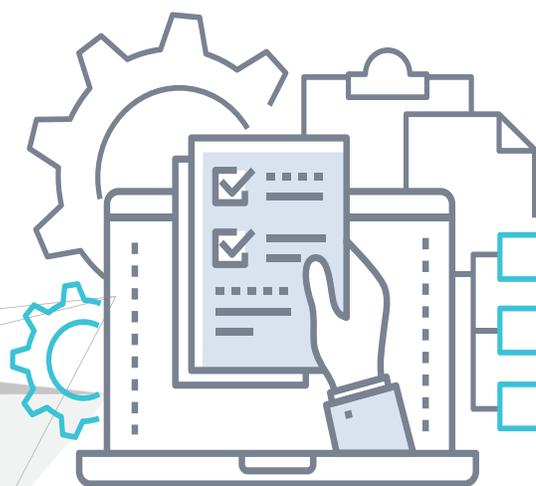


# Deployment Guide for Unitrends Backup in Microsoft Azure

Release 10.9 | Document Date 07152025



# Copyright

Copyright © 2025 Unitrends Incorporated. All rights reserved.

Content in this publication is copyright material and may not be copied or duplicated in any form without prior written permission from Unitrends, Inc (“Unitrends”). This information is subject to change without notice and does not represent a commitment on the part of Unitrends.

The software described in this publication is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of the license agreement. See the End User License Agreement before using the software.

The software described contains certain open source components that are copyrighted. For open source licenses, see the Unitrends Open Source Compliance section of the product Administrator Guide.

Because of the nature of this material, numerous hardware and software products are mentioned by name. In most, if not all, cases these product names are claimed as trademarks by the companies that manufacture the products. It is not our intent to claim these names or trademarks as our own.

The following applies to U.S. Government End Users: The Software and Documentation are “Commercial Items,” as that term is defined at 48 C.F.R.2.101, consisting of “Commercial Computer Software” and “Commercial Computer Software Documentation,” as such terms are used in 48 C.F.R.12.212 or 48 C.F.R.227.7202, as applicable. Consistent with 48 C.F.R.12.212 or 48 C.F.R.227.7202-1 through 227.7202-4, as applicable, the Commercial Computer Software and Commercial Computer Software Documentation are being licensed to U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein. Unpublished-rights reserved under the copyright laws of the United States. Unitrends agrees to comply with all applicable equal opportunity laws including, if appropriate, the provisions of Executive Order 11246, as amended, Section 402 of the Vietnam Era Veterans Readjustment Assistance Act of 1974 (38 USC 4212), and Section 503 of the Rehabilitation Act of 1973, as amended, and the regulations at 41 CFR Parts 60-1 through 60-60, 60-250, and 60-741. The affirmative action clause and regulations contained in the preceding sentence shall be incorporated by reference.

The following applies to all contracts and subcontracts governed by the Rights in Technical Data and Computer Software Clause of the United States Department of Defense Federal Acquisition Regulations Supplement:

RESTRICTED RIGHTS LEGEND: USE, DUPLICATION OR DISCLOSURE BY THE UNITED STATES GOVERNMENT IS SUBJECT TO RESTRICTIONS AS SET FORTH IN SUBDIVISION (C)(1)(II) OF THE RIGHTS AND TECHNICAL DATA AND COMPUTER SOFTWARE CLAUSE AT DFAR 252-227-7013. UNITRENDS CORPORATION IS THE CONTRACTOR AND IS LOCATED AT 200 WHEELER ROAD, NORTH TOWER, 2ND FLOOR, BURLINGTON, MASSACHUSETTS 01803.

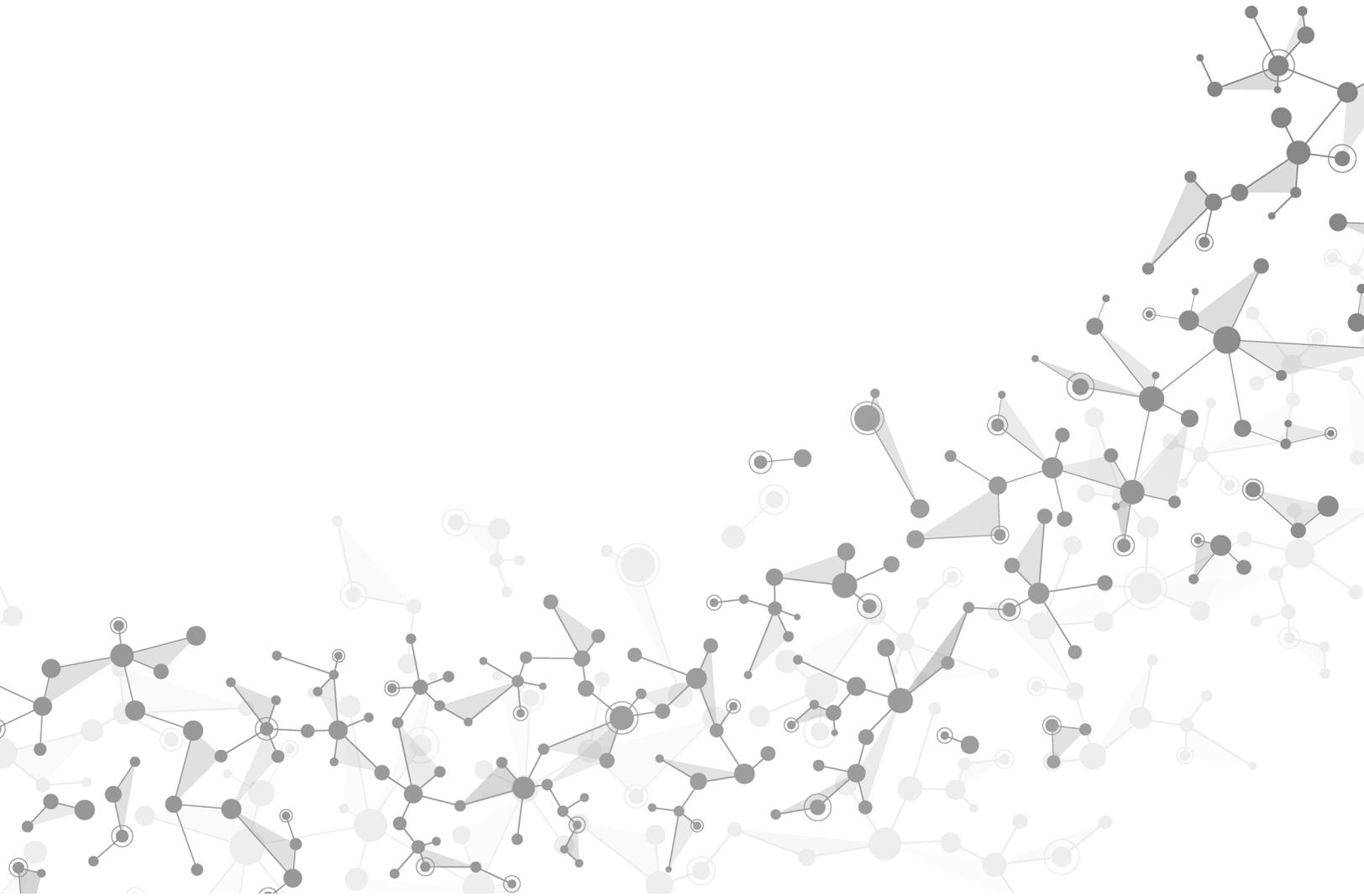
Unitrends, Inc  
200 Wheeler Road  
North Tower, 2nd Floor  
Burlington, MA 01803, USA  
Phone: 1.866.359.5411

# Contents

---

<b>Chapter 1: Introduction</b> .....	<b>5</b>
Key Terms .....	5
<b>Chapter 2: Requirements and Considerations</b> .....	<b>7</b>
Network and web access requirements .....	7
Minimum resource requirements .....	9
Backup storage .....	9
Additional considerations .....	9
Limitations .....	9
Licensing .....	10
<b>Chapter 3: Deploying the Unitrends Backup VM</b> .....	<b>11</b>
Step 1: Download the Unitrends Backup VHD .....	11
Step 2: Create a storage account .....	12
Step 3: Create a storage container .....	17
Step 4: Create an image from the Unitrends VHD .....	20
Step 5: Create the Unitrends Backup virtual machine .....	21
Step 6: Set up the appliance using the Quick Setup Wizard .....	27
Step 7: Register and license the appliance .....	32
Step 8: Start protecting your environment .....	36

*This page is intentionally left blank.*



# Chapter 1: Introduction

Unitrends Backup in Azure leverages Unitrends Backup technology as a deployable virtual machine in the Microsoft Azure Marketplace. Our Azure-based Unitrends Backup VM can be used as either a backup appliance or a backup copy target.

As your data set grows, you can scale up by adding compute resources (CPU, RAM), or scale out by deploying additional Unitrends Backup appliances. Azure allows up to 64TB of storage on a single VM.

This deployment guide provides requirements, considerations, and instructions for deploying a Unitrends Backup appliance in Azure.

For requirements and considerations for particular features and instructions on using them, see the [Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup](#).

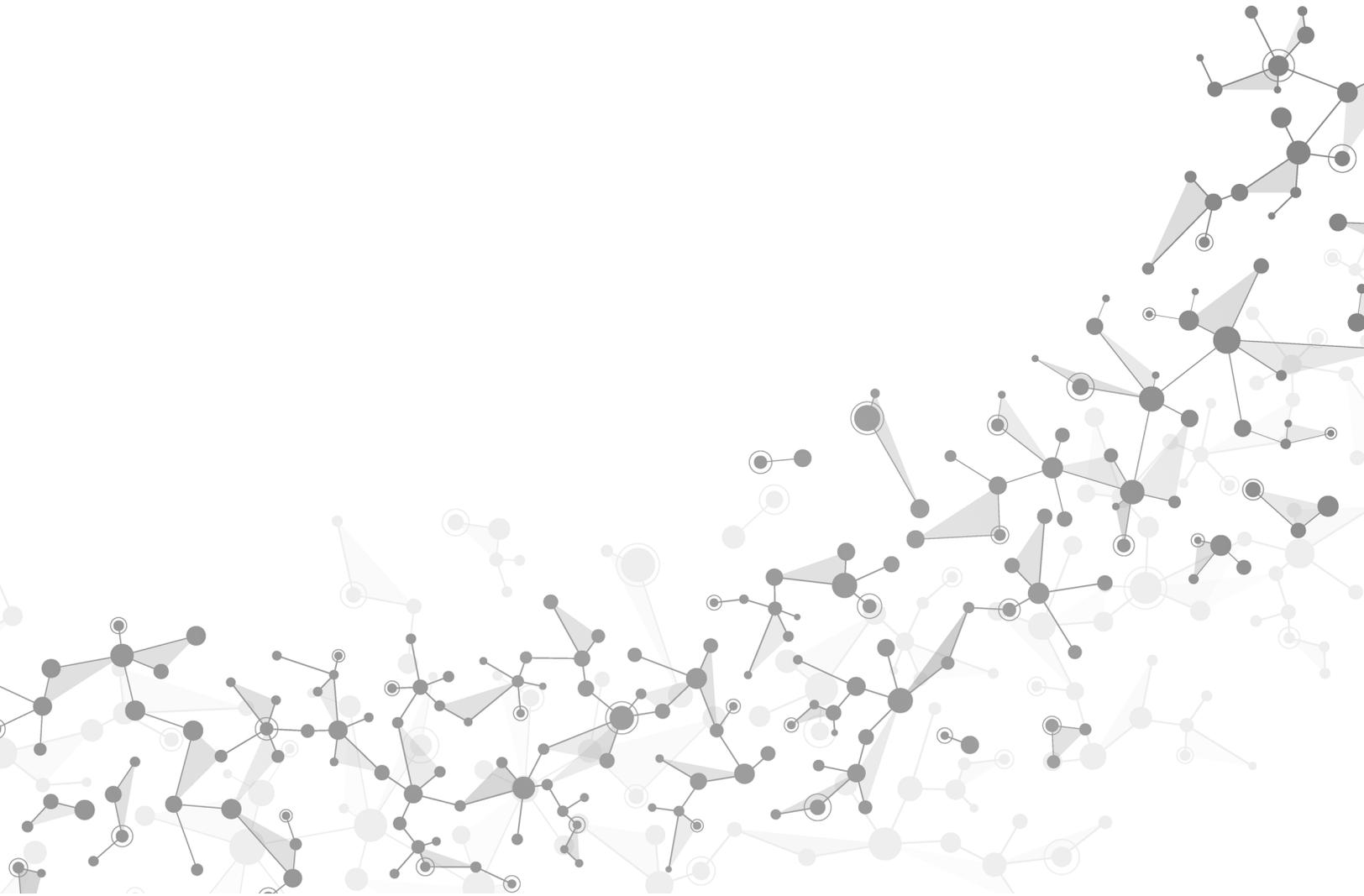
See the following topics for details on deploying the Unitrends Backup appliance:

- "Requirements and Considerations" on page 7
- "Deploying the Unitrends Backup VM" on page 11

## Key Terms

Term	Definition
Appliance	The Unitrends Backup system that backs up and recovers data.
Data Disk	The standard unit of storage in Microsoft Azure.
Deployment	The process of creating a Unitrends Backup VM and configuring the appliance it contains.
Quick Setup Wizard	The Quick Setup Wizard automatically launches the first time you access the appliance UI from a web browser. Work your way through this wizard to configure additional appliance settings, such as date and time, hostname, and email.
Unitrends Backup VM	A virtual machine that contains a Unitrends Backup Appliance.

