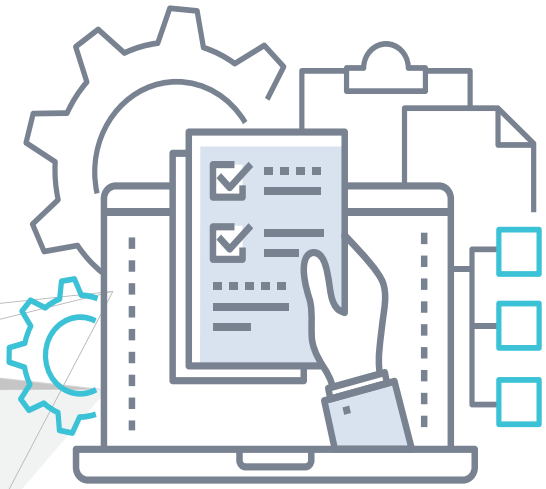
UNITRENDS

Deployment Guide for Unitrends Backup on Hyper-V

Release 10.8 | Document Date 08202024

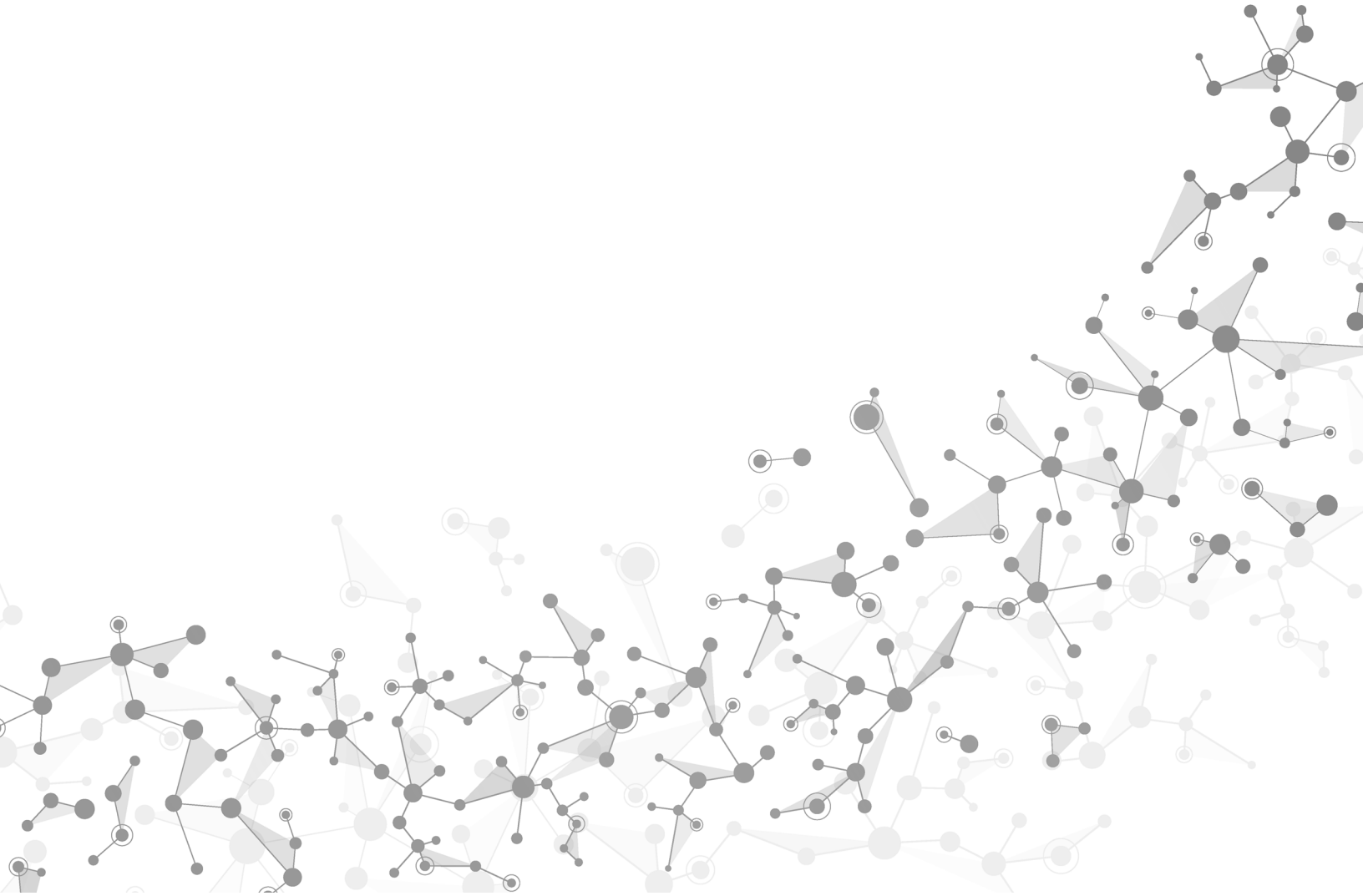


Copyright

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

Contents

This page is intentionally left blank.



Chapter 1: Introduction

Thank you for choosing the Unitrends Backup virtual appliance. You are minutes away from protecting your environment.

With Unitrends Backup deployments, the appliance's initial disk stores no unique data or backups. Storing this data on different disks or external storage arrays enables you to reattach the storage to a different Unitrends Backup appliance, so you can retain your original appliance's settings and backup data if you need to deploy a new virtual appliance.

This guide includes instructions for deploying using new storage and for deploying using storage that contains backup data from another virtual appliance. The process is similar for both deployment types, and the applicable sections cover any variations.

Note: Attaching backup storage that contains backups from another Unitrends Backup appliance is supported only if the original appliance is running the same operating system as the newly deployed appliance. Appliances deployed with version 10.3.6 or higher run CentOS 7. Appliances deployed with older versions run CentOS 6.

Deployment consists of creating the Unitrends Backup virtual machine (VM), attaching backup storage, and configuring appliance settings. Terms used in this guide are defined in the following table:

Term	Definition
Added disk	VHD(X) virtual disk storage created by running the Unitrends Backup EXE installer or by using the Hyper-V host. A VHD(X) can be created from direct attached storage (DAS) that is internal to the Hyper-V host, or from external SAN or NAS storage that is connected to the Hyper-V host over the iSCSI, NFS, or CIFS protocol. Also called *attached disk storage*.
Appliance	The Unitrends Backup system that backs up and recovers data. Consists of the Unitrends Backup VM, Unitrends software, attached storage, and additional configuration settings.
EXE installer	Unitrends Windows executable installer used to deploy the Unitrends Backup VM on your Hyper-V host. Use to deploy to these Hyper-V Server and Windows Server versions: 2022, 2019, 2016, 2012 R2, and 2012.
External storage	SAN or NAS storage that is connected directly to the Unitrends Backup VM over the iSCSI, CIFS, or NFS protocol.
Host	Hyper-V server that houses the Unitrends Backup VM. Also called a *hypervisor*.

Term	Definition
Initial backup storage	Storage you attach to the Unitrends Backup VM that is used to store appliance configuration settings and backups. You attach this storage after deploying the Unitrends Backup VM, but before you configure the appliance using the Quick Setup Wizard. The initial backup storage must be 200GB - 64TB in size.
Initial disk	100GB disk used to create the Unitrends Backup VM. While installing the EXE or VHD, you select a volume on the Hyper-V host that the installer uses to create this disk.
VHD file	Unitrends VHD file used to deploy the Unitrends Backup VM on your Hyper-V host. Use to deploy to these Hyper-V Server and Windows Server versions: • 2022 Server Core • 2019 Server Core • 2016 Server Core • 2012 R2 Server Core • 2008 R2 SP1 • 2008 R2 Server Core with SP1 or higher
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	Virtual machine created either by running the Unitrends Backup EXE installer or by deploying the Unitrends Backup VHD file.

Chapter 2: Requirements and Considerations

Before deploying your Unitrends Backup appliance, verify the following requirements have been met:

Hypervisor requirements and considerations

Unitrends recommends running your appliance and the VMs it protects on different hosts to avoid losing your VMs and their backups if one of the hosts fails.

You can deploy Unitrends Backup on a Windows server with the Hyper-V role enabled or on a dedicated Hyper-V server. Depending on the server type, you deploy by using a Windows EXE installer or a VHD file. See the tables below to determine which method to use for your server.

Verify the following requirements for the hypervisor on which you are deploying the Unitrends Backup VM:

- To deploy on a Windows server, enable the Hyper-V role. Make sure the server is running one of the following supported operating systems and service pack levels:

Windows Server	Deployment method
Windows Server 2022 (Nano Server installations are not supported)	EXE
Windows Server 2019 (Nano Server installations are not supported)	EXE
Windows Server 2016 (Nano Server installations are not supported)	EXE
Windows Server 2012 R2	EXE
Windows Server 2012	EXE
Windows 2012 R2 Server Core*	VHD
Windows Server 2008 R2 SP1	VHD
Windows 2008 R2 Server Core*, with SP1 or higher	VHD

*For Server Core, you must install the Hyper-V management tools and sub-features separately by running the PowerShell `Install-WindowsFeature` command with the `-IncludeManagementTools` and `-IncludeAllSubFeature` parameters. After installing, restart the server. For details on using this command, see the Microsoft article Install-WindowsFeature.

- To deploy on a Hyper-V server, make sure the server is running one of the following supported operating systems and service pack levels:

  Note: Hyper-V Server 2022 will be supported in an upcoming release.

Hyper-V Server	Deployment method
Hyper-V Server 2022 (Nano Server installations are not supported)	EXE
Hyper-V Server 2019 (Nano Server installations are not supported)	EXE
Hyper-V Server 2016 (Nano Server installations are not supported)	EXE
Hyper-V Server 2012	EXE
Hyper-V Server 2012 Core*	VHD
Hyper-V Server 2012 R2	EXE
Hyper-V Server 2012 R2 Core*	VHD
Hyper-V Server 2008 R2 SP1	VHD

*Server Core – Hyper-V management tools and sub-features are required for deployment. If needed, install the Hyper-V management tools and sub-features by running the PowerShell `Install-WindowsFeature` command with the `-IncludeManagementTools` and `-IncludeAllSubFeature` parameters. After installing, restart the server. For details on using this command, see the Microsoft article Install-WindowsFeature.

- To deploy by using the EXE installer:
  - You must download the EXE directly to the server on which you will deploy the Unitrends Backup VM.
  - The Hyper-V server where you run the EXE installer must have both .NET Framework 3.5 and 4 installed. For details, see the following Microsoft documents:
    - Installing the .NET Framework 3.5
    - Microsoft .NET Framework 4

Network 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.

Network requirements vary by whether DHCP is available in your environment.

DHCP is available

If DHCP is available in your environment, review these requirements and considerations before you deploy the appliance VM:

- If your environment goes offline for an extended period of time, your appliance may be assigned a new IP address from the DHCP server. This may cause a temporary loss of backup and recovery functionality. If this occurs, see How to resolve recovery issues related to appliance IP address changes for instructions on how to proceed.
- The eno1 adapter is, by default, configured for DHCP.
- DHCP cannot be a configured for more than one network adapter at any given time.
- A network adapter configured for DHCP cannot be managed via the appliance user interface (UI) unless you intend to assign it a static IP address.
- Unitrends appliances intended for use as backup copy targets must be assigned static IP addresses.

DHCP is not available

If DHCP is not available in your environment, or if you intend to use this appliance as a backup copy target, you must configure a static IP address for the appliance. Initially, the Unitrends Backup VM is created with the IP address 10.10.10.1 and the subnet mask 255.255.255.0. If this IP is currently being used in your environment, disable it until you bring the Unitrends Backup VM online and assign it a new IP address. During deployment, you must configure the following settings:

- An IP address and subnet. The IP address and the subnet enable communication between the appliance and other machines on your network.
- A gateway. A gateway enables communication between the appliance and machines on different subnets.
- Appliance DNS settings, required for the following:
  - To connect the appliance to the Internet.
  - To add assets using only their hostnames (rather than by fully qualified domain names).
  - To update your appliance from the user interface (UI).
  - To access the Unitrends Community forums from the UI.

Note: You can obtain the above information from your network administrator.

Port requirements

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

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 Updates	443/HTTPS Outbound from the Unitrends appliance 22/SFTP Outbound from the Unitrends appliance	repo.unitrends.com sftp.unitrends.com	repo.unitrends.com is used 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	notifications.unitrends.com	Used for SNMP trap collection for all proactive monitoring.

Task	Port, Protocol, and Rule	Destination	Notes
	162/UDP Outbound from the Unitrends appliance 162/TCP Outbound from the Unitrends appliance		

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 **Or** 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 IP	Used for copying data to the Unitrends Cloud or your Unitrends target appliance.

Web access

Once you have configured network settings, you can access the appliance UI by entering its IP address in a Firefox or Chrome browser. (Internet Explorer is not supported.)

Virtual machine resource requirements

Before deploying, verify that your host has sufficient resources to create the Unitrends Backup VM. If minimum required resources are not available, deployment may fail. The following resources are required to deploy the Unitrends Backup VM:

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 (CPUs).
- A minimum of 8GB of RAM.

- 100GB of space for the VM's initial disk.
- At least 200GB of backup storage.

Hyper-V 2022/2019/2016 requirements

This release supports host-level protection of VMs that reside on Windows Server 2022/2019/2016 and Hyper-V Server 2022/2019/2016 platforms. The Nano Server installation option is not supported.

Host-level protection is supported for VMs that meet the requirements below. For VMs that do not meet these requirements, install the Unitrends agent on the VM and run asset-level backups.

Hyper-V 2022/2019/2016 VM requirements:

- If the VM configuration is 6.2 or higher, the Hyper-V host must be running Windows agent version 10.0 or higher.

  Notes:

  - Starting with VM configuration 6.2, Microsoft implemented a binary-based configuration format (VMCX). On Windows Server 2022, 2019, and 2016, VMs are created by default with this VMCX configuration. VMCX requires new backup and recovery methods that are available in Unitrends release 10.0 and later.
  - Additional VM configuration version checking is used to support the VMCX format. A new full backup is required in these cases: the VM's configuration version is not present in the last backup, or the VM's configuration version has changed since the last backup. In these cases, the appliance cannot run an incremental until a full backup runs and:
    - If you attempt an on-demand incremental, the appliance promotes the backup to a full.
    - If the next job is a scheduled incremental, the job fails due to the configuration change. After this failure, the appliance promotes the next scheduled run to a full. Once this full succeeds, subsequent incrementals run as scheduled. (If you upgrade a VM's configuration version, you can opt to run an on-demand full, rather than letting the appliance fail then promote the next incrementals.)

- The VM cannot be configured with shared VHDX disks.
- The VM cannot be configured with pass-through disks.
- The VM cannot be configured in a VHDS cluster or in a VHD Set.
- The VM cannot be configured as a shielded VM.
- The VM cannot be configured in a Hyper-V container.

Additional Hyper-V requirements apply. For details, see Hyper-V virtual machines in the Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup.

Chapter 3: Determining your Storage Strategy

Before deploying your Unitrends Backup appliance, you must determine the strategy to use for all backup storage. It is important to plan your approach carefully because you cannot change this initial configuration. The following backup storage options are available:

- Added disk: VHD(X) disks created by using the Hyper-V host or by running the EXE installer. These disks can use direct attached storage (DAS, internal to the hypervisor) or external SAN or NAS storage that is connected to the hypervisor. Unitrends recommends using added disk storage.
- External storage:
  - A SAN LUN connected directly to the Unitrends Backup VM over the iSCSI protocol.
  - A NAS share connected directly to the Unitrends Backup VM over the CIFS or NFS protocol.

Although you cannot change the initial configuration, you can add more storage to your appliance as your storage needs change. If you choose to use added disk storage, Unitrends recommends adding virtual disks to the Unitrends Backup VM by using the hypervisor and expanding the initial backup storage to include them. If you choose to use a SAN or NAS directly attached to the Unitrends Backup VM, expanding the initial backup storage is not supported. Instead, you can add LUNs or shares as separate storage areas.

How Unitrends Backup storage works

An initial disk of approximately 100GB is used to deploy the Unitrends Backup VM. You must also add a minimum of 200GB as the initial backup storage. You cannot complete deployment without adding the initial backup storage because this storage contains the appliance's unique data and is used to store backups.

Storing the appliance's unique data separately from the initial disk enables you to reattach the backup storage to a new Unitrends Backup VM to recover the original appliance's settings and backups.

