Quest

Rapid Recovery 6.9

Azure Setup Guide

© 2024 Quest Software Inc. ALL RIGHTS RESERVED.

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

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

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

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

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

Patents

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

Trademarks

Quest, 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

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 Azure Setup Guide
Updated - November 2024
Version - 6.9

Contents

Introduction to Rapid Recovery Core VM for Microsoft Azure **4**
About this guide 4
Working with Microsoft Azure 5
Azure interface disclaimer 5
Country codes used on the Azure website 6
Microsoft Azure documentation 6
Relevant Microsoft links 6
Logging into your Azure user account 7
Practical limitations for Rapid Recovery Core in an Azure environment 7

Considerations for upgrading your Azure VM **9**
Updating configuration scripts on the Azure VM 9
Strategies for migrating data to a new Rapid Recovery Core VM 10
Migration using archiving 10
Migration using replication 11

Setting up your Rapid Recovery Core VM **12**
Creating a Rapid Recovery Core virtual machine in Azure 12
Accessing your virtual machine from Azure 14
Exploring your Rapid Recovery Core VM desktop 16
Adding storage to your Azure VM 17
Running the Core configuration script from the VM desktop 19
Disabling Compatibility View in Internet Explorer 19
Obtaining the Publish Settings file for your Azure account 20

Understanding licensing **22**
About Rapid Recovery licenses 22
For more information about licenses 23
Bring your own license 24
Activating your Rapid Recovery license 24
General Data Protection Regulation compliance 25
Licensing and privacy considerations 26
Agreeing to use personal data 27

Considerations for seeding data to your target Core **28**
Seeding data to Azure using the Microsoft Azure Import/Export service 28

About us **30**
Technical support resources 30

Introduction to Rapid Recovery Core VM for Microsoft Azure

Welcome to the Rapid Recovery Azure Setup Guide.

Topics include:

- About this guide
- Working with Microsoft Azure
- Practical limitations for Rapid Recovery Core in an Azure environment

About this guide

This document is for Microsoft Azure users who want to use Rapid Recovery in the Azure cloud. It describes how to set up a VM to run a Rapid Recovery Core in Azure, Microsoft's cloud computing platform.

> **NOTE:** This document does not describe how to use Rapid Recovery. For more information on using Rapid Recovery Core, see the latest version of *Rapid Recovery User Guide*.

As with previous versions, you can use this VM to replicate your on-premise backups to a source Core in the Azure cloud. Quest now also supports running Rapid Recovery Core in the Azure cloud as a primary Core. You can add other Azure VMs to protection on your Core, capturing backup snapshots as recovery points in your repository. From these recovery points, you can restore data, create or import archives, perform virtual export, and replicate to a target Core.

To reflect this additional functionality:

- Our updated VM available in the Azure Marketplace is called *Rapid Recovery Core*, replacing the previous VM, which was named *Rapid Recovery Replication Target.* The updated VM includes Rapid Recovery Core release 6.9 running on a Microsoft Windows Server 2019 Data Center OS platform.
- This document, the *Rapid Recovery Azure Setup Guide,* replaces the *Rapid Recovery Replication Target for Microsoft Azure Setup Guide*.

This setup guide assumes the following:

- **You are a Rapid Recovery Core user.**
  This document assumes that you use (or plan to use) a supported version of Rapid Recovery Core software to provide backup, replication and recovery solutions for your enterprise. In Release 6.9, supported versions include Rapid Recovery Core versions 6.8 and 6.9

  For more information, see our product life cycle (PLC) support policy on our support website at https://support.quest.com/rapid-recovery/. Click Product Life Cycle & Policies, and then expand Software Product Support Life Cycle Policy).

  For more information about Rapid Recovery, please visit http://quest.com/products/rapid-recovery/.
- **You have a subscription to Microsoft Azure.**
  This setup guide pertains to running a Core as a VM in the Azure cloud, not for running a Core on premises. For more information about the Azure cloud platform, or to sign up, see http://azure.microsoft.com/en-us/.

- **You know how to use Microsoft Azure.**
  Microsoft includes information about using Azure in its documentation center. For more information, see the topic Microsoft Azure documentation or visit https://azure.microsoft.com/en-us/documentation.
- **You plan to create a VM procured through the Marketplace as your Rapid Recovery Core.**
  Use our VM template from the Azure Marketplace to set up your Rapid Recovery Core VM in just minutes. Instructions are provided in the topic Creating a Rapid Recovery Core virtual machine in Azure. You will be guided to select appropriate configuration options.
- **You will procure and attach Azure storage disks to your VM for use as your repository.**
  Storage space for your working data repository is not included in the Core VM. You must obtain dedicated storage in your Azure subscription, and associate it with your Core VM. For more information, see Adding storage to your Azure VM.

This setup guide includes the following sections:

- **Introduction to Rapid Recovery Core VM for Microsoft Azure**. This section includes conceptual information about Azure and using a Rapid Recovery Core in the Azure environment. It includes links to Azure resources and documentation.
- **Considerations for upgrading your Azure VM**. If you are upgrading a Rapid Recovery Core VM created with a template in the marketplace, read this section. If using a new VM, skip this section.
- **Setting up your Rapid Recovery Core VM**. This section describes how to create your VM from our template in the Azure marketplace. It also includes procedures for adding storage volumes, running configuration scripts to provision the storage into a working DVM repository, and disabling Compatibility View in Internet Explorer. Setup is simple and quick; all steps should take less than an hour.
- **Understanding licensing**. Once your Core on the Azure VM is configured, you must register a software license. This section includes information about Rapid Recovery licenses, how to activate your license, and references to relevant documentation and resources.
- **Considerations for seeding data to your target Core**. This section outlines the process of seeding data from your source Core to your replicated Core. It describes steps specific for your replication target on Azure, and references other relevant content about replication.

Working with Microsoft Azure

Microsoft Azure is a subscription-based cloud computing platform. The following information is provided to Rapid Recovery customers to facilitate using Azure with our product.

Azure login requires JavaScript. You may need to enable JavaScript or otherwise adjust security settings in the browser accordingly. For more information, consult your systems administrator.

- Azure interface disclaimer
- Country codes used on the Azure website
- Microsoft Azure documentation

Azure interface disclaimer

CAUTION: The Microsoft Azure interface is subject to change.

The information provided in this document relating to steps required in Azure were current as of the date of publication. This information is provided as a service to our customers to assist them with Azure prerequisites.

However, when working with Azure, be aware that specific steps, URLs or even the Azure interface may change at any time, which is beyond our control.