*This page is intentionally left blank.*



# Chapter 2: Requirements and Considerations

Before deploying your Unitrends Backup appliance, review the following requirements:

- "Network and web access requirements"
- "Minimum resource requirements" on page 9
- "Backup storage" on page 9
- "Additional considerations" on page 9
- "Limitations" on page 9
- "Licensing" on page 10

## Network and web access requirements

There are several addresses you should permit for all deployments. All of these ports are outgoing connections from the Unitrends appliance. We do not require incoming NAT of ports or exposing the unit to a public IP, only outgoing communication from a local source Unitrends appliance is needed.

**IMPORTANT!** Never expose the appliance Web UI or SSH connections to open external ports. Doing so may void your support agreement until the appliance can be secured properly. Never deploy the Unitrends appliance on a public IP. All incoming ports to a Unitrends appliance must be firewall protected. Privately operated hot backup copy targets should be deployed in such a way as to secure the VPN connection to only trusted source external IPs.

Additional ports must be open for connectivity to the Internet and for connectivity to any hot backup copy target. See the following for details:

**Note:** Unitrends does not officially support backup through firewalls. For details, see this KB article: [Backup fails through Router, DMZ, or Firewall.](#)

- "Connectivity between the appliance and the Internet"
- "Connectivity between the appliance and a hot backup copy target"

### Connectivity between the appliance and the Internet

Task	Port, Protocol, and Rule	Destination	Notes
Backup and backup copy operations	443/HTTPS Outbound from the Unitrends appliance	kaseyagroup-appliance-registry.jfrog.io	A secure docker container registry required to update backup and backup copy components.
Product	443/HTTPS	repo.unitrends.com	repo.unitrends.com is used

Task	Port, Protocol, and Rule	Destination	Notes
Updates	Outbound from the Unitrends appliance  22/SFTP Outbound from the Unitrends appliance	sftp.unitrends.com	by the Unitrends appliance to perform software updates.  sftp.unitrends.com is used to collect files related to active support tickets.
Remote Support	443/HTTPS Outbound from the Unitrends appliance	support-itivity.unitrends.com	Used for opening a remote tunnel to the Unitrends support team.
Proactive Monitoring	161/UDP Outbound from the Unitrends appliance 161/TCP Outbound from the Unitrends appliance 162/UDP Outbound from the Unitrends appliance 162/TCP Outbound from the Unitrends appliance	notifications.unitrends.com	Used for SNMP trap collection for all proactive monitoring.

### Connectivity between the appliance and a hot backup copy target

Task	Port, Protocol, and Rule	Destination	Notes
Backup copy to the Unitrends Cloud or your Unitrends target appliance.	The OpenVPN port provided by Unitrends <b>Or</b> The port number you have configured for the secure tunnel connection to the backup copy target appliance must be open Outbound for the TCP and UDP protocols. Port 443 must also be open Outbond for the UCP protocol.	For Unitrends Cloud, the public-facing IP address provided by Unitrends.  Target appliance hostname and	Used for copying data to the Unitrends Cloud or your Unitrends target appliance.

Task	Port, Protocol, and Rule	Destination	Notes
		IP	

## Minimum resource requirements

To meet the minimum criteria for successful deployment, the Unitrends Backup VM requires the following:

**Note:** These are the minimum resources required to deploy and begin using the Unitrends Backup appliance. As you add jobs and storage, be sure to monitor the system and add resources as needed over the lifetime of the appliance.

- A minimum of two virtual processors (vCPUs).
- A minimum of 8GB of RAM.
- 38.47GB of space for the VM's initial disk.
- At least 200GB of additional backup storage.

Azure VMs that meet the above requirements include: D2as\_v4, D2ds\_v4, D2s\_v3, and D2s\_v4.

## Backup storage

After you create the Unitrends Backup VM, you will attach disks to use for backup storage. An Azure disk has a maximum capacity of 4095GB, but you can attach multiple disks for additional storage. The total number of disks is limited by the Azure VM size. You then expand storage in the Unitrends Backup UI to create a single logical volume.

## Additional considerations

- A Unitrends Backup appliance can be used as either a backup appliance or a backup copy target. For details, see the [Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup](#).
- After deploying your Unitrends Backup appliance, you should perform all operations, including updates, from the UI, unless you are following a specific procedure described in Unitrends documentation. Running unsupported commands from the terminal can have undesirable results.
- By default, the password for the web UI root user of the Unitrends appliance is *unitrends1*. You will change this password during appliance setup, as described in "[Set up the appliance using the Quick Setup Wizard](#)" on page 27. (Changing this password has no impact on the OS root user password.)
- By default, appliance deduplication level is set to 1. For further information, see [Managing Appliances](#) in the Unitrends Backup and Recovery Series Administrator's Guide.

## Limitations

The following Unitrends Backup features are not currently supported within the Azure environment:

- Backups that are not agent-based application or file-level. (Host-level and image-level backups are not supported.) For details on installing the Unitrends agent, see [Unitrends agents](#) in the [Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup](#).
- The Windows agent push installation feature is not supported. Instead, install the Windows agent manually. For details, see [Installing the Windows agent](#) in the [Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup](#).
- The virtual machines you protect with Unitrends backups must be configured with private IPs only. Public IPs are not supported. (For the Unitrends Backup appliance VM, a public IP is used.)
- Bare metal recovery.
- Instant Recovery.
- Using a physical seed device to move data into or out of the Azure environment.
- Exporting a Unitrends Backup appliance to a host outside of the Azure environment.

## Licensing

You must register and license the appliance after deploying your Unitrends Backup appliance. You can use the software for free with a 30-day trial license, but after this period, you must purchase a license.

# Chapter 3: Deploying the Unitrends Backup VM

Once you have verified that all "Requirements and Considerations" on page 7 have been met, complete the following steps to deploy the Unitrends Backup appliance:

- Step 1:** "Download the Unitrends Backup VHD"
- Step 2:** "Create a storage account"
- Step 3:** "Create a storage container"
- Step 4:** "Create an image from the Unitrends VHD"
- Step 5:** "Create the Unitrends Backup virtual machine"
- Step 6:** "Set up the appliance using the Quick Setup Wizard"
- Step 7:** "Register and license the appliance"
- Step 8:** "Start protecting your environment"

## Step 1: Download the Unitrends Backup VHD

Download the Unitrends Backup VHD from the Unitrends Downloads page:

- 1 Go to <https://helpdesk.kaseya.com/hc/en-gb/articles/4407526882193-Unitrends-Downloads>.
- 2 Scroll down to Unitrends Backup Virtual Appliance Deployments.
- 3 Click the **.VHD** link in the Microsoft Azure row.

Unitrends Backup Virtual Appliance Deployments

For existing customers looking to redeploy an instance of Unitrends Backup, the following [installer downloads](#) are available (right-click and "Save As..."):

Environment	Applies To	Format
VMware vSphere	VMware 5.x - 8.0	.OVA
Microsoft Hyper-V	Windows Server 2012-2022 (Wizard Deployment)	.EXE
	Windows Server 2008 R2-2022	.VHD
Citrix XenServer	XenServer 6.5-7.x	.XVA
Nutanix AHV	Nutanix AHV 5.1-6.5	.VMDK
Amazon AWS	Deployments are available within the Amazon cloud	
Microsoft Azure	Microsoft Azure	.VHD <a href="#">Click here</a>

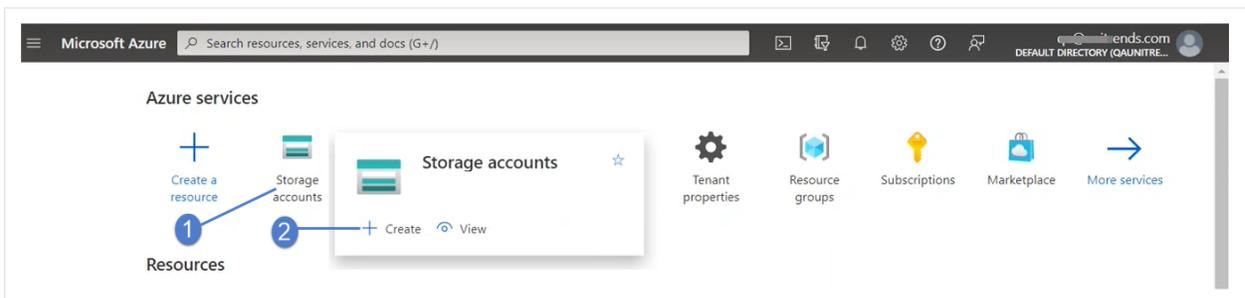
Ready to register and activate your Unitrends Backup? Follow the knowledge article [Registering a Unitrends Backup - Activating your Product - Licensing \(Internet or Air Gap\)](#) to apply for your permanent license.

*Note: Be sure to activate your Unitrends Backup before the 30-day trial expires to ensure there is no gap in your protection.*

## Step 2: Create a storage account

To create a storage account:

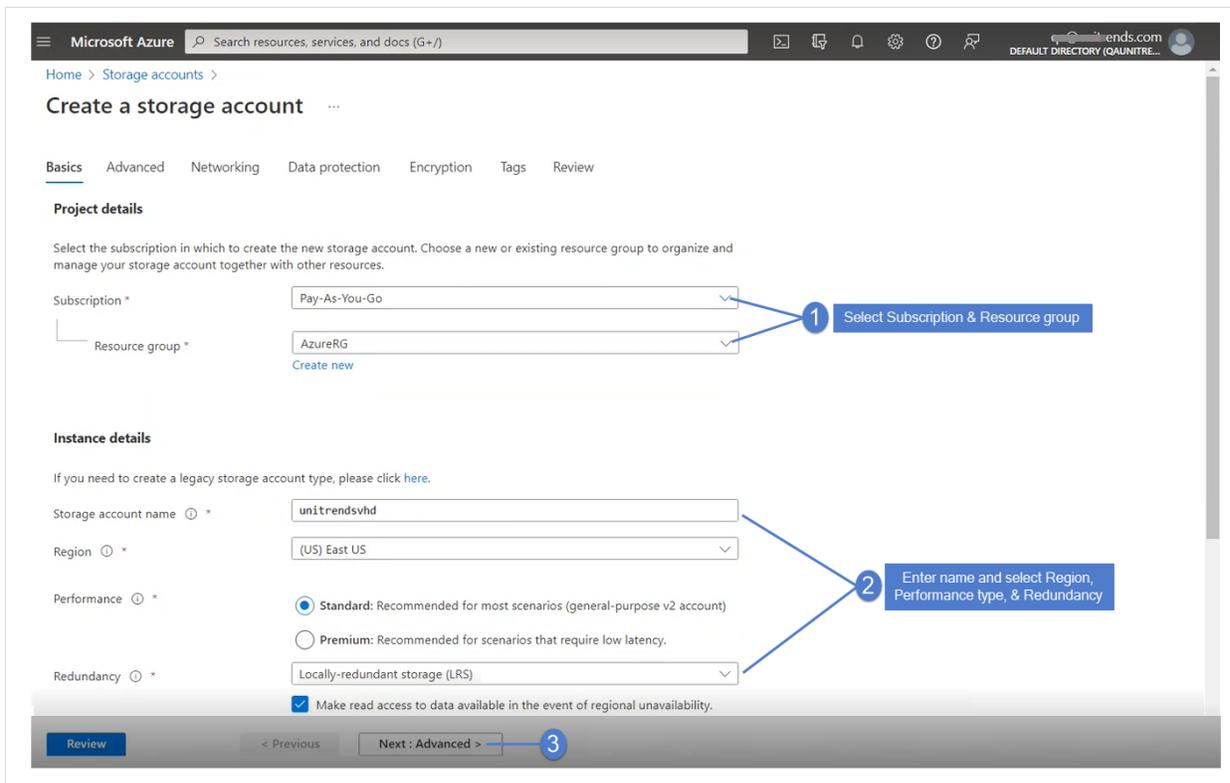
- 1 Open the Azure dashboard.
- 2 Click **Storage accounts** and select **+ Create**.