Storage recommendations

Consider the following recommendations when determining your storage approach.

WARNING!	Unitrends strongly recommends that all Unitrends Backup storage is either direct attached storage (DAS, internal to the hypervisor) or resides on one external storage array. If you configure storage across multiple storage arrays and one becomes unavailable, all backup data ends up corrupted, resulting in total data loss.

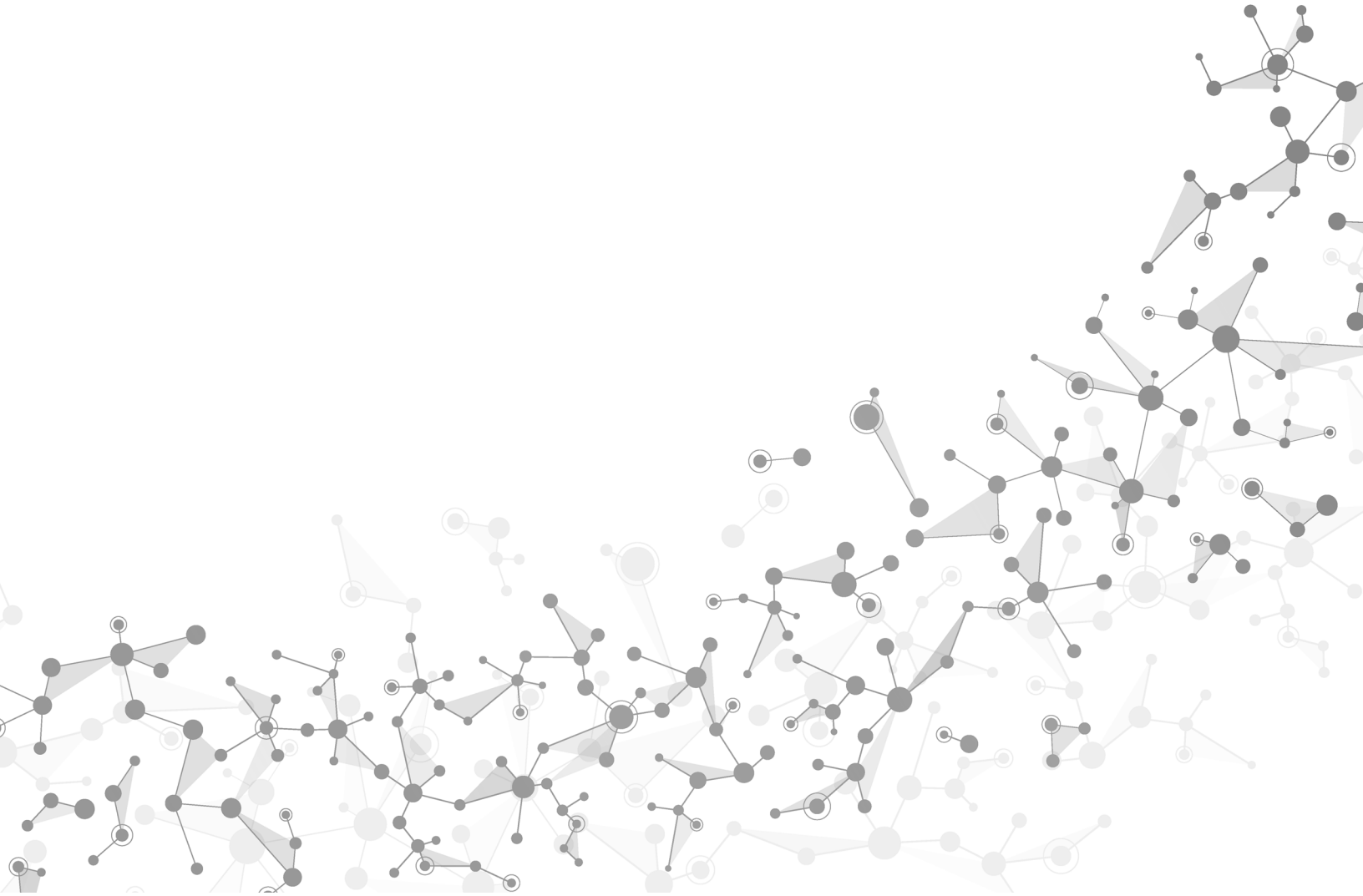
Unitrends Backup Storage Component	Recommendations
All	These recommendations apply to all Unitrends Backup storage (initial disk, initial backup storage, and additional backup storage): • Unitrends strongly recommends using hypervisor-certified storage arrays on Hyper-V's hardware certified list for deploying Unitrends Backup appliances. • Once you have selected a type of backup storage, Unitrends recommends using the same type of storage to add more backup storage in the future. • Do not use Storage Migration. Storage must remain in a fixed location. • Unitrends recommends using DAS, internal to the hypervisor, or to leverage SAN or NAS storage that you expose to the hypervisor. – You can create VHD(X)s on storage internal to the hypervisor (DAS). – You can expose a SAN or NAS to the hypervisor and use the hypervisor to create a volume from this storage. You can then select this volume to create VHD(X)s. – For optimal performance and scalability, add VHD(X) disks to SCSI controllers. • To use external SAN or NAS storage that is directly attached to the Unitrends Backup VM, follow these recommendations: Note: Unitrends does not recommend attaching external storage directly to the Unitrends Backup VM. If you do choose to connect external storage to the Unitrends Backup VM directly over network protocols (CIFS, NFS, or iSCSI), make sure to use a supported vendor from the list in Supported external storage vendors for use with Unitrends Backup appliances. – The shares or LUNs used by the Unitrends Backup VM should be dedicated to that Unitrends Backup VM and not shared by other virtual machines, applications, etc. – You can deploy the Unitrends Backup VM on a hypervisor in a cluster configuration and use shared storage. However, in this configuration, the Unitrends Backup VM should use a dedicated NAS share or SAN LUN. – For best performance with SAN storage, use a thick-provisioned LUN and a fixed size VHD (X).

Unitrends Backup Storage Component	Recommendations
Initial disk	You create the Unitrends Backup VM by either running the EXE installer or by deploying the VHD file. During deployment (described in "Step 3: Deploy the Unitrends Backup VM" on page 22), you make various selections within your hypervisor, including the volume and disk format used to create the initial disk for the Unitrends Backup VM. The initial disk can reside on DAS, internal to the hypervisor, or on external storage attached to the hypervisor. **Note:** If you intend to use external storage attached directly to the Unitrends Backup VM as the initial backup storage, be sure to use the same external storage array for both the initial disk and the initial backup storage.
Initial backup storage	You must add a minimum of 200GB of initial backup storage (see "Step 4: Attach backup storage (if needed)" on page 39). The following requirements and recommendations apply: • For disaster recovery, it is important to know which VHD(X), LUN, or share was used as the initial backup storage, so make sure to keep a record of your selection. • If you opt to use a LUN attached to the hypervisor for the Unitrends Backup VM's initial disk, do not attach that LUN directly to the Unitrends Backup VM to use as backup storage. Allocate a separate LUN (on the same array) to use as backup storage instead. • Additional configuration is required if you are using external CIFS or NFS storage attached to the Unitrends Backup VM as the initial backup storage. For details, see Special Configuration for NFS or CIFS with UB Initial Deployment Storage. How you set up the initial backup storage varies by storage type and deployment method: • If you are using added disk storage and deploying with the EXE, you add the initial storage disk right from the EXE installer. (See "Deploying with EXE" on page 22). • If you are using added disk storage and deploying with the VHD file, you must add a VHD(X) to the Unitrends Backup VM by using the Hyper-V host (see "Step 4: Attach backup storage (if needed)" on page 39). The appliance automatically uses the first VHD(X) disk that was added to the Unitrends Backup VM as the initial backup storage. • If you are using external SAN or NAS storage attached directly to the Unitrends Backup VM, you must expose the storage to the Unitrends Backup VM and add it as initial backup storage in the Unitrends Backup UI after completing the Quick Setup Wizard (see "Step 6: Add the initial backup storage device if using external storage directly attached to the Unitrends Backup VM" on page 48).

Unitrends Backup Storage Component	Recommendations
Additional backup storage	It is a best practice to add storage in the same way you created the initial backup storage. Unitrends recommends expanding storage for best performance, but you can add a separate storage area of roughly the same size if necessary. When you add attached disk or external NAS or SAN storage, the VHD(X)s, LUNs, or shares display in the Unitrends Backup UI as */dev/sdx/*. The *x* indicates alphabetically the order in which the storage was added. For example, the initial disk is always */dev/sda/*, the initial backup storage is */dev/sdb/*, the next would be */dev/sdc/*, and so forth. The following requirements apply to additional backup storage: • Your backup storage devices must be at least 200GB to enable deduplication or to use the device as a backup copy target. • As you add more storage, be sure to add resources to the Unitrends Backup VM, such as CPU and memory. • You can expand backup storage only across new disks. To expand the existing backup storage, you must add a new virtual disk. Expanding an existing VHD(X) or growing a SAN volume is not supported.
Examples of expanding storage	To add backup storage, Unitrends recommends expanding your initial backup storage to include the newly allocated space. Once storage is expanded in the Unitrends Backup UI, the appliance treats the original disk and added disks as one larger data volume. **Note:** Expanding storage is only supported for added disk storage (DAS or external storage attached to the hypervisor). See the following examples: • To expand DAS storage, use the hypervisor to add a new VHD(X) that uses the same volume you selected for the initial backup storage. Then use the Unitrends Backup UI to expand existing storage to include the new disk. • To expand SAN or NAS storage that is exposed to the hypervisor, add a new share or LUN to the hypervisor, then use the hypervisor to add the share or LUN to the volume that was used for the initial backup storage. Create a VHD(X) using this volume. Once the VHD(X) is created, use the Unitrends Backup UI to expand existing storage to include the new disk. • For details on expanding storage, see Procedures for adding attached disk backup storage in the Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup.

Unitrends Backup Storage Component	Recommendations
Examples of adding storage	If expanding storage is not an option, or you need to create a distinct storage area, you can add a separate storage device to your appliance. The storage you add is treated as a separate storage area. This approach allows you to set up backups to write to a specified device. See the following examples: • DAS or external storage attached to the hypervisor - Use the hypervisor to create a volume and VHD(X) from the storage you added. Then go to the Add Backup Storage dialog in the UI, click **Create a separate storage area for an alternate backup device** and select the type **Added Disk**. Select the disk to add. • External storage attached to the Unitrends Backup VM - **Note:** If you used an external NAS or SAN storage array attached directly to the Unitrends Backup VM for the initial backup storage, use the same storage array for all additional backup storage. – Allocate additional space on the NAS and expose it to the Unitrends Backup VM. Then go to the Add Backup Storage dialog in the UI, click **Create a separate storage area for an alternate backup device** and select the type **CIFS** or **NFS**. Enter the IP address of the NAS and other required information. – Allocate additional space on the SAN and expose it to the Unitrends Backup VM. Then go to the Add Backup Storage dialog in the UI, click **Create a separate storage area for an alternate backup device** and select the type **iSCSI**. Enter the IP address of the SAN and other required information. • For details on adding storage, see Procedures for adding attached disk backup storage and Procedures for adding external storage in the Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup.

This page is intentionally left blank.



Chapter 4: Deploying a Unitrends Backup Appliance

Deployment consists of creating the Unitrends Backup VM, attaching backup storage, and configuring appliance settings.

To create the Unitrends Backup VM, you either run a Windows EXE installer or deploy a VHD file. (See "Hypervisor requirements and considerations" on page 7 to determine which method to use for your Hyper-V server.) During deployment, you define network and storage settings for the appliance.

The following steps summarize the procedures used to deploy your Unitrends Backup appliance. Detailed instructions for each procedure follow:

Note: Required steps vary depending on the type of storage you are using and whether you deploy using the EXE or VHD method. Step 4: and Step 6: may not be required.

Step 1: Set up storage on the hypervisor

Verify that the hypervisor has enough storage available:

- 100GB for the Unitrends Backup VM's initial disk.
- At least 200GB for the initial backup storage.

If necessary, add storage. Storage options are described in the following table.

For more on storage, see "Determining your Storage Strategy" on page 13.

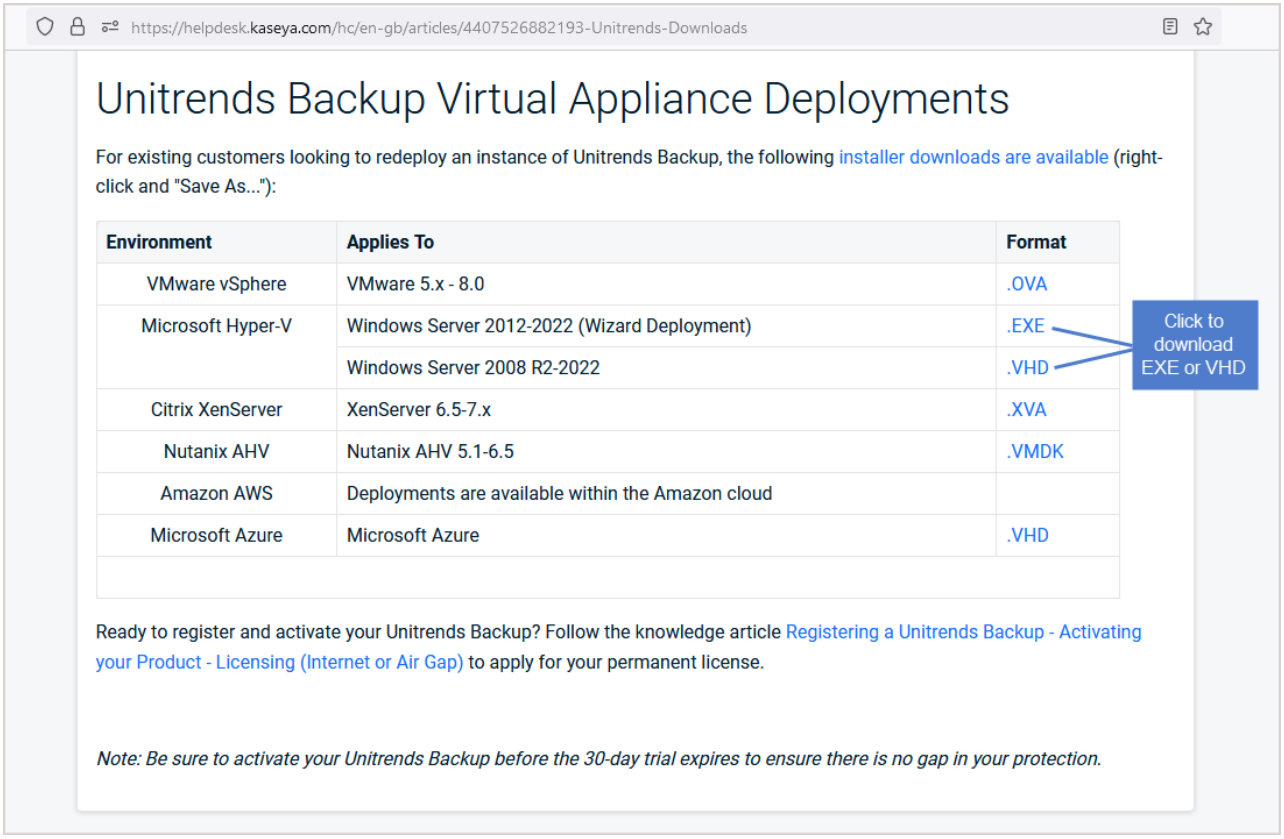
Storage option	Requirements
Use added disk (DAS or external) storage for both the initial disk and initial backup storage (recommended)	Verify that the hypervisor has enough storage to create the initial disk and the initial backup storage. To use external storage (rather than DAS), use the hypervisor to add the SAN or NAS and to create the associated volumes.
Use added disk external storage for the VM's initial disk, and use external storage directly attached to the Unitrends Backup VM for the initial backup storage (not recommended)	To use external storage that is directly attached to the Unitrends Backup VM for the initial backup storage, Unitrends recommends that you use external storage on the same array for the VM's initial disk. Use the hypervisor to add the SAN or NAS and to create the associated volume to use for the initial disk. You will select this volume while deploying the Unitrends Backup VM to create the initial VHD(X) disk (in "Step 3: Deploy the Unitrends Backup VM").
Deploy using storage containing backups from another Unitrends Backup appliance	Verify that the hypervisor has enough storage available to create the initial disk. You will add the storage that contains backups after you deploy the Unitrends Backup VM (as described in "Step 4: Attach backup storage (if needed)"). **IMPORTANT!** If you will be using the EXE installer, do NOT select the option to create and attach a virtual disk to use as backup storage in "Step 3: Deploy the Unitrends Backup VM". You will need to create the initial backup storage after you deploy the Unitrends Backup VM (as described in "Step 4: Attach backup storage (if needed)").