If you are having difficulty performing any steps related to your Azure subscription, please seek the advice of a Microsoft Azure representative.

Country codes used on the Azure website

The Azure website uses language and country codes for its web addresses, which affect display of the content in the appropriate language. The typical URL construction uses the format: `https://[Microsoft or Azure domain]/[country-code]/[destination]/`, in which the country code controls the language display and the remainder of the URL specifies the content.

For example, when viewing the documentation center for US English, the URL is `https://docs.microsoft.com/en-us/azure/`. If viewing the same page for Spanish (Spain), the correct URL is `https://docs.microsoft.com/es-es/azure/`.

The URLs for Azure used throughout this document include the country code for English in the United States. For other languages, URLs may differ based on the settings on your computer, and the languages and country codes Microsoft supports.

If you are browsing in a language other than US English, or if your machine settings are configured for a different language, the language and country code portion of the various URLs cited in this guide may differ accordingly.

Microsoft Azure documentation

Microsoft has substantial documentation on using Azure available in its documentation center.

For information on creating an Azure subscription or user account, selecting Azure resources for VMs you create on Azure, adding a storage account to your VMs, and more, see the Microsoft documentation at https://azure.microsoft.com/en-us/documentation.

For example, for information on provisioning or managing Windows VMs, see https://azure.microsoft.com/en-us/documentation/services/virtual-machines/windows/.

For online videos about using Azure, see http://azure.microsoft.com/en-us/get-started/.

Relevant Microsoft links

Some relevant articles on Microsoft websites are listed below:

- Azure login page (US)
- Microsoft Azure home page
- Microsoft documentation center
- Windows virtual machines documentation
- Subscriptions, licenses, accounts, and tenants for Microsoft's cloud offerings
- Videos: Get started with Azure
- Azure Virtual machines pricing
- Azure services by region

- About Azure storage accounts
- Creating a storage account on Azure
- How to attach a data disk to a Windows VM in the Azure portal
- Use the Microsoft Azure Import/Export Service to Transfer Data to Blob Storage
- Import/Export Pricing
- Storage: Import/Export Hard Disk Drives to Windows Azure (blog post)
- Overview of Availability Zones in Azure

Logging into your Azure user account

This procedure assumes that you have a Microsoft Azure subscription associated with a Microsoft user account.

NOTE: Microsoft uses URL redirects. There may be several methods to log into your Azure subscription. Specific steps can change at any time. If you have trouble logging in using this method, contact Microsoft.

Follow this procedure to log into your Azure user account.

1. From a web browser, access the Azure login URL.
   The format for this web address is `https://azure.microsoft.com/[country-code]/account/`.
   For example, in the United States, go to https://azure.microsoft.com/en-us/account/.
   The Manage your Azure Account page appears.
2. Click **Azure portal.**
3. If you are redirected to a Microsoft Azure login page, proceed to the next step. If you cached your Azure credentials in your browser, the Azure dashboard appears, and this task is complete.
4. In the Sign in to Microsoft Azure dialog box, in the **Email, phone or Skype** field, enter the information associated with your Microsoft user account , and then click **Next**.
5. In the Password field, enter the password associated with your Microsoft user account. and then click **Sign in**.
6. Confirm whether to stay signed in. Optionally, to cache your answer, select the **Don't show this again** option.
7. The Azure dashboard appears. If there is no subscription associated with your user account, a toast message will appear briefly in the top right corner of the dashboard.

Practical limitations for Rapid Recovery Core in an Azure environment

The full range of capabilities provided by *Rapid Recovery Core* on premises is available to users in the Azure cloud. From the Rapid Recovery perspective, no features are restricted. However, there are practical limitations, and some restrictions due to the limitations of the Azure platform. Following are a few examples:

- Rapid Recovery Core provides the ability to perform a bare metal restore (BMR) on physical machines. In this process, you can restore the full software configuration for a specific system—the operating system and related confguration files as well as the data from all protected volumes. This process involves creating a boot ISO image, and restarting a restored system from the boot image using the Rapid Recovery Universal Recovery Console UI. Currently, Azure users are restricted from booting an ISO image. As a result, BMR is not supported in Azure. Practically speaking, this Azure restriction does not limit the effectiveness of Rapid Recovery. To recover an entire system from a recovery point for a VM, it is easier, faster, and more efficient to perform virtual export from a recovery point rather than perform a BMR.
- *Rapid Recovery Core* lets you protect machines physical machines and virtual machines by adding them for protection on your Core. It is technically possible to protect on-premises physical machines in Azure. However, since the bandwidth requirements from the physical machine to the Azure data center would be substantial, this use case is not effective or practical, and is therefore not recommended.
- The Rapid Snap for Virtual (agentless) feature of Rapid Recovery lets you protect virtual machines hosted on ESXi and Hyper-V machines without installing the Rapid Recovery Agent software on each VM guest. Since Azure users have no access to a hypervisor, this feature is not supported. This is an Azure limitation.

Considerations for upgrading your Azure VM

If you are new to the Rapid Recovery Core VM in release 6.9, proceed to the topic Setting up your Rapid Recovery Core VM.

When you upgrade to a new Core version, best practice is to upgrade your configuration scripts.

If upgrading from an older version to Rapid Recovery Core version 6.9, you should download the latest Azure configuration script, and replace the old script on your VM. This action lets you continue to use the configuration script to provision newly attached Azure storage disks, creating or adding an extent to your repository. For information on obtaining the latest configuration script, see Updating configuration scripts on the Azure VM.

You can expand storage for your existing Rapid Recovery Core VM at any time. Simply attach additional storage disks to your VM, and then run the configuration script on your desktop. If you did not already have a DVM repository created on your Core, running the script creates one. If you already had a repository, the script adds new disks as extents to your existing repository.

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.

The same is true for VMs created in Azure. The VM size and other properties you select when creating the VM determine the processing, compute, and memory resources associated with the VM. If you outgrow the original VM, Quest recommends creating a new VM using the latest Rapid Recovery Core VM template, and migrating your information from the original Core VM to the updated Core VM.

This section includes the following topics:

- Updating configuration scripts on the Azure VM
- Strategies for migrating data to a new Rapid Recovery Core VM

Updating configuration scripts on the Azure VM

> **NOTE:** Skip this task if using a new VM running Rapid Recovery Core version 6.9.0. This task only applies to VMs created using a Replication Target template from the Azure marketplace, on which the Core was upgraded to version 6.9 or later.

