsprogs, python-minimal, apprecoverly-dkms, rapidrecovery-mono, systemd
 - The apprecoverly-dkms requires:
module-init-tools, gcc, build-essential, coreutils (>= 7.4), patch
- For Red Hat Enterprise Linux 6, CentOS 6, and Oracle Linux 6:
 - The rapidrecovery-agent requires:
lsscsi, make, gcc, pam, pcre, glibc, python, perl, e2fsprogs, apprecoverly-dkms, rapidrecovery-mono, nbd, libblkid, e2fsprogs-libs, xfsprogs, ntsysv
 - The nbd requires:
apprecoverly-dkms
 - i** **NOTE:** nbd is a Network Block Device, used to access storage remotely across the network instead of residing locally. If the nbd module is compiled into the kernel, Linux can use a remote server as one of its block devices. Every time the client machine wants to read `/dev/nbd0`, it sends a request to the server using TCP. The server replies with the data requested. Unlike NFS, it is possible to put any file system on it, but nbd does not allow shared access from multiple machines.
 - The apprecoverly-dkms requires:
coreutils, cpio, findutils, gawk, gcc, grep, gzip, sed, tar, bash > 1.99, module-init-tools
- For Red Hat Enterprise Linux 7, CentOS 7, and Oracle Linux 7:
 - The rapidrecovery-agent requires:
lsscsi, make, gcc, pam, pcre, glibc, python, perl, e2fsprogs, apprecoverly-dkms, rapidrecovery-mono, nbd, libblkid, e2fsprogs-libs, xfsprogs, systemd
 - The nbd requires:
apprecoverly-dkms
 - The apprecoverly-dkms requires:


```
bash > 1.99, coreutils, cpio, findutils, gawk, gcc, grep, gzip, kmod, sed,
systemd, tar, rpmlib
```

- For SUSE Linux Enterprise Server 11:

- The rapidrecovery-agent requires:

```
lsscsi, make, libblkid1, libext2fs2, pam, pcre, glibc, xfsprogs, python,
perl, apprecrecovery-dkms, rapidrecovery-mono, sysvinit
```

- The apprecrecovery-dkms requires:

```
coreutils, cpio, findutils, gawk, gcc, grep, gzip, sed, tar, bash > 1.99,
module-init-tools
```

- For SUSE Linux Enterprise Server 12:

- The rapidrecovery-agent requires:

```
lsscsi, make, libblkid1, libext2fs2, pam, pcre, glibc, xfsprogs, python,
perl, apprecrecovery-dkms, rapidrecovery-mono, systemd
```

- The apprecrecovery-dkms requires:

```
bash > 1.99, coreutils, cpio, findutils, gawk, gcc, grep, gzip, kmod, sed,
systemd, tar, rpmlib
```

Linux scripting information

Information about Bourne Shell scripting supporting Linux protected machines is now included in the *Rapid Recovery Commands and Scripting Reference Guide*. See the topic "Using Bourne Shell and Bash scripting with Rapid Recovery."

Installing or upgrading Rapid Recovery Agent on a Linux machine

This procedure assumes that AppAssure Agent is not installed. If that software is currently installed on the Linux machine and you want to upgrade to Rapid Recovery Agent to take advantage of new features, you must first uninstall AppAssure Agent. Before removing, consider backing up the agent ID for each Linux machine before upgrading. For more information, see [Backing up and restoring the AppAssure agent ID](#) and [Uninstalling the AppAssure Agent software from a Linux machine](#).

See the prerequisite steps in the topic [About installing the Agent software on Linux machines](#) before continuing with this procedure.

Standard online installations of Rapid Recovery Agent require an internet connection on the Linux machine you want to protect. You can obtain the latest Agent software from the Rapid Recovery License Portal in the form of a repository package (a Linux archive with the appropriate files). The files are extracted and installed using a package manager appropriate for the Linux version you want to protect.

If you want to protect a Linux machine that is offline (such as an air-gapped secure computer or a machine in a remote location), instead of using package managers and repository packages, you can download a shell script from the license portal. This single script can be used to install Rapid Recovery Agent on any supported Linux distribution and version. For more information, see [Installing the Agent software on offline Linux machines](#).

The Linux distributions that Rapid Recovery supports use the package manager utilities shown in the following table.

Table 1. Linux distributions and relevant package managers

Linux Distribution	Package Manager
Linux distributions based on Red Hat Enterprise Linux (RHEL), including RHEL, CentOS, and Oracle Linux	yum
SUSE Linux Enterprise Server (SLES)	zypper
Linux distributions based on Debian, including Ubuntu	apt

To install or upgrade Agent on a Linux machine, you must obtain the repository package relevant to your Linux distribution and version. These packages are found on the Rapid Recovery License Portal, as described in step 6.

The package managers work with a local Rapid Recovery repository created as part of this process. The local repository retrieves packages and files from remote repositories that Quest maintains for each specific Linux distribution. This process guarantees you have the correct files accessible for the Linux machine you want to protect.

If installing Rapid Recovery Agent for the first time, there is no need to uninstall software, or back up any configuration files.

If Rapid Recovery Agent is already installed and you are upgrading your Linux machine to a new version, steps are included to remove the previous local software repository.

Complete the following steps to install or upgrade the Rapid Recovery Agent on any supported Linux distribution.

1. Open a terminal session with root access.
2. If Rapid Recovery Agent was never installed on this machine, skip to step 6. Otherwise, proceed to the next step.
3. If upgrading from a previous version of Rapid Recovery Agent, verify whether a local software repository is installed. Type the command shown below for the appropriate Linux distribution, and then press **Enter**:

Option	Command
RHEL, CentOS, and Oracle Linux	<code>rpm -qa grep rapidrecovery-repo</code>
SLES	<code>rpm -qa grep rapidrecovery-repo</code>
Debian and Ubuntu	<code>dpkg -l grep rapidrecovery-repo</code>

If the repository for staging Rapid Recovery Agent files already exists, a value is returned; otherwise, no output results from this command.

4. If the repository exists, remove it. Type the command shown below for the appropriate Linux distribution, and then press **Enter**:

Option	Command
RHEL, CentOS, and Oracle Linux	<code>rpm -e rapidrecovery-repo</code>
SLES	<code>rpm -e rapidrecovery-repo</code>
Debian and Ubuntu	<code>dpkg -P rapidrecovery-repo</code>

The repository is removed.

5. Determine if the package manager is configured to download Rapid Recovery. Run the following command, and view the output. Type the command shown below for the appropriate Linux distribution, and then press **Enter**:

Option	Command
RHEL, CentOS, and Oracle Linux	<code>yum repolist</code>
SLES	<code>zypper repos</code>
Debian and Ubuntu	<code>ls /etc/apt/sources.list.d</code>

The output lists existing local repositories. If Rapid Recovery is not listed in the output, then the local software repository has not been installed.

6. Download the new repository package from the license portal following the steps below.
 - a. Log into the Rapid Recovery License Portal at <https://licenseportal.com>.
 - b. From the left navigation menu, select **Downloads**.
 - c. On the **Downloads** page, scroll down to the Linux-Based Applications section.
 - d. Download the Agent repository package for the appropriate Linux distribution and version.
7. Update the local repository. Type the command shown below for the appropriate Linux distribution, and then press **Enter**:

Option	Command
RHEL, CentOS, and Oracle Linux	<code>yum clean all</code> (to delete files in the cache and update metadata) <code>yum makecache</code> (to leave cached files and update metadata)
SLES	<code>zypper refresh 'rapidrecovery repository'</code>
Debian and Ubuntu	<code>apt-get update</code>

The local repository is updated with the correct files from the repository package to install Agent.

8. Instruct the package manager to install the Rapid Recovery Agent software. Type the command shown below for the appropriate Linux distribution, and then press **Enter**:

Option	Command
RHEL, CentOS, and Oracle Linux	<code>yum install rapidrecovery-agent</code>
SLES	<code>zypper install rapidrecovery-agent</code>
Debian and Ubuntu	<code>apt-get install rapidrecovery-agent</code>

The package manager prepares to install all dependent files.

9. If prompted to confirm installation of unsigned files, enter **y** and then press **Enter**.

The Rapid Recovery Agent files are installed and updated.

i **NOTE:** To ensure that the proper kernel module version is used to protect your machine, the best practice is to restart the machine after the Rapid Recovery Agent upgrade is complete.

Linux commands by package manager

Each supported Linux distribution uses a specific package manager, as listed in the table below. The package managers use commands that sometimes differ to accomplish the same task. The appropriate Linux commands

required to remove AppAssure Agent, or install, upgrade, or remove Rapid Recovery Agent, are included in each individual topic. Those commands are repeated in this topic, listed by package manager for easy reference. Each cell in this table contains one complete command.

Table 2. Commands by package manager and Linux distribution

Command description	yum (RHEL, CentOS, Oracle Linux)	zypper (SLES)	apt (Debian, Ubuntu)
Manually remove AppAssure Agent and dependent files manually	<code>rpm --nodeps -e appassure-vss appassure-vdisk appassure-mono appassure-agent</code>	<code>rpm --nodeps -e appassure-vss appassure-vdisk appassure-mono appassure-agent</code>	<code>dpkg --force-all -P appassure-vss appassure-vdisk appassure-mono appassure-agent</code>
List all local software repositories	<code>yum repolist</code>	<code>zypper repos</code>	<code>ls /etc/apt/sources.list.d</code>
Confirm if a local repository for Rapid Recovery Agent exists	<code>rpm -qa grep rapidrecovery-repo</code>	<code>rpm -qa grep rapidrecovery-repo</code>	<code>dpkg -l grep rapidrecovery-repo</code>
Remove existing rapidrecovery-repo	<code>rpm -e rapidrecovery-repo</code>	<code>rpm -e rapidrecovery-repo</code>	<code>dpkg -P rapidrecovery-repo</code>
Update the local repository	<code>yum clean all (deletes cache first) yum makecache (just updates metadata)</code>	<code>zypper refresh 'rapidrecovery repository'</code>	<code>apt-get update</code>
Install Rapid Recovery Agent from the repository package	<code>yum install rapidrecovery-agent</code>	<code>zypper install rapidrecovery-agent</code>	<code>apt-get install rapidrecovery-agent</code>
Remove Rapid Recovery Agent and Mono database	<code>yum remove rapidrecovery-agent rapidrecovery-mono</code>	<code>zypper remove rapidrecovery-agent rapidrecovery-mono</code>	<code>apt-get remove rapidrecovery-agent rapidrecovery-mono</code>
Remove dependent files	<code>yum autoremove</code>	[Included in previous command]	<code>apt-get autoremove</code>
Remove the repository package	<code>yum remove rapidrecovery-repo</code>	<code>zypper remove rapidrecovery-repo</code>	<code>apt-get remove rapidrecovery-repo</code>

Installing the Agent software on offline Linux machines

This task requires access to an online Linux machine, removable storage media, and access to the final offline Linux machine. If AppAssure Agent is installed on the offline Linux machine, you must first uninstall it before installing Rapid Recovery Agent. For more information, see [Uninstalling the AppAssure Agent software from a Linux machine](#).