Step 2: Download the Unitrends Backup EXE or VHD

An EXE installer or a VHD file deploys the Unitrends Backup VM.

To download the EXE or VHD:

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 **.EXE** or **.VHD** link in the Microsoft Hyper-V row.



4 Do one of the following:

- For EXE, download the file directly to the server on which you will deploy the appliance.
- For VHD:

  Note: The VHD file is 5,977.2 MB. Be sure to download to a location that has at least 5,977.2 MB of available space.

  - If you are deploying on Windows Server (non-core), download the VHD and place it in a location that can be accessed by Hyper-V Manager on the Windows server.

    You can download directly to the Windows server or download to a different machine. If you download to a different machine, copy the VHD to a network location or to the Windows server itself by using a CD, DVD, or USB drive.

  - If you are deploying on Windows Server Core or Hyper-V Server, download the VHD to an alternate machine on the same network, then copy the VHD to the Hyper-V server. Example VHD target directory on the Hyper-V server: *C:\HyperV\VHDs*.

Step 3: Deploy the Unitrends Backup VM

Deployment instructions remain the same whether you are setting up Unitrends Backup with new storage or with storage that contains backups from another Unitrends Backup appliance. Use one of the following procedures:

- "Deploying with EXE"
- "Deploying with VHD" on page 27

Deploying with EXE

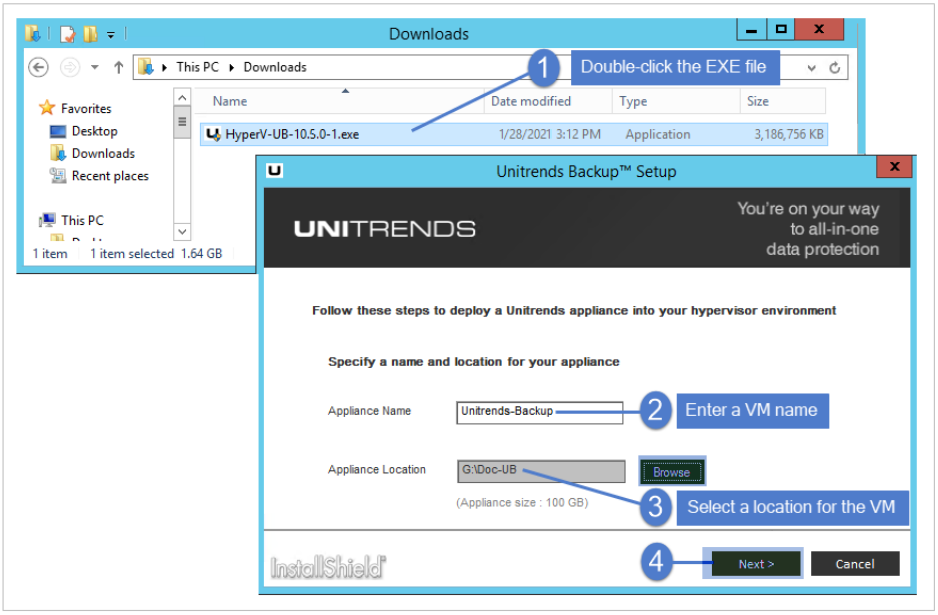
Use the following procedure to deploy the Unitrends Backup VM using the EXE installer.

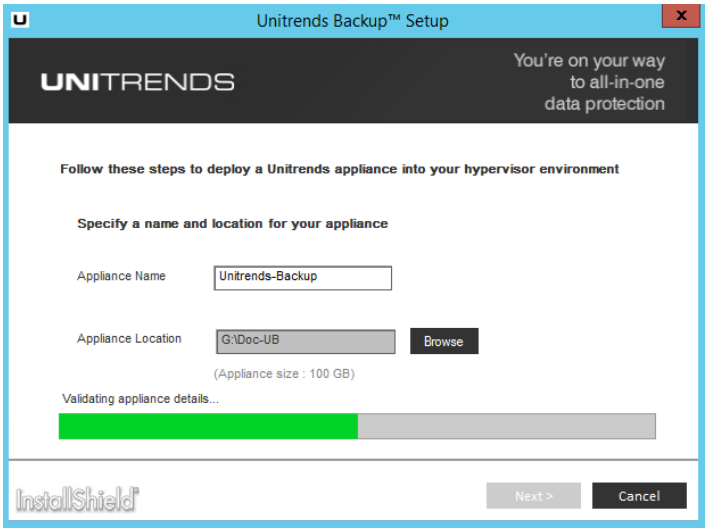
Prerequisite if using external storage

To create the VM's initial disk from external storage, use the hypervisor to add the SAN or LUN and associated volumes before running the EXE installer.

To deploy using the EXE installer

1. On the Hyper-V server where you downloaded the EXE file, double-click **HyperV-UB-*version*.exe**. It runs automatically.
2. On the first installer screen, enter the following:
   - Appliance Name — Enter a display name for the Unitrends Backup VM. The name can contain only alphanumeric characters, dashes, and underscores. This is the name that will display for the VM in your hypervisor.
   - Appliance Location — Browse to select a location for the Unitrends Backup VM on the Hyper-V server. If needed, you can create a new folder for the VM.
3. Click **Next**.





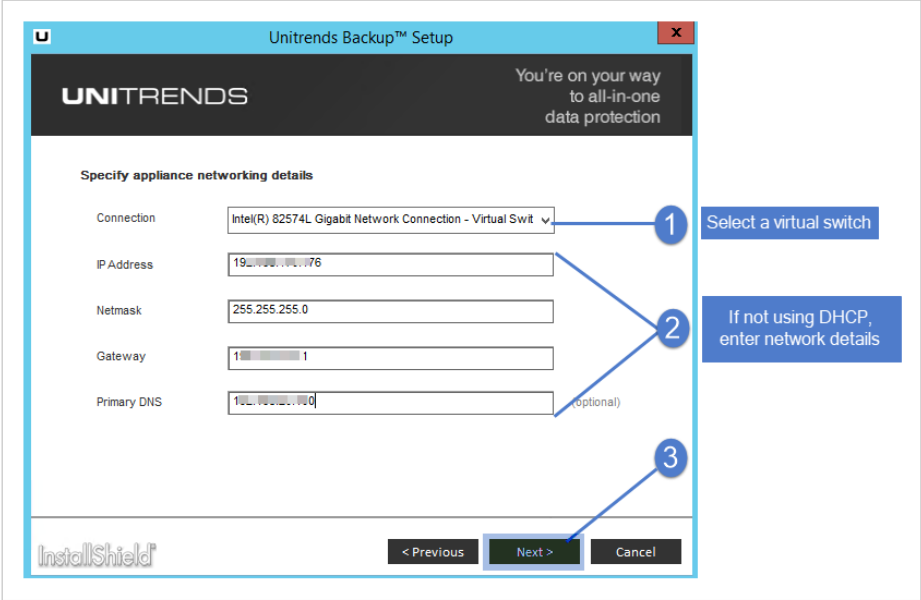
4 In the Connection drop-down, select a virtual switch for the Unitrends Backup VM to use on the host:

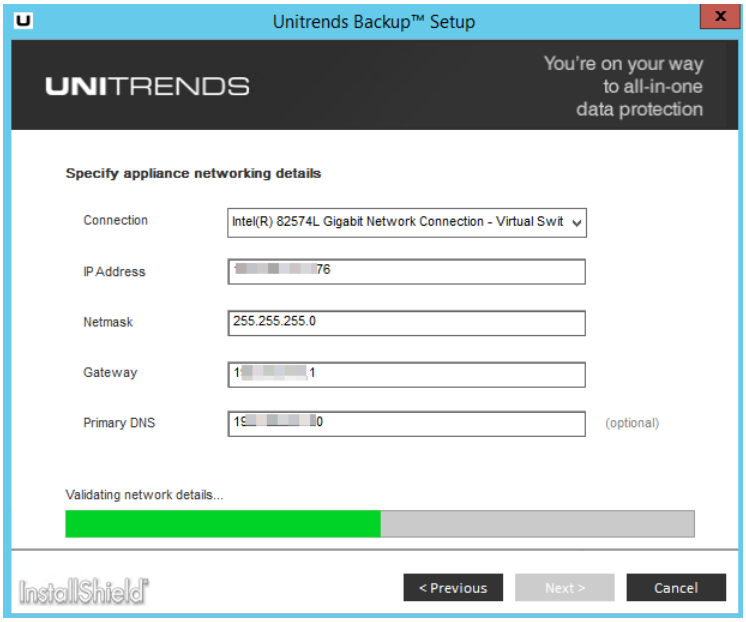
- If DHCP is available, networking details are added automatically.
- If DHCP is not available or if you prefer to assign a static IP address to the appliance, enter an **IP address**, **Netmask**, **Gateway**, and **Primary DNS**.

Notes:

- You must assign a static IP address if you intend to use the appliance as a hot backup copy target.
- Make a note of the appliance IP address. You will need it later to log in to the appliance user interface.

5 Click **Next**.





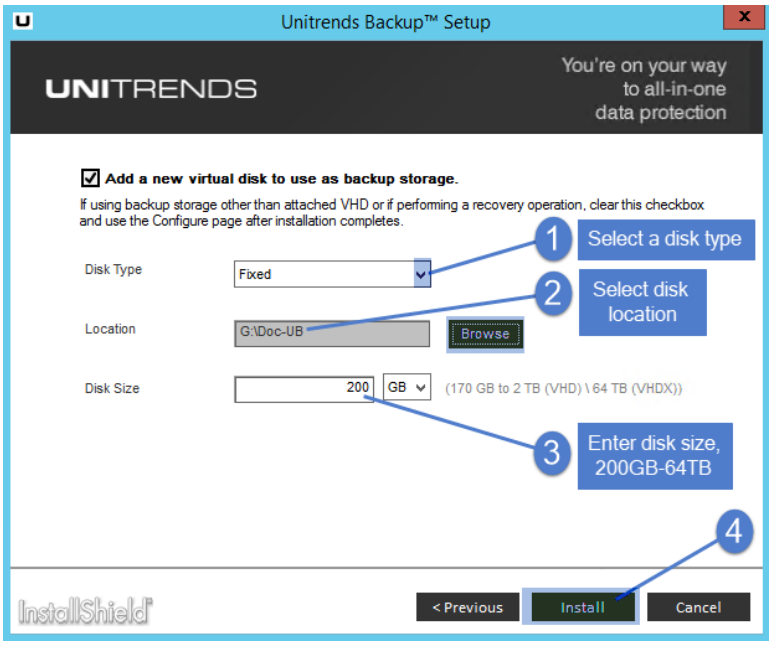
6 Create a virtual disk to use as the initial backup storage (or opt to use existing storage or external storage instead) by entering the following information:

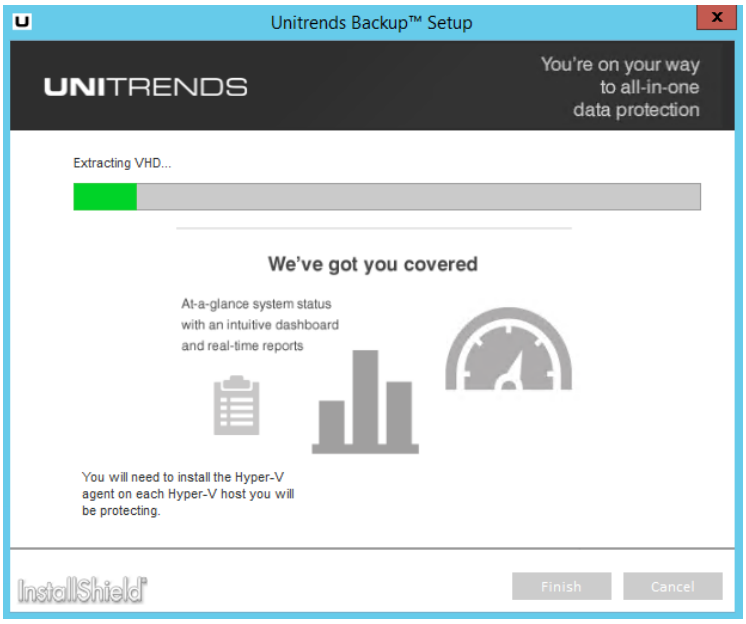
- Add a virtual disk to use as backup storage — Selected by default. Do one of the following:
  - Leave this box checked to create added disk storage. The appliance automatically designates this disk as the initial backup storage. (You will select the volume to use below. The volume can reside either on DAS storage internal to the hypervisor or on external storage that you have exposed to the hypervisor.)

- Clear this box to use storage that contains backups from another Unitrends Backup appliance. (You will add this storage later). Proceed to step 7.
- Clear this box to use external storage attached directly to the Unitrends Backup VM instead. (You will add this storage later.) Proceed to step 7.

- Disk Type — Select a disk type. For best performance, choose Fixed.
- Location — Browse to select a location for the disk. If necessary, you can use the browser to create a new folder for the disk.
- Disk Size — Defaults to 200GB. Adjust the size of the attached disk, up to 64TB. The size cannot be less than 200GB.

7 Click **Install**. This creates the Unitrends Backup VM on the Hyper-V server using the settings you defined in the previous steps.

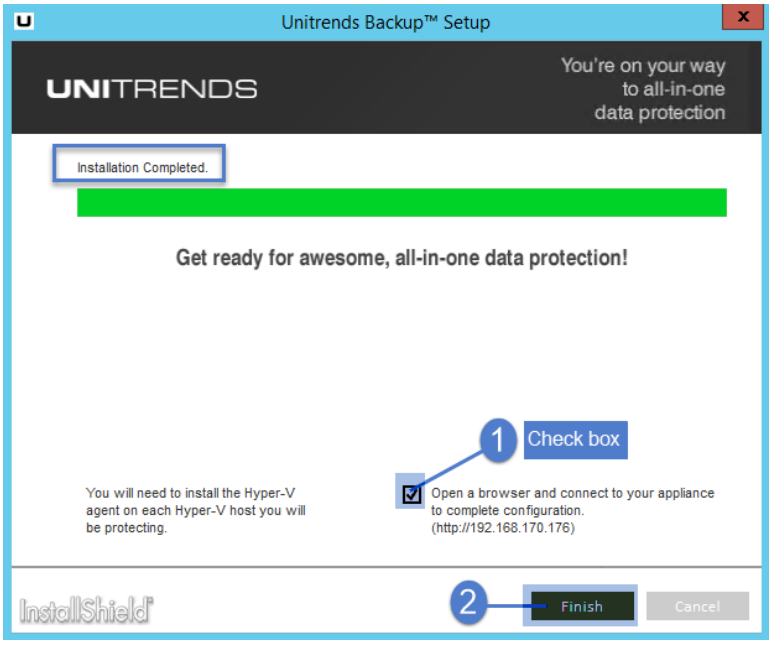




8 Once installation completes, select **Open a browser and connect to your appliance to complete configuration**. This opens Chrome or Firefox to the IP address defined for the appliance. If neither of these browsers is available on your machine, Internet Explorer opens. This browser is not supported, and Unitrends recommends using Chrome or Firefox; however, you can complete the Quick Setup Wizard using Internet Explorer.

(If you do not select **Open a browser and connect to your appliance to complete configuration**, you must manually open a browser and enter the IP address you assigned to your Unitrends Backup appliance after the installation completes.)

9 Click **Finish**.



10 Proceed to one of the following:

- If you created the virtual disk in step 6, proceed to "Step 5: Set up the appliance using the Quick Setup Wizard" on page 44.
- If you did NOT create the virtual disk in step 6, proceed to "Step 4: Attach backup storage (if needed)" on page 39.