Each AppAssure or Rapid Recovery Core VM includes a shortcut to a configuration script on the VM desktop. The script prepares the VM to run Core and configures a repository for any attached storage disks. For the shortcut to continue functioning when the Core is upgraded on the VM, update the scripts to the latest version.

Complete the procedure below to replace outdated configuration scripts with current scripts.

1. From your Core VM, visit your preferred download location for Rapid Recovery software.
   For more information, see the *Rapid Recovery Installation and Upgrade Guide* topic Obtaining Rapid Recovery software.
2. Download the **AzureConfigurationScripts.zip** file to your VM.
3. Decompress the package to a temporary location such as your *Downloads* folder.

4. Open the `readme.txt` file included in the archive, and follow the instructions to replace outdated configuration scripts with the latest scripts.
5. Optionally, close unneeded open windows.

Strategies for migrating data to a new Rapid Recovery Core VM

This section discusses general approaches for migrating data from an older Core VM to a new Rapid Recovery Core VM on Microsoft Azure.

> **NOTE:** For detailed information on accomplishing these tasks, see the Rapid Recovery User Guide or see Knowledge Base articles on the Quest support website, at https://support.quest.com/rapid-recovery/kb.

If you want to migrate your data in a physical environment that uses direct attached storage, you could conceivably shut down your Core, detach the storage volumes, and connect them to the new Core location. Then, from the new Core, add all previously protected machines to protection in the newly relocated repository.

Both processes assumes you are replicating from an on-premises Core to the Azure replication target VM.

Since this option is not available for data maintained in Azure, consider at minimum the following approaches:

- Archiving
- Replication

Migration using archiving

Archiving is a ready-made approach for migrating data. This approach is best for creating a point-in-time complete archive of data in your repository, and moving it to a new repository. However, this process is very time-consuming both for capturing the original archive and for consuming the archive in the new Core VM.

This process assumes you are replicating from an on-premises Core to the Azure replication-only target VM.

General steps for this approach include:

1. **Pause replication to your target Core.** Most Cores currently in Azure are target Cores for replication. You must pause replication during migration.
2. **Save an archive.** Based on the amount of data in your Core, the range of dates of data, and your network infrastructure, cabling, and throughput, this process can be time-consuming.
3. **Create a new Rapid Recovery Core VM**. Follow the steps in this guide to create a new Core VM in Azure.
4. **Consume the archive in the new Core VM.** Import the archive into your new Core. This process is likely to take a similar amount of time as saving the original archive.
5. **Start new replication from your source to your new Core VM.** On your source Core, enable replication to your new Core VM in Azure.
6. **Delete your original Azure VM.** After your new VM is in place and working, Quest recommends deleting the outdated VM from your Azure account.

For more information, see Quest Knowledge Base article 182089, "How to Migrate Agents from one DVM Repository to Another."

Migration using replication

1. **Create a new Rapid Recovery Core VM**. Follow the steps in this guide to create a new Core VM in Azure.
2. **Start replication to your new Core VM.** From your replication-only VM, enable replication to your new Core VM in Azure.
3. **Disable all replication**. After all data has been replicated to the new Core VM, disable all replication.
4. **Start new replication from your source to your new Core VM.** On your source Core, enable replication to your new Core VM in Azure.
5. **Delete your original Azure VM.** After your new VM is in place and working, Quest recommends deleting the outdated VM from your Azure account.

For more information, see Quest Knowledge Base article 118382, "How to migrate AppAssure Core to a new server."

Setting up your Rapid Recovery Core VM

This section includes the tasks required to set up your Rapid Recovery Core VM for use on Azure.
Topics include:

- Creating a Rapid Recovery Core virtual machine in Azure
- Adding storage to your Azure VM
- Accessing your virtual machine from Azure
- Exploring your Rapid Recovery Core VM desktop
- Running the Core configuration script from the VM desktop
- Disabling Compatibility View in Internet Explorer

Creating a Rapid Recovery Core virtual machine in Azure

This procedure includes general guidance for creating a VM in Azure to serve as your Rapid Recovery Core, and configuring the required speed, networking and compute resources. Available resources may include VM disk type, number of virtual CPUs, amount of random access memory (RAM), and performance range (measured in Input/Output Per Second, or IOPS). You may be prompted for other Azure options such as disk support type and load balancing. Because the Azure interface changes frequently, some steps may not match precisely. Conceptually, this procedure includes the following aspects:

- Locating the Rapid Recovery Core VM template in the Azure marketplace and adding it to your subscription.
- Configuring the VM basic settings. These may include VM name, authentication information, and properties such as resource group and location.
- Choosing the VM size. While details for this option often change, this step involves selecting a disk type (solid state or standard hard disk drive). Choose an option with enough RAM and Input/Output per Second (IOPS).
- Configure optional features. These may include managed disks, network and IP address settings, security group settings (which may include public inbound ports), and other Azure options such as auto shut-down, monitoring, and so on.
- Review the summary, which includes a cost per hour to run the VM with the selected attributes.

NOTE: The configuration options and resources you select can affect your hourly cost to operate the VM. before you click **Create**, you can confirm the price per hour for your selected configuration.

CAUTION: Once you enable the VM, you incur hourly charges in your Azure subscription for the duration of time that the VM is allocated. To perform regular backups or replication, the VM must be enabled and allocated. When not using your Rapid Recovery Core VM, you can de-allocate the VM, which pauses hourly billing. The VM remains associated with your subscription but does not incur hourly charges until it is allocated.

For more information about Azure configurations and pricing, see the virtual machines pricing page on the Azure website. For links to other useful references on Microsoft websites, see Microsoft Azure documentation.

This procedure assumes you have not yet created your Core VM.

Follow this procedure to create your Rapid Recovery Core VM.

1. Log into your Azure subscription.
2. From the left Azure navigate menu, click **Create a resource** to access the Azure marketplace.
3. In the **Search the Marketplace** field, type **Rapid Recovery Core** and then press **Enter**.
4. Click to select the Rapid Recovery Core VM in the *Compute* category.
   A *Description* pane expands on the right side, showing information about the Core VM. Optionally, read information about Rapid Recovery Core and explore the web links. Note that this VM uses the Resource Manager model.
5. In the bottom of the Description pane, click **Create**.
   The Create Virtual Machine pane appears, listing the 4 basic steps required for this process. To the right, the *Basics* pane appears, with prompts for basic information about your VM.
6. Configure basic VM settings, as appropriate.
   While basic settings available in the Azure UI may change, please note the following:
   - **Name** refers to the name you want to use for the virtual machine.
   - The values you provide in the **Username** and **Password** fields define login credentials for the Windows user account on the virtual machine. When you connect to the VM in the future, use these credentials.
   - A **Resource group** is a unique name Azure Resource Manager applies to resources (associated with your current Azure subscription only) that groups resources together.
   - If you own a Windows license than you can apply to this VM, you can select an option that will result in a less expensive overall VM cost. Other steps are required as directed in the Azure UI.