When installing the Agent software on Linux machines that do not have access to the Internet, follow this procedure. After installation is complete, configure the Agent as described in the topic [Configuring the Rapid Recovery Agent on a Linux machine](#).



NOTE: If installing on multiple Linux distributions, perform this procedure once for each distribution.

1. From a Linux machine with access to the Internet, download the shell script for off-line Agent installation from the license portal:
 - a. Browse to <https://licenseportal.com>.
 - b. Log into the license portal and, from the left navigation menu, click **Downloads**.

The **Downloads** page appears.

- c. Under Linux-Based Applications, scroll down to the **Offline Agent installation for Linux** entry, and click **Download**.

The shell script downloads to your current directory.

- d. Using removable storage media compatible with both machines, transfer the shell script file to the appropriate offline Linux machine.
2. Run the shell script by executing the following command:

```
bash packages-downloader.sh
```

The script executes and prompts you to select a specific Linux distribution and architecture.

3. Type the index of the installation package you want and press **Enter**.

For example, to obtain an installation package for Red Hat Enterprise Linux 7, enter 3 and press **Enter**.

The appropriate installer is extracted into the `~/rapidrecovery.packages/` directory.



NOTE: The tilde `~/` characters represent your home directory.

4. Copy the packages for Rapid Recovery Agent to removable media. The specific location of your removable media can differ based on Linux distribution. Type the following command and then press **Enter**:

```
cp -R ~/rapidrecovery.packages/ <your_removable_media>
```

For example, if using a removable USB drive that is mounted to location `/media/USB-drive-1`, type the following command and then press **Enter**:

```
cp -R ~/rapidrecovery.packages/ /media/USB-drive-1/
```

All the necessary files are copied to the removable medium.

5. Take the removable medium to the offline Linux machine and mount the drive.
6. Copy the data from the mounted device to your home directory or other desired location. For example, type the following command and then press **Enter**:

```
cp -R /media/USB-drive-1/ ~/rapidrecovery.packages/
```

7. Change to the Rapid Recovery directory. For example, type the following command and then press **Enter**:

```
cd ~/rapidrecovery.packages/
```

8. Run the installation of Agent with root privileges. This command differs based on Linux distribution.

- For Red Hat, SLES, Oracle, and CentOS, type the following command and then press **Enter**:

```
sudo rpm -i *.rpm
```

- For Debian and Ubuntu, type the following command and then press **Enter**:

```
sudo dpkg -i *.deb
```

The local package manager runs the installation of Rapid Recovery Agent.

After installation is complete, configure the Agent as described in the topic [Configuring the Rapid Recovery Agent on a Linux machine](#).



CAUTION: After configuring the newly installed Agent software on a Linux machine, you must restart the machine. Restarting ensures that the proper kernel module version is used to protect your machine.

Configuring the Rapid Recovery Agent on a Linux machine

Run the Rapid Recovery Configuration utility after installing Rapid Recovery Agent software on a Linux machine.

The configuration utility compiles the kernel module (in option 4) and offers several configuration options. The utility provides hints in the numbered steps of the instructions when it detects your specific configuration information.

Complete the steps below to configure the Rapid Recovery Agent software on any Linux machine. Some configuration options differ based on the Linux distribution you are installing.

1. Open a terminal session with root access, or use `sudo` (as demonstrated in the example below).
2. Launch the configuration utility by typing the following command, and then press **Enter**:

```
sudo /usr/bin/rapidrecovery-config
```

The configuration utility starts. The utility lists several configuration options, each with an index number to enter for the appropriate configuration step.

3. Configure the port for this protected machine by typing the following command, and then press **Enter**. The default port is 8006.

```
1 <agent_port>
```

For example, if using the default port, type the command:

```
1 8006
```

Enter

4. Configure users available for protection, by typing the following command, and then press **Enter**:

```
2 <user_names_separated_by_comma>
```

For example, if using usernames `michael`, `administrator`, and `test_user1`, type the command:

```
2 michael,administrator,test_user1
```

i | **NOTE:** The root account is not allowed.

5. Configure firewall rules to select a firewall configuration manager. This establishes firewall exceptions for the port designated in step 3.

If the utility detects one or more firewall configuration managers (such as `lokkit` or `firewalld`), each is listed in the utility in line 3. Select the appropriate configuration manager and enter it, starting with the command number (3), and then press **Enter**:

```
3 <firewall_configuration>
```

For example, if using `firewalld`, type the command:

```
3 firewalld
```

6. Query the list of compatible kernel modules from the utility by entering the command number, and then press **Enter**.

i | **NOTE:** This step is required. Without performing this step, backups will fail.

```
4
```

A sub-shell returns all kernel modules compatible for installation. For example, the following could be returned:

```
Searching for all available for installation kernels.  
This might take a while, depending on the Internet connection speed.  
Kernels compatible for module installation:
```

- 0 - linux-image-3.16.0.23-generic
- 1 - linux-image-3.16.0.31-generic
- 2 - linux-image-3.16.0.33-generic
- 3 - linux-image-3.16.0.34-generic

Input indices of the kernel modules you wish to install, delimited by space; use 'all' to install into all supported kernels, or 'q' to quit.

7. Configure the appropriate Rapid Recovery kernel module.

For example, to enter kernel modules for 3.16.0-23 and 3.16.0-34, type `1 4` and then press **Enter**.

To enter all kernel modules, enter `all` and press **Enter**.

8. After configuring the newly installed Agent software, restart the machine. Restarting ensures that the proper kernel module version is used to protect your machine.

After completing this process, the local repository has been configured on this Linux machine. The Agent software is installed and the kernel module is loaded.

Your next step is to protect the machine on the Rapid Recovery Core.

Starting and stopping the Linux Agent Daemon

After installing or upgrading the Agent software on a Linux machine, you should configure the Agent, and then restart. Restarting ensures that the Rapid Recovery Agent services start automatically, which is required to protect your Linux machine.

You can manually start, stop, and view the status of the Rapid Recovery Agent and `rapidrecovery-vdisk` services in all supported distributions by using the default commands as described in the following tables, respectively.



NOTE: To run a command with administrative privileges, begin the command with `sudo`. For example: To start the Rapid Recovery Agent service with administrative privileges on a SystemV system, use `sudo service rapidrecovery-agent start`.

Table 3. Using the Linux agent service

This table lists the commands to start, stop, and view the status of the agent service manually from the command line, based on the type of Linux system used.

Action	Systemd Command	SystemV Command
Start	<code>systemctl start rapidrecovery-agent</code>	<code>service rapidrecovery-agent start</code>
Restart	<code>systemctl restart rapidrecovery-agent</code>	<code>service rapidrecovery-agent restart</code>
Stop	<code>systemctl stop rapidrecovery-agent</code>	<code>service rapidrecovery-agent stop</code>
View status	<code>systemctl status rapidrecovery-agent</code>	<code>service rapidrecovery-agent status</code>

Table 4. Using rapidrecovery-vdisk

This table lists the commands to start, stop, and view the status of the `rapidrecovery-vdisk` manually from the command line, based on the type of Linux system used.

Action	Systemd Command	SystemV Command
Start	<code>systemctl start rapidrecovery-vdisk</code>	<code>service rapidrecovery-vdisk start</code>

Action	Systemd Command	SystemV Command
Restart	<code>systemctl restart rapidrecovery-vdisk</code>	<code>service rapidrecovery-vdisk restart</code>
Stop	<code>systemctl stop rapidrecovery-vdisk</code>	<code>service rapidrecovery-vdisk stop</code>
View status	<code>systemctl status rapidrecovery-vdisk</code>	<code>service rapidrecovery-vdisk status</code>

Automatically installing updates

i **NOTE:** The automatic update feature of Rapid Recovery Core is effectively disabled for release 6.2 (but will be enabled for future releases). For more information, see the "Automatic update advisory" subtopic in the "About this release" section of *Rapid Recovery Release Notes*.

When installing the Rapid Recovery Core, you can choose whether to automatically update the Rapid Recovery Core software. For specific steps on selecting these options, see [Installing the Rapid Recovery Core](#).

You can also choose to be notified when an updated version of the Core software is available, or to ignore updates. Once installation is complete, settings related to Updates can be changed at any time. For more information on changing automatic update settings, see "Configuring Update Settings" in the *Rapid Recovery User Guide*.

If you choose automatic updates, or if you choose to be notified about updates, then the software on the Rapid Recovery Core is checked against new versions available from the Rapid Recovery License Portal periodically.

- If you choose automatic updates, then when a new version is detected, the version on the Core is updated after other scheduled nightly jobs have completed.
- If you choose to be notified about updates, then when a new version is detected, a message appears on the Core Console under the button bar indicating that a new version is available. The message includes a link to obtain the update.

Generally, Quest recommends using the automatic update option. Upgrading a source Core before upgrading its target Core could result in replication failure. For replication users, Quest recommends administrators apply automatic upgrades only to the target Core, and then manually upgrade the source Core, and lastly upgrade the Agent software on protected machines.

The default setting for automatic updates is to check for updates weekly. You can change how frequently the system checks for updates (options include daily, weekly, monthly, or never) at any time by configuring the update settings for the Core on the Settings page of the Rapid Recovery Core Console. For more information on how to change these settings, see the topic "Configuring Update Settings" in the *Rapid Recovery User Guide*.

i **NOTE:** The automatic update feature requires a license using the standard phone-home mode. If using a software license in non-phone home mode, your Core does not have permission to communicate with the Rapid Recovery License Portal and cannot update the Core or notify you of available updates. For more information, see the topic "Managing privacy" in the *Rapid Recovery User Guide*.