Deploying with VHD

Deployment procedures vary by server operating system. For detailed steps, see one of the following procedures:

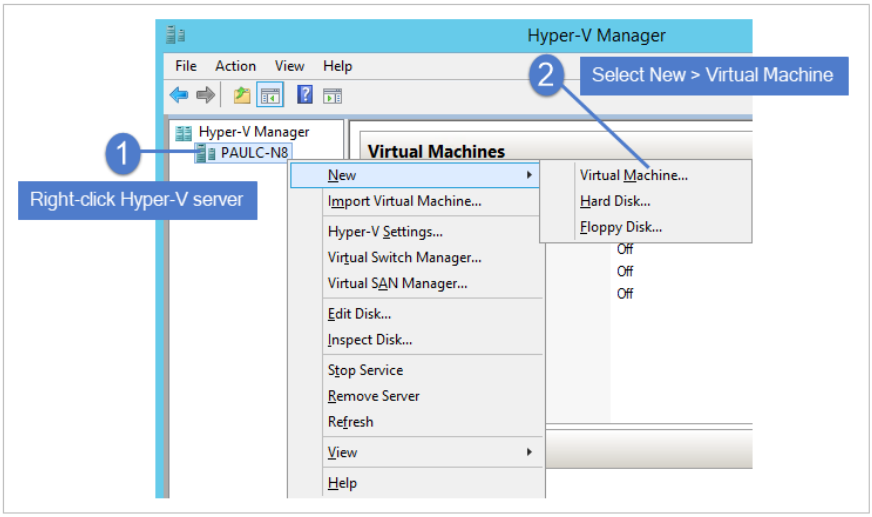
- "Deploy the VHD to Windows Server Hyper-V"
- "Deploy the VHD to Windows Server Core Hyper-V or Hyper-V Server" on page 32

Deploy the VHD to Windows Server Hyper-V

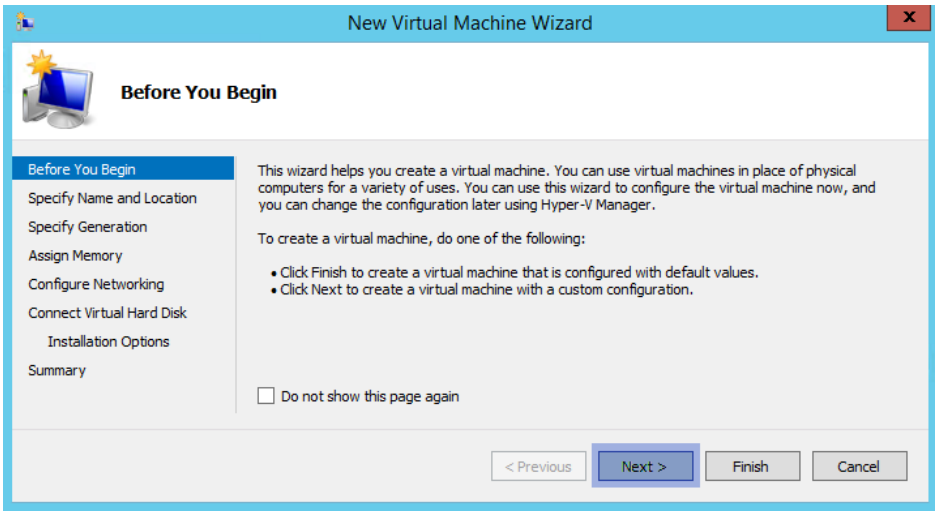
Use these steps to deploy the VHD to Windows Server Hyper-V:

1 Log in to the Windows server and launch Hyper-V Manager.

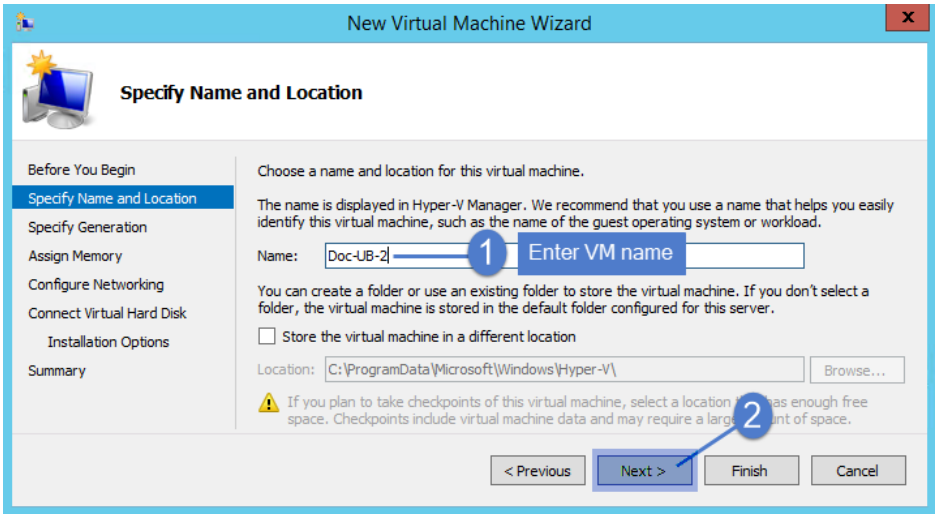
2 Right-click the Hyper-V server and select **New > Virtual Machine**.



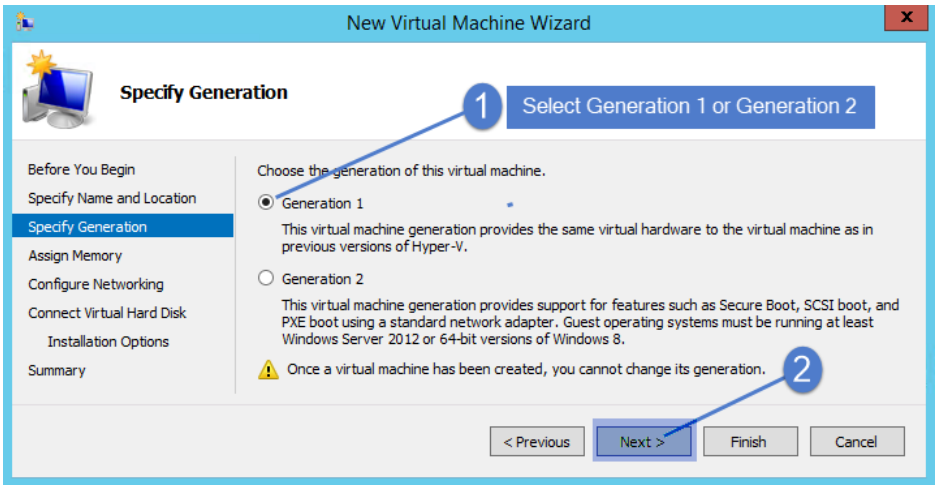
3 Click **Next**.



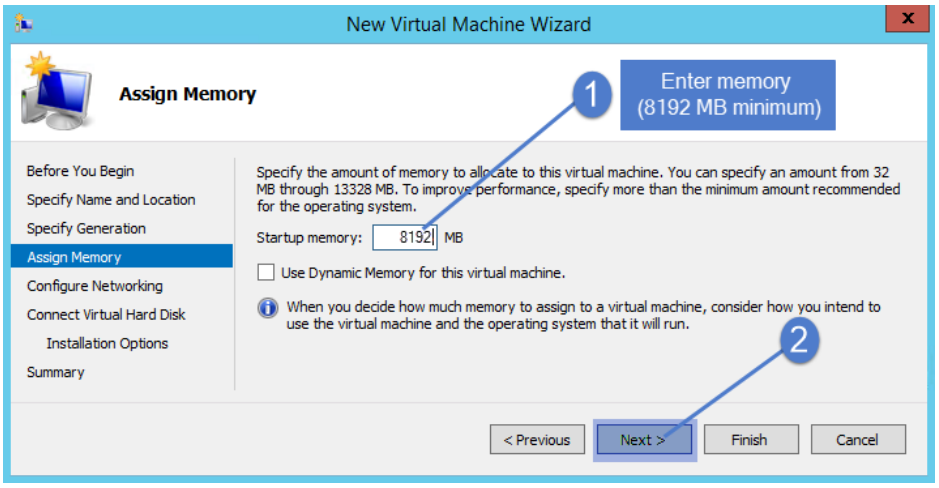
4 Enter a **Name** for the Unitrends Backup VM. Click **Next**.



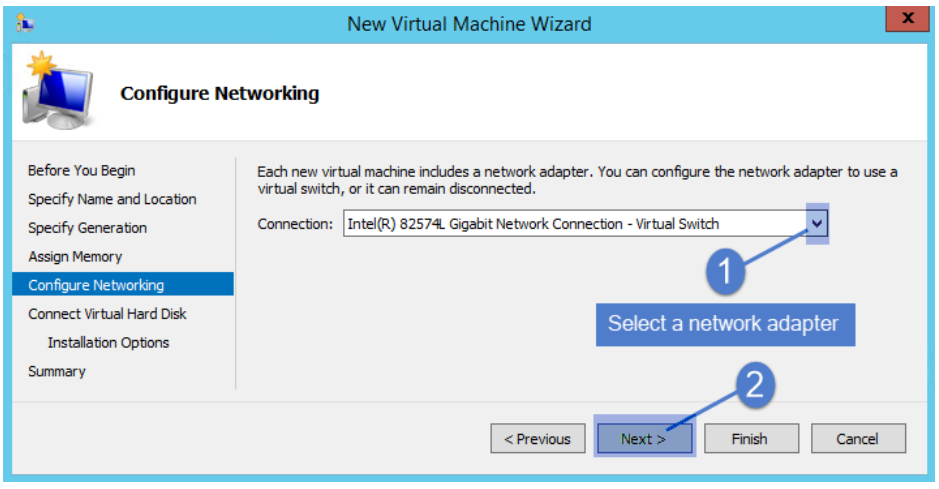
5 Select Generation 1 or Generation 2 to specify the virtual hardware generation of the Unitrends Backup VHD disk. Click **Next**.



6 Assign **Startup memory** (minimum required is 8192 MB). Click **Next**.

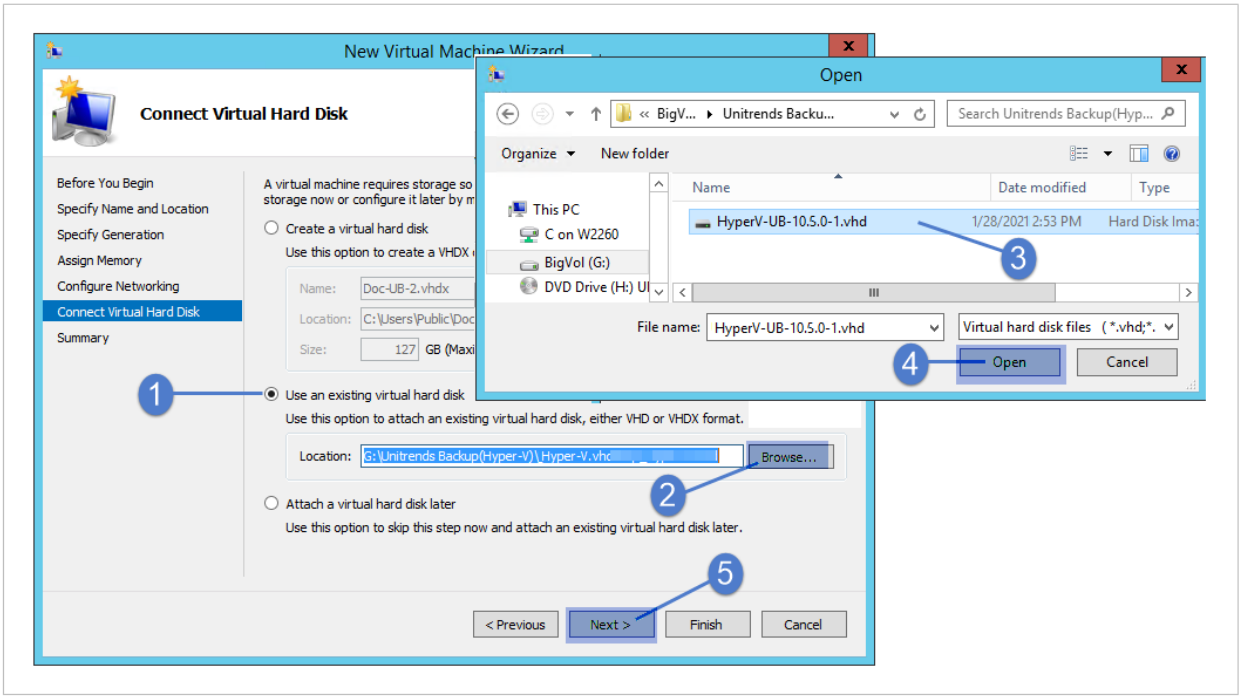


7 Select a network adapter from the **Connection** list. Click **Next**.

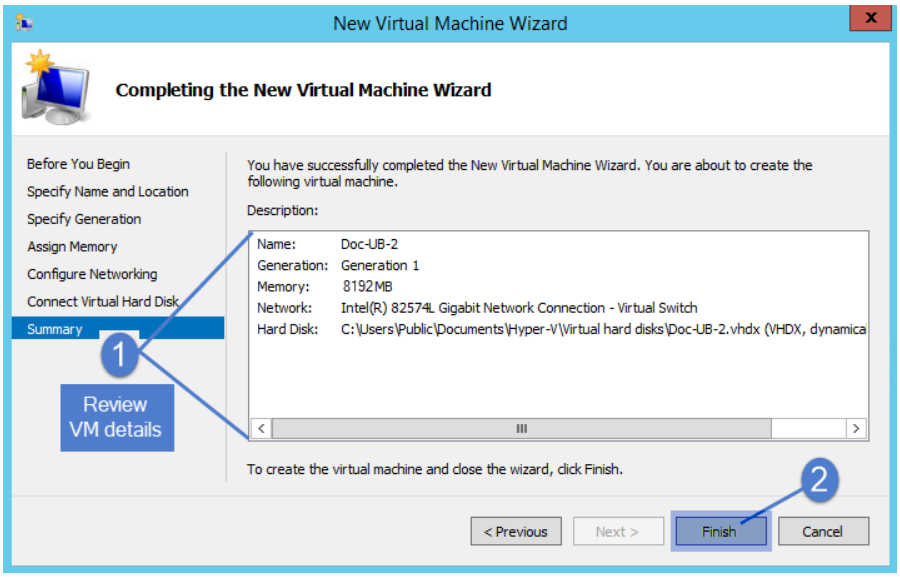


8 Connect the Unitrends Backup VHD:

- Select **Use an existing virtual hard disk**.
- **Browse** to the folder where you copied the VHD and select the VHD file (*HyperV-UB-release.vhd*).
- Click **Next**.