   When satisfied, click **OK**. The *Choose a size* pane appears. You can search or filter to select from various VM size configurations.
7. Configure VM size settings, as appropriate, noting the following considerations:
   - The VM sizes that appear in the list are relevant for the selected disk type (SSD or HDD).
   - Some VM sizes that meet minimum requirements are marked with a star . If those sizes are not clearly displayed, click the **Recommended** column to sort the view using this criterion.
   - You can select any VM size that meets or exceeds the sizes of the recommended VMs. However, you cannot change the VM size for your Core in Azure later, so consider the intended use.
   - The processing, compute, and memory resources you select determine the robustness of your Rapid Recovery Core VM. Physical Rapid Recovery Cores in release 6.9 require a minimum of 8GB RAM and quad-core processor; these are minimum recommended specifications. The minimum disk size is not relevant, since repository storage is considered separately.

   When satisfied, click **Select**. Your selections are saved and the *Settings* pane appears.

8. Configure optional features, as appropriate, noting the following considerations:
    - If you select high availability, you must reside in a region supporting availability zones. This requires using managed disks. For more information, see Overview of Availability Zones in Azure.
    - If prompted to specify public inbound ports, specify **RDP** at minimum, since you must connect to your Azure VM by Remote Desktop Protocol after it has been created.
    - If your Core requires other ports to be opened, select the appropriate options. For example, if your Core also requires **SQL Server**, select **MS SQL**.

      CAUTION: Quest strongly recommends avoiding Azure's Auto-shutdown feature. Allowing Azure to shut down the VM without gracefully stopping the Rapid Recovery Core service may lead to repository corruption or data inconsistencies.
    - For more information about the options available, see Azure documentation.

    When satisfied, click **OK**. Your selections are validated, and the *Create* pane appears.
9. Review a summary of your VM configuration options, including the estimated hourly cost for running the VM on Azure These costs are charged by Microsoft on a monthly basis according to your subscription details and usage. When satisfied, click **Create**.

When the VM creation and deployment is complete, the VM creation options window closes, and the Azure dashboard displays. While the VM deploys, you can see a representation of it on the desktop. When complete, a notification appears briefly, and an overview with details for your VM appears in Azure.

Next steps

Before you can use your Rapid Recovery Core VM, you must attach one or more storage disks. Proceed to the next step in the setup process, Adding storage to your Azure VM.

Accessing your virtual machine from Azure

This procedure assumes that you have a Microsoft Azure subscription associated with a Microsoft user account, and that you have already created a Rapid Recovery Core VM in that Azure account.

1. If necessary, log into your Azure user account.
2. From the dashboard, from the Microsoft Azure left navigation menu, click **Virtual Machines**.
   The *Virtual machine*s page appears, showing all VMs in your current Azure subscription.

3. Click the VM name for your Rapid Recovery Core VM.
   The *Virtual machines details* pane appears, with icons at the top. Some of the actions you can perform with each VM are described in the following table.
   Table 1: Virtual machine pane options

Icon	Function	Description
	Connect	Starts an RDP or SSH session to connect to your VM.
	Start	Starts the VM from a paused or unallocated state.
	Restart	Restarts the VM.
	Stop	Stops, or de-allocates, the VM. This causes compute costs to stop accruing.
	Move	Moves the selected VM to another resource group or subscription.
	Delete	Delete the virtual machine from your account.
	Refresh	Update the view of the VMs displayed on the page.

4. To access your VM, you must connect to it using the Remote Desktop Protocol (RDP). From the top menu, click **Connect**.
5. If you see the *Connect to virtual machine* pane, select the **RDP** protocol, verify the IP address and port number (the default RDP port is 3389), and then click **Download RDP File**.
6. If prompted to save the RDP file, click **Save**, or select **Save as** and name the file, and then click **Open**.
7. If prompted in a dialog box to connect, do the following:
   a. Optionally, if you want the browser to remember this selection, select **Don't ask me again for connections to this computer**. If you select this option, the Connect prompt does not display in the future.
   b. Confirm any requests to connect by clicking **Connect**.
8. In the *Enter your credentials* dialog box, enter credentials for the Rapid Recovery Core VMfor the do the following:
   a. If necessary, in the **User name** field, enter the Windows username associated with this VM.
   b. In the **Password** field, enter the password associated with this VM.
   c. Optionally, to remember your credentials, select **Remember me**.
   d. To enter credentials other than the currently displayed user account, click **More choices** and then select **Use a different account** and enter the correct credentials.
   e. When satisfied, click **OK**.
9. If you see a *Remote Desktop Connection* dialog box related to the security certificate, and you are prompted to confirm the connection, click **Yes**.
   The RDP session connects, and your Rapid Recovery Core VM desktop displays.

Next steps

For more information about the items that appear on the desktop of your VM, see Exploring your Rapid Recovery Core VM desktop

Exploring your Rapid Recovery Core VM desktop

This topic describes the items you see on your Rapid Recovery Core VM before and after setup using the configuration script.

Your Rapid Recovery virtual machine uses the Windows Server 2019 Data Center operating system. Each time a virtual or physical machine using this OS starts, Windows opens the Server Manager utility. Unless you need it, you can click the **X** in the top right of the Server Manager window to close Server Manager.

When you first connect to your Rapid Recovery Core VM, and before you run the configuration script, four desktop shortcuts appear. After you run the configuration script, two additional items appear. These items are described in the following table. The last column in the table describes whether the desktop item appears before the configuration script is initially run.