About the Quest Data Protection Portal

Rapid Recovery release 6.2 integrates with the Data Protection Portal, accessible from the web location <https://dataprotection.quest.com/dashboard>. This feature, particularly useful for managed service providers, lets you manage multiple Cores; access a dashboard where you can monitor tasks and events, view repository status, and

check system health; generate reports; and perform a growing list of other functions from a single web-based user interface.

Rapid Recovery users with a valid maintenance agreement are entitled to use the Data Protection Portal. No plugin or additional software is required to integrate Rapid Recovery release 6.2 with the Data Protection Portal. The connection between the Rapid Recovery Core Console and the Data Protection Portal is enabled by default in the Core settings.



NOTE: While enabled by default, you can change the settings from the **Settings** page on the Core Console. The single **Data Protection Portal** setting lets you enable or disable the connection to the portal as appropriate.

This portal is backward compatible to Core release 5.4.3. If using a Core version older than release 6.2, you need a plugin to use the portal. From each pre-release 6.2 Core server, log in to the Rapid Recovery License Portal, and navigate to the **Downloads** page. The plugin installer is available under Windows-Based Applications. Download and run the installer on the Core server. It will automatically install the correct components for your Core server.

Rapid Recovery release 6.2 and the Data Protection Portal comply with the General Data Protection Regulation (GDPR), which governs the handling of individuals' personally identifiable information (PII). If using a software license in standard phone-home mode, Rapid Recovery Core collects a small amount of PII. For information about compliance with GDPR, to understand the PII that Rapid Recovery can collect, how it is used, and how you can control it, see "Managing privacy" in the *Rapid Recovery User Guide*. If you choose not to share PII with Quest, and register a non-phone home license on your Core, the connection between the Core and the Data Protection Portal is disabled.

Uninstalling the Rapid Recovery Core

If you are uninstalling a Rapid Recovery Core release prior to 6.2, and the Core connects to the Data Protection Portal, a portal plug-in is also present on the Core machine. Before you uninstall the Core, first remove the portal plug-in from the machine.

Complete the steps in this procedure to uninstall the Rapid Recovery Core. The same steps apply to uninstall an AppAssure Core. Only the version number will be different.

1. On the Windows server from which you want to uninstall the Rapid Recovery Core, open the Control Panel, click **Programs and Features**, and then click **Uninstall a Program**.
2. In the **Programs and Features** window, double-click the installed Rapid Recovery Core instance; for example:

```
Core-X64-6.0.x.xxxxx.exe
```

If uninstalling AppAssure Core, the version number will be different, for example:

```
Core-X64-5.4.x.xxxxx.exe
```

3. Do one of the following:
 - If the version of Rapid Recovery Core installed does not include support for localization, then the Rapid Recovery Core Installation Wizard appears, showing the **Repair/Remove** page. Skip to [Step 4](#).
 - If the version of Rapid Recovery Core installed includes support for localization, then the **Setup** dialog box appears.
 - In the **Setup** dialog box, from the **Choose your language** drop-down menu, select the appropriate display language, and then click **OK**.
For example, select **English**.
 - Proceed to [Step 4](#).

The Rapid Recovery Core Installation Wizard appears, showing the **Repair/Remove** page.

4. On the **Repair/Remove** page of the Rapid Recovery Core Installation wizard, select **Remove**, and then click **Next**.

The **Remove Options** page appears.

5. Do one of the following:
 - To remove your repository, as well as all recovery points and change logs, select **Uninstall the configuration settings and data including all backup images and change logs**, and then click **Uninstall**.

i **NOTE:** If you select this option, you will delete all data in the repository, including the repository folder and all subfolders. This option is appropriate for typical installations where the repository is installed on an otherwise empty volume. If you have other data on the directory where your repository is located, do not select this option.

- To leave your repository but remove the Rapid Recovery Core software, clear this option and then click **Uninstall**.

The **Progress** page appears. You can view the progress of the uninstall action on the Progress page. When the uninstall is complete, the **Completed** page appears.

6. Click **Finish** to close the wizard and exit.

Uninstalling the Rapid Recovery Agent software from a Windows machine

Complete the steps described in this procedure to uninstall the Rapid Recovery Agent software from a Windows machine.

i **NOTE:** If uninstalling the AppAssure Agent software from a Windows machine, the steps are the same except for the product name in the control panel or uninstall wizard.

1. On the computer from which you want to uninstall the Rapid Recovery Agent software, open the Control Panel, click **Programs and Features**, and then click **Uninstall a Program**.
2. In the **Programs and Features** window, double-click the installed version of the Rapid Recovery Agent (or AppAssure Agent) software.

The Rapid Recovery Agent Installation Wizard appears, showing the **Repair/Remove** page.

3. Select **Remove**, and then click **Next**.

The **Remove Options** page appears.

4. To remove all data and settings installed by the Rapid Recovery Agent software, select **Uninstall the configuration settings and data, including all backup images and change logs** and then click **Uninstall**.

! **CAUTION:** If you select this option, one setting that is removed is the agent ID, a unique identifier assigned to this protected machine. If you remove the agent ID, and install Rapid Recovery Agent on this machine in the future, you will not be able to connect to existing recovery points saved in the repository. If you want to protect this machine with all of the previous settings and be able to access the existing recovery points in the future, do not select this option.

The **Progress** page appears. You can view the progress of the uninstall action on the **Progress** page.

When the removal is complete, the **Completed** page appears.

5. On the **Completed** page, you see a message indicating that the system must be restarted before the configuration changes take effect. Take one of the following actions, and then click **Finish**:
 - To restart now, select **Yes, I want to restart my computer now**.
 - To restart later, clear the **Yes, I want to restart my computer now** option.

i | **NOTE:** You must restart your system to complete the removal of the Agent software.

Uninstalling the Rapid Recovery Agent software from a Linux machine

Rapid Recovery Agent is uninstalled using the package manager relevant to the Linux distribution on the protected machine.

Table 5. Package managers and commands for removing Rapid Recovery Agent

The following table shows, by Linux distribution, the package manager which must be present on the local Linux machine to remove Rapid Recovery Agent, and the commands required for each package manager.

Linux Distribution	Package Manager	Command to remove Agent and dependent files	Command to remove Agent dependent files	Command to remove repository package
Linux distributions based on Red Hat Enterprise Linux (RHEL), including RHEL, CentOS, and Oracle Linux	yum	yum remove rapidrecovery-agent rapidrecovery-mono	yum autoremove	yum remove rapidrecovery-repo
SUSE Linux Enterprise Server (SLES)	zypper	zypper remove rapidrecovery-agent rapidrecovery-mono	[Included in zypper remove]	zypper remove rapidrecovery-repo
Linux distributions based on Debian, including Ubuntu	apt	apt-get remove rapidrecovery-agent rapidrecovery-mono	apt-get autoremove	apt-get remove rapidrecovery-repo

i | **NOTE:** This procedure describes how to remove the contemporary Rapid Recovery Agent software. To uninstall the legacy AppAssure Agent, use the original installer shell script, or manually uninstall it. For more information, see [Uninstalling the AppAssure Agent software from a Linux machine](#).

When you first install Rapid Recovery Agent on a Linux machine, the repository package creates a local software repository. Then the package manager is able to retrieve and install the packages needed for installation or removal of Rapid Recovery Agent and related software components, such as aamount (now called local mount), aavdisk (now called rapidrecovery-vdisk), and Mono (an open source, Ecma standard-compliant, .NET Framework-compatible tool set used for porting the Agent software to Linux platforms).

Complete the following steps to uninstall the Rapid Recovery Agent software from a Linux machine.

1. Open a terminal session with root access.
2. If you want to remove the configuration file for the software repository, as well as remove Rapid Recovery Agent and related files, skip to step 4.
3. To remove Rapid Recovery Agent and related files, but leave the repository package configuration file, type the command shown below for the appropriate Linux distribution, and then press **Enter**:

Option	Description
RHEL, CentOS, and Oracle Linux	yum remove rapidrecovery-agent rapidrecovery-mono
SLES	zypper remove rapidrecovery-agent rapidrecovery-mono
Debian and Ubuntu	apt-get remove rapidrecovery-agent rapidrecovery-mono

The package manager removes the Rapid Recovery Agent application and related files. Skip to step 5.

4. To remove Rapid Recovery Agent, related files, and the repository package configuration file, type the command shown below for the appropriate Linux distribution, and then press **Enter**:

Option	Description
RHEL, CentOS, and Oracle Linux	yum remove rapidrecovery-agent rapidrecovery-mono rapidrecovery-repo
SLES	zypper remove rapidrecovery-agent rapidrecovery-mono rapidrecovery-repo
Debian and Ubuntu	apt-get remove rapidrecovery-agent rapidrecovery-mono rapidrecovery-repo

The package manager removes the application, related files and the software repository. On SLES, dependent files are also removed. For other Linux distributions, continue to the next step.

5. To remove files that are dependencies of the software (including dkms, gcc, and so on), type the command shown below for the appropriate Linux distribution, and then press **Enter**:

Option	Description
RHEL, CentOS, and Oracle Linux	yum autoremove
Debian and Ubuntu	apt-get autoremove

The package manager removes the dependent files from the Linux machine.

After Rapid Recovery Agent is removed from the system, to protect your machine in the Rapid Recovery Core, re-install the Rapid Recovery Agent software or use agentless protection.

Uninstalling the AppAssure Agent software from a Linux machine

This topic describes how to remove AppAssure Agent from a Linux machine for any supported distribution. Uninstalling AppAssure Agent is required before installing Rapid Recovery Agent.

i **NOTE:** If you want the Linux machine to be able to connect to existing recovery points, before uninstalling, Quest recommends first backing up the unique agent ID. For more information, see [Backing up and restoring the AppAssure agent ID](#).

The standard method to install or remove AppAssure Agent on a Linux machine is to run the appropriate AppAssure installer (a shell script). If you did not retain the installer, manual steps are included to remove AppAssure Agent.

i **NOTE:** Quest recommends retaining the binary installer file for any currently installed Rapid Recovery software product. You can use this file in the future to reinstall, repair, or remove the software.