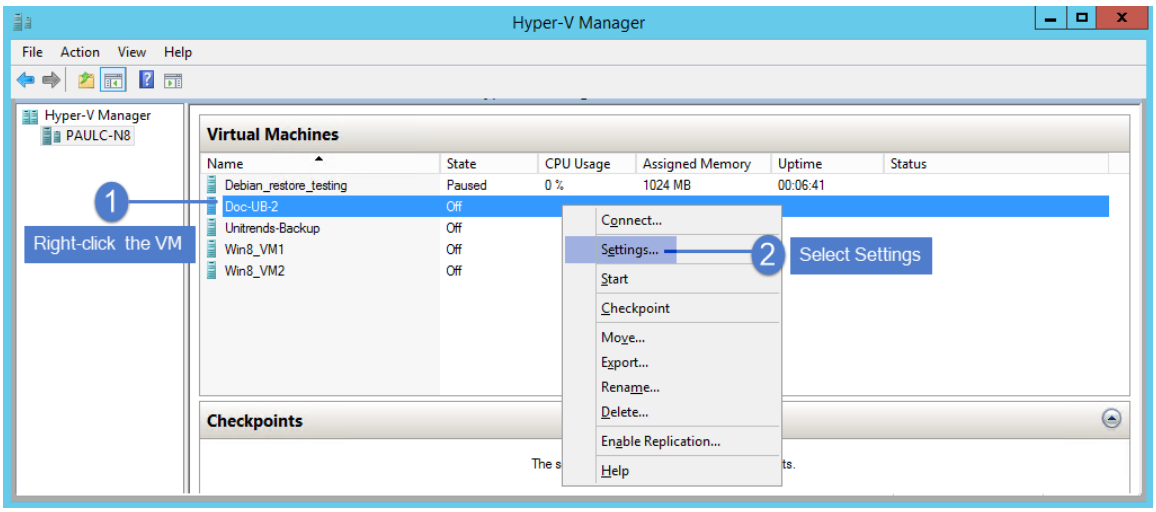


9 Review VM details. Click **Finish**. (Or click **Previous** to modify VM settings).



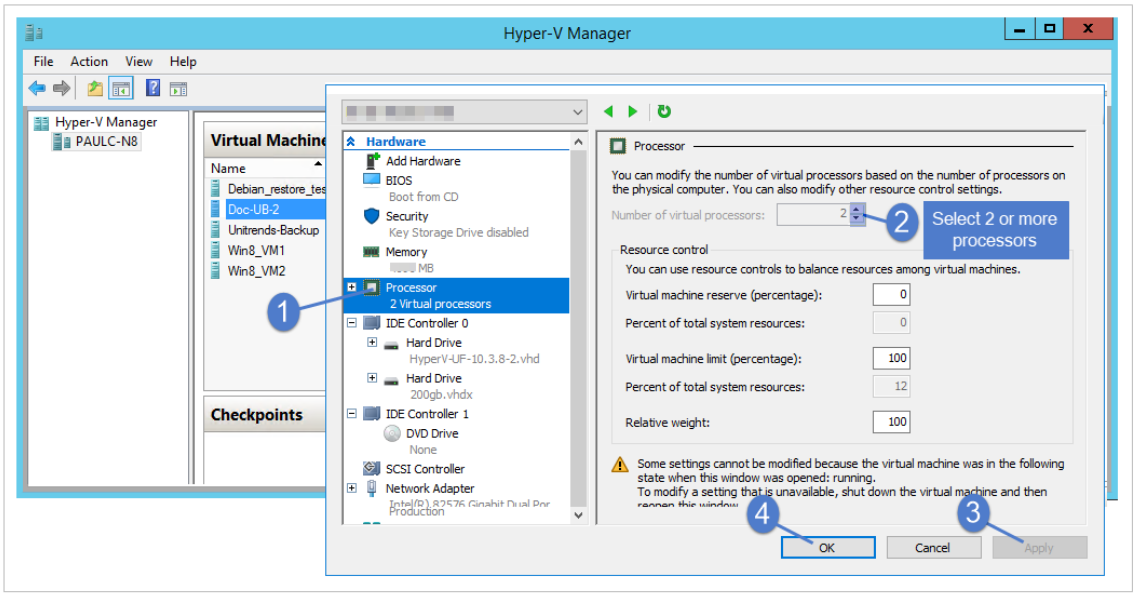
The VM is created and displays in Hyper-V Manager.

10 Right-click the VM and select **Settings**.

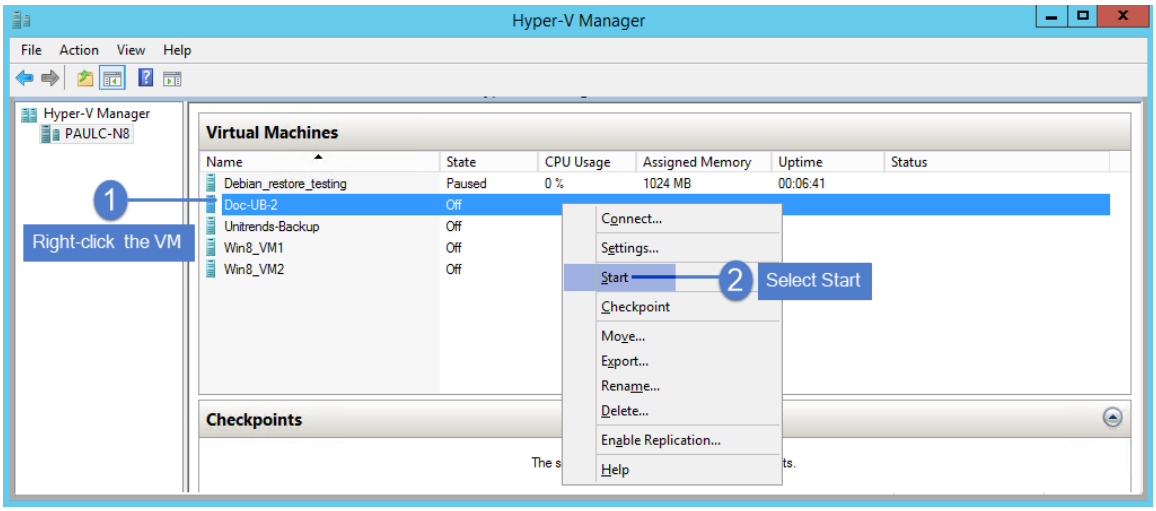


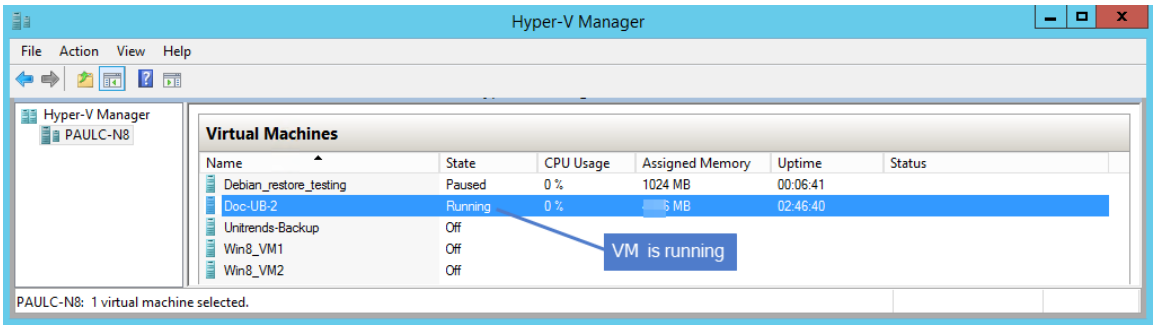
11 Set the number of virtual processors that will be assigned to the VM. Click **Apply**, then **OK**:

Note: You must assign a minimum of 2 virtual processors.



12 Right-click the VM and select **Start**.





13 Do one of the following:

- If the VM's network adapter has DHCP available, proceed to "Attach backup storage (if needed)" on page 39.
- If DHCP is not available or if you prefer to assign a static IP address, proceed to "To set up the appliance with a static IP address" on page 34.

Notes:

- You must assign a static IP address if you intend to use the appliance as a hot backup copy target.
- Make a note of the appliance IP address. You will need it later to log in to the appliance user interface.

Deploy the VHD to Windows Server Core Hyper-V or Hyper-V Server

Use these steps to deploy the VHD to Windows Server Core Hyper-V or Hyper-V Server:

1 Log in to the host server.

2 Launch PowerShell:

```
# Powershell
```

3 Enter the following command:

```
# New-VM –Name "Unitrends Backup" –Path "full_path_to_storage_location"
–MemoryStartupBytes 8GB -VHDPath "full_path_to_vhd_location"
```

Where:

- *Unitrends Backup* is the name of the Unitrends Backup VM that will be created from the VHD.
- *full_path_to_storage_location* is the full path to the *HyperV-UB*-release.*vhd* that you downloaded from Unitrends.

  Note: The VHD that you downloaded from Unitrends is used as both the storage location and the VHD location.

- *full_path_to_vhd_location* is the full path to the *HyperV-UB*-release.*vhd* that you downloaded from Unitrends.

Example where the VHD resides in *C:\HyperV\VHDs*:

```
# New-VM –Name "Unitrends Backup" –Path "C:\HyperV\VHDs" –MemoryStartupBytes 8GB
-VHDPath "C:\HyperV\VHDs"
```

4 Set the number of virtual processors by entering this command, where *2* is the number of processors that will be assigned to the VM:

Note: You must assign a minimum of 2 virtual processors.

```
# SET-VMProcessor –VMName "Unitrends Backup" –Count 2
```

5 Assign a virtual switch to the Unitrends Backup VM by issuing these commands:

- (Optional) Enter this command to list the virtual switches on the Hyper-V server:

  ```
  # GET-VMSwitch
  ```

- Enter this command to assign a virtual switch to the VM, where *name_of_vswitch* is the name of the virtual switch:

  ```
  # GET-VMSwitch –VMName "Unitrends Backup" | GET-VMNetworkAdapter | Connect-
  VMNetworkAdapter –Switchname "name_of_vswitch"
  ```

  Example where *Production* is the switch name:

  ```
  # GET-VMSwitch –VMName "Unitrends Backup" | GET-VMNetworkAdapter | Connect-
  VMNetworkAdapter –Switchname "Production"
  ```

6 Enter this command to list the VMs on the server:

```
# GET-VM
```

The Unitrends Backup VM displays in the list in a powered off state.

7 Enter this command to start the Unitrends Backup VM:

```
# Start-VM "Unitrends Backup"
```

8 Do one of the following:

- If the VM's network adapter has DHCP available, proceed to "Step 4: Attach backup storage (if needed)" on page 39.
- If DHCP is not available or if you prefer to assign a static IP address, proceed to "To set up the appliance with a static IP address".

Notes:

- You must assign a static IP address if you intend to use the appliance as a hot backup copy target.
- Make a note of the appliance IP address. You will need it later to log in to the appliance user interface.

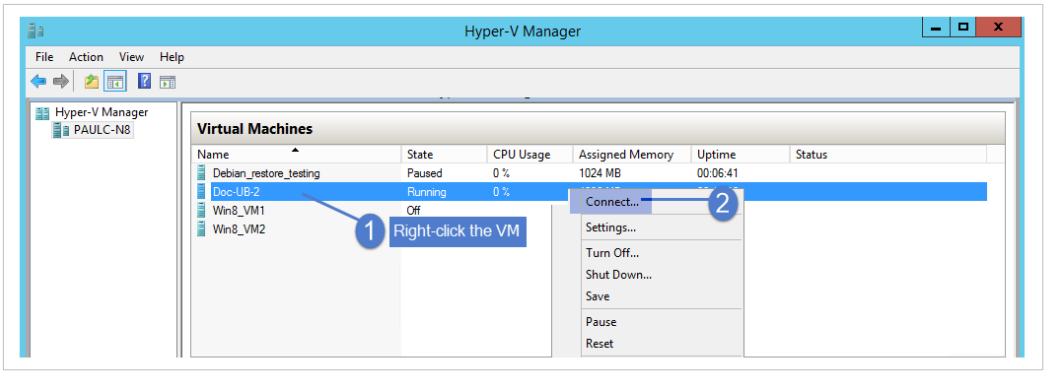
To set up the appliance with a static IP address

Note: If you are deploying by using storage from another Unitrends Backup appliance that contains backup data, you can enter the same network settings as the original appliance or use different network settings.

1 Connect to the Unitrends Backup VM by using one of the following methods:

- Hyper-V Manager – From Hyper-V Manager, right-click the Unitrends Backup VM and select **Connect**.

  Note: The Unitrends Backup VM must be powered on. If necessary, right-click the VM and select **Start**.



- Command line – Navigate to *C:\Program Files\Hyper-V* and enter this command, where *hyper_v_server* is the name of the Hyper-V server and *virtual_machine_name* is the name of the Unitrends Backup VM:

  ```
  # vmconnect.exe hyper_v_server "virtual_machine_name"
  ```

  Example where the Hyper-V server is *HVHOST* and the VM is *Unitrends Backup*:

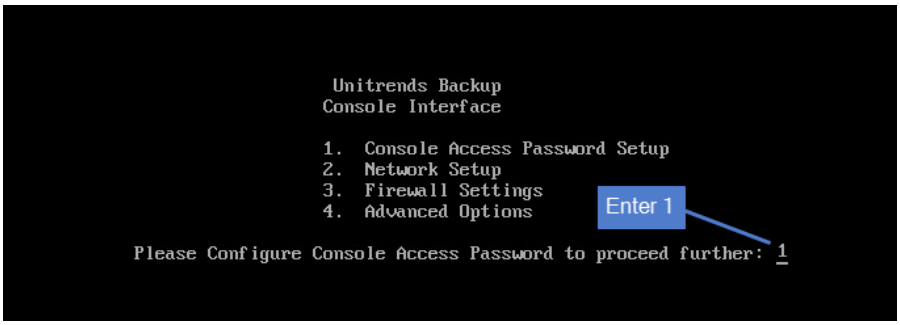
  ```
  # vmconnect.exe HVHOST "Unitrends Backup"
  ```

The remaining steps are run from the Unitrends Backup Console Interface. On these screens, you select a menu option by entering a number in the **Please enter choice** field.

Notes:

- As you complete each step in the Unitrends Backup Console Interface, you are presented with the next configuration screen.
- You can press **Enter** to accept the default or current setting.

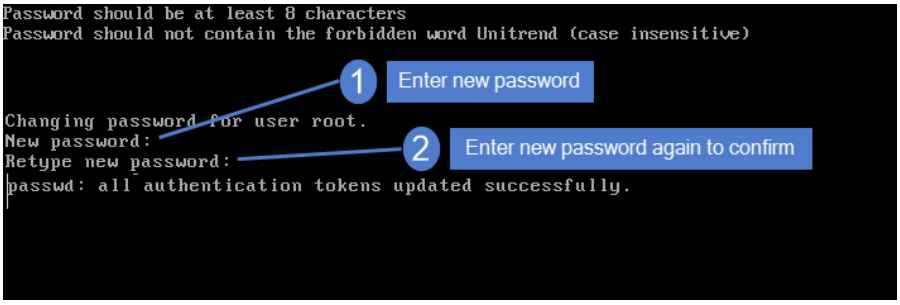
2 On the Console Interface screen, enter **1** in the **Please Configure Console Access Password...** field.



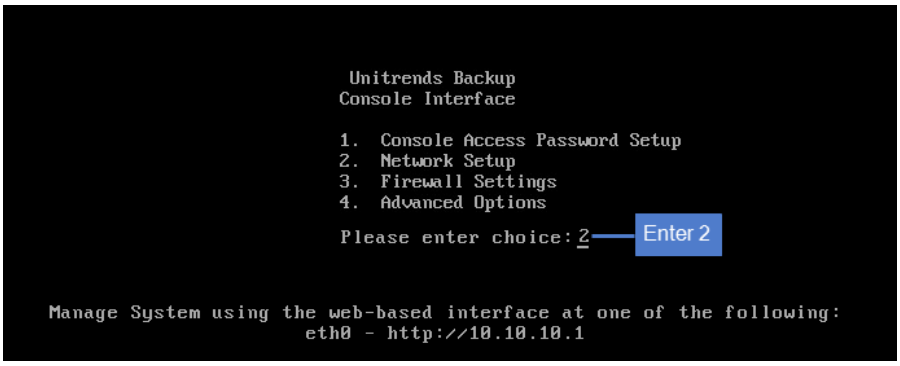
3 To change the direct console password, enter a new password, then enter the password again to confirm.

Notes:

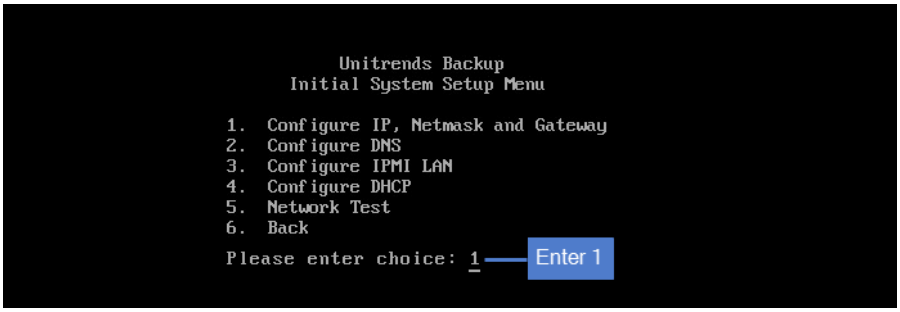
- This is the root operating system password that accesses the console. This password does not access the UI. (You will change the UI password in "Step 5: Set up the appliance using the Quick Setup Wizard" on page 44.)
- All appliances are deployed with these default operating systems credentials: user *root*, password *unitrends1*. For appliance security, you must change this password.



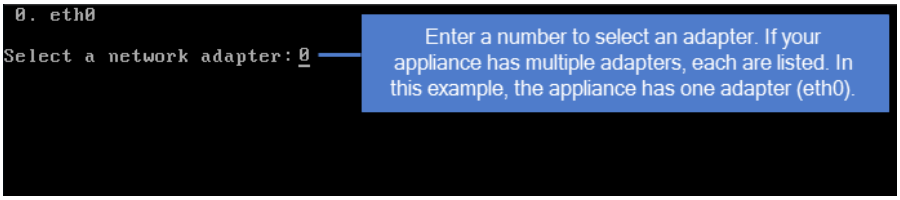
4 On the Console Interface screen, enter **2**.