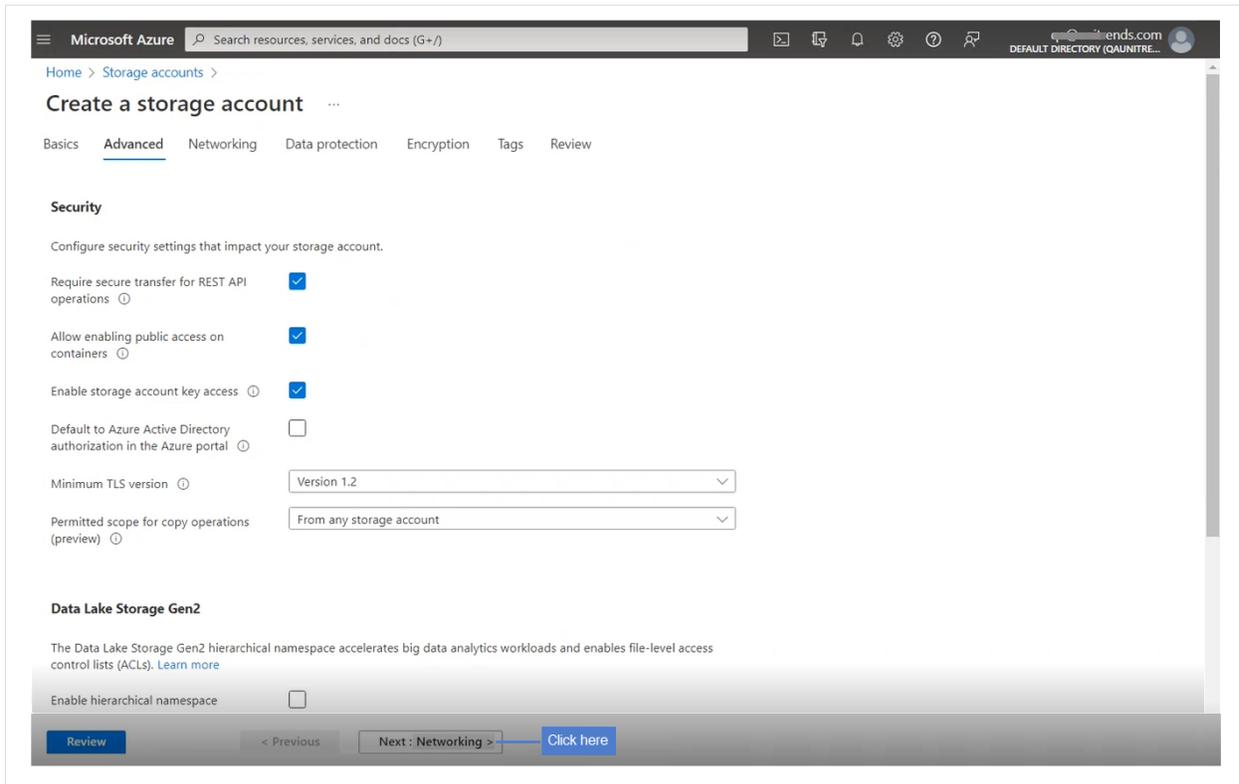
- 3 Enter the **Basics**:
  - In the Project details, select a Subscription type and Resource group (or create a new one).

Release 10.9 | July 2025

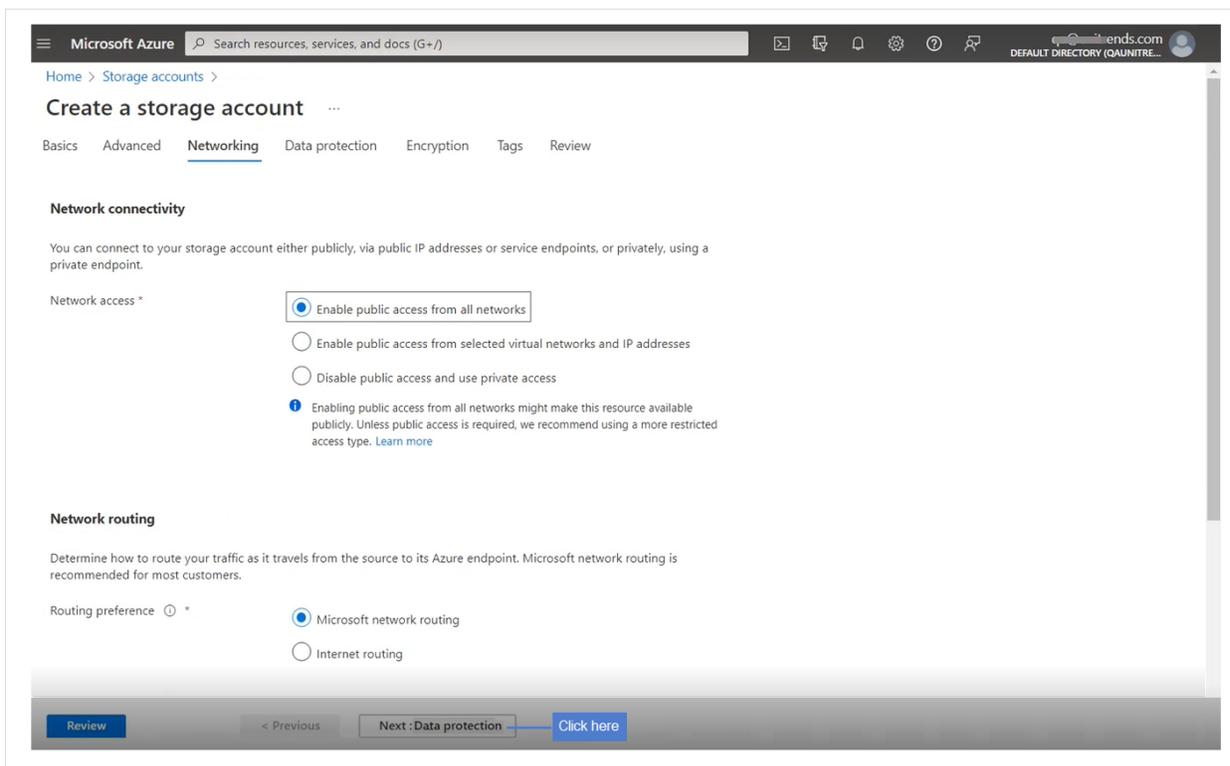
- In the Instance details, enter a name for the storage account and select a Region, Performance type, and Redundancy.
- Click **Next: Advanced**.



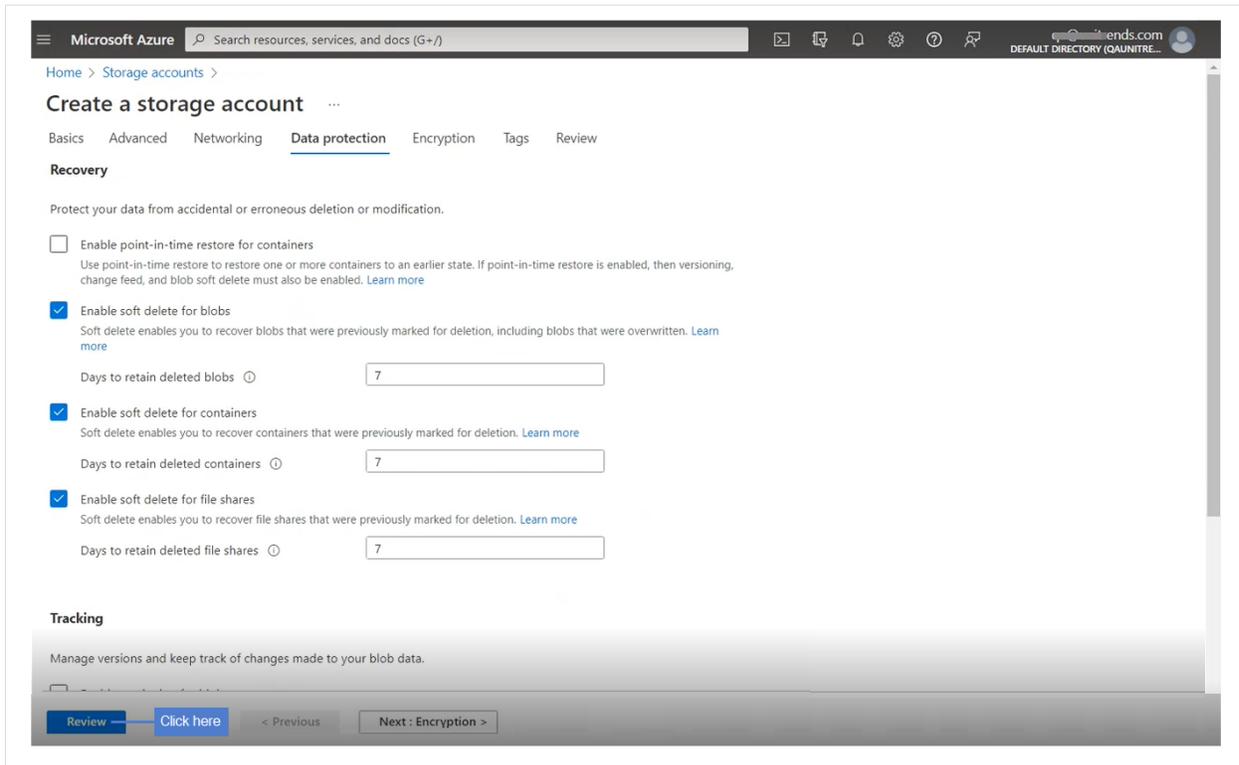
- 4 On the Advanced page, keep the default settings and click **Next: Networking**:



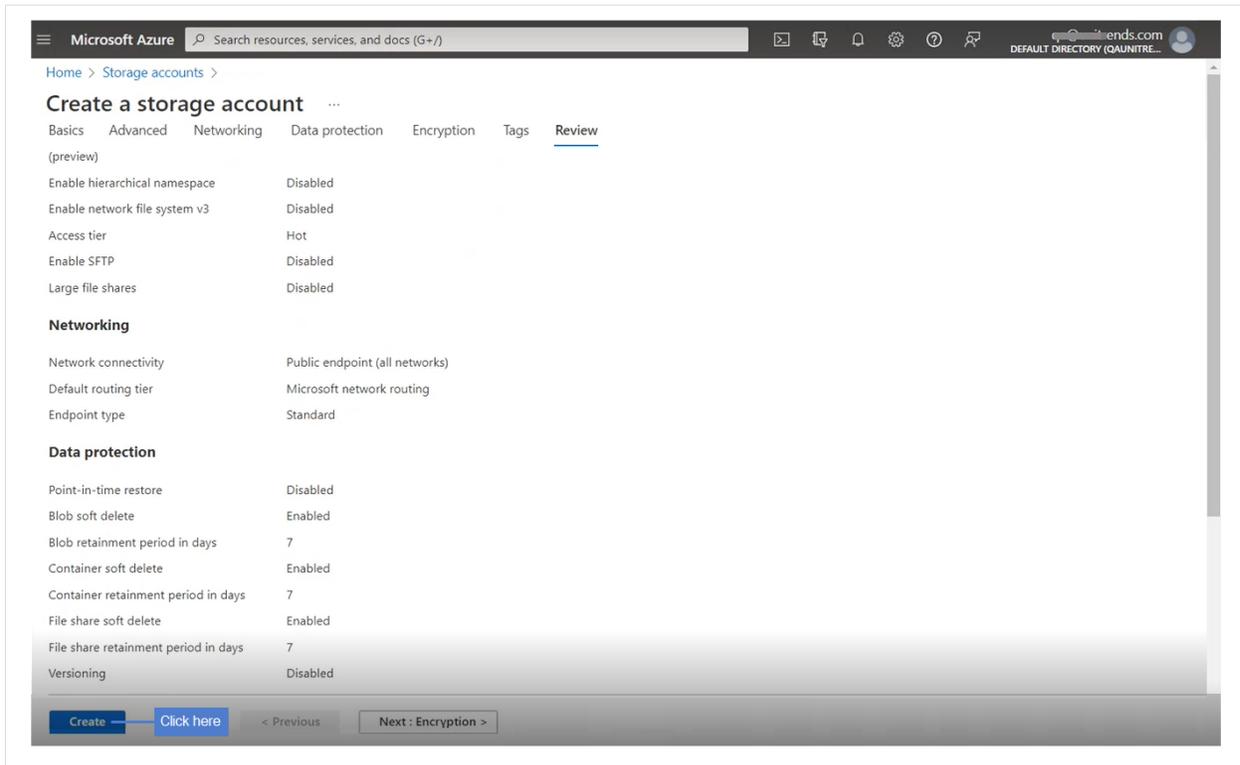
- 5 On the Networking page, keep the default settings and click **Next: Data Protection**:



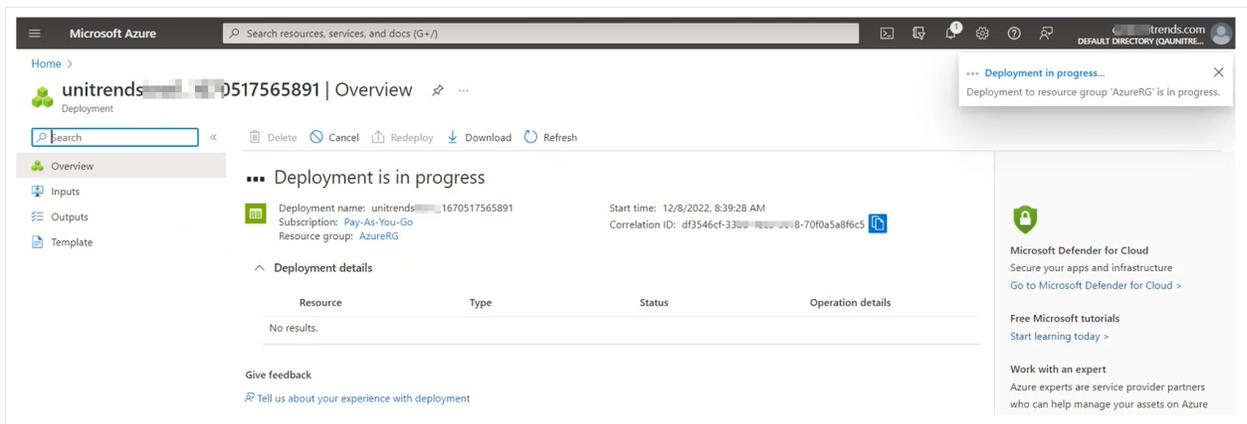
6 On the Data Protection page, keep the default settings and click **Review**:



7 On the Review page, click **Create** to create the storage account:



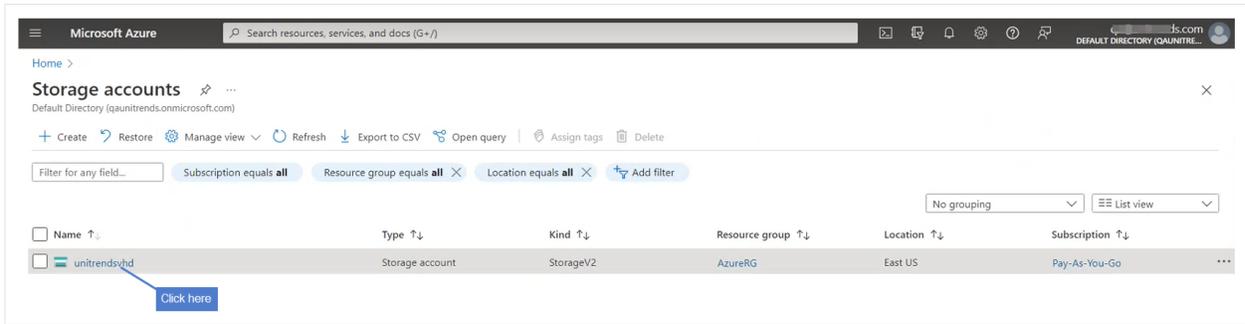
The storage account is created:



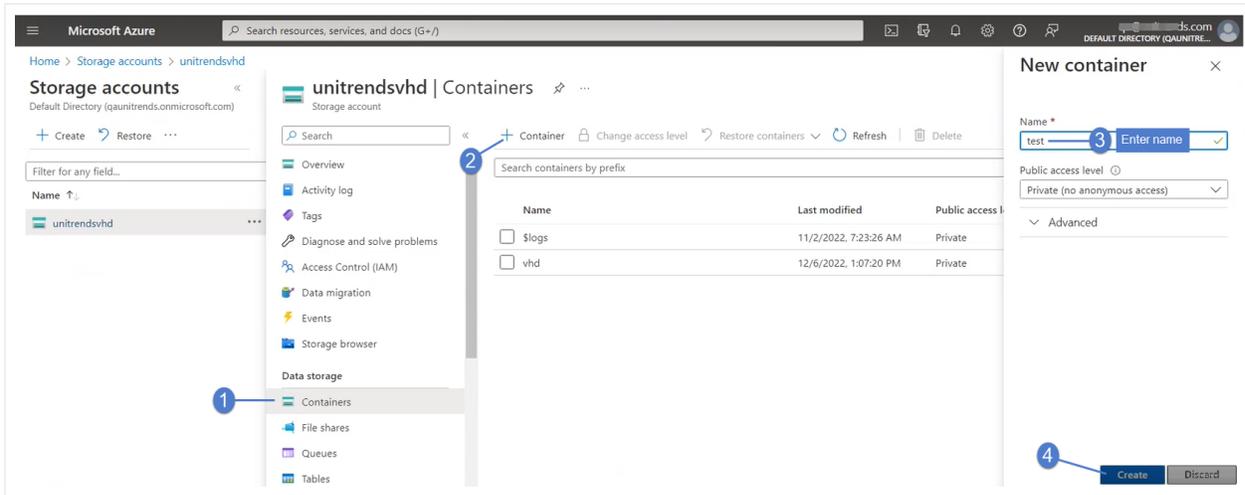
## Step 3: Create a storage container

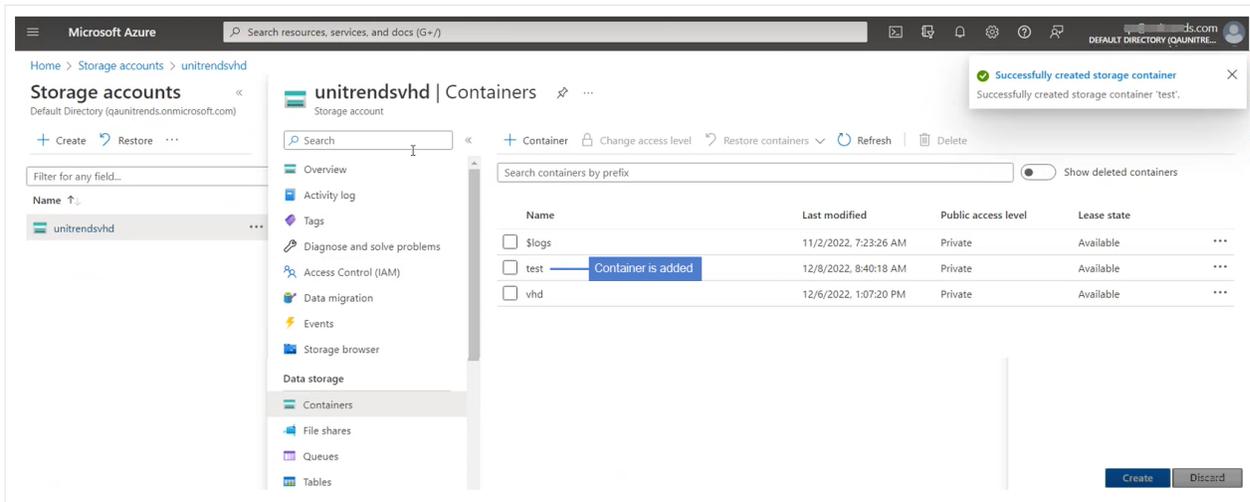
To create a storage container:

- 1 Go to **Home > Storage Accounts** and select the storage account you created above.



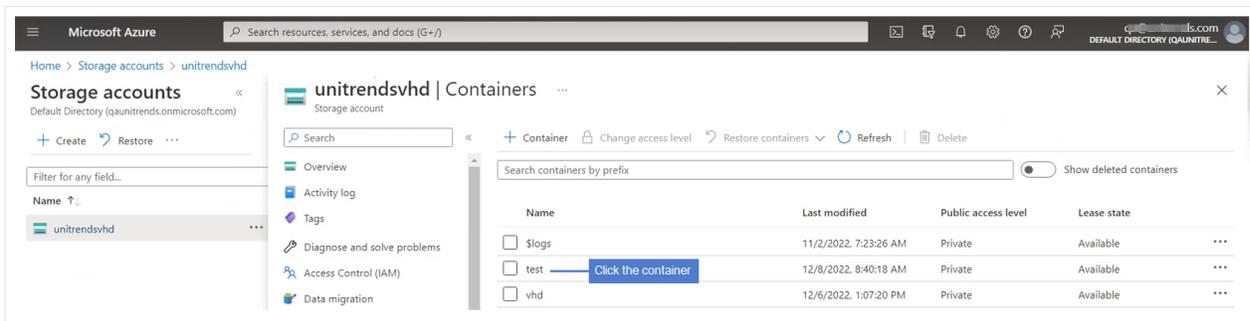
- 2 Click **Containers**.
- 3 Click **+**.
- 4 Enter a container Name.
- 5 Click **Create**.



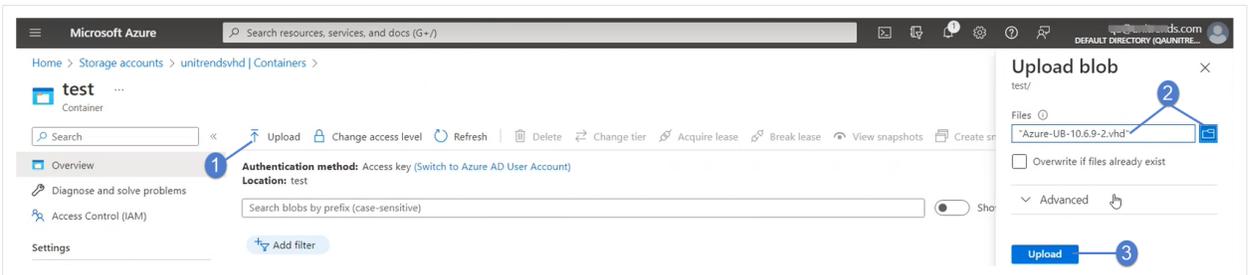


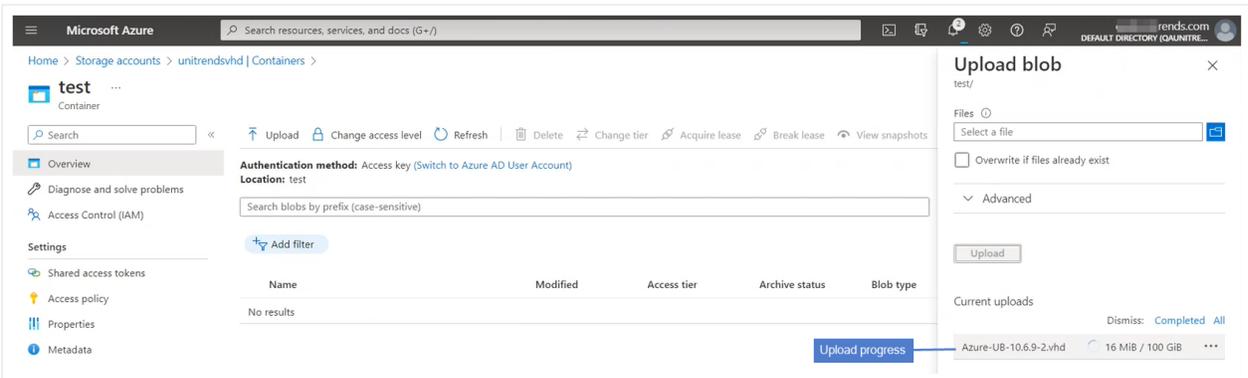
6 Use these steps to upload the Unitrends VHD to the new container:

- Click the new container.



- Click **Upload**.
- Browse to and select the VHD you downloaded in "[Step 1: Download the Unitrends Backup VHD](#)".
- Click **Upload**. The VHD is uploaded to the container. (The upload can take some time, depending on your network throughput.) Wait for the upload to complete before continuing with this procedure.