For information about removing Rapid Recovery Agent, see [Uninstalling the Rapid Recovery Agent software from a Linux machine](#).

Complete the following steps to uninstall the AppAssure Agent software from a Linux machine.

i **NOTE:** The following steps apply to both 32-bit and 64-bit environments. For 32-bit RHEL, CentOS, Ubuntu, and SLES systems, the file extension in the steps below will change from "x86_64" to "i386".

1. Open a terminal session with root access.
2. If you do not have access to the installer script, proceed to step 6.
3. If you have access to the installer script, change to the directory that includes the AppAssure installation script, for example:

```
cd /home/AppAssure/
```

4. Run the following command to identify the specific build number of the Agent software you want to remove:

```
cat /var/log/appassure/appassure*.log | grep "Agent Version" | awk '{print $3}'  
| tail -n1
```

For example, you may have AppAssure Agent Version 5.4.3.106 installed.

5. Based on the Linux distribution installed, run the following command, modifying it to specify the build number you identified in the previous step:

Distribution	Command
RHEL and CentOS	<pre>bash appassure-installer_rhel_amd64_5.x.x.xxxxx.sh -u</pre>
SLES	<pre>bash appassure- installer_sles_amd64_5.x.x.xxxxx.sh -u</pre>
Ubuntu	<pre>bash appassure- installer_ubuntu_amd64_5.x.x.xxxxx.sh -u</pre>

For example, if uninstalling AppAssure Agent Version 5.4.3.106, the modified command is:

- For 32-bit RHEL or CentOS: `bash appassure-installer_ubuntu_i386_5.4.3.106.sh -u.`
- For 64-bit RHEL or CentOS: `bash appassure-installer_ubuntu_amd64_5.4.3.106.sh -u.`
- For 32-bit SUSE Linux Enterprise Server (SLES): `bash appassure-installer_sles_i386_5.4.3.106.sh -u`
- For 64-bit SLES, `bash appassure-installer_sles_amd64_5.4.3.106.sh -u`
- For 32-bit Debian and Ubuntu, `bash appassure-installer_ubuntu_i386_5.4.3.106.sh -u`
- For 64-bit Debian and Ubuntu, `bash appassure-installer_ubuntu_amd64_5.4.3.106.sh -u`

The system removes the AppAssure Agent files and directories.

6. Alternatively, to remove the AppAssure Agent software manually without the use of the script, run the following command:

```
dpkg --force-all -P appassure-vss appassure-vdisk appassure-mono appassure-agent
```

The AppAssure Agent components specified are removed from the system.

After AppAssure Agent is removed from the system, to protect your machine in the Rapid Recovery Core, install the Rapid Recovery Agent software or use agentless protection.

Related information

[Uninstalling the AppAssure Agent software on Ubuntu systems](#)

[Uninstalling the AppAssure Agent software on Red Hat Enterprise Linux, CentOS, and Oracle Linux systems](#)

[Uninstalling the AppAssure Agent software on SUSE Linux Enterprise Server systems](#)

Backing up and restoring the AppAssure agent ID

When you remove the AppAssure Agent software in preparation for installing the more recent Rapid Recovery Agent, you also remove the unique identification number associated with that machine. This removal results in the inability to connect to the recovery points saved to the Core for that protected Linux machine.

Before removing AppAssure Agent, you can back up the agent ID values. Then you can install Rapid Recovery Agent and restore the settings.

Use the following procedure to back up agent ID values, and then to restore them afterward.

1. On the Linux machine from which you intend to remove AppAssure Agent, open a command prompt. Type the following command and then press **Enter**:

```
sudo cp -p /root/.mono/registry/CurrentUser/software/apprecovery/agent/agentid/values.xml ~/values-backup.xml
```

A file named `values-backup.xml` containing your unique agent ID is saved to the specified location.

2. Remove AppAssure Agent following the steps specific to the appropriate Linux distribution. For more information, see [Uninstalling the AppAssure Agent software from a Linux machine](#).
3. Install Rapid Recovery Agent online using the appropriate package manager, or offline using the appropriate steps. For more information, see [About installing the Agent software on Linux machines](#).
4. Run the appropriate configuration steps for the updated Linux machine. For more information, see [Configuring the Rapid Recovery Agent on a Linux machine](#).
5. Copy the `values-backup.xml` file to the new location by typing the following command and then pressing **Enter**:

```
sudo mv ~/values-backup.xml /root/.mono/registry/CurrentUser/software/
apprecovery/agent/agentid/values.xml
```

- Restart the rapidrecovery-agent service or reboot the machine.

The original agent ID for that machine is now associated with the updated Rapid Recovery Agent software.

Check the Rapid Recovery Core to see if the machine appears. If not, use the Protect Machine wizard to add the upgraded machine to protection in the Core.



NOTE: After updating Rapid Recovery Agent, the first snapshot will result in a base image, creating a new recovery point chain.

Uninstalling the Rapid Recovery Central Management Console

The tools for managing multiple Rapid Recovery Cores have changed in release 6.2. The Central Management Console is now in limited support only. If you manage two or more Cores, Quest recommends that you migrate to the Quest Data Protection Portal. Only the new portal is supported for management of release 6.2 Cores. This new web-based portal is accessible to Rapid Recovery users with a current maintenance agreement.

Complete the steps in this procedure to uninstall the Rapid Recovery Central Management Console.

- On the Windows server from which you want to uninstall the Rapid Recovery Central Management Console, open the Control Panel, click **Programs and Features**, and then click **Uninstall a Program**.
- In the **Programs and Features** window, double-click the installed Rapid Recovery Central Management Console instance; for example:

```
Central Console-X64-6.x.x.xxxxx.exe
```

The Rapid Recovery Central Management Console Installation Wizard appears, showing the **Repair/Remove** page.

- Select **Remove**, and then click **Next**.

The **Remove Options** page appears.

- Select **Uninstall configuration settings and data including all backup images and change logs**, and then click **Uninstall**.

The **Progress** page appears. You can view the progress of the uninstall action on the Progress page.

When the uninstall is complete, the **Completed** page appears.

- Click **Finish** to close the wizard and exit.

About the Local Mount Utility

The Local Mount Utility (LMU) is a downloadable Windows-based application that lets you mount a Rapid Recovery recovery point in any of the three available modes on any compatible Windows machine. The light-weight utility can be installed on the same 32-bit and 64-bit Windows operating systems as the Rapid Recovery Agent software, but it does not have to be installed on the same machine as the Agent. The LMU includes the rapidrecovery-vdisk (formerly aavdisk) and aavstor drivers, but it does not run as a service. When you install the utility, by default, it is installed in the directory `C:\Program Files\AppRecovery\Local Mount Utility` and a shortcut appears on the machine's desktop.

While the utility was designed for remote access to a Rapid Recovery Core machine, you can also install the LMU on the same machine as a Rapid Recovery Core. When it runs on a Core, the application recognizes and displays all mounts from that Core, including mounts performed through the Rapid Recovery Core Console. Likewise, mounts performed on the LMU also appear in the Core Console.

When the LMU is installed on the same machine as Mailbox Restore, the LMU automatically launches Mailbox Restore when you use it to open an Exchange database. Mailbox Restore is the Rapid Recovery application used to restore Microsoft Exchange data stores and items. You can install it upon installation of the LMU or the Rapid Recovery Core. For more information about Mailbox Restore, see the *Rapid Recovery Mailbox Restore for Microsoft Exchange User Guide*.

i **NOTE:** Linux machines use a command-line utility, `local_mount`, to query the Core for protected machines and their corresponding recovery points. Similarly, that tool lets users remotely mount a recovery point volume; lets users explore the volume contents at the file levels; and lets users restore a individual files or an entire volume from the recovery point, including BMR of the system volume. For more information, see the *Rapid Recovery User Guide*.



Downloading the Local Mount Utility

You can download the web installer version of the Local Mount Utility software directly from the Rapid Recovery Core Console, described as follows.

For other ways to obtain the LMU software, see the topic [Obtaining Rapid Recovery software](#).

i **NOTE:** Quest recommends retaining the binary installer file for any currently installed Rapid Recovery software product. You can use this file in the future to reinstall, repair, or remove the software.

Complete the following steps to download the Local Mount Utility from the Rapid Recovery Core Console.

1. From the machine on which you want to install the LMU, access the Rapid Recovery Core Console by entering the console URL into your browser and logging on with your user name and password.
2. From the Rapid Recovery Core Console, in the icon bar, click  (More), and then select  **Downloads**.
3. Under Local Mount Utility, click **Download web installer**.
A window or dialog box displays. On some systems, you have the option to run the installation or save the installer.
4. Save the web installer to your **Downloads** folder.
For detailed steps on installing, see [Installing the Local Mount Utility](#).

i **NOTE:** For more information about using the LMU, see the "Local Mount Utility" section of the *Rapid Recovery User Guide*. Information about managing licenses in the Rapid Recovery Core Console is described in the "Managing licenses" section of the *Rapid Recovery User Guide*. For more information about licenses for Rapid Recovery and the licensing portal, see the *Rapid Recovery License Portal User Guide*.

Installing the Local Mount Utility

The Local Mount Utility (LMU) can be installed using the web installer, or using an executable installation file specific to the architecture of the machine on which it is being installed. The process is the same regardless of which installer you use. Follow the procedure below to install or upgrade the Local Mount Utility.

1. From the machine on which you want to install the LMU, locate the executable installation file.
 - If you downloaded the installer from the Core, the install file uses the web installer, which is named `LocalMountUtility-Web.exe`.
 - If you downloaded from the Rapid Recovery License Portal, the installer name includes the architecture of your operating system, for example `LocalMountUtility-X32-6.X.X.xxxxx.exe` or `LocalMountUtility-X64-6.X.X.xxxxx.exe`.
2. Double-click on the executable LMU installer file to start the installer.

Depending on the configuration of your machine, the **User Account Control** window or the **Open File - Security Warning** window may appear.