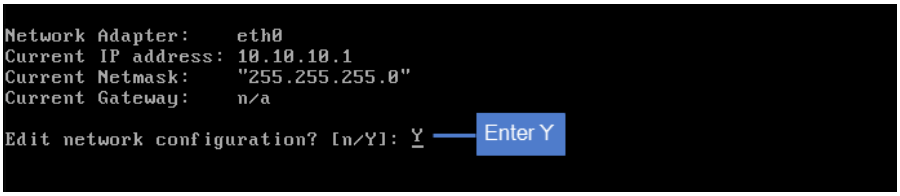
5 On the Initial System Setup Menu screen, enter **1** in the **Please enter choice** field.

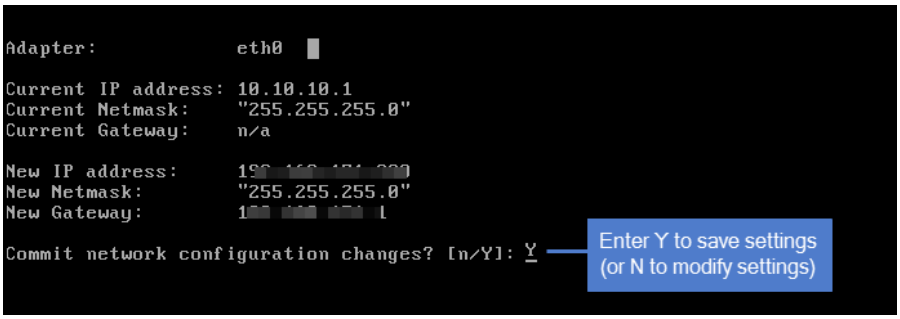


6 Enter a number in the **Select a network adapter** field. For example, enter **0** to select *eth0*.

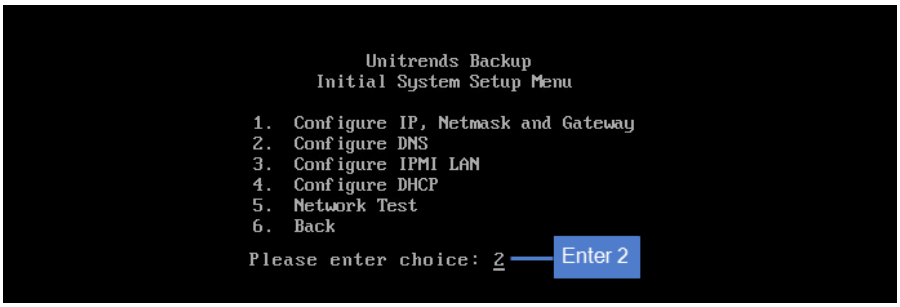


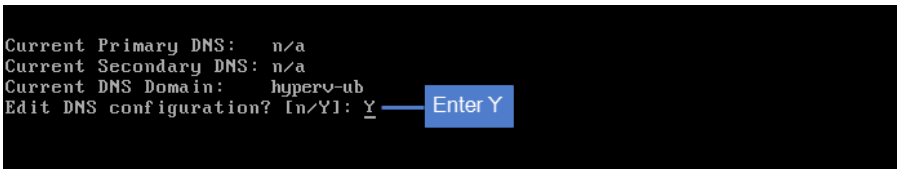
7 Enter **Y** in the **Edit network configuration** field. Then enter an **IP address**, **Netmask**, and **Gateway**. Review the settings and enter **Y** to save.

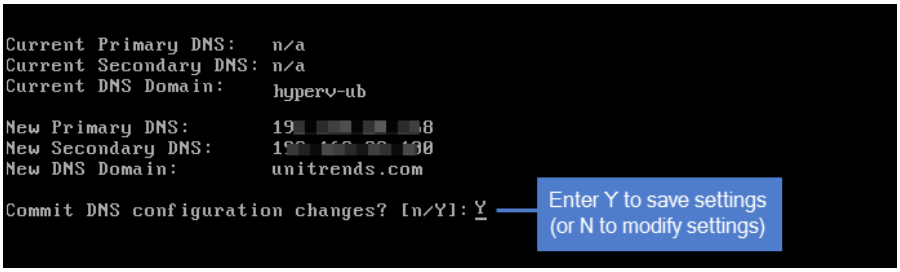




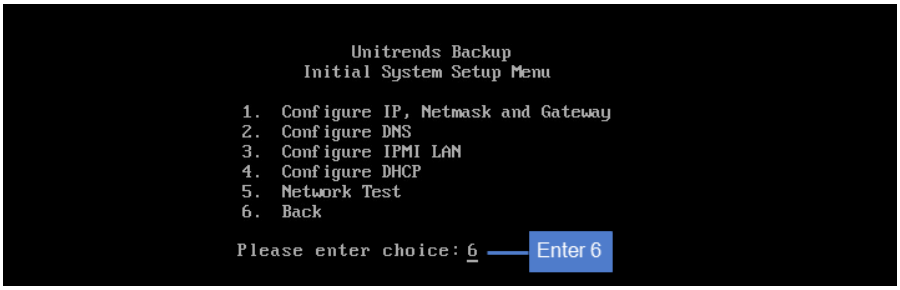
8 To configure DNS settings, enter **2**, then enter **Y** to edit. Enter the **Primary DNS** IP address, a **Secondary DNS** IP (optional), and a **DNS Domain**. Review the settings and enter **Y** to save.



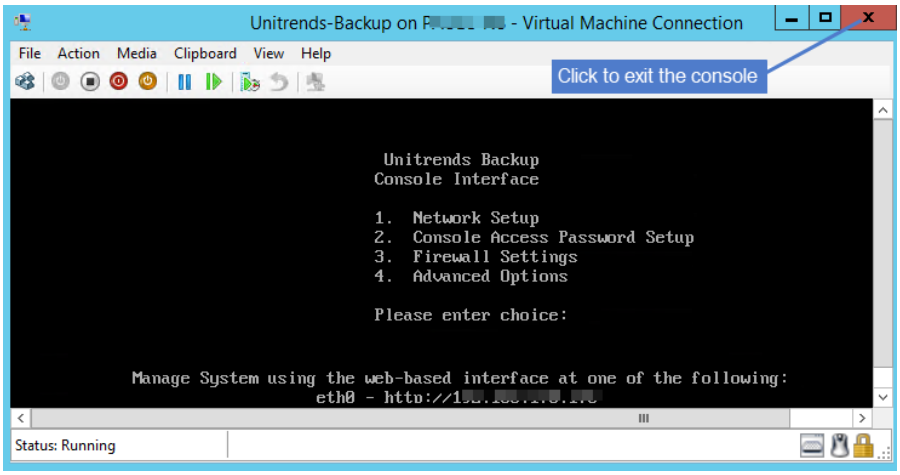




9 To exit network setup, enter **6**.



10 Exit the VM console.



11 Proceed to "Step 4: Attach backup storage (if needed)".

Step 4: Attach backup storage (if needed)

Note: If you ran the EXE installer and selected the option to create the virtual disk, the initial backup storage has already been attached. Proceed to "Step 5: Set up the appliance using the Quick Setup Wizard" on page 44.

In this step you will attach the initial backup storage. Note that once you finish deploying and setting up your Unitrends Backup appliance, you can add disks, LUNs, or shares at any time to increase backup storage capacity.

Attach backup storage using one of the procedures in this section if either of the following apply to your deployment:

- You deployed the Unitrends Backup VM by using the VHD file.
- You deployed by using the EXE installer but opted to create the initial backup storage by attaching external storage directly to the Unitrends Backup VM or are using storage that contains backups from another Unitrends Backup appliance.

Instructions for attaching storage vary by whether you are setting up the Unitrends Backup with new storage or with storage that contains backups from another Unitrends Backup appliance. See one of the following topics:

- "Attaching new backup storage"
- "Attaching storage that contains backups from another appliance" on page 40

Attaching new backup storage

For new backup storage, you can use added disk storage (DAS or external storage attached to the hypervisor) or external storage attached directly to the Unitrends Backup VM. The initial disk is added to an IDE controller, but for optimal performance and scalability, you should add all additional disks to SCSI controllers and use VHD(X) disks where possible.

See the following topics for details:

- "Added disk storage attached to the hypervisor"
- "External storage attached to the Unitrends Backup VM"

Added disk storage attached to the hypervisor

If you deployed with the VHD file, add a VHD(X) to the Unitrends Backup VM by using Hyper-V Manager. The appliance automatically uses the first VHD(X) disk added to the Unitrends Backup VM as the initial backup storage. Once you have added the VHD(X), proceed to "Step 5: Set up the appliance using the Quick Setup Wizard" on page 44.

See the following Microsoft documents for details on creating and adding a virtual disk:

- To create a virtual hard disk
- To add a hard disk to a virtual machine

External storage attached to the Unitrends Backup VM

To use external NAS or SAN storage attached directly to the Unitrends Backup VM, add the share or LUN and expose it to the Unitrends Backup VM. You will select the share or LUN to use as the initial backup storage after you complete

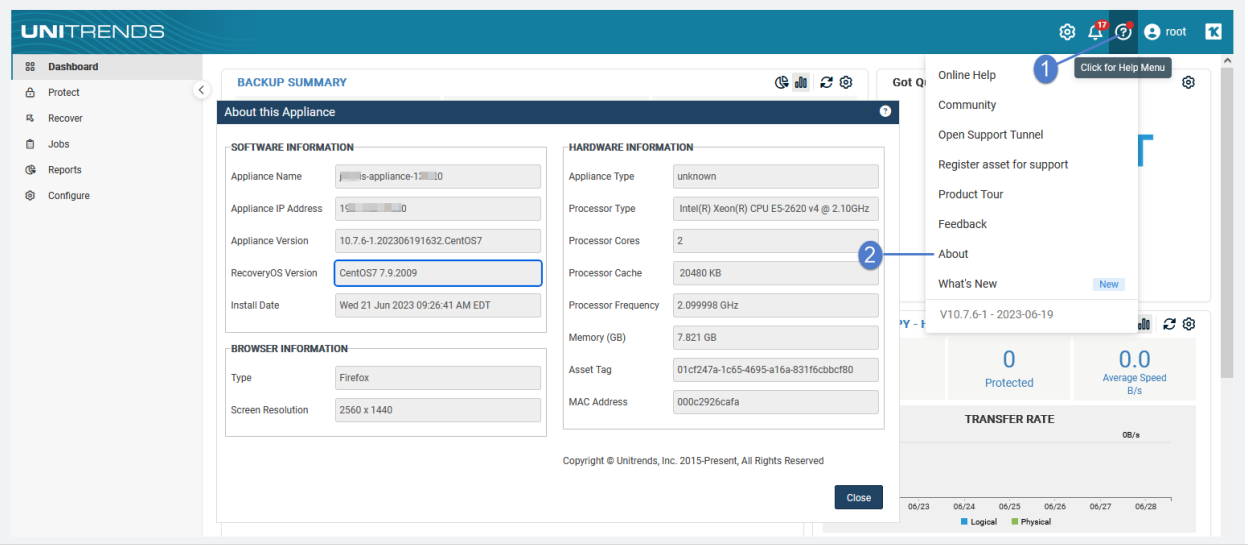
the steps in the Quick Setup Wizard. Once you have added storage and exposed it to the Unitrends Backup VM, proceed to "Step 5: Set up the appliance using the Quick Setup Wizard" on page 44.

Attaching storage that contains backups from another appliance

Use one of the procedures in this section to attach storage that contains backups from another Unitrends Backup appliance.

IMPORTANT!

- You must configure all storage that contains backup data from another Unitrends Backup appliance before you do "Step 5: Set up the appliance using the Quick Setup Wizard". If you add this storage after you set up the appliance, any data on the storage is deleted.
- Attaching backup storage that contains backups from another Unitrends Backup appliance is supported only if the original appliance is running the same operating system as the newly deployed appliance. Appliances deployed with version 10.3.6 or higher run CentOS 7. Appliances deployed with older versions run CentOS 6. To check the appliance Recovery OS version, click on **? > About**:



Instructions for attaching storage that contains Unitrends backups vary by whether the storage was attached directly to the original VM or attached through the hypervisor.

See the following topics for details:

- "Backup data on disks that were attached to the original Unitrends Backup VM through the hypervisor "
- "Backup data on external storage that was connected directly to the original Unitrends Backup VM"

Backup data on disks that were attached to the original Unitrends Backup VM through the hypervisor

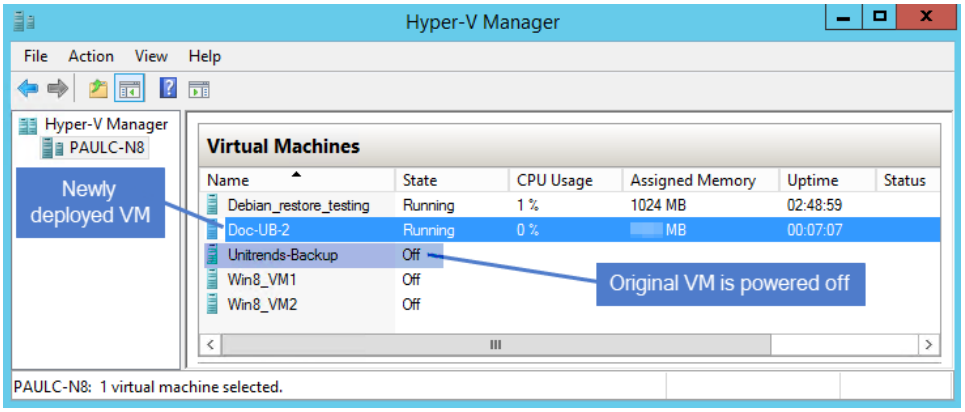
If your backup data resides on VHD(X) disks, you must attach the VHD(X) disks to the Unitrends Backup VM by using Hyper-V Manager before setting up the appliance.

IMPORTANT! Be sure to attach the VHD(X) disk that was used as the initial backup storage first (before adding any other VHD(X) disks). The appliance automatically uses the first VHD(X) disk you attach as the initial backup storage. Adding the wrong VHD(X) disk first will yield undesirable results. The appliance then recognizes all other attached disks and can access all existing backup data.

To add a VHD(X) that contains backups from another Unitrends Backup appliance:

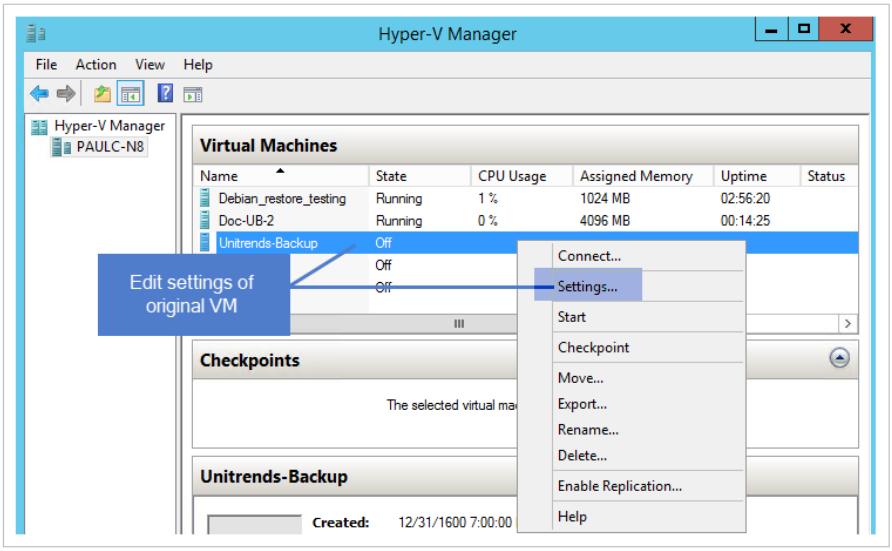
1 Access your Hyper-V server using Hyper-V Manager.

2 Power off the original Unitrends Backup VM.



3 Identify the disk(s) that you want to add to the newly deployed VM by doing these steps:

- Right-click the original VM and select **Settings**.