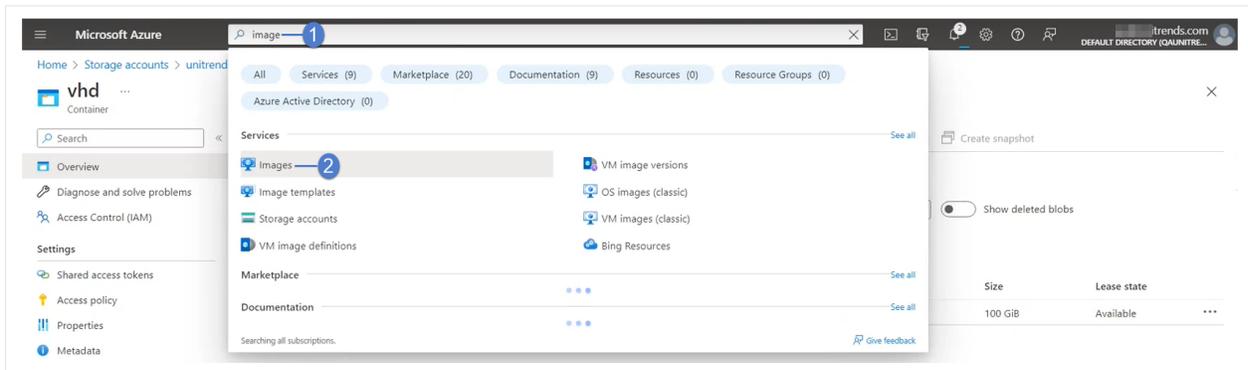




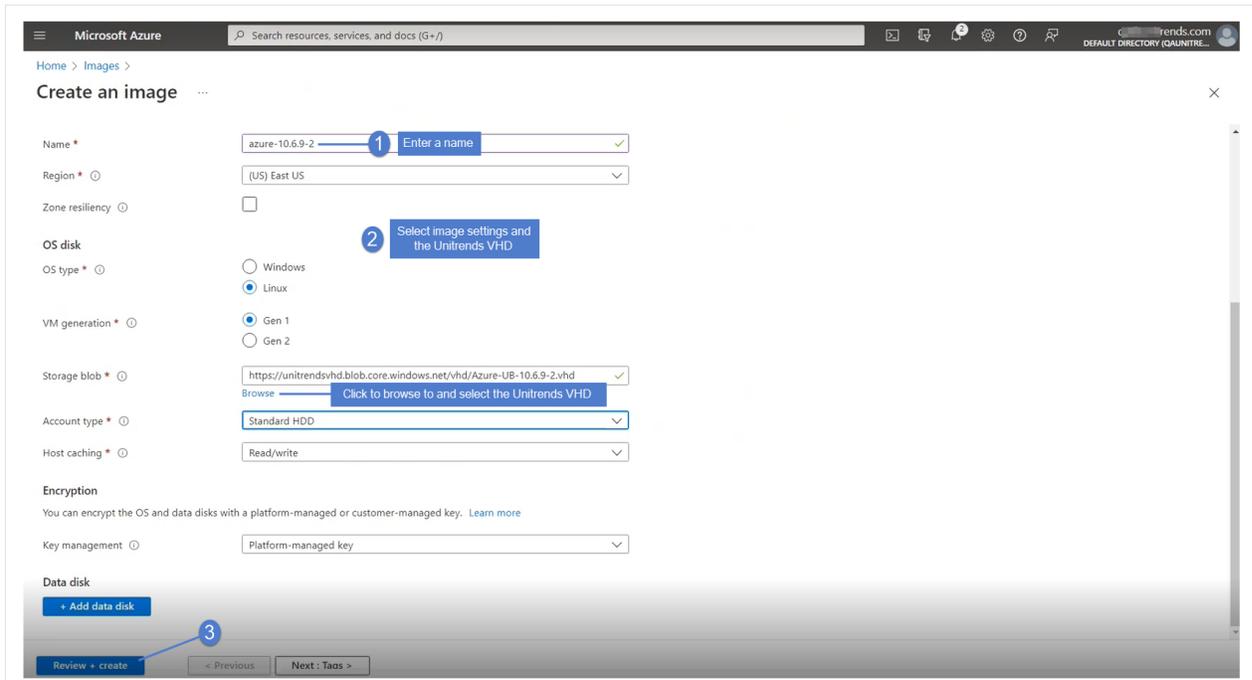
## Step 4: Create an image from the Unitrends VHD

To create an image from the Unitrends VHD:

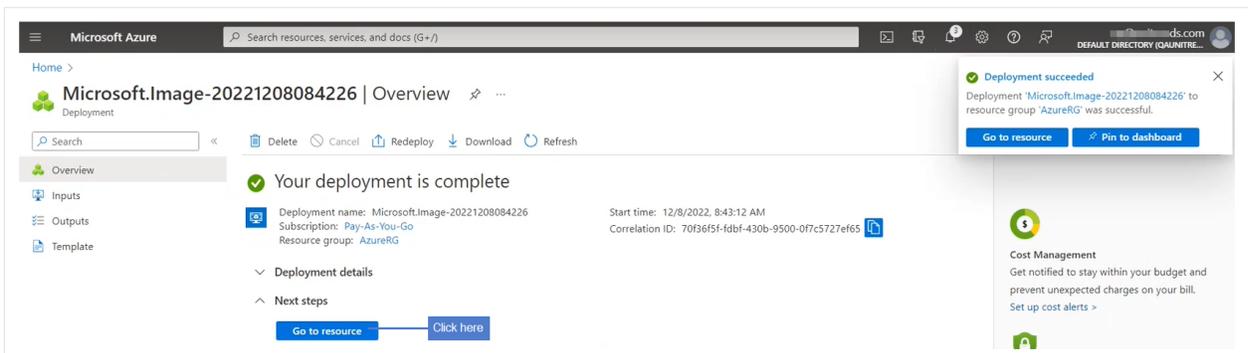
- 1 Search for *image* and select **Images**.



- 2 Enter a name for the image.
- 3 Select a region, **Linux** for OS type, **VM Gen 1**, **Standard HDD**, **read/write** host caching, and **Platform-managed key**.
- 4 For storage blob, browse to and select the Unitrends VHD.
- 5 Click **Review and Create**.



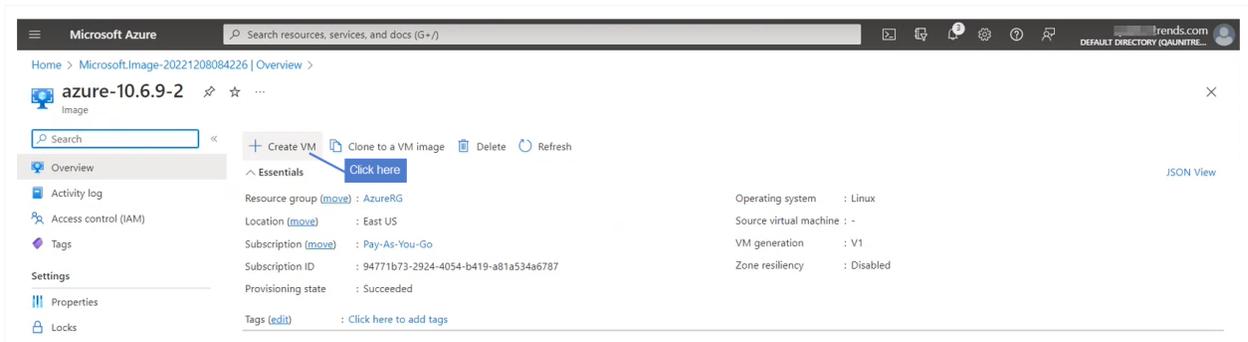
6 The image is created. Click **Go to Resource**.



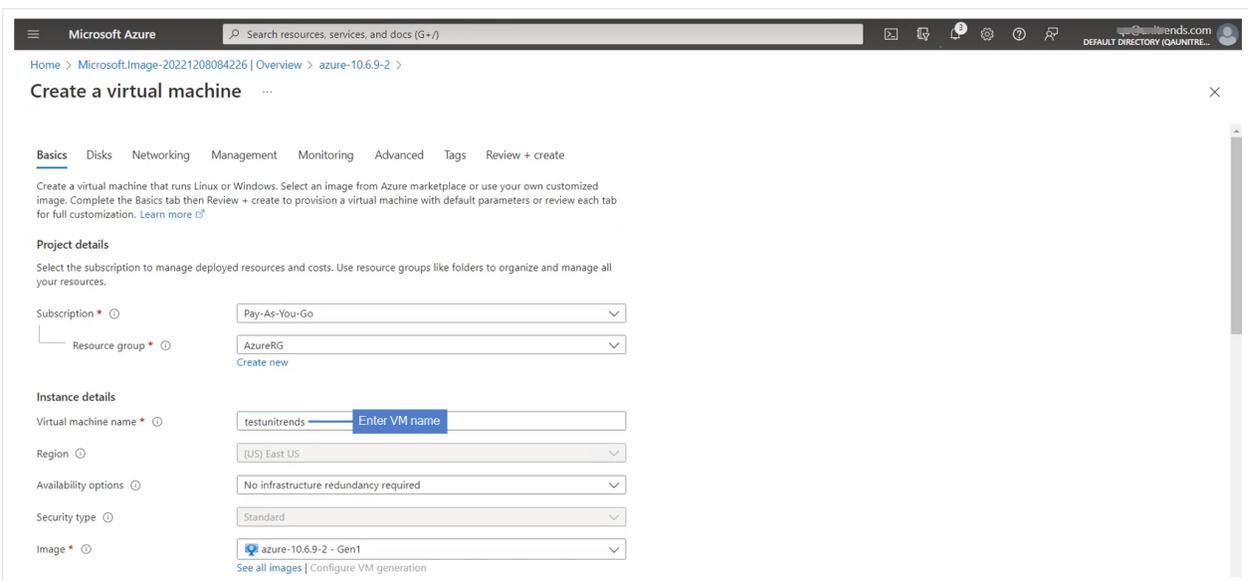
## Step 5: Create the Unitrends Backup virtual machine

To create the Unitrends Backup virtual machine:

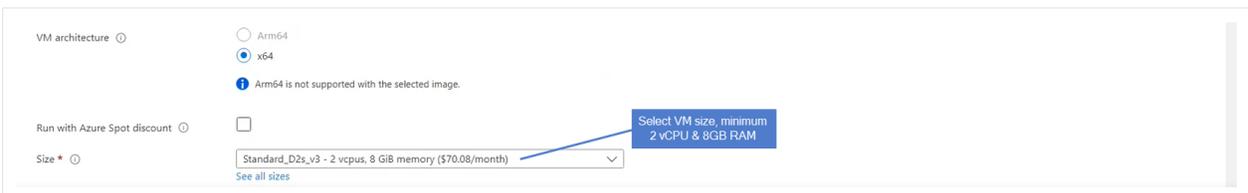
1 Click **Create VM**.



## 2 Enter a name for the VM.

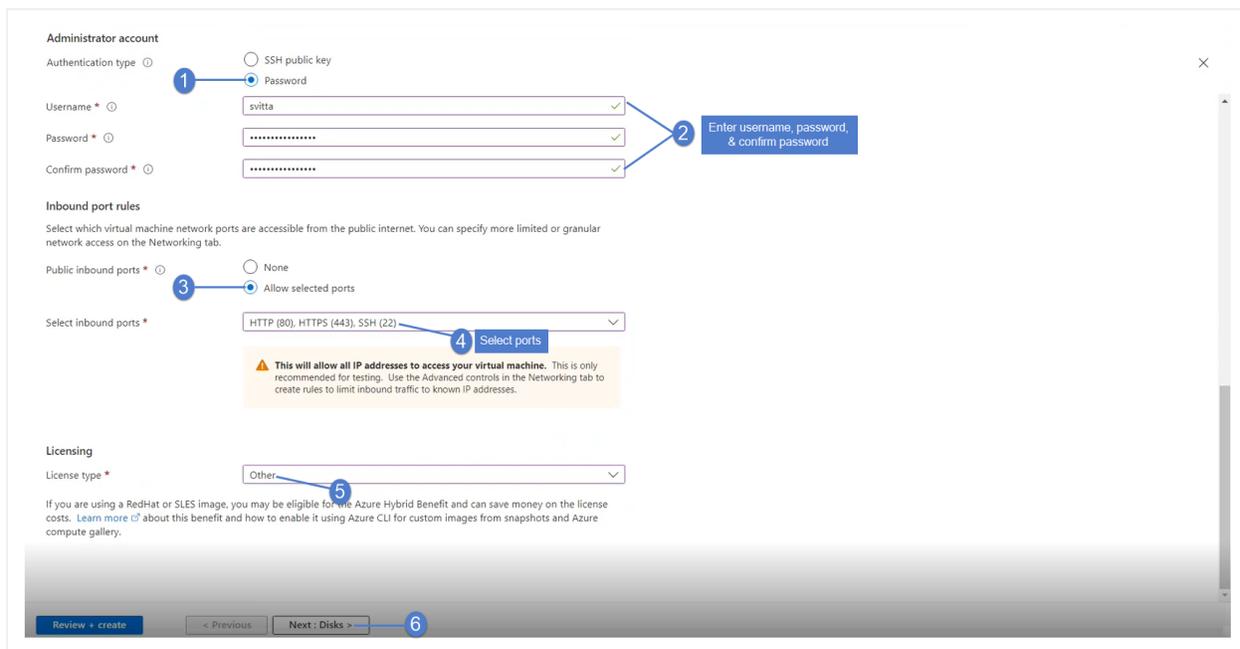


## 3 Select the VM size (minimum 2 vCPU and 8GB RAM).



- 4 Select **Password** as the authentication type. (SSH keys are not used.)
- 5 Enter a user name for the OS user account. (This account will not have superuser privileges.)
- 6 Enter and confirm a password for the OS user account.
- 7 Select **Allow selected ports** and these inbound ports: 80, 443, and 22.
- 8 Select **Other** for licensing type.