3. If prompted for permission, confirm that you want to run the installer and make changes to the system.
4. If .NET components are missing or need to be upgraded, accept the prompts to download and install the framework. This may require a reboot.
5. In the **Setup** dialog box, from the language field, select the appropriate language and then click **OK**.
6. Choose from one of the following:
 - If this is the first time the Rapid Recovery LMU software is being installed on this machine, the installer prepares the installation, and then the Rapid Recovery Local Mount Utility Installation Wizard appears. Proceed to [Step 7](#).
 - If this machine has an earlier version of the Rapid Recovery Local Mount Utility software installed, you will see a message asking if you want to upgrade to the current version.

1. Click **Yes**.

The Rapid Recovery **Local Mount Utility Installation Wizard** appears, showing the **Progress** page of the wizard. The application downloads to the destination folder, with progress displayed in the progress bar. When finished, the wizard automatically advances to the **Completed** page.

Skip to [Step 13](#).

7. In the Rapid Recovery Local Mount Utility Installation Wizard, on the **Welcome** page, click **Next** to continue with the installation.

The **License Agreement** page appears.

8. On the **License Agreement** page, select **I accept the terms in the license agreement**, and then click **Next**.

The **Prerequisites** page appears.

9. The Rapid Recovery LMU Installer verifies the existence of the prerequisite files.
 - If the prerequisites do not exist, the Installer identifies which files are needed and displays the results accordingly. Click **Install Prerequisites**.
 - If the prerequisite files exist, a message appears indicating that all prerequisites are installed on the machine.

10. Once the installation of the prerequisite files is completed, click **Next**.

The **Installation Options** page appears.

11. On the **Installation Options** page, review the installation options. If necessary, modify them as described below.

- In the **Destination Folder** text field, review the destination folder for the installation. If you want to change the location, do the following:
 - Click the folder icon.
 - In the **Browse to Destination Folder** dialog box, select a new location.
 - Click **OK**.
- Optionally, in the **Select optional components** area, if you want to install Mailbox Restore, select **Mailbox Restore for Exchange**. If you do not wish to install Mailbox Restore, clear this option.

Mailbox Restore for Microsoft Exchange is a comprehensive email recovery program that works with Rapid Recovery and the Rapid Recovery LMU to recover Exchange items from a full data store to a single email message. For more information about Mailbox Restore, see the *Mailbox Restore for Exchange User Guide*.



NOTE: You can install Mailbox Restore only on 64-bit machines.

12. Once you are satisfied with the installation options, click **Install**.

The **Progress** page of the wizard appears, and the application downloads to the destination folder, with progress displayed in the progress bar. When finished, the wizard automatically advances to the **Completed** page.

13. On the **Completed** page, click **Finish** to close the wizard.

Uninstalling the Local Mount Utility

Complete the steps in this procedure to uninstall the Rapid Recovery Local Mount Utility.

1. On the Windows server from which you want to uninstall the Rapid Recovery Local Mount Utility, open the Control Panel, click **Programs and Features**, and then click **Uninstall a Program**.
2. In the **Programs and Features** window, double-click the program you want to remove.
3. Do one of the following:
 - If the version of Rapid Recovery LMU installed does not include support for localization, then the Rapid Recovery Local Mount Utility Installation Wizard appears, showing the Repair/Remove page. Skip to [Step 4](#).
 - If the version of Rapid Recovery LMU installed includes support for localization, then the Setup dialog box appears.
 - In the Setup dialog box, from the **Choose your language** drop-down menu, select the appropriate display language, and then click **OK**.
For example, select **English**.
 - Proceed to [step 4](#).
The Rapid Recovery Local Mount Utility Installation Wizard appears, showing the **Repair/Remove** page.
4. On the **Repair/Remove** page of the Rapid Recovery Local Mount Utility Installation wizard, select **Remove**, and then click **Next**.
The **Remove Options** page appears.
5. Do one of the following:
 - To remove the LMU application and any supporting log files, select **Uninstall the configuration settings and data including all backup images and change logs**, and then click **Uninstall**.
 - To leave LMU log files on this machine but remove the Rapid Recovery LMU software, clear this option and then click **Uninstall**.
The **Progress** page appears. You can view the progress of the uninstall action. When the uninstall is complete, the **Completed** page box appears.
6. Click **Finish** to close the wizard and exit.

Upgrading to Rapid Recovery

Upgrading to the latest release of Rapid Recovery ensures that your environment is equipped with the latest features, fixes and enhancements available. For a summary of each, and a list of known issues, see *Rapid Recovery Release Notes*. Quest requires users to carefully review release notes and system requirements pertaining to each release prior to upgrading, to help identify and preclude potential issues. As of release 6.2, system requirements are now found in the *Rapid Recovery System Requirements Guide*.

Release notes, system requirements, and other Rapid Recovery technical documents are available on the Quest documentation website at <https://support.quest.com/rapid-recovery/technical-documents/>. The default view of the [technical documentation](#) website shows documentation for the most recent generally available version of the Rapid Recovery software. Using the filters at the top of the page, you can view documentation for a different software release or for a Quest DL series backup and recovery appliance. You can also filter the view by guide category.

Read this section in its entirety before deciding whether to upgrade to Rapid Recovery release 6.2. Upgrade only after careful consideration about the effect it may have on your machines. For example:

- Most work environments expand over time, adding computer systems and complexity. Quest recommends customers review their environments before upgrading and adjust accordingly. As a best practice, Quest recommends performing this review at least once annually, whether or not you are upgrading.
- To help determine that enough resources are dedicated to sufficiently protect your environment with Rapid Recovery, review knowledge base article 185962, "[Sizing Rapid Recovery Deployments](#)".
- Rapid Recovery Core and Agent require the Microsoft .NET Framework version 4.6.2 as of this release. On the Core, some operating systems require the corresponding ASP .NET 4.6.2 role or feature. Due to the requirement for this version of .NET on the machine hosting the Rapid Recovery Agent, and new support for Secure Hash Algorithm 2 (SHA2) in release 6.2, older Windows versions that do not fully support these requirements are no longer supported. See release notes for details.
- You can continue to protect machines with older versions of Rapid Recovery Agent. Naturally, for these machines, you cannot take advantage of newer features added to the Agent software. You can also protect VMs agentlessly. Ensure you review the requirements for your Cores and protected machines before you upgrade.

When upgrading from any version of Rapid Recovery to release 6.2, you can install the new version without removing the old version. This is known as an in-place upgrade. Simply run the installer on the machine with the older version. This applies to Rapid Recovery Core, Rapid Recovery Agent, and the Local Mount Utility.

Quest recommends retaining the binary installer file for any currently installed Rapid Recovery software product. You can use this file in the future to reinstall, repair, or remove the software.

You can also perform an in-place upgrade of AppAssure Core or AppAssure Agent release 5.4.3 to Rapid Recovery release 6.2.

If upgrading older versions, intermediate steps may be required. See [Upgrading AppAssure 5.x Core to Rapid Recovery Core](#).

Automatic Update advisory

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

Other documentation resources for upgrading

This section applies to upgrading Rapid Recovery Core, Rapid Recovery Agent, and the Local Mount Utility. For documentation on upgrading other Rapid Recovery components, see the following:

- For installation or upgrade of Mailbox Restore, see the *Mailbox Restore for Exchange User Guide*.
- For installation or upgrade of DocRetriever, see the *DocRetriever for SharePoint User Guide*.
- For installation or upgrade of Rapid Recovery on a cloud instance of a target Core hosted in Microsoft Azure, see the *Rapid Recovery Replication Target for Microsoft Azure Setup Guide*.
- For installation of the Rapid Recovery Add-on for Kaseya plug-in that integrates with the Kaseya Virtual System Administrator system management interface, see the *Rapid Recovery Third-Party Integration Guide*.

Rapid Recovery Core and Agent compatibility

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

Table 6. Interoperability between Core and Agent versions

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

	AppAssure 5.4.3 Core¹	Rapid Recovery 6.0.2 Core	Rapid Recovery 6.1.3³ Core	Rapid Recovery 6.2 Core
AppAssure 5.4.3 Agent ^{1,2}	Fully compatible	Fully compatible ³	Fully compatible ³	Fully compatible ³
Rapid Recovery 6.0.2 Agent	Not compatible	Fully compatible	Fully compatible ³	Fully compatible ³
Rapid Recovery 6.1.3 ⁴ Agent	Not compatible	Not compatible	Fully compatible	Fully compatible ³
Rapid Recovery 6.2 Agent	Not compatible	Not compatible	Not compatible	Fully compatible

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

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

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

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

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

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

Upgrading factors to consider

When upgrading from AppAssure to Rapid Recovery on your machines, or upgrading from one version of Rapid Recovery to a more recent version, it is important to be mindful of the following best practices:

- If upgrading to Rapid Recovery Core release 6.2, you can continue to protect machines with older versions of Agent. If you have a current maintenance contract and are experiencing difficulties, contact Quest Data Protection Support for assistance with any release version covered under full or limited support.

To see Rapid Recovery Core or Agent software releases under full, limited, or discontinued support, and to understand those terms, refer to the product life cycle information on the Support website. Navigate to <https://support.quest.com/rapid-recovery/>, select the appropriate release in the product filter, and then click the "Product Life Cycle and Policies" tab.

To use any new features or enhancements in the Agent software, upgrade to Rapid Recovery Agent release 6.2.

- Quest supports the compatibility of transfers, replication, virtual export, and restores of machines protected with Rapid Recovery Agent versions 6.0.2, 6.1.3, and 6.2. For compatibility with agentless protection, Quest suggests you upgrade to Rapid Recovery Core and Agent release 6.1.3 or later. For support of all current features between the Core and protected machines, including Exchange Server or SQL Server application support with Rapid Snap for Virtual agentless protection, upgrade your Core and protected machines to release 6.2.
- Rapid Recovery installers (for both the Core and Agent software) can be used for first-time installation or for upgrading. The latest installers can be downloaded from the Rapid Recovery License Portal at <https://licenseportal.com>.



NOTE: Quest recommends retaining the binary installer file for any currently installed Rapid Recovery software product. You can use this file in the future to reinstall, repair, or remove the software.