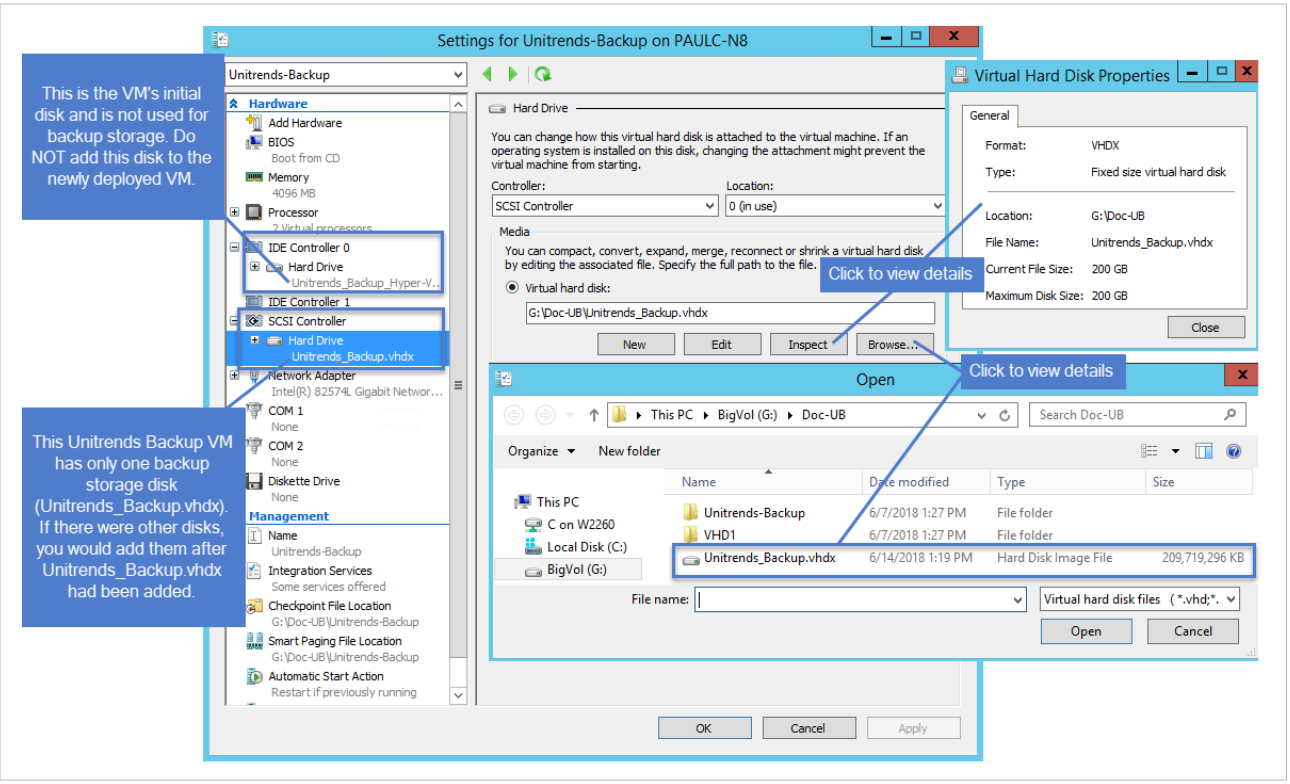


- Select each hard drive to view details. Note the name and location of the disks you will add to the newly deployed VM.

Notes:

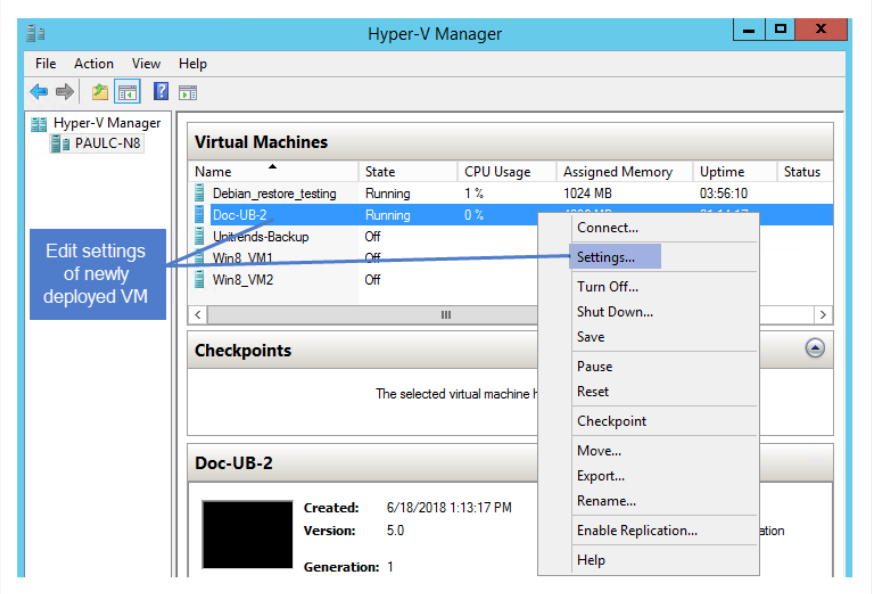
- You must add all backup storage disks from the original VM.
- Do not add the Hard Drive created under IDE Controller 0. This disk was created during VM deployment and is NOT used to store backups.
- You must add the first backup storage disk created under SCSI Controller before you add any other backup storage disks.

In our example, the VM has only one backup storage disk:

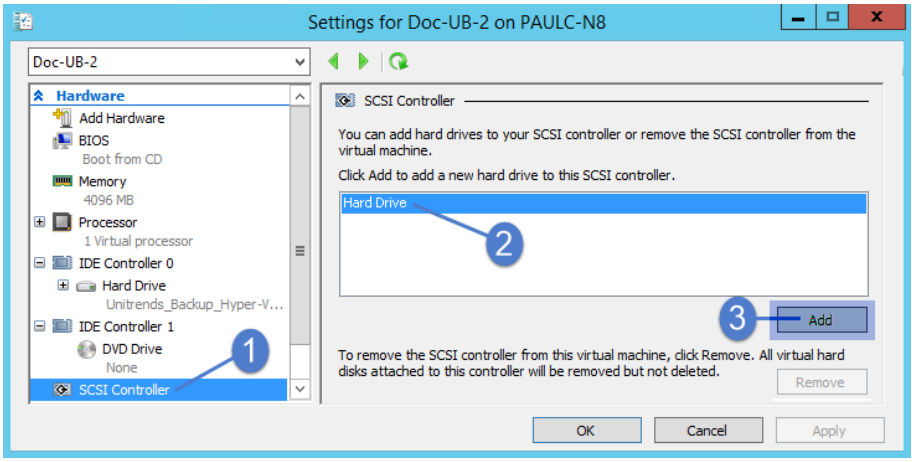


4 Add the disk(s) to the newly deployed VM by doing these steps:

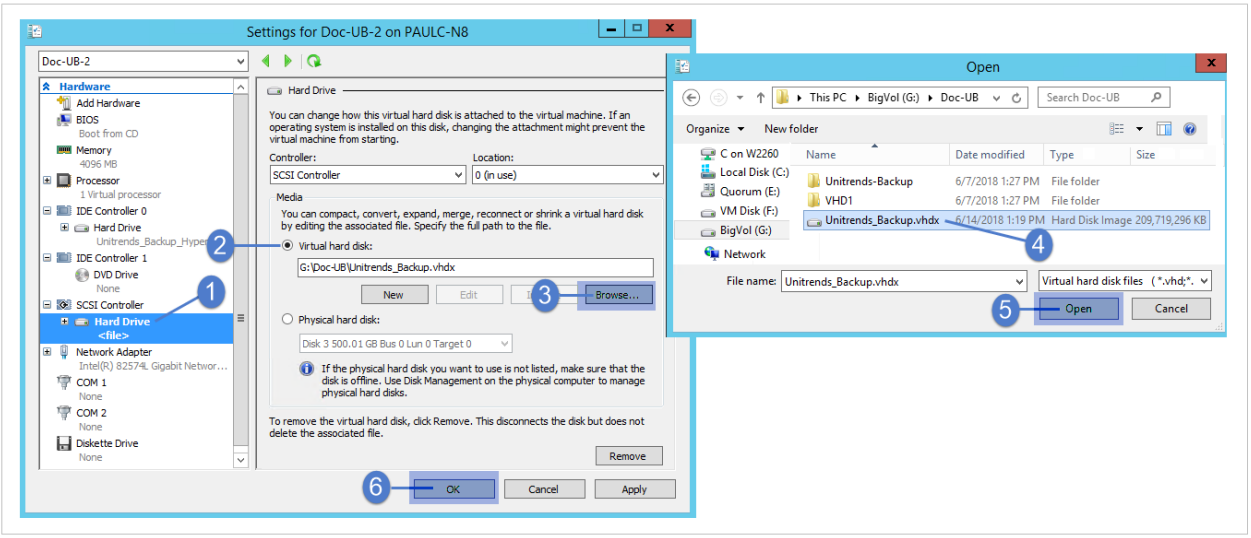
- Right-click the newly deployed VM and select **Settings**.



- Select **SCSI Controller**, click **Hard Drive**, then **Add**.



- Select **Hard Disk** and **Virtual hard disk**.
- Click **Browse**. Browse to the original VM's first backup storage disk and click **Open**.
- Click **OK** to add the disk.



5 (If needed) If the original VM has multiple backup storage disks, repeat step 4 to add those disks.

6 After attaching all backup storage disks, proceed to "Step 5: Set up the appliance using the Quick Setup Wizard".

Backup data on external storage that was connected directly to the original Unitrends Backup VM

If the backup data resides on NAS or SAN storage that is connected directly to the original Unitrends Backup VM:

1 Expose the share or LUN to the new Unitrends Backup VM.

2 Proceed to "Step 5: Set up the appliance using the Quick Setup Wizard".

Step 5: Set up the appliance using the Quick Setup Wizard

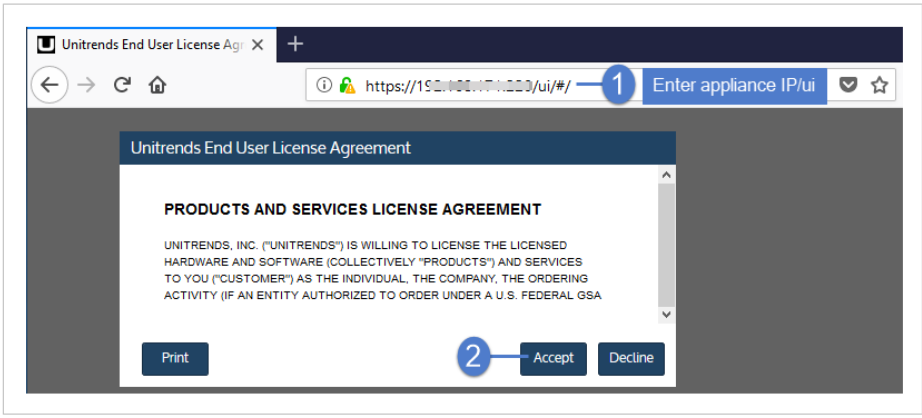
To start the setup process, log in to the appliance UI from any machine on the same network by opening a browser and entering the appliance's IP address followed by */ui/*. The Quick Setup Wizard launches when you access the UI for the first time.

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.

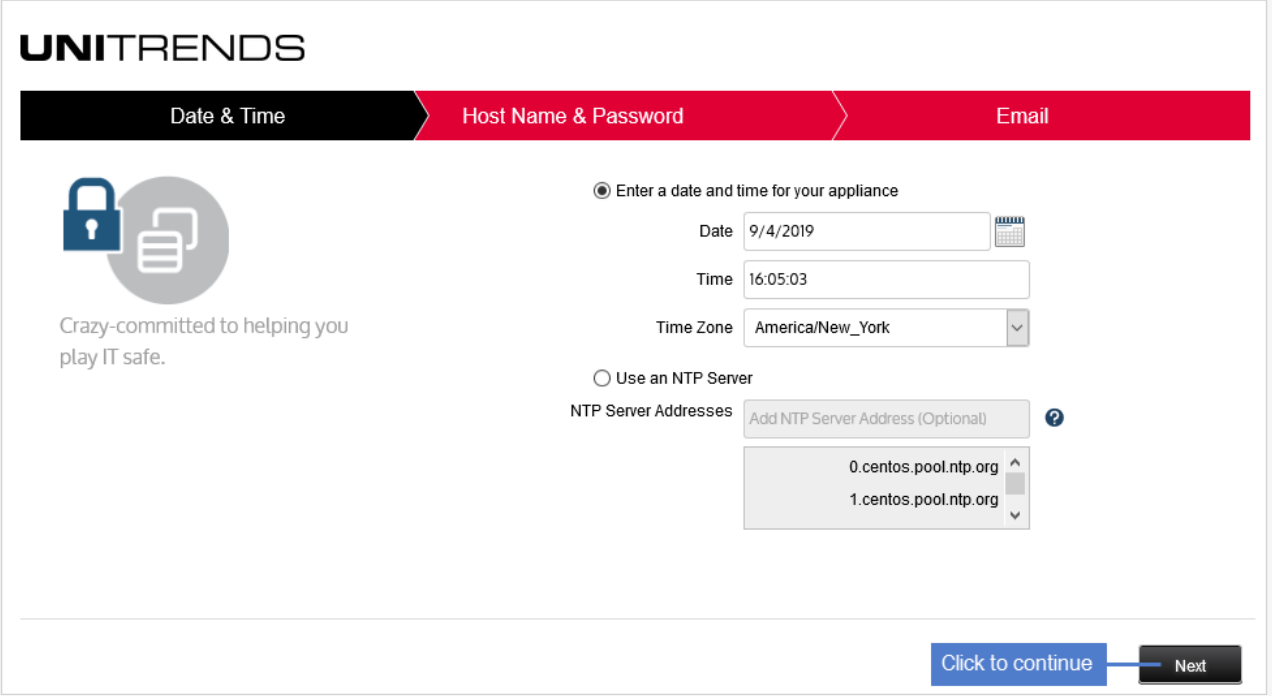


3 Set the appliance date and time by doing one of the following, then click **Next**:

- 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.

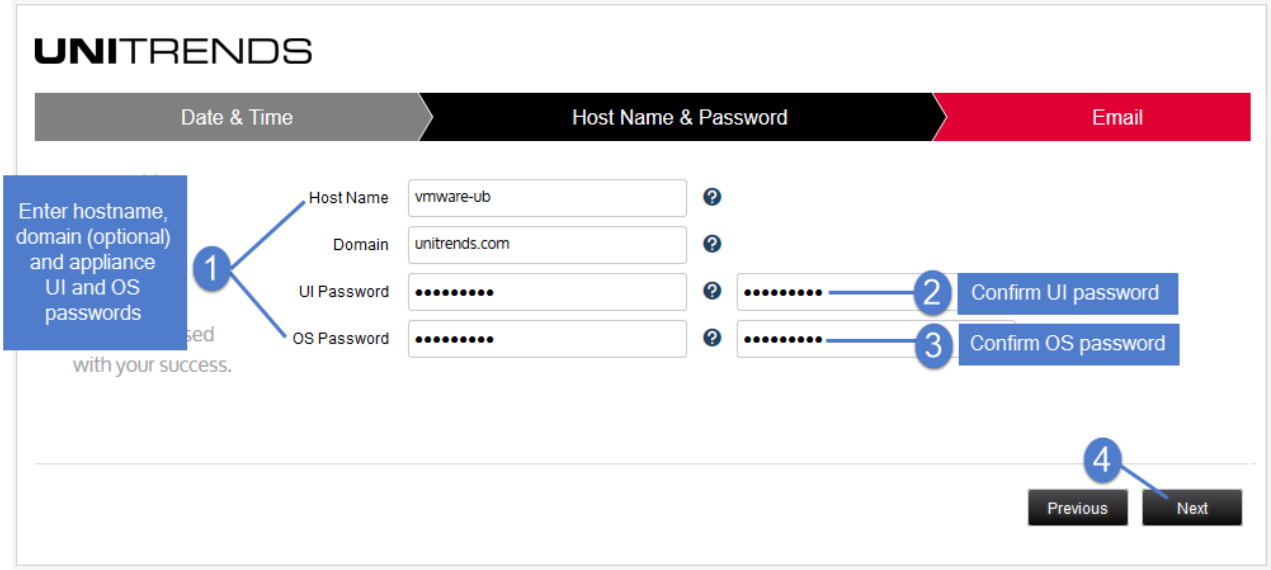


4 Enter a **Host Name**, a **Domain**, and a new **UI Password** for the appliance. If needed, enter a new **OS Password**. Confirm the passwords by entering them again in the fields to the right. Click **Next**.

Notes:

- The hostname can contain only alphanumeric characters, dashes, and underscores.