9 Click **Next: Disks**.



10 Click **Create and attach a new disk**.

11 Add a disk to use for backup storage (minimum 200GB). Click **OK**.

12 Click **Next: Networking**.

Microsoft Azure

Home > Microsoft.Image-20221208084226 | Overview > azure-10.6.9-2 >

## Create a virtual machine

Basics **Disks** Networking Management Monitoring Advanced Tags Review + create

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more](#)

### VM disk encryption

Azure disk storage encryption automatically encrypts your data stored on Azure managed disks (OS and data disks) at rest by default when persisting it to the cloud.

Encryption at host

Encryption at host is not registered for the selected subscription. [Learn more about enabling this feature](#)

### OS disk

OS disk type

Delete with VM

Key management

Enable Ultra Disk compatibility

Ultra disk is supported in Availability Zone(s) 1,2,3 for the selected VM size Standard\_D2s\_v3.

### Data disks for testunitrends

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching	Delete with VM

[Create and attach a new disk](#) [Attach an existing disk](#)

[Review + create](#) [Previous](#) [Next: Networking](#)

### Create a new disk

Create a new disk to store applications and data on your VM. Disk pricing varies based on factors including disk size, storage type, and number of transactions. [Learn more](#)

Name

Source type

Size  [Add disk, minimum 200GB](#)

Key management

Enable shared disk  Yes  No

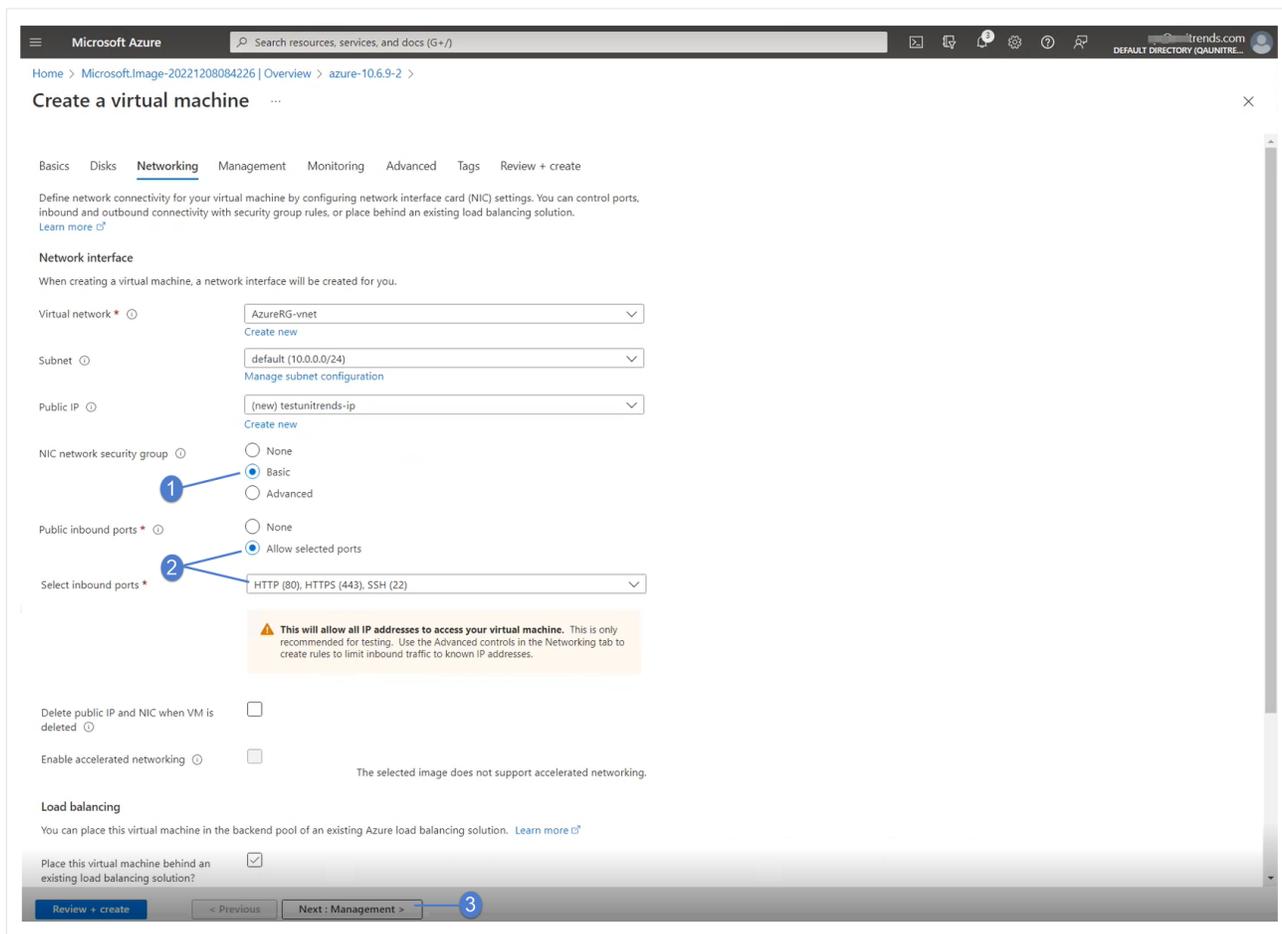
Delete disk with VM

[Disk](#)

- 13 In the NIC network security group, select **Basic**.
- 14 For Public inbound ports, select **Allow selected ports**.
- 15 Select these inbound ports: **80, 443, and 22**.

**Note:** If you are using custom rules, add the rules for outbound ports after you create the virtual machine.

- 16 Click **Next: Management**.

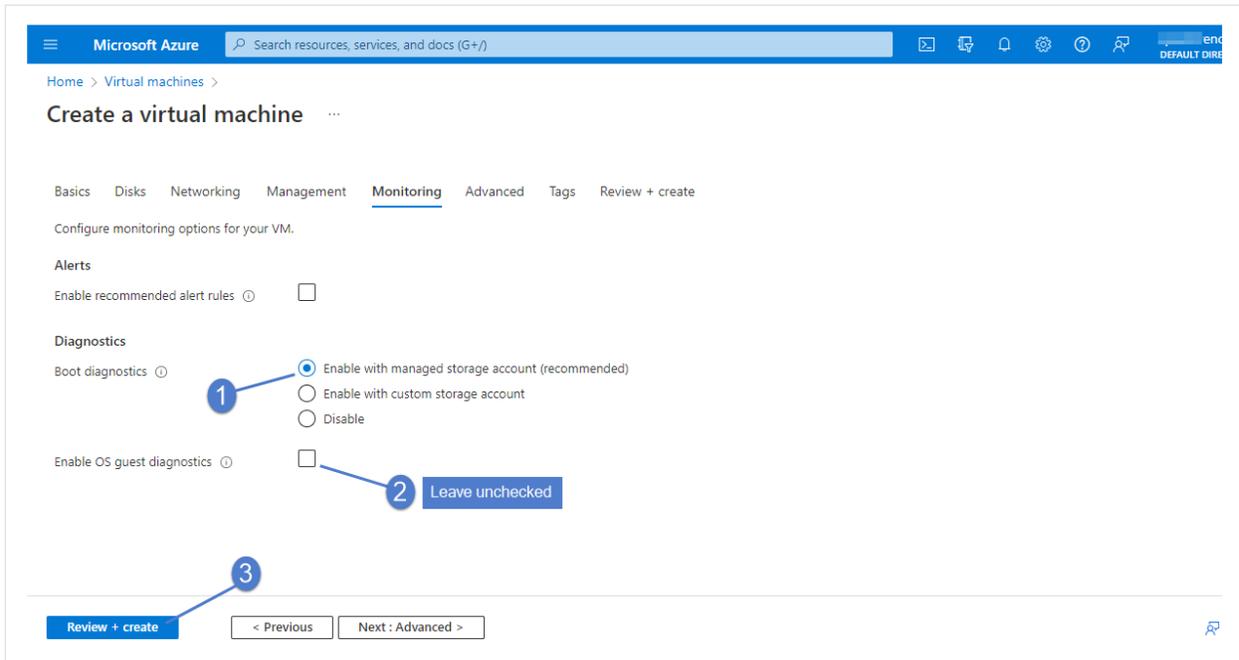


17 On the Management page, keep the default settings and click **Next: Monitoring**.

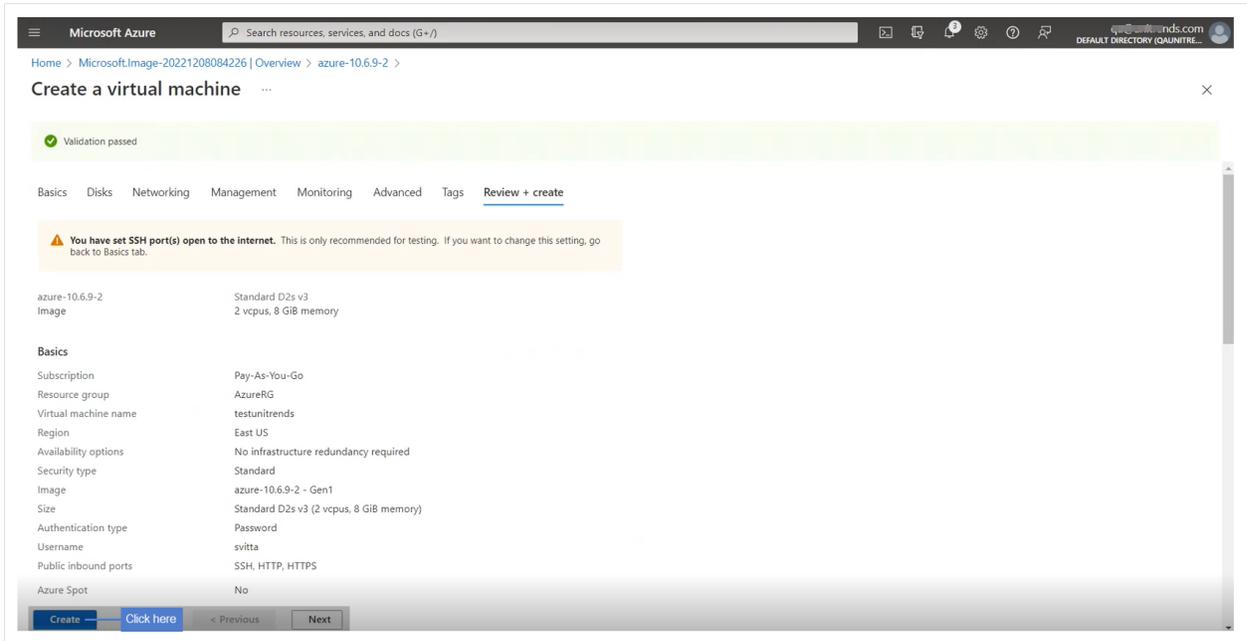
18 On the Monitoring page:

- For Boot diagnostics, select **Enable with managed storage account (recommended)**.
- For Enable OS guest diagnostics, leave the box unchecked (do NOT enable guest OS diagnostics).

19 Click **Review + Create**.



20 Click **Create**. The VM is deployed.



21 After the VM is deployed:

- If you are using custom firewall rules, ensure that the outbound rules (in **VM Settings > Networking**) for ports and addresses meet the "Network and web access requirements" on page 7.

- If you opt to use inbound firewall rules for 443 and SSH, secure them to trusted static IPs only.
- Restart the virtual machine.

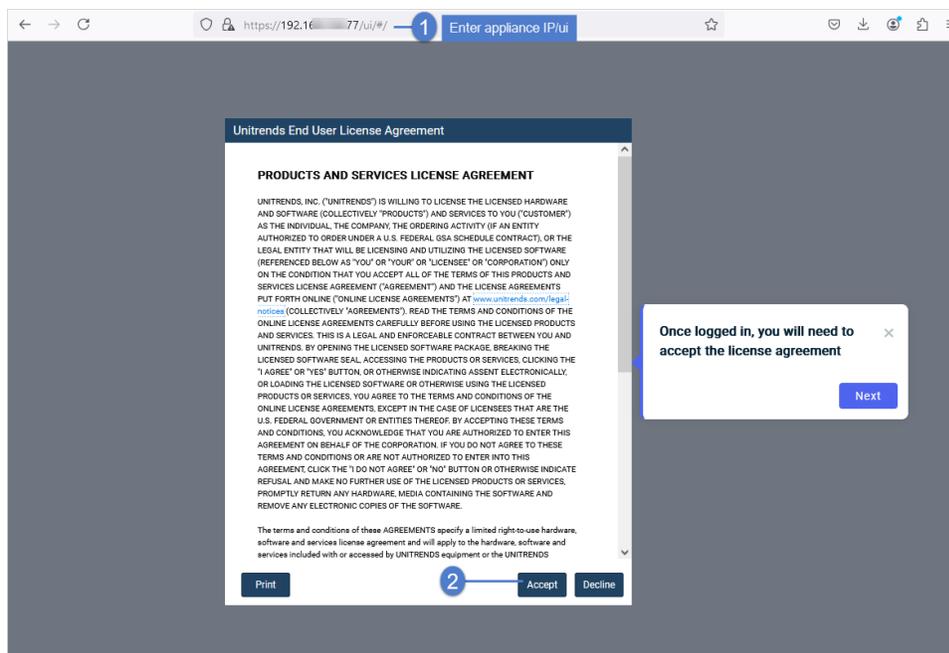
## Step 6: Set up the appliance using the Quick Setup Wizard

After Azure indicates the VM is running, you can access the appliance UI from any machine on the same network by opening a Chrome or Firefox browser and entering the appliance's IP address followed by `/ui/`. The Quick Setup Wizard launches when you access the UI for the first time.