- You can install or upgrade Rapid Recovery Core from the Core installer or the web installer. The Core installer downloads the executable file in one task. The Core web installer streams a download of the latest version of the Rapid Recovery Core installer, which runs directly from the web and lets you pause and resume the process as needed. From a compatibility perspective, there is no difference between using the Core installer or the web installer. For more information about sources for downloading Core and other software, see [Obtaining Rapid Recovery software](#).
- Installations of Rapid Recovery Core prior to release 6.2 that integrate with the Data Protection Portal do so using a plug-in. Connectivity to the Data Protection Portal is included in release 6.2 and later. When you upgrade Core release 6.2 or later, the Core installer automatically removes the outdated plug-in.
- When using the Core Web Installer or automatic upgrade, a silent installation of the Core takes place in the background. In release 6.2, additional parameters have been added to support GDPR. Until your Core has been updated to 6.2 to interpret these parameters, silent installation would fail. In response, release 6.2 has been excluded from the manifest of available Core software versions. Users of earlier versions must

upgrade to release 6.2 manually. Thereafter, the Core can interpret the new parameters, and later releases will be able to be included in the manifest and detected by users of the automatic update feature.

- Before upgrading, verify that your system meets operating system, memory, processor, storage, and network requirements. For additional guidance for sizing your hardware, software, memory, storage, and network requirements, see knowledge base article 185962, “[Sizing Rapid Recovery Deployments](#)”.
- Always upgrade the Core before upgrading protected machines with the most recent Rapid Recovery Agent software. The Core machine can run a version of Rapid Recovery that is the same as, or more recent than, the Agent version installed on protected machines.
- Protected machines must not run a version of the Agent software that is more recent than the version installed on the Core. This guideline only applies to the first three sets of digits in a release name (for example, 5.4.3, 6.0.1, 6.0.2, 6.1.0, 6.2.0). Build numbers (the set of numbers in a release designation that appear after the third decimal point) can differ without interoperability concerns. Your Cores may protect machines with the same major/minor version of Agent but with different build numbers if automatic update is enabled for some but not all protected machines.
- If using replication, always upgrade the target Core first, then upgrade the source Core, and lastly upgrade the Agent software on your protected machines.
- The source Core must not run a version of Rapid Recovery more recent than the target Core.

CAUTION: If automatic update notification is enabled, you may see a message in the Core Console of a source Core indicating that a newer version of the Core software is available. If the message also indicates that a replicated (target) Core has an earlier version, Quest recommends pausing replication on both Cores, manually upgrading first the target Core and then the source Core, and then resuming replication. If you see that message but opt to select Update Now on the source Core first, the next attempt to replicate will fail until you also upgrade the target Core.

- If using cross replication (when two Cores are replicating recovery points from each other's protected machines), Quest recommends manually pausing replication (and backups and other scheduled activities). Then both Cores should be upgraded prior to resuming replication functions.

Before upgrading any Core server, please read the topic [Preparing the Core server to upgrade](#).

Consider localization before upgrading

Rapid Recovery release 6.2 is an international release. In addition to availability in English, this release is localized into simplified Chinese, French, Korean, German, Japanese, Brazilian Portuguese, and international Spanish. When a localized version is installed, you can see or change the current display language set for the Core Console in the general settings for the Core.

Rapid Recovery beta program considerations

Customers who participated in the Rapid Recovery beta program did so with the requirement that the beta software be installed in a lab environment, not a production environment. There is no direct upgrade path from a beta release to the generally available release. Interoperability of beta releases and production releases is not supported.

If you participated in the beta program, do not attempt to upgrade the beta version of the Rapid Recovery Core. Instead, if using the same server, perform the following steps:

- Delete your repository or repositories.
- Perform a full uninstall of the Rapid Recovery Core using the installer or from Control Panels, Add/Remove.
- Obtain the production version of the Core installer or Core web installer and perform a clean install of the Core.

For more information about downloading Rapid Recovery software, see [Obtaining Rapid Recovery software](#).

Upgrading AppAssure 5.x Core to Rapid Recovery Core

To install the latest version of Rapid Recovery, download the installers as described in the topic [Obtaining Rapid Recovery software](#).



NOTE: Quest recommends retaining the binary installer file for any currently installed Rapid Recovery software product. You can use this file in the future to reinstall, repair, or remove the software.

If upgrading from any version of AppAssure, also read [Upgrading from AppAssure](#).

When upgrading from any version of Rapid Recovery to release 6.2, you can perform an in-place upgrade. Always upgrade the Core before upgrading protected machines. If using replication, upgrade target Cores before source Cores.

Upgrading from AppAssure

Before upgrading the AppAssure Core to Rapid Recovery Core, verify if you have any custom binary patches applied, and note the patches used. On the Core machine, access the Programs and Features control panel, and take note of any custom binaries (identified by the letter P, a dash and six digits; for example, P-000678). Having this list accessible can increase the ability of Quest Data Protection Support to assist you in the event of upgrading difficulties.

Keep in mind the following:

- If upgrading from AppAssure Core 5.2.x to Rapid Recovery Core, you must use a three-step process. First, upgrade to AppAssure Core 5.3.7. Then upgrade to AppAssure release 5.4.3. Finally, upgrade to Rapid Recovery Core release 6.2.
- If you want to upgrade from AppAssure Core 5.3.x, 5.4.1, or 5.4.2, best practice is to perform a two-step upgrade process. The first step is to upgrade to AppAssure 5.4.3. As the second step, run the Rapid Recovery release 6.2 installer as in-place upgrade for the Rapid Recovery Core and Agent components, respectively.
- If upgrading from AppAssure Core 5.4.3 to Rapid Recovery Core release 6.2, you can obtain the new Rapid Recovery Core release 6.2 installer, and run it on your 5.4.3 Core as an in-place upgrade. You can also perform in-place upgrades from AppAssure Agent release 5.4.3 to Rapid Recovery Agent release 6.2 on Windows machines.



NOTE: Due to legal divestiture agreements between Dell and Quest, only rebranded versions of Rapid Recovery documentation and software (release 6.1.2 and later) can be downloaded from the [technical documentation website](#) and the [Quest support website](#), respectively. If you have not retained the installer, Quest cannot provide it. In such cases, uninstall the earlier software version.



CAUTION: Before uninstalling AppAssure Agent, make sure the protected machine backs up to the Core. When you see the option to Uninstall the configuration settings and data, including all backup images and change logs, clear the option. You must retain settings and data. Then, perform a clean install of a supported Rapid Recovery version on the same machine.

In all cases, before upgrading the version of the Agent software on protected machines, verify that the operating system on each relevant machine is still supported. For supported operating systems, refer to the *Rapid Recovery System Requirements Guide*.

When upgrading the Agent software on Linux machines from any AppAssure release to Rapid Recovery Agent, first remove the old Agent software version. When removing AppAssure Agent on Linux machines, the preferred process is to use the shell script in the original installer. However, a process is included to manually remove the Agent if necessary. For more information, see [Uninstalling the AppAssure Agent software from a Linux machine](#).

Then, perform a clean install of Rapid Recovery Agent. When upgrading the Agent software on Linux machines from Rapid Recovery Agent release 6.0.1 or later, you can use the appropriate package manager for your distribution of Linux. For more information, see [Uninstalling the Rapid Recovery Agent software from a Linux machine](#). You may need to remove the local software repository. This requirement is included in upgrading steps.

Additionally, be aware of the following information when upgrading from AppAssure 5.3.x and later:

- Recovery points are represented differently in AppAssure release 5.4.x and later, as part of the changes made to improve application performance. When upgrading from AppAssure 5.3.x to AppAssure 5.4.x, existing recovery points are converted to the new representation, which is not backward-compatible. You cannot downgrade an AppAssure release 5.4.x installation to 5.3 (or a Rapid Recovery release) unless you recreate your repository.
- When launching the Core for the first time after upgrading from versions prior to Rapid Recovery 5.4.1, the conversion of existing recovery points will take approximately twice as long as loading the same recovery points under previous versions. After this initial conversion, however, loading recovery points will be significantly faster than with previous versions.

i **NOTE:** When upgrading from AppAssure 5.3.x to 5.4.x, ensure that you factor extra time for converting recovery points into your planning before your upgraded environment is ready for use.

- After upgrading from versions prior to Rapid Recovery 5.4.1, if you attempt to set up a retention policy on a replicated target Core that differs from the replication policy on the source Core, you will first be prompted to perform a repository Integrity Check Job. The same requirement applies if you want to set up a custom retention policy for a replicated agent. Running this job can preemptively identify inconsistencies in replicated recovery points, providing the opportunity to replace those with error-free recovery points.


! **CAUTION:** Running the Integrity Check Job is expected to take an extended period of time. The time required differs for each environment, based on the quantity and type of data in your repository and also based on the underlying storage system. While the job is running, no other transactions can be performed in that repository, including transfers (snapshot and base image backups, and replication), nightly jobs, and so on. Ensure that you factor extra time for completing a lengthy Integrity Check Job into your planning if these situations apply to you.

Upgrading steps overview

This topic provides an overview for upgrading your AppAssure or Rapid Recovery Core environment from an earlier version to Rapid Recovery Core release 6.2. When this topic contains links to other tasks, view those topics before proceeding.

i **NOTE:** If upgrading your Core from a version earlier than AppAssure version 5.4.3, please first upgrade the Core to release 5.4.3.

When upgrading AppAssure to Rapid Recovery, perform the following steps:

1. Review upgrading factors such as compatibility, replication scenarios, and best practices as described in this document. Factors include the following:
 - Review the operating system of the Core machine and any machines you want to protect. For more information about system requirements, see the *Rapid Recovery System Requirements Guide*.
 - Ensure the Core you want to upgrade is sized appropriately. For guidance on sizing your hardware, software, memory, storage, and network requirements, see knowledge base article 185962, "[Sizing Rapid Recovery Deployments](#)."
 - If using replication, be sure to follow the order of operations for upgrading described in the topic [Upgrading factors to consider](#).
2. If using a standard phone-home license or a trial license, verify that your Cores can contact the Rapid Recovery License Portal. The UI may differ slightly based on the version of Rapid Recovery or AppAssure Core you are using, but the following is a guideline:
 - a. Navigate to the Rapid Recovery Core Console.
 - b. On the icon bar, click  **Settings** and then select **Licensing**.
 - c. Scroll down to the **License Server** pane and click **Contact Now**.

After a brief pause, you can briefly see a message indicating that the license server was contacted.