Table 2: Rapid Recovery Core VM desktop items

Item Name	Description	Path	Appears Before Setup
Configure Rapid Recovery Core	This Windows shortcut launches a script or sequence of scripts to configure your Core. Also use each time you attach new virtual disks for repository storage for your Core.	C:\Program Files\AppRecovery\Core\PowerShellScripts\VM_FTBU\Setup.cmd	Yes
Core Console	This Windows shortcut to the Rapid Recovery Core Console. A sample URL is `https://MyVM:8006/apprecovery/admin/`	https://[vmname]:[port]/apprecovery/admin/	No
Rapid Recovery Documentation	This Internet URL opens technical product documentation on the Quest Support website.	https://support.quest.com/rapid-recovery/6.9/technical-documents	Yes
Rapid Recovery License Portal	This Internet URL opens the Rapid Recovery License Portal in your web browser, where you can manage Rapid Recovery licenses.	https://rapidrecovery.licenseportal.com/	Yes
Rapid Recovery Software Support	This Internet URL opens the Rapid Recovery Support portal for self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. You can browse video tutorials, knowledge base articles, access user forums, start a Live Chat session, and more. When you click **Contact Support** from this page, you have direct access to product support engineers through an online Service Request system.	https://support.quest.com/rapid-recovery/6.9	Yes
Rapid Recovery 14-day trial key.lic	The first time you open the Rapid Recovery Core Console, you are prompted to associate a license key with your Core. You can use the temporary key on the desktop, or obtain a perpetual or subscription license from Quest and enter the long-term license key.	C:\Users\[username]\Desktop\ Rapid Recovery 14-day trial key.lic	No

The first time you open your Core and associate it with a license, the Quick Start Guide appears. This is a Rapid Recovery feature that provides you with a guided flow of suggested tasks for configuring and using Rapid Recovery Core.

You are not required to perform any steps suggested by the guide. You can simply view the suggested tasks, navigating through them using the **Skip Step** and **Back** options. Optionally, to hide the guide at any point, click **Exit Guide**. For more information, see the topics "Understanding the Quick Start Guide" and "Hiding the Quick Start Guide" in the latest version of *Rapid Recovery User Guide*.

Next steps

- If you have not yet done so, add storage to your VM. See the topic Adding storage to your Azure VM.
- Each time you add more storage to your VM, run the configuration script. See the topic Running the Core configuration script from the VM desktop.
- For more information about using Rapid Recovery release 6.9, see the latest version of *Rapid Recovery User Guide*.

Adding storage to your Azure VM

This procedure assumes that you have a Microsoft Azure subscription, and that you have already created a VM in Azure to use as a Rapid Recovery Core.

When you create a virtual machine from the Azure Marketplace, the VM includes only the amount of storage reserved for the operating system and Core application. From your Azure subscription, you must attach at least one additional data disk to your Core VM, which will be used as the storage location for the repository.

> **CAUTION:** The current maximum storage size for any single disk that can be purchased from the Marketplace is 1023GB (for practical purposes, in this document we refer to this as 1TB). For best results, Quest recommends that you add storage disks for working with Rapid Recovery in 1TB increments. If you need more storage for your Rapid Recovery Core, you can attach additional 1TB disks to your Azure VM.

You can add storage to your Azure VM before you run the script to configure your Rapid Recovery Core VM, or any time afterward. Quest recommends adding storage first, for the sake of simplicity.

- If you add storage *before* setting up your Rapid Recovery Core VM using the configuration script, the repository is automatically defined as the storage location for your repository.
- If you attach storage to your VM *after* the Core is configured, you can run the configuration script again to automatically associate that storage disk with your repository. From a Rapid Recovery perspective, additional storage disks are viewed as extents to your DVM repository.

If you attach storage to your VM *after* the Core is configured, you can run the configuration script again to automatically associate that storage disk with your repository. From a Rapid Recovery perspective, additional storage disks are viewed as extents to your repository. Alternatively, you can add a new storage location to an existing Rapid Recovery DVM repository from the Core Console GUI on your VM. For more information, see the latest version of *Rapid Recovery User Guide* topic "Adding a storage location to an existing repository."

> **NOTE:** While the precise steps or the user interface for adding storage to your Azure VM may change, the main purpose of this step is to attach at least one data disk to your replication target VM. You can also search for relevant articles in the Azure documentation center. For example, see How to attach a data disk to a Windows VM in the Azure portal.

Perform the following procedure in your Azure subscription to attach storage to the replication target VM.

1. Log into your Azure VM.
2. In the Azure dashboard, from the left navigation menu, click Virtual machines.
   The Virtual machines page appears.
3. In the list of virtual machines, click the name of your Rapid Recovery Core VM.
   Two more panes appear. The first shows details for the selected VM, and the second pane shows settings for the VM.

4. In the VM settings pane, click Disks.
   The *Disks* pane expands. You can see the OS disk attached to the VM, and below that, the data disks (if any) currently attached to the selected VM.
5. In the *Disks* pane, in the Data Disks section, follow the UI to **+ Add data disk** or **Create disk**.
6. In the resulting pane, enter values as described in the following table to specify storage disk attributes.

Option	Description
Name	Type an appropriate name for your storage disk. For example, type **RapidRecoveryCore_StorageVolume1**.
Source type	Select the appropriate disk type.
Account type	Select the appropriate storage account type. Standard disks use standard magnetic disks. Premium (SSD) disks use solid state drives and have low latency. Quest recommends using premium disks on Azure for high transfer rates or frequent replication.
Size (GiB)	Enter the appropriate disk size. Quest strongly recommends using a 1023GB disk (the current maximum for Azure). **NOTE:** When you run the configuration utility (described in the topic Running the Core configuration script from the VM desktop), any empty storage disks that you attached to your Azure VM are automatically added to your Core as a DVM repository. If multiple disks are attached, each is configured as a separate storage location in the DVM repository. If you want to add more than one storage disk at the outset, add them all before running the configuration script. If you add more storage to your Azure VM later, you can run the configuration script again to automatically add the new disk as an extent (storage location) to your existing DVM repository. You can also add a new disk manually, by adding a storage location to a DVM repository from within the Core Console. For more information, see the latest version of *Rapid Recovery User Guide* topic "Adding a storage location to an existing repository."
Storage container	Navigate through your existing storage account, locate, and select the appropriate existing storage container. Rapid Recovery uses a default container called vhds that stores virtual hard disks that are shared among all VMs.
Storage blob name	Define a storage binary large object (blob) name, or leave the default name. This is the name of the virtual disk that you are attaching to the selected VM.

7. Review the information you specified for the new disk, and then click **OK**. Then click **Save**.

   CAUTION: If you do not click **Save**, the disk configuration is not saved and the disk is not attached to your VM.

   .
   After a brief wait, the new disk appears in the *Disks* pane.

   NOTE: After creating the virtual disk, Quest recommends waiting 2 to 5 minutes before running the configuration script, to ensure the storage resources are discoverable.
8. Optionally, if you want to add any additional disks, repeat steps 5 through 7 of this procedure.
9. Optionally, verify whether each storage volume you attached is recognized by the VM by using utilities such as Disk Management or Device Manager from the VM. If any volume is not recognized, Microsoft recommends rebooting the VM to ensure all storage drives are accessible.
10. Optionally, you can close the browser with your Azure account information.