### To set up the appliance

Use this procedure to set up the appliance:

- 1 Open a browser and connect to your appliance by entering: **`https://<applianceIP>/ui`**. For example: **`https://10.10.10.1/ui`**.
- 2 Click **Accept** to accept the license agreement.



- 3 Set the appliance date and time by doing one of the following, then click **Next**:
  - Select a **Timezone**. If needed, modify the appliance **Date** and **Time**.OR
  - Check the **Use an NTP Server** box to sync to an NTP server. (Optional) Enter your preferred NTP server address.

**UNITRENDS**

Date & Time    Host Name & Password    Email

Crazy-committed to helping you play IT safe.

Enter a date and time for your appliance

Date:  

Time:

Time Zone:

Use an NTP Server

NTP Server Addresses:  

0.centos.pool.ntp.org

1.centos.pool.ntp.org

- 4 Enter a **Host Name**, a **Domain**, and a new **UI Password** for the appliance. Confirm the UI password by entering it again in the field to the right. Click **Next**.

#### Notes:

- The hostname can contain only alphanumeric characters, dashes, and underscores.
- The appliance has a UI root user and an OS root user. These are separate accounts. Changing the password of one root user account does NOT change the password of the other root user account. The UI root user is used to log in to the appliance UI. The OS root user is used to log in to the appliance console or for command line access.
- Because you have already set the OS password, this field is disabled in the Quick Setup Wizard.
- Passwords cannot contain the word *Unitrend* (case insensitive).
- All appliances are deployed with these default UI credentials: user *root*, password *unitrends1*. For appliance security, you must change this password in the Quick Setup Wizard. For increased security, ensure that the UI password you enter is different than the OS user password.
- After you finish the deployment procedures in this guide, you can set up additional UI users for the appliance at any time. For details, see *Users and roles* in the [Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup, Appliance settings](#) topic.

**UNITRENDS**

Date & Time    Host Name & Password    Email

Enter hostname, domain (optional) and appliance UI password

1

Host Name: [ ] ?

Domain: [ ] ?

UI Password: [ ] ?    Confirm UI password: [ ] 2

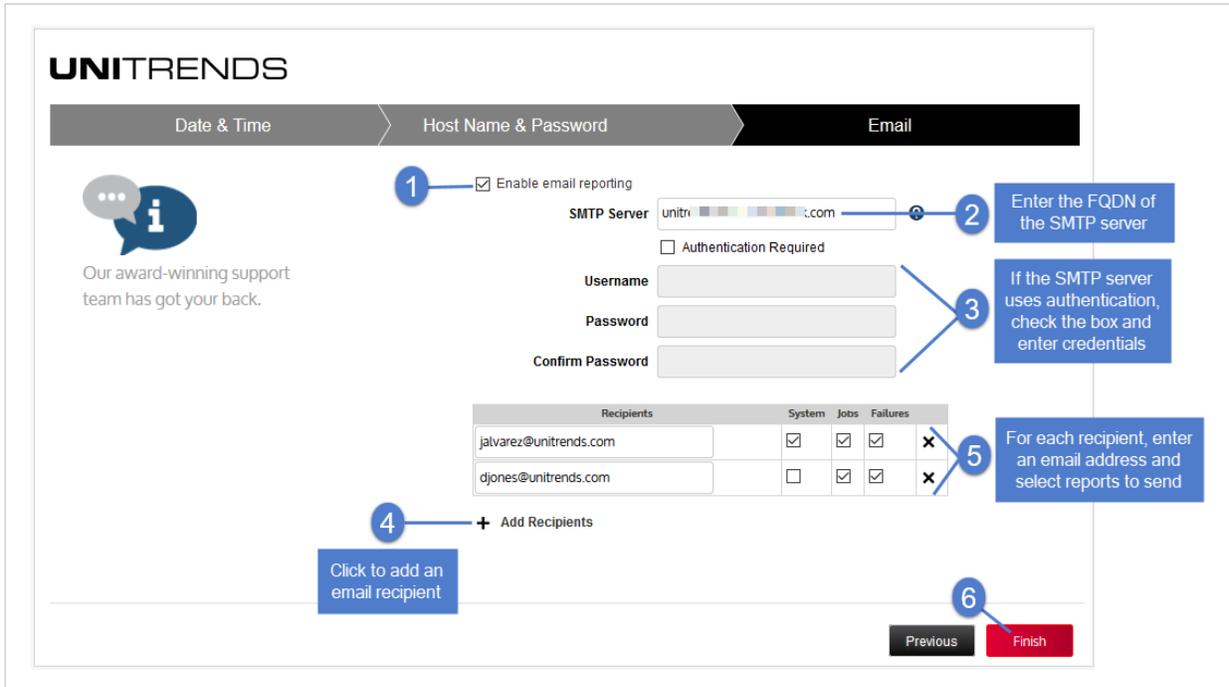
OS Password: [ ] ?    Confirm Password: [ ]

We're obsessed with your success.

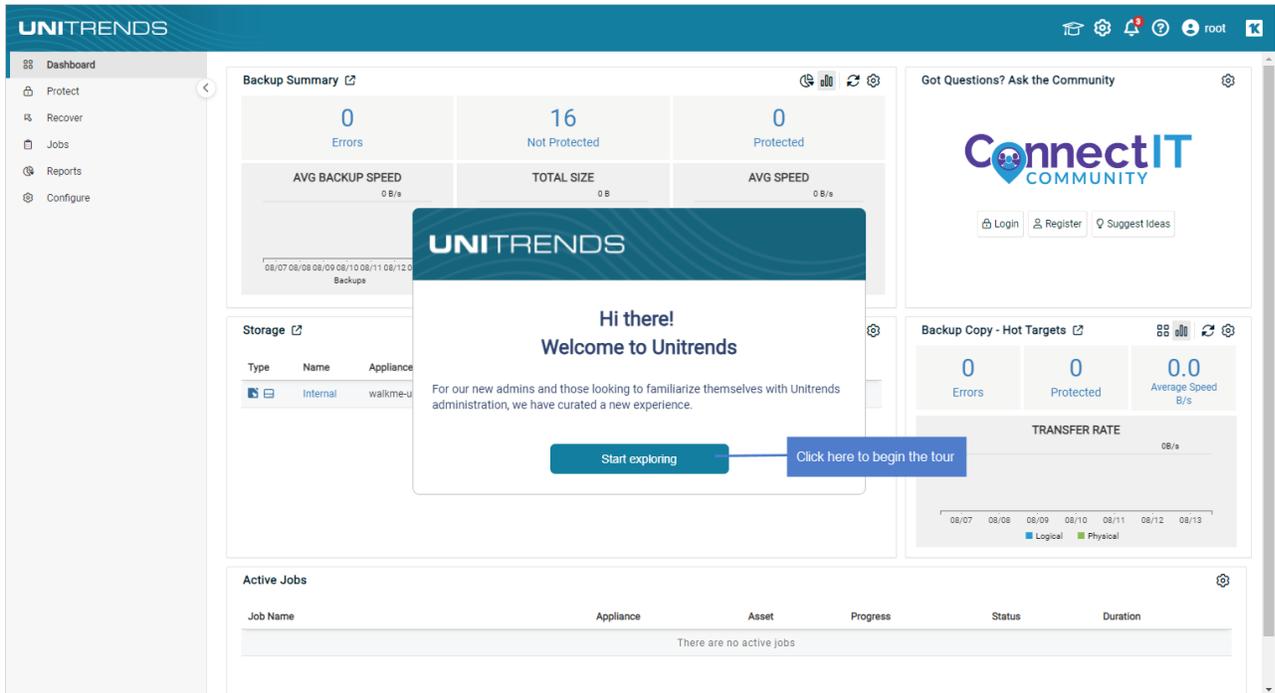
3

Previous    Next

- 5 (Optional) To enable email from the appliance, check **Enable email reporting** and enter the following:
  - The fully qualified domain name of the **SMTP server**.
  - (If needed) If the SMTP server requires authentication, select **Authentication required** and enter a **Username** and **Password**.
  - Click **+ Add Recipients** to add an email recipient. Enter an email address in the **Recipient** field and select one or more of the **System**, **Jobs**, and **Failures** options to specify which reports the appliance will send to the recipient. Repeat as needed to add more recipients.
- 6 Click **Finish**.



You are logged in to the Unitrends appliance and the Welcome to Unitrends dialog displays. Click **Start exploring** to view the interactive product tour. Leave the appliance UI open as you will use it later in this procedure.



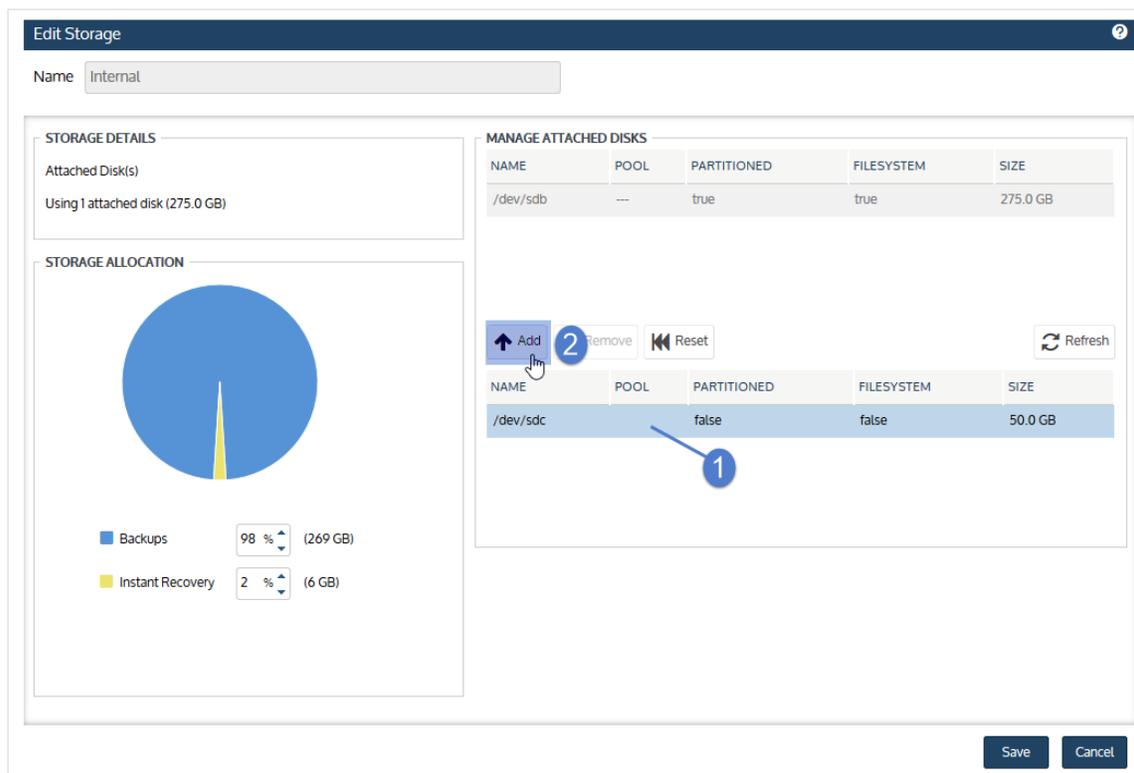
- 7 (Optional) Attach one or more disks to your Unitrends Backup VM. The number of disks you can attach is limited by the size of the Azure VM you purchased.