3. Download the Rapid Recovery Core release 6.2 installer program (full installer or web installer, as applicable), but do not launch it yet. If you see a notification on the Core Console for an automatic update, you can click the link to download the installer. For more software download options, see [Obtaining Rapid Recovery software](#).
4. Review the topic [Upgrading AppAssure 5.x Core to Rapid Recovery Core](#) to determine whether you are eligible to upgrade in place.
5. For each Core you want to upgrade, pause and disable all data transfer activities, including replication, snapshots, and nightly jobs. Doing so expedites the Core Service shut-down process during the upgrade. For specific details, see [Preparing the Core server to upgrade](#).
6. Run the installer programs on each Core you want to upgrade. If using replication, be sure to follow the upgrade order described in the topic [Upgrading factors to consider](#). For specific instructions on using the Core installer, see [Installing the Rapid Recovery Core](#).
7. After you install the Core software, launch the Rapid Recovery Core Console. If upgrading from a trial version, or if prompted to enter a license key, ensure your Rapid Recovery software license is accessible to the Core server. Then, associate license keys on each Core as appropriate. For more information, see the topic [Updating or changing a license](#).
8. Optionally, if you want to take advantage of the latest Agent features, verify that the OS on each protected machine is supported, and then upgrade the Rapid Recovery Agent software. Keep in mind the following:
 - For various options for obtaining and deploying Rapid Recovery Agent, see the topic [Obtaining Rapid Recovery software](#).
 - For release 6.2 direct upgrade of the Agent software using the Agent installer is supported from machines with releases 5.4.3 and higher. Other versions may require an interim upgrade. For more information, see the topic [Upgrading AppAssure 5.x Core to Rapid Recovery Core](#).
 - You can also protect machines agentlessly using Rapid Snap for Virtual. For more information, see the *Rapid Recovery User Guide* topic "Understanding Rapid Snap for Virtual."
9. As a best practice, restart all machines on which you installed or upgraded the Agent software.



Restarting ensures that the Agent service is running, and that proper kernel module is used to protect the machine, if relevant.

10. If using agentless protection in release 6.2 and later, associate each guest VM with its protected hypervisor host to reduce the consumption of licenses from your Enterprise license pool. For instructions, see step 3 in the *Rapid Recovery User Guide* topic "Viewing and modifying protected machine settings."
11. As a best practice, after making changes that affect licensing or after applying a new license on your Core, you should refresh the Core's association with the license server as described in [step 2](#) above.

The Core reaches the license portal and refreshes information accordingly.

Preparing the Core server to upgrade

Perform the following steps on the Core server to prepare the server for an upgrade of the Rapid Recovery Core. These steps are not applicable to new Core installations.

1. Suspend future jobs by pausing protection, replication, scheduled archive, and virtual standby.
For more information about pausing each of these functions, see the *Rapid Recovery User Guide* topics "Pausing and resuming protection," "Pausing and resuming replication," "Pausing or resuming a scheduled archive," and "Managing exports," respectively.
2. Allow all active jobs to complete, or cancel running jobs.
For more information about viewing and canceling active tasks from the Core Console, see "Viewing running tasks from any Core Console" in the *Rapid Recovery User Guide*.
3. Stop the Core service as follows:
 - a. Navigate to the  Settings page for the Core.
 - b. At the top of the page, click  **Shut Down Core Service**.
4. Close all instances of related Rapid Recovery applications.
These applications include AAInfo or the Information Gathering Tool, Local Mount Utility, Mailbox Restore, and DocRetriever.
5. Close all open instances of PowerShell and any browser running the Core Console.
6. Download the appropriate installer from the **Downloads** page of the Rapid Recovery License Portal.
7. Remember to run the Core installer with administrative privileges.
If the logged-in user is not an administrator, right-click on the installer file and select **Run as administrator**, providing administrative credentials if prompted.

Upgrading the Rapid Recovery Core

For step-by-step instructions for installing or upgrading the Rapid Recovery Core, see the topic [Installing the Rapid Recovery Core](#).

Upgrading the Rapid Recovery Agent software

This topic addresses upgrading the Agent software that protects your machine in a Rapid Recovery Core. Be sure to read this section before you upgrade. If installing the Rapid Recovery Agent software for the first time, see the topic [Installing the Rapid Recovery Agent software](#).

To take advantage of the latest features, Quest recommends that you upgrade the Rapid Recovery Agent software on machines that you want to protect using Rapid Recovery Core release 6.2. The same Agent installer executable program (standard, or web installer) can be used for a clean installation or to upgrade an existing version of Rapid Recovery Agent.

- **CAUTION:** Before upgrading Agent, it is critical that you verify that the machine you want to protect is supported by the current version of Rapid Recovery Agent. See the topic "Rapid Recovery Agent software requirements" in the *Rapid Recovery System Requirements Guide*. If the operating system of the machine you want to protect is no longer supported, you can continue to run an earlier version of Rapid Recovery Agent on that machine and still protect it in the Core. New features supported by Rapid Recovery Core may not be available on machines protected with an older version.

For information about getting the appropriate version of the Rapid Recovery Agent software, see [Obtaining Rapid Recovery software](#). When the upgrade is complete, restart the machines as necessary, and then check the Core to verify that each upgraded machine is being protected.

Install or upgrade to the latest version of the Rapid Recovery Agent software on machines that you want to protect:

- On every physical machine in your environment.
- On every Hyper-V host or VirtualBox virtual machine you want to protect.
- On every node in a Hyper-V cluster.

Optionally, you can protect VMware vCenter/ESXi virtual machines and Hyper-V virtual machines using our Rapid Snap for Virtual feature. This is also known as agentless protection. To protect VMs agentlessly, some additional requirements may apply. Application support for SQL Server and Exchange Server is included in Rapid Recovery as of release 6.2. Naturally, when protecting machines agentlessly, you cannot take advantage of features unique to Rapid Recovery Agent. For a clear understanding of advantages of and limitations for agentless protection, see the topic "Understanding Rapid Snap for Virtual" in the *Rapid Recovery User Guide*.

If you opt not to use Rapid Snap for Virtual, then install or upgrade to the latest version of the Rapid Recovery Agent software on Hyper-V virtual machines, and on every VMware vCenter/ESXi virtual machine you want to protect with the Agent, instead of agentlessly.

Upgrading on a Windows machine

On a Windows machine, when upgrading AppAssure Agent release 5.4.3 to Rapid Recovery Agent release 6.2, you can upgrade in place. There is no need to uninstall the older version of Agent. You can also upgrade in place from any earlier version of Rapid Recovery Agent to release 6.2.

When upgrading a version of AppAssure earlier than release 5.4.3, you must perform a two-step or three-step upgrade process, as described in the topic [Upgrading AppAssure 5.x Core to Rapid Recovery Core](#). If you have the installers (which are no longer available), first update the machine to AppAssure release 5.4.3. Then run the Rapid Recovery release 6.x installer, as applicable. If you did not save installers, then uninstall the older version and then install the current version.

i **NOTE:** Due to legal divestiture agreements between Dell and Quest, only rebranded versions of Rapid Recovery documentation and software (release 6.1.2 and later) can be downloaded from the [technical documentation website](#) and the [Quest support website](#), respectively. If you have not retained the installer, Quest cannot provide it. In such cases, uninstall the earlier software version.

! **CAUTION:** Before uninstalling AppAssure Agent, make sure the protected machine backs up to the Core. When you see the option to Uninstall the configuration settings and data, including all backup images and change logs, clear the option. You must retain settings and data. Then, perform a clean install of a supported Rapid Recovery version on the same machine.

Because there is more than one type of Windows machine, the steps for upgrading depend on the version of Windows installed. Upgrading a Windows machine includes the following options:

- To upgrade Agent on a machine with a standard Windows operating system, see [Installing the Rapid Recovery Agent software on Windows machines](#). Supported Windows operating systems are listed in the topic "Rapid Recovery release 6.2 operating system installation and compatibility matrix" in the *Rapid Recovery System Requirements Guide*.
- To upgrade a machine with a Windows Server Core Edition operating system, see [Installing the Agent software on Windows Server Core Edition machines](#).

i **NOTE:** When upgrading to Rapid Recovery Agent on Windows machines on which the software drivers have changed, you are prompted to restart your system.

Upgrading on a Linux machine

When upgrading a Linux machine from AppAssure Agent to Rapid Recovery Agent, you must first uninstall the AppAssure Agent software. For more information, see [Uninstalling the AppAssure Agent software from a Linux machine](#).

If upgrading from one release of Rapid Recovery Agent to another, please note:

- You must remove the local software repository created by previous installations of the Agent. Steps are included to help you determine if a local repository exists and to remove it.
- A new local repository is created automatically when you can run the installer from the package manager to upgrade from a supported earlier release of Rapid Recovery Agent to the current release.
- The procedure for upgrading Rapid Recovery Agent on any compatible distribution of Linux is combined with instructions for installing Agent on Linux.

i **NOTE:** To ensure that the proper kernel module version is used to protect your machine, the best practice is to restart the machine after the upgrade to Rapid Recovery Agent is complete.

For more information, see [Upgrading Rapid Recovery Agent on a Linux machine](#).

Upgrading Rapid Recovery Agent on a Linux machine

For steps to upgrade the Rapid Recovery Agent, see the procedure [Installing or upgrading Rapid Recovery Agent on a Linux machine](#).

Managing licenses

There are three types of Rapid Recovery software licenses:

- **Trial**, which stops taking snapshots after 14 days,
- **Subscription**, which has an expiration date, and
- **Perpetual**, which has no expiration.

Many Rapid Recovery Core users start with a trial license, which has limited capabilities. After 14 days, if the circumstance requires, a group administrator can extend the trial license by 28 days. Otherwise, you can purchase and register a subscription or perpetual license.



NOTE: For information about entering license key or file information (for example, to update or change a trial license to a valid long-term license), see [Updating or changing a license](#).