Next steps

Proceed to the next step in the setup process, Running the Core configuration script from the VM desktop.

Running the Core configuration script from the VM desktop

The configuration script included on the VM desktop runs a sequence of actions to prepare the VM to use the Core. It removes the Core ID associated with the VM (to avoid Cores with duplicate IDs); starts the Core service; moves the trial license to the desktop; creates a desktop shortcut for the Core Console; and automatically creates a repository on any new disks attached to your VM.

This task describes the process of running this configuration script from the shortcut on the desktop of your Rapid Recovery Core VM. Quest recommends performing this process after first attaching storage to the Azure VM, and repeating it each time you add additional storage to your VM. Running this script initially typically takes about five minutes, after which the command window closes.

After initial configuration of your VM, if you attach additional storage from the Azure Marketplace, running this script again configures the virtual disk as the storage location for your repository. When run subsequently, the script takes less than a minute to run.

Perform this procedure to configure your Core the first time, and each time you add additional storage.

1. From the Azure VM desktop, right-click on the **Configure Rapid Recovery Core** shortcut, and from the context-sensitive menu, select **Run as administrator**.
   A command window entitled Administrator: Windows PowerShell appears, and the script begins to run. Several operations occur sequentially, and the progress of the script is logged in the command window.
2. If a Microsoft Windows dialog box appears prompting you to format the disk before you can use it, click **Cancel**.
   The script continues to run; the script formats the storage drive in the most efficient manner for using the Rapid Recovery Core. When the script is complete, the command window closes. The **Core Console** shortcut appears on the desktop, to let users easily launch the Rapid Recovery Core Console.

Next steps

Before protecting machines in your Core or replicating from another Core, you must disable the Compatibility View feature in the Internet Explorer web browser. For more information, see Disabling Compatibility View in Internet Explorer.

Before using your Core, you must associate a license key. For more information, see Activating your Rapid Recovery license.

If using a standard license with Rapid Recovery Core, you must agree to the use of privacy information. For more information, see X.

Disabling Compatibility View in Internet Explorer

Internet Explorer includes a Compatibility View feature. The purpose of this feature is to correct the display of websites optimized for old versions of Internet Explorer (version 7 or earlier). By default, this option is typically enabled for all intranet sites, but can present problems when viewing modern web interfaces.

This task describes the process to disable the Compatibility View option of Internet Explorer, which is required for using the Rapid Recovery Core Console on the Azure VM. This is a one-time setup step.

Perform the steps described in the following procedure to disable Compatibility View in Internet Explorer.

1. Open an Internet Explorer web browser window on the Azure VM.
   For example, double-click the **Core Console** shortcut on the VM desktop.
   An Internet Explorer web browser window opens. If the content does not display, check for and disable the Compatibility View feature as follows.
2. If the Set up Internet Explorer 11 dialog box appears, do the following:
   a. Select **Don't use recommended settings**.
   b. Optionally, clear **Send Do not Track requests to tell sites you prefer not to be tracked**.
   c. Click **OK**.

   The dialog box closes, and Compatibility View is now disabled.
3. If the dialog box does not appear, from Internet Explorer, click the Tools icon, and then select **Compatibility View settings**.
   The Compatibility View settings dialog box appears.
4. In the Compatibility View settings dialog box, clear the following settings:

Option	Description
Display intranet sites in Compatibility View	You must clear this option.
Use Microsoft compatibility lists	You must clear this option.

5. Click **Close**.
   The dialog box closes, and Compatibility View is now disabled.

Obtaining the Publish Settings file for your Azure account

To perform this task, you must be using a Windows machine on which PowerShell is enabled. You must also have access to an Azure account that is granted the service administrator or service co-administrator role.

The Publish Settings file is an XML document generated on Azure. The file contains the AzureServiceManagement API definition, and information about your Azure subscription, including secure encoded credentials, your subscription type, and an Azure management certificate. This file contains a file extension of .publishsettings, from which the description is derived. Without the Publish Settings file, you cannot connect your Core to an Azure account.

You can obtain a copy of the Publish Settings file from a Windows machine logged into your Azure account.

> **CAUTION:** Since the publish settings file contains your credentials and information about your Azure account, Microsoft recommends storing the publish settings file in a secure location. Once you have loaded the certificate, you can delete the file from your local system.

Microsoft imposes a limit of 100 management certificates per subscription, with an additional maximum limit of 100 management certificates for all subscriptions under a specific service administrator's user ID. If you need to access the same Azure account from multiple Cores, you can generate the Publish Settings file one time and re-use the same file to load the management certificate into multiple Cores. In this way, you can avoid exceeding the certificate generation limit.

> **NOTE:** For more information on this limit, see the "Limitations" section of the Microsoft KB article "Certificates overview for Azure Cloud Services" at https://docs.microsoft.com/en-us/azure/cloud-services/cloud-services-

certs-create. y.

Complete the steps in this procedure to obtain the Publish Settings file.

1. From a Windows machine, log into the Azure dashboard.
2. While logged into Azure, open another browser window.
3. Execute a PowerShell script to download the file by entering the following address into the URL of the browser:
   `https://manage.windowsazure.com/publishsettings/index?client=powershell`.
   When successful, the Publish Settings file is saved to your default download directory.
4. Move this file to a machine accessible to the Core Console.

To associate Azure subscription information with your Rapid Recovery Core, see the *Rapid Recovery User Guide* topic "Loading an Azure management certificate."

Understanding licensing

Generally, each Core must have a software license that registers with the license portal. This section contains information relevant to using Rapid Recovery in Azure.

The following topics describe information about licensing.

- About Rapid Recovery licenses
- Bring your own license
- Activating your Rapid Recovery license
- General Data Protection Regulation compliance
- Licensing and privacy considerations
- Agreeing to use personal data

About Rapid Recovery licenses

To use and manage any version of Rapid Recovery, AppAssure, or DL series backup and recovery appliance software, you need two items:

1. **An account on the Rapid Recovery License Portal**.
   License portal accounts are free. If you are a new user, register at https://licenseportal.com. When you register, use the email address that is on file with your Quest Sales representative. If upgrading from a trial version, use the email address associated with the trial version. If you need to use a different email address, contact your Quest Sales representative for assistance.

   NOTE: This license portal was previously known as the AppAssure License Portal. If you already have a license portal account that you have used for AppAssure, use that account information. Previous license portal users do not need to register a new account for Rapid Recovery.

   For more details about the license portal, please see the *Rapid Recovery License Portal User Guide* .