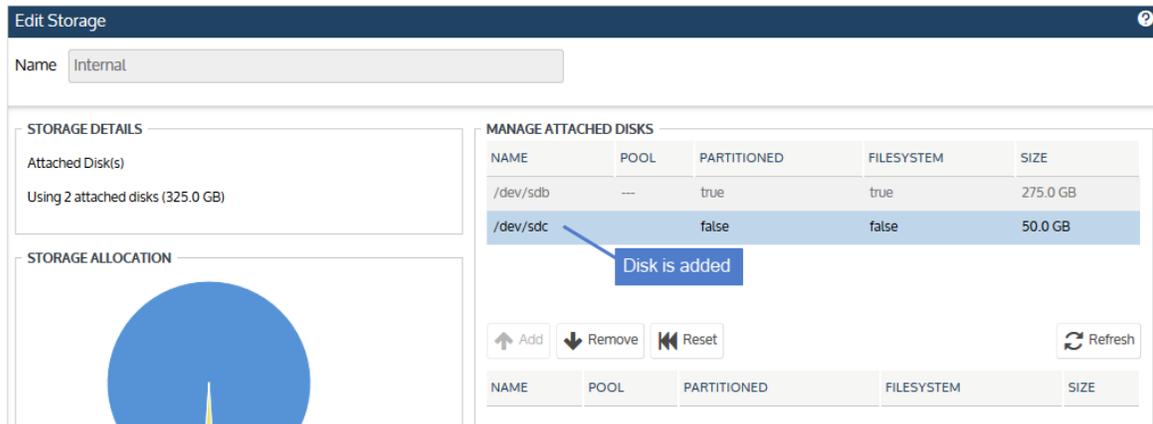
**Note:** For further information on attaching disks in Azure, see Microsoft KB article [How to attach a data disk to a Linux VM in the Azure portal.](#)

- 8 Expand backup storage in the Unitrends Backup UI:

**Note:** Once a disk has been added, it cannot be removed.

- On the **Configure > Appliances** page, select your appliance.
- Click the **Storage** tab.
- Select the *Internal* storage and click **Edit**.
- In the Manage Attached Disks area:
  - To add an attached disk, select the desired disk from the list of available attached disks and click **Add**.
  - To remove an attached disk, select it from the list of available attached disks and click **Remove**.
  - Clicking **Reset** reverts all disk settings to the original settings.
  - To refresh the list of available disks, click **Refresh**.





- Adjust the storage allocation for Backups and IR as desired.
- Click **Save**.  
On the **Configure > Appliances** page, the status initially displays as *Pending*. When the disk is finished attaching, the status converts to *Active* and the storage can be used.
- If desired, repeat this procedure to add another disk.

Be sure to register your appliance within 30 days, as described below.

## Step 7: Register and license the appliance

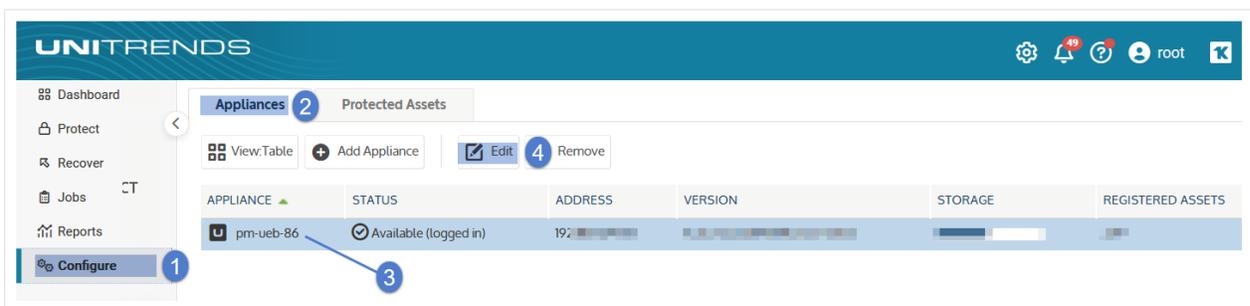
Your appliance is now configured and you can begin using it to protect your environment. For details, see the [Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup](#).

You must register and license the appliance within 30 days of deploying Unitrends Backup.

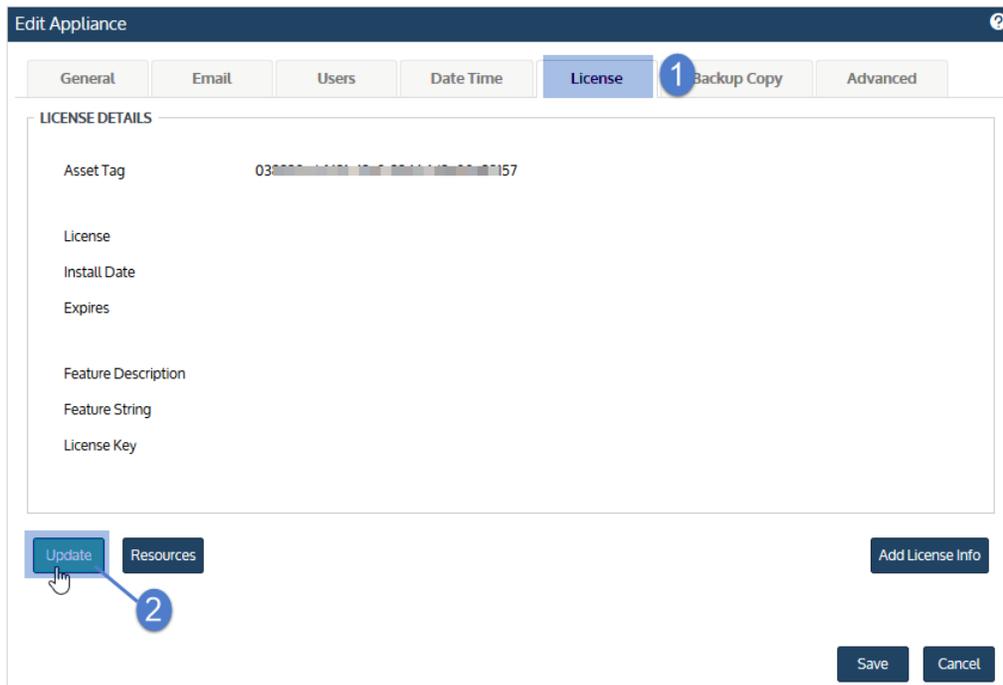
Each appliance requires an activation code and license key. Use the procedures below to register and license the appliance:

### To register a Unitrends Backup appliance

- 1 On the **Configure > Appliances** page, select the appliance and click **Edit**.

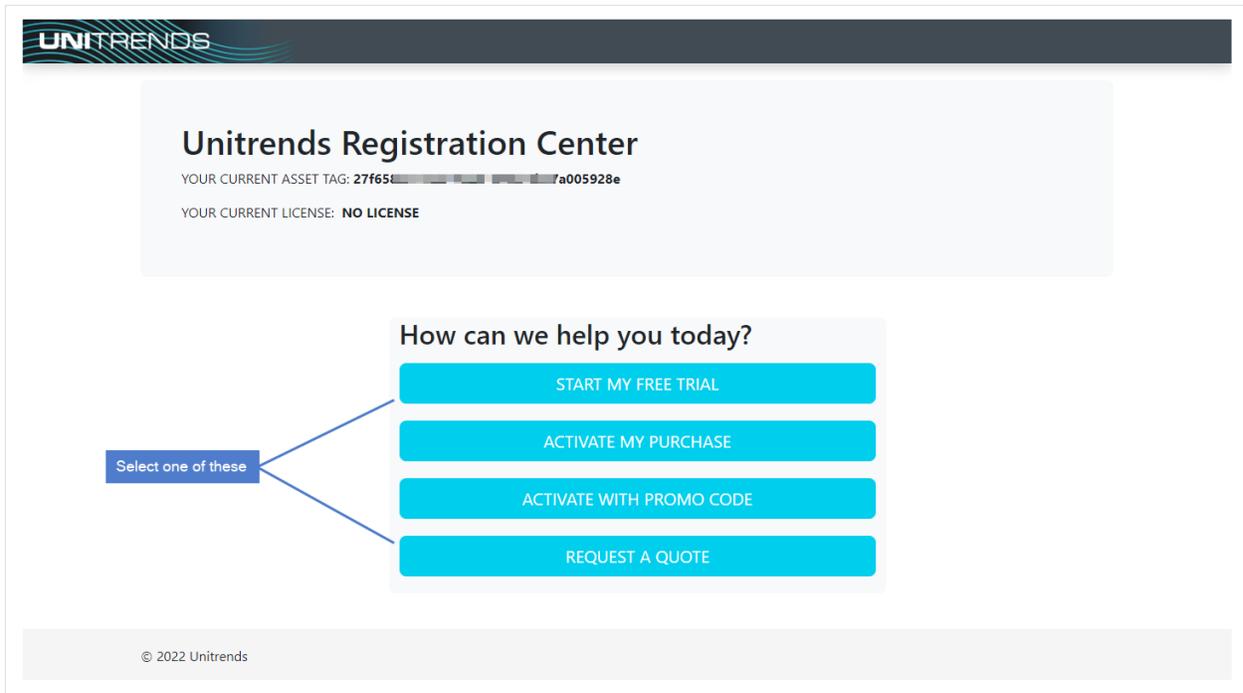


- 2 Select the **License** tab and click **Update**. The Registration Center displays.



- 3 Select one of the following:

Selection	Description
Start my free trial	Submit this form to start your free 30-day trial.
Activate my purchase	Enter your email address and activation code. Your license key will be emailed to the address you enter here.
Activate with promo code	Enter your promotional code to register your product and receive your license key.
Request a quote	Request a license quote.



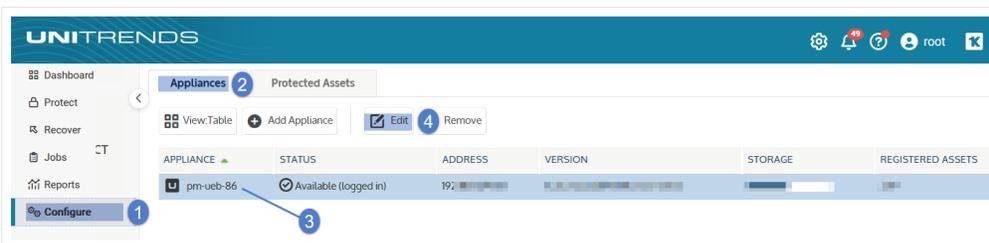
- 4 Complete and submit the applicable form.

Once you have purchased a license, Unitrends sends an email containing license details. Use the next procedure to apply this license information to the appliance.

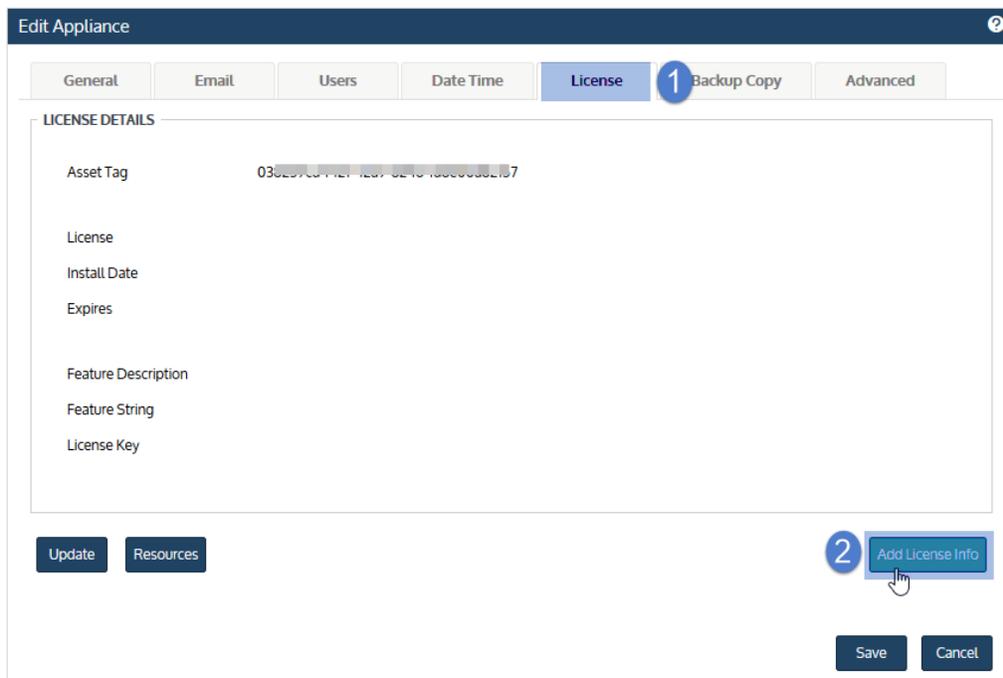
### To license a Unitrends Backup appliance

Use these steps to enter license information you have received from Unitrends.

- 1 On the **Configure > Appliances** page, select the appliance and click **Edit**.



- 2 Select the **License** tab and click **Add License Info**.



3 Enter the License Key, Expiration Date, and Feature String.

4 Click **Save**. The license is applied.