Rapid Recovery delivers licenses in a file. A Rapid Recovery license file contains a pool of licenses that you can distribute to the machines that you want to protect. This pool is reflected on the Rapid Recovery License Portal. For each license type previously listed, there are two types of license pools:

- **Enterprise.** Each license in this pool can be applied to an installation of the Rapid Recovery Agent or one socket on a hypervisor host using agentless protection, regardless of space used.
- **Capacity.** These licenses are applied to how much data you plan to protect, measured in terabytes (TBs), regardless of the number of Rapid Recovery Agents installed or sockets you have. If you exceed the amount of space allocated to the license you purchased, you must purchase another license. For capacity licensing:
 - DL appliances use a back-end capacity license model, in which the capacity specified in the license limits the size of the repository (in TB) you can use on the appliance.
 - Software installations use a front-end capacity license model, in which the capacity specified in the license specifies limits the amount of data (in TB) from the machines you want to protect that you can save to your repository. Front-end capacity is measured prior to compression and deduplication.


In release 6.2, a Core can use only one license pool type. For example, if your Core uses a capacity-based license pool, it cannot also use an enterprise license pool. The reverse is also true.

License pool types cannot be combined into a single license file. For example, you cannot include an enterprise license pool and a capacity license pool under the same perpetual license.

License files are text files that end with the `.lic` file extension. The following are examples of license files:



- License files can appear as nine characters in length, consisting of three groups of numbers, each separated by a hyphen; for example, `123-456-789.lic`.
- Software-based licenses can appear in the format `Software-<Group name>.lic`, with the group named after the customer name or account; for example, `Software-YourCompany.lic`.
- DL series appliance licenses can appear in the format `<Appliance Series>-<Group name>.lic`, with the group named after customer name account; for example, `DL4X00 Series-YourCompany.lic`.

Rapid Recovery supports these license types in two modes: the standard phone-home mode, and non-phone home mode, which has several limitations. Subscription licenses run only in phone-home mode. Perpetual and trial licenses can use phone-home or non-phone home licenses. To see how this mode affects the use of personal data in Rapid Recovery, see the topic "Managing privacy." To see restrictions on non-phone home licenses, or information on obtaining a license using this mode, see "Obtaining and using non-phone-home licenses." These topics are in the *Rapid Recovery User Guide*.

Rapid Recovery lets you manage licenses or contact the license server directly from the Core Console by selecting  (Settings) from the icon bar and clicking **Licensing**.

The Licensing settings include the following information:

License Details:

-  **Change License.** Lets you change an existing license associated with the Core by uploading a license file or entering a license key.
- **Add License.** This option is available only for DL series backup appliances and lets you upload a license file or entering a license key.
-  **License Portal Group.** This option opens the license portal for group management.
- **License type.** Types of licenses include Trial, Subscription, or Enterprise. For more information, see the topic "Understanding software license types" in the *Rapid Recovery License Portal User Guide*.
- **License status.** Indicates the status of the license. An active status ensures snapshots can continue as scheduled. If the license is blocked, or expired, or if the Core has not been able to communicate with the Rapid Recovery License Portal past the grace period, snapshots are paused until the license status is corrected.
- **License key expires in.** This option is available only when using a subscription license, and shows the duration of time before the subscription expires, in days.

License Constraints:

- **Maximum snapshots per day.** Indicates the number of backups that are limited by the specific license.

License Pool:

- **Pool size.** The license pool is the number of non-trial licenses available to allocate across groups and subgroups in the Rapid Recovery License Portal. The size of the pool determines how many licenses can be allocated. For more information, see the topic "Understanding license pools" in the *Rapid Recovery License Portal User Guide*.
- **Used by this Core.** Indicates the number of machines from the license pool that are protected by this Core.
- **Total used in group.** Indicates the total number of machines protected within the same license group as this Core.
- **Phone home disabled.** If visible, this status indicates that the Core does not communicate with the Rapid Recovery License Portal or the Data Protection Portal. Auto update is disabled, and no personal information is communicated between the Core and Quest Software Inc. or any other entity, in compliance with GDPR policies.

License Server. These settings apply to standard (phone home) licenses. These settings are not applicable for appliances and other non-phone-home licenses:

- **License server address.** Displays an active URL for the license server associated with this Core.
- **Last response from the licensing server.** Indicates whether the last attempted communication with the license server portal was successful.
- **Last contact with licensing server.** Displays the date and time of the last successful contact with the licensing server.
- **Next attempt to contact the licensing server.** Indicates the next scheduled date and time to attempt communication with the licensing server.
- **Contact Now.** This button contacts the license server on demand. Use this option after making changes to your license configuration, to register changes immediately rather than waiting for the next scheduled attempt.

For more information on licenses, see the *Rapid Recovery License Portal User Guide*.

For more information on updating or changing a license key or file, see [Updating or changing a license](#).

Users of DL series backup appliances can also add licenses to the Core if necessary. For more information, see [Adding a license](#).

For more information on contacting the license portal server, see [Contacting the Rapid Recovery License Portal server](#).

You can also view licensing information for a single protected machine. For more information, see [Viewing license information on a machine](#).

Updating or changing a license

After you upgrade or purchase a long-term Rapid Recovery license, you receive by email either a license file or a license key.

Complete the steps in this procedure to upgrade your trial license or change your existing license, and associate it with the Rapid Recovery Core Console.



NOTE: Users of DL series backup appliances can also add licenses to the Core if necessary. For more information, see [Adding a license](#).

NOTE: For information about obtaining a license key, or for details about using the license portal to download software, register appliances, manage license subscriptions and license groups, and generate license portal reports, see the *Rapid Recovery License Portal User Guide*.

If you just installed a new Core, and are viewing a message in the Core Console requesting that you choose a license file or key, skip to [Step 5](#).

1. Navigate to the Rapid Recovery Core Console.
2. On the icon bar, click (Settings).
3. Scroll down on the right side of the **Settings** page until you can see the **License Server** heading.
The Core settings for licensing appear.
4. To update or change the existing license associated with your Core, at the top of the License Details core settings area, click **Change License**.
The **Change License** dialog box appears.
5. If you want to manually enter the license key, skip to [step 6](#). If you want to upload a license file, do the following:
 - a. To upload a license file, from the **Choose license file or enter license key** field, click **Choose File**.
In the **File Upload** dialog box, navigate through the file system and locate the new license file you want to use. For example, locate `Software-YourCompany.lic`.
 - b. Click the license file, and then click **Open**.
The **File Upload** dialog box closes. The license file you selected appears in the license text field.
 - c. In the **Change License** dialog box, click **Continue**.
The license file you selected is authenticated, and that license is associated with your Core.
 - d. Skip to [step 7](#).
6. To manually enter the license key, in the **Choose license file or enter license key** text field, enter the license key carefully, and then click **Continue**.
The dialog box closes, the license file you selected is authenticated, and that license is associated with your Core.
7. If you see the **Quick Start Guide** welcome page, you can start the guide, or close this tool. This is the last step required for this procedure.



NOTE: For more information about the Quick Start Guide, see "Understanding the Quick Start Guide" in the *Rapid Recovery User Guide*.

8. If performing these steps on the Core **Settings** page, scroll down on the right side of the **Settings** page until you can see the License Server heading.
9. In the License Server area, click **Contact Now**.

Once the license is applied to the license server, any associated protected machines automatically update with the new license.

If you see error messages at the top of the Rapid Recovery Core Console (such as specific services not starting), follow the guidance in the error message to resolve those errors.

Adding a license

DL series backup appliance owners can add one or more licenses to the Rapid Recovery Core Console.

Once you have upgraded or purchased your Rapid Recovery license, you receive by email either a license file or a license key.


You can also update or change an existing license on the Core Console. For more information, see [Updating or changing a license](#).



NOTE: Only DL series backup appliance users see the **Add Appliance** button.



NOTE: For information about obtaining a license key, see the *Rapid Recovery License Portal User Guide*.

1. Navigate to the Rapid Recovery Core Console.
2. On the icon bar, click  (Settings).
3. Scroll down on the right side of the **Settings** page until you can see the Licensing heading.
The Core settings for licensing appear.
4. To add a license and associate it with your Core, at the top of the License Details core settings area, click **Add License**. In the resulting dialog box, do one of the following:
 - a. If you want to manually enter the license key, type the key carefully, and then click **Continue**.
The dialog box closes, and the license file you selected is authenticated, and that license is associated with your Core.
 - b. If you want to upload a license file, click **Choose File**.
In the **File Upload** dialog box, navigate through the file system and locate the new license file you want to use. For example, locate `Software-YourCompany.lic`.
 - c. Click the license file, and then click **Open**.
The File Upload dialog box closes. The selected license file appears in the current dialog box.
 - d. In the dialog box, click **Continue**.
The dialog box closes, and the license file you selected is authenticated, and that license is associated with your Core.
5. Scroll down on the right side of the **Settings** page until you can see the License Server heading.
The Licensing core settings appear.
6. In the License Server area, click **Contact Now**.
Once the license is applied to the license server, any associated protected machines automatically update with the new license.

Contacting the Rapid Recovery License Portal server

The Rapid Recovery Core Console frequently contacts the Rapid Recovery License Portal server to remain current with any changes made in the license portal.

For non-trial licenses, the Rapid Recovery Core contacts the license portal once every hour. If the Core cannot reach the license portal after a 10-day grace period, the Core stops taking snapshots.

Typically, communication with the license portal server occurs automatically at designated intervals; however, you can initiate communication on-demand.

Complete the steps in this procedure to contact the license portal server.

1. Navigate to the Rapid Recovery Core Console.
2. On the icon bar, click **Settings**, and then scroll down on the right side of the **Settings** page until you can see the License Server heading.
3. From the License Server area, click **Contact Now**.

Viewing license information on a machine

You can view current license status information for the Rapid Recovery Agent software installed on a protected machine.

1. From the Rapid Recovery Core Console, under Protected Machines , click the machine that you want to modify.
The **Summary** page for the selection machine appears.
2. Click the **Settings** menu.
The **Settings** page appears, showing configuration settings for the selected machine.
3. Click the **Licensing** link to scroll down in the Settings page to view machine-specific licensing settings.
The Status screen appears and presents details about the product licensing.

About us

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation™.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece — you — to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit <https://www.quest.com/contact>.

Technical support resources

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

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

- Submit and manage a Service Request.
- View Knowledge Base articles.
- Sign up for product notifications.
- Download software and technical documentation.
- View how-to videos.
- Engage in community discussions.
- Chat with support engineers online.
- View services to assist you with our product