2. **A software license.**
   The Rapid Recovery Core software requires a valid software license to perform uninterrupted backups, replication, or data restoration.

   For the time period that it is valid, you can use a trial license. However, after a trial license expires, the Rapid Recovery Core stops taking snapshots, replicating, and restoring until you obtain and register a valid long-term license. For simple steps to register a temporary or long-term license, follow the procedure in the topic Activating your Rapid Recovery license.

   - **Rapid Recovery Core managed on-premises or by an application service provider.** If you registered for a trial version of Rapid Recovery Core, the installer is configured with a trial license which you can use immediately. This temporary license is valid for 14 days, and can be extended one time by the group administrator to a 28-day license.
   - **Running Rapid Recovery in Azure**. The Rapid Recovery Core VM on Azure in release 6.9 or later comes with a Rapid Recovery 14-day trial key.lic file. After running the configuration script, this file appears on the VM desktop. This temporary license works in non-phone-home mode. License requirements for running Rapid Recovery on Azure are as follows:
     - **Replication to a target Core in Azure.** If replicating an on-premises Core to a target Core in Azure, you can use the 14-day trial license. To continue replicating after that period, you are required to obtain and register a permanent replication-only license. This type of license is included for free to any licensed user of Rapid Recovery Core or AppAssure Core. To obtain a long-term replication-only license, contact your Quest Sales representative.
     - **Rapid Recovery primary Core in Azure.** If running a primary Core as a VM in Azure, you can capture recovery points in your repository. From these, you can restore data, create archives, perform bare metal restore, perform virtual export, and replicate to another Core. You can perform all of these actions using your temporary license. To continue these operations uninterrupted, you must register a long-term subscription or perpetual license. If you have a license available in your current license pool, you can assign that license to your Core VM. Otherwise, contact your Quest Sales representative to purchase a long-term license.
   - **Quest DL backup and recovery appliances.**
     If you purchased a Quest DL backup and recovery appliance, your appliance is configured with a 30-day temporary license that is activated automatically the first time you start the Core on the appliance.

     After you purchase software or a Quest DL appliance, you receive by email a long-term (non-trial) license file or license number. If specified on the sales order, the license is sent to the end user email address. Otherwise, the long-term license is sent to the contact email address on the sales order.

   The process for registering a temporary or long-term license are identical.

For more information about licenses

For more information about Rapid Recovery licenses, see the following resources:

- For simple steps to register a temporary or long-term license, follow the procedure in the topic Activating your Rapid Recovery license.
- You can extensively manage Rapid Recovery licenses using the Rapid Recovery License Portal at https://licenseportal.com/. You must create an account to use this portal.
- For information on using the license portal, see the appropriate *Rapid Recovery License Portal User Guide*.

- For more information on managing Rapid Recovery licenses from the Rapid Recovery Core Console, see the latest version of *Rapid Recovery User Guide* topic "Managing licenses." After upgrading your license, it is best practice to refresh the connection between the Core and the license portal. For more information, see the latest version of *Rapid Recovery User Guide* topic "Contacting the Rapid Recovery License Portal server."

Bring your own license

All installations of the *Rapid Recovery Core* require a software license. Rapid Recovery Cores running in Azure use a "Bring your own license" model. The Rapid Recovery Core VM ships with a 14-day temporary license, accessible from the Core VM desktop after you run the configuration script. This temporary license lets you perform any Core function: capturing backup snapshots in the repository, archiving, exporting to a virtual machine, replicating to a target Core VM in Azure, or recovering from a recovery point. After the trial license expires, you can continue to recover data from existing recovery points, but new operations will be paused until you obtain and register a subscription or perpetual license. To continue using the Core in Azure without interruption, register the long-term license before the trial period expires.

If you are a new Rapid Recovery user, you can purchase licenses from your Quest Sales representative. To purchase Rapid Recovery, visit https://www.quest.com/contact.

If using your Core only as a replication target for on-premises backups, and you have an active Core license, you can obtain and register a free Replication-only license. Any other use, including using your Rapid Recovery Core VM as a primary Core, require you to register and consume a license from your active subscription or perpetual license pool. If you do not have enough existing licenses in your available license pool, you can purchase more from your Quest Licensing team. You can contact them by visiting https://support.quest.com/contact-us/licensing.

Activating your Rapid Recovery license

The Rapid Recovery Core software requires a software license. Follow this procedure to activate your Rapid Recovery Core license the first time you log in to the Rapid Recovery Core Console.

Before using the Rapid Recovery Core on an Azure VM as an incoming replication target, you must first disable Compatibility Mode. For more information, see Disabling Compatibility View in Internet Explorer.

Use this process to activate your temporary license, or to activate a perpetual license you received from a Quest Sales or Licensing representative.

NOTE: If you select the temporary license, then to continue using Rapid Recovery Core after the introductory period, you must obtain a valid software license. For more information, see About Rapid Recovery licenses.

1. On your Azure VM desktop, double-click the **Core Console** shortcut icon.
   If Compatibility View is disabled, then the first time you open the Core Console, you see a prompt to upload a license file or enter a license key.

2. To upload a license file, do the following:

    a. From the **Choose license file or enter license key** field, click **Choose File**.
    The *Choose File to Upload* dialog box appears.

    b. Navigate to the license file and select the filename.
    For example, navigate to the desktop and select the **Rapid Recovery [n]-day trial key.lic** file.

    c. From the *Choose File to Upload* dialog box, click **Open** to confirm the license file selection.
    The dialog box closes, and the filename of the license appears in the Choose license file or enter license key field.

3. To enter a license key you received from a Quest Support representative, do the following:

    a. In the **Choose license file or enter license key** field, type the license key precisely.
    You must enter the exact key. If you copy the key and paste it into the Choose license file or enter license key field, ensure that you do not include any spaces before or after the key.

    b. Confirm the license key you entered key is correct.

4. To confirm the license file or key, click **Continue**.
    The license dialog box closes, and the license is applied to the Core. The Rapid Recovery Core Console user interface appears. In the Rapid Recovery Core Console, the *Welcome to the Core Quick Start Guide!* dialog box appears. Your software license is now registered for the appropriate period.

Next steps

- If you attached storage to your Azure VM before running the configuration script, the script automatically formats the virtual disk and uses it as the storage location for your repository. Your Core is then fully configured, and your repository is ready to use as a target for incoming replication from other Cores.
- If you ran the configuration script before you attached storage, or if you later attach additional storage, the easiest way to format the virtual disk and add it to your repository is to run the configuration script again. For more information, see Running the Core configuration script from the VM desktop
- You can also add storage locations from the Rapid Recovery Core Console. For more information, see the latest version of *Rapid Recovery User Guide* topic "Managing a DVM repository," including the topic "Adding a storage location to an existing DVM repository."
- If you want to include full recovery point chains in your replicated target Core, you must seed the data on the target Core. See Considerations for seeding data to your target Core.
- For information about using the Quick Start Guide, see the latest version of *Rapid Recovery User Guide* topic "Understanding the Quick Start Guide."
- For general information about replication, see the latest version of *Rapid Recovery User Guide* topic "Replication."
    For information about configuring replication, see the latest version of *Rapid Recovery User Guide* topics "Configuring replication" and "Replicating to a self-managed target Core."

General Data Protection Regulation compliance

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

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

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

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

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

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

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

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

Licensing and privacy considerations

The Rapid Recovery License Portal periodically checks each Rapid Recovery Core to verify licensing and to monitor uptime status for reporting. A limited amount of PII is used to compare the Core and protected or replicated machines with the license portal. This includes IP addresses, hostnames, or email addresses associated with Rapid Recovery licenses. This mode is known as "phone-home" mode. Most Rapid Recovery licenses are used in this mode, which has several advantages.

For GDPR compliance, Rapid Recovery requires users to read about how the application uses their PII, and to explicitly consent to this use in order to use a standard phone-home license. Thus, after creating and configuring a Rapid Recovery Core on Azure, you must access Core general settings and confirm that you agree to this use of personal data. See Agreeing to use personal data for details. This is a one-time requirement. Once you consent, you will not need to specify this setting when upgrading to new Core versions.

Of course, users have the ability to control this already limited use of PII. If you opt out, you must obtain a "non-phone-home" license which does not use your PII. However, use of a non-phone-home license prevents the Core from providing auto-update notifications and updates. You also cannot use the Data Protection Portal if using a non-phone-home key. If you want to operate Rapid Recovery licenses in non-phone-home mode, you must explicitly contact the Quest licensing team and request non-phone-home licenses.

For details, see the "Managing Privacy" section of the *Rapid Recovery User Guide*.

Next steps

To consent to the use of PII for using a standard phone-home license, see Agreeing to use personal data

To obtain a non-phone-home key, see the "Managing Privacy" section of the *Rapid Recovery User Guide*.

Agreeing to use personal data

To use your Rapid Recovery Core VM in the standard phone-home license mode, you must agree to the use of personal data in General settings in the Rapid Recovery Core Console. For more information, see Licensing and privacy considerations.

Follow this procedure to let your Core use personal data.

1. Log into your Rapid Recovery Core VM on Azure.
2. Navigate to the Rapid Recovery Core Console.
3. On the icon bar, click (Settings), and then click **General**.
4. In General settings, if the value associated with the option **Agree to use of personal data** is **Yes**, no changes are required.
5. In General settings, if the value associated with the option **Agree to use of personal data** is **No**, click the setting once to make it editable; then click inside the checkbox so that a check mark appears; finally, click the check mark to the right of your selection to confirm it.
6. Click **OK** to confirm that auto update, license portal, and Data Protection Portal settings must be changed individually, if appropriate.
   When you allow the use of personal data, this choice automatically enables three Core features: auto-update, communication with the license portal, and enabling connection to the Data Protection Portal. If you want to disable any of these while agreeing to the use of personal data, adjust each Core setting individually.
   Use the new license key when first starting your Cores. You must obtain a long-term license to continue using the Core. For more information about licenses, see Understanding licensing. For instructions on activating a license, see Activating your Rapid Recovery license.

Next steps

Setup and configuration of your Rapid Recovery Core VMis now complete. For information about using Rapid Recovery, see the *Rapid Recovery User Guide*.

Considerations for seeding data to your target Core

Once you start replicating to your target Core VM, any new recovery points saved to your source Core are replicated on your VM in the Azure cloud.

For more information on replication in Rapid Recovery, see the *Rapid Recovery User Guide*, including the parent topic Replication and the topic Replication with Rapid Recovery.

If your source Core captured one or more base image backups before you started replicating to the Azure VM, you may have incomplete recovery point chains in your target Core. Until all backup data from the source Core is transmitted to the target Core, creating full recovery point chains from the orphans, you can only perform file-level restore.

For more information on recovery point chains and orphans, see the *Rapid Recovery User Guide* topics Recovery point chains and orphans and When replication begins.

If you want your replicated target Core to have access to data saved previously on the original source Core, seed your target Core. The process of seeding unites each incremental backup with its base image, repairs the orphaned data with full recovery point chains. There are two approaches to seeding:

1. You can seed to the target Core over a network connection.
   For large data or slow connections, seeding by this method can take a substantial amount of time.
2. You can also create a seed drive from the source Core, saving backup data to external media and then transferring the initial data to the target Core.

If you do not need to seed data (for example, if you capture a base image after starting replication, and don't need access to earlier data), then replication can be completed entirely from the source Core.

To help decide which seeding approach is more appropriate, see the *Rapid Recovery User Guide* topics Determining your seeding needs and strategy and Performance considerations for replicated data transfer.

If using a seed drive to seed data for your replication target, you must send the storage media containing the seed drive file to a Microsoft Azure data center. An Azure data center representative attaches the media, and notifies you when it is ready (typically within hours). You can then consume (or import) the seed data in your target Core.

For information and links specific to seeding for Azure, see Seeding data to Azure using the Microsoft Azure Import/Export service.

For a detailed procedure to consume the data, see the *Rapid Recovery User Guide* topic Consuming the seed drive on a target Core.

Seeding data to Azure using the Microsoft Azure Import/Export service

If seeding your data to an Azure replication target, use the Microsoft Azure Import/Export service. This service has certain prerequisite and requirements. These are documented on the Azure website, and links to some relevant articles are included below.

Following are some guidelines for seeding to Azure.

- Transfer your repository archives to one or more 3.5-inch Serial Advanced Technology Attachment (SATA) II or SATA III internal hard drives, 8TB or smaller.
- You can transfer a maximum of 80TB of data, based on Microsoft's guidelines. Microsoft charges a nominal fee per drive to seed your data. For current pricing, see the Azure website or contact an Azure representative.
- You must have an existing Azure subscription and one or more Classic storage accounts to use the Azure Import/Export service.

Since Microsoft can change prerequisites, requirements, costs, and so on, always verify this information.

For more information, including specific articles regarding pricing and procedure for using the Microsoft Azure Import/Export service, see Microsoft Azure documentation.

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit www.quest.com.

Technical support resources

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

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

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