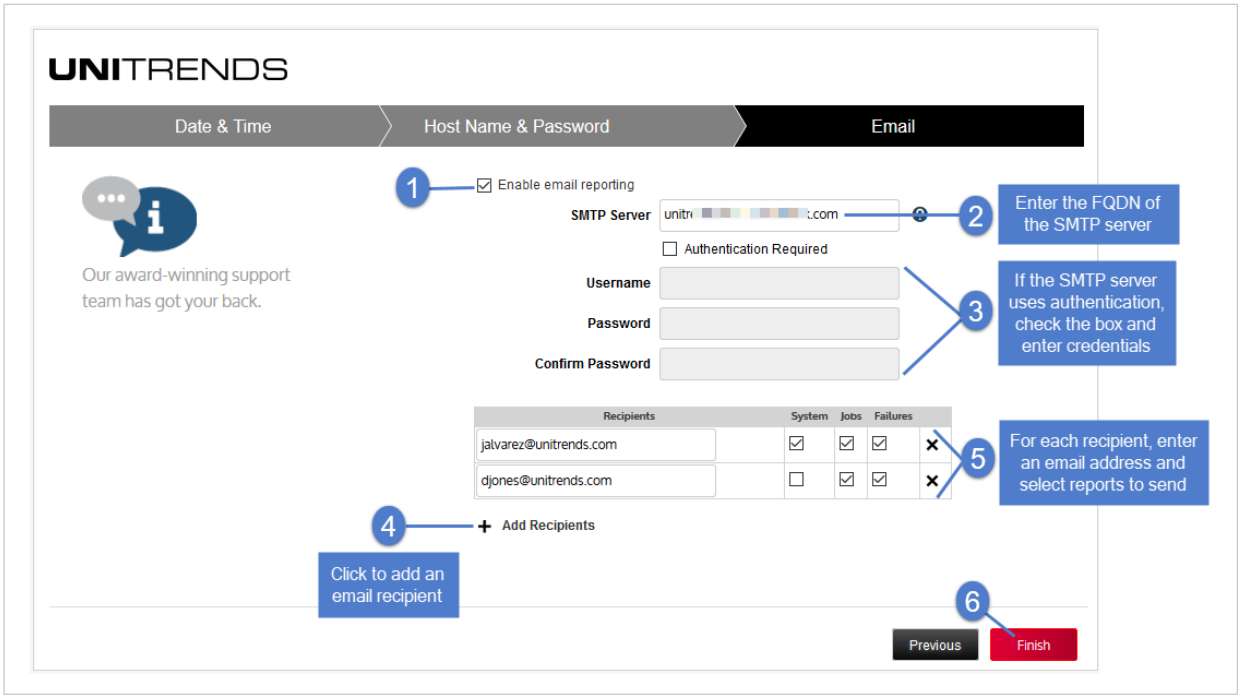
- The appliance has a UI root user and an OS root user. These are separate accounts. Changing the password of one root user account does NOT change the password of the other root user account. The UI root user is used to log in to the appliance UI. The OS root user is used to log in to the appliance console or for command line access.
- If you have already set the OS password, these fields are disabled in the Quick Setup Wizard.
- Passwords cannot contain the word *Unitrend* (case insensitive).
- The OS password must contain 8 or more characters.
- All appliances are deployed with these default UI and OS credentials: user *root*, password *unitrends1*. For appliance security, you must change these passwords in the Quick Setup Wizard. For increased security, ensure that the OS password you enter is different than the UI 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.



5 (Optional) To enable email from the appliance, check **Enable email reporting** and enter the following:

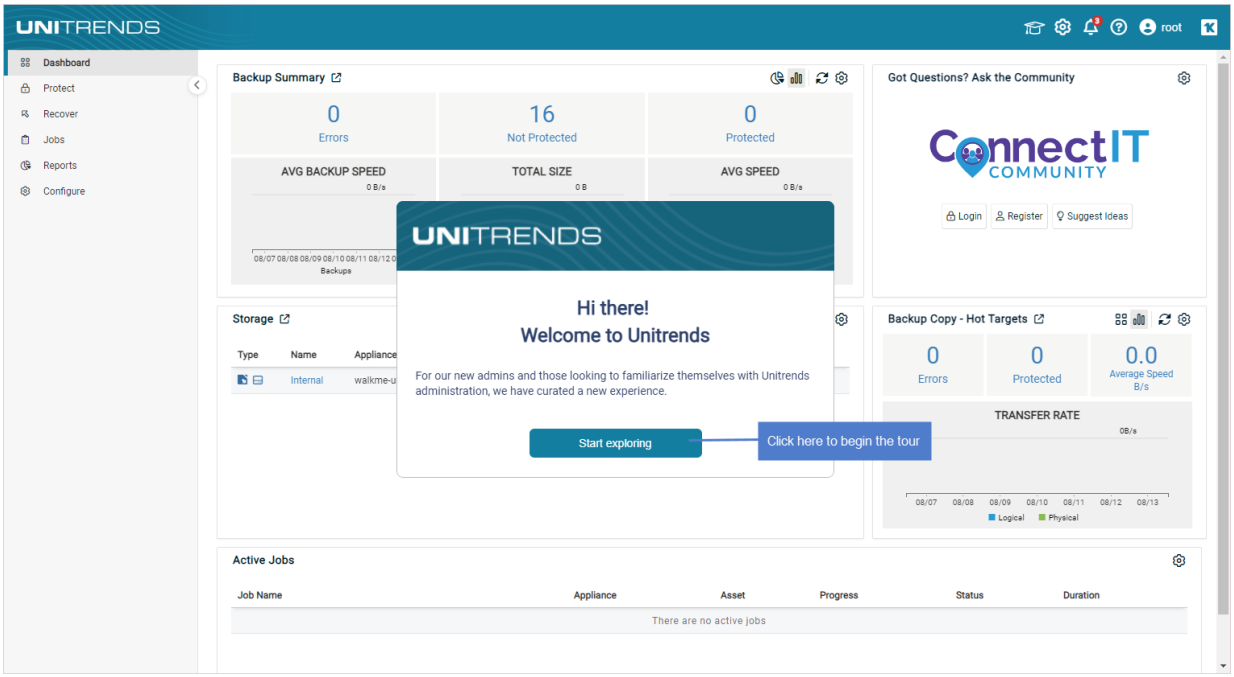
- The fully qualified domain name of the **SMTP server**.
- (If needed) If the SMTP server requires authentication, select **Authentication required** and enter a **Username** and **Password**.
- Click **+ Add Recipients** to add a an email recipient. Enter an email address in the **Recipient** field 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**.



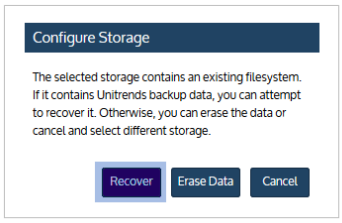
7 Do one of the following:

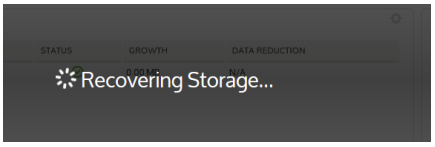
- If you deployed by using new storage for the initial backup storage, the Welcome to Unitrends dialog displays. Click **Start exploring** to view the interactive product tour. Then proceed to the next step in this procedure.



OR

- If you deployed by using storage that contains backups from another Unitrends Backup appliance, click **Recover** to add the backups to the appliance. Then proceed to the next step in this procedure.





8 Do one of the following:

- If you deployed using added VHD(X) disk storage, proceed to "Step 7: (Optional) Modify deduplication settings" on page 51.

OR

- If you deployed using external storage, proceed to "Step 6: Add the initial backup storage device if using external storage directly attached to the Unitrends Backup VM".

Step 6: Add the initial backup storage device if using external storage directly attached to the Unitrends Backup VM

Perform this step only if you are deploying using external SAN or NAS storage connected directly to the Unitrends Backup VM.

IMPORTANT! If you have deployed using added disk storage, do not do this step. The initial backup storage device has already been added to your appliance.

Once you have exposed the share or LUN to the Unitrends Backup VM, you must create the initial backup storage device and configure the appliance to use this storage. Run one of the following procedures from the Unitrends Backup UI to create this initial backup storage:

- "To add the initial backup storage device if using an external LUN"
- "To add the initial backup storage device if using an external NFS share" on page 50
- "To add the initial backup storage device if using an external CIFS share" on page 51

To add the initial backup storage device if using an external LUN

This procedure assumes you have allocated a LUN on the SAN and exposed it to the Unitrends Backup VM.

Notes: If your SAN is configured with CHAP authentication, you must configure CHAP on the appliance before adding the iSCSI storage device. To configure CHAP on the appliance:

1. Log in to the appliance UI.
2. On the **Configure > Appliances** page, select the appliance and click **Edit**.
3. In the Edit Appliance dialog, click **iSCSI CHAP**.
4. Verify that the **Use System CHAP Credentials** box is checked.
5. Enter credentials in the **Username**, **CHAP Password**, and **Confirm CHAP Password** fields, then click **Save**. One set of credentials is used to access all iSCSI targets that have been configured to use CHAP authentication.
   - By default, **Username** contains the appliance's iSCSI qualified name (IQN). It is required that the username and password on the initiator (backup appliance) match those defined on the targets. Modify the Username entry if necessary.
   - The password must be 12-16 characters in length.

To add the iSCSI device:

1. Log in to the appliance UI:
   - Open a browser and connect to your appliance by entering: ***https://<applianceIP>/ui***
   - In the Username field, enter **root**.
   - In the Password field, enter the UI password you specified above in "Step 5: Set up the appliance using the Quick Setup Wizard".
2. On the **Configure > Appliances** page, select your appliance.
3. Click the **Storage** tab below.
4. Select **Add Storage > iSCSI**.
5. Enter a unique **Name** for the storage device. This name cannot contain spaces.
6. Enter the IP address of the SAN storage array in the **Host** field.
7. The default port used for iSCSI communication is 3260. If the LUN is configured to use a different port, enter it in the **Port** field.
8. Click **Scan for targets** to retrieve a list of targets on the remote storage array, then choose one from the list.

   Notes: If you do not see the LUN in the list, go to your SAN manager and check your LUN configuration by doing the following:
   - Verify that you can see the Unitrends Backup appliance in your SAN manager.

- Verify that you have a LUN assigned to the Unitrends Backup appliance with the correct permissions.
- Check with your Storage Administrator for more information.

9 Click **Scan for LUNs** and select one from the list.

Note: If you receive an error indicating CHAP authentication has failed, CHAP has been configured on the target and either CHAP has not been enabled on the Unitrends Backup appliance, or the Unitrends Backup CHAP credentials do not match those of the target.

10 Click **Save**.

11 Proceed to "Step 7: (Optional) Modify deduplication settings" on page 51.

To add the initial backup storage device if using an external NFS share

This procedure assumes you have allocated a share on the NAS and exposed it to the Unitrends Backup VM.

1 Log in to the appliance UI:

- Open a browser and connect to your appliance by entering: ***https://<applianceIP>/ui***
- In the Username field, enter **root**.
- In the Password field, enter the UI password you specified above in "Step 5: Set up the appliance using the Quick Setup Wizard".

2 On the **Configure > Appliances** page, select your appliance.

3 Click the **Storage** tab below.

4 Select **Add Storage > NFS.**

5 Enter the required NFS share information and click **Save**. Descriptions of each field are given here:

Field	Description
Name	Name of the storage. Cannot contain spaces.
Host	IP address or hostname of the NAS share.
Port	Contains the default NFS port. To use a custom port, enter that port number.
Share Name	Enter the full directory pathname of the NAS share. Do not use leading or ending slashes.
Username (optional)	If the share is configured for authentication, enter the domain username as user@domain.com.
Password (optional)	If the share is configured for authentication, enter the password.

6 Proceed to "(Optional) Modify deduplication settings".

To add the initial backup storage device if using an external CIFS share

This procedure assumes you have allocated a share on the NAS and exposed it to the Unitrends Backup VM.

1 Log in to the appliance UI:

- Open a browser and connect to your appliance by entering: ***https://<applianceIP>/ui***
- In the Username field, enter **root**.
- In the Password field, enter the UI password you specified above in "Step 5: Set up the appliance using the Quick Setup Wizard".

2 On the **Configure > Appliances** page, select your appliance.

3 Click the **Storage** tab below.

4 Select **Add Storage > CIFS**.

5 Enter the required CIFS share information and click **Save**. Descriptions of each field are given here:

Field	Description
Name	Name of the storage. Cannot contain spaces.
Host	IP address or hostname of the NAS share.
Port	Contains the default CIFS port. To use a custom port, enter that port number.
Share Name	Enter the full directory pathname of the NAS share. Do not use leading or ending slashes.
Username (optional)	If the share is configured for authentication, enter the domain username as user@domain.com.
Password (optional)	If the share is configured for authentication, enter the password.

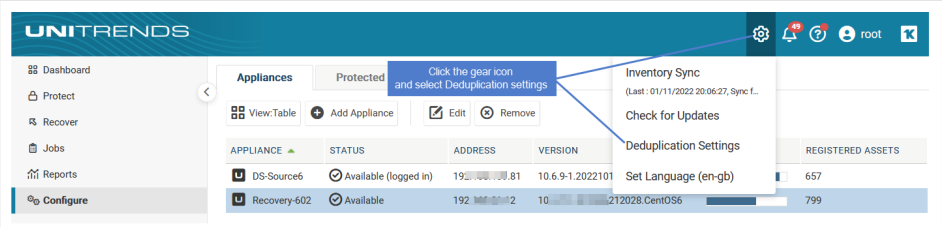
6 Proceed to "Step 7: (Optional) Modify deduplication settings".

Step 7: (Optional) Modify deduplication settings

Deduplication is a data compression technique that eliminates duplicate data blocks. To yield fastest performance, the appliance is configured to use the Level 1 deduplication setting. You can opt to modify this setting to increase on-appliance retention. Keep in mind that increasing the deduplication level decreases job speed.

To modify the deduplication level

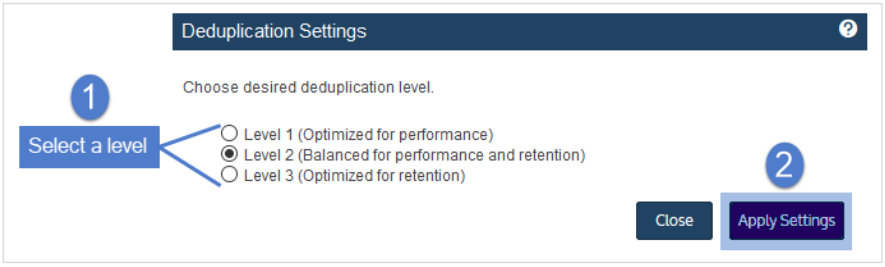
1 From the Global options at the top of the UI, select **Options > Deduplication Settings**.



2 Select one of the following deduplication settings:

- Level 1 — Use this setting to optimize performance.
- Level 2 — Use this setting to balance performance and on-appliance retention.
- Level 3 — Use this setting to optimize retention.

3 Click **Apply Settings**.



Step 8: Register and license the Unitrends Backup appliance

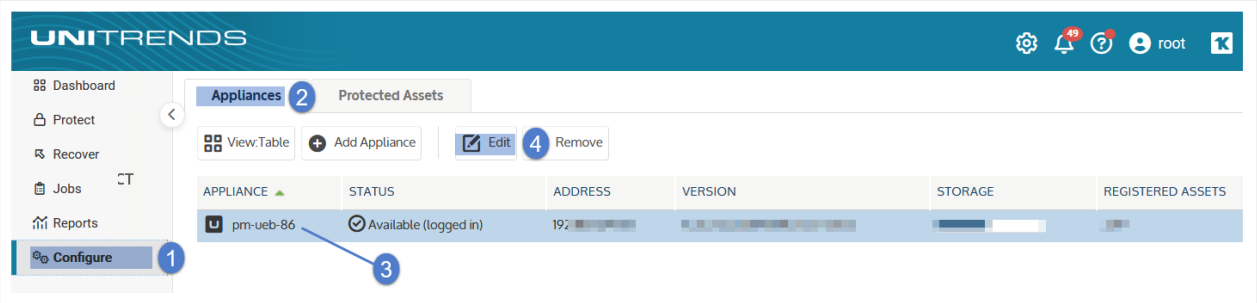
Your appliance is now configured and you can begin using it to protect your environment. For details, see the Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup.

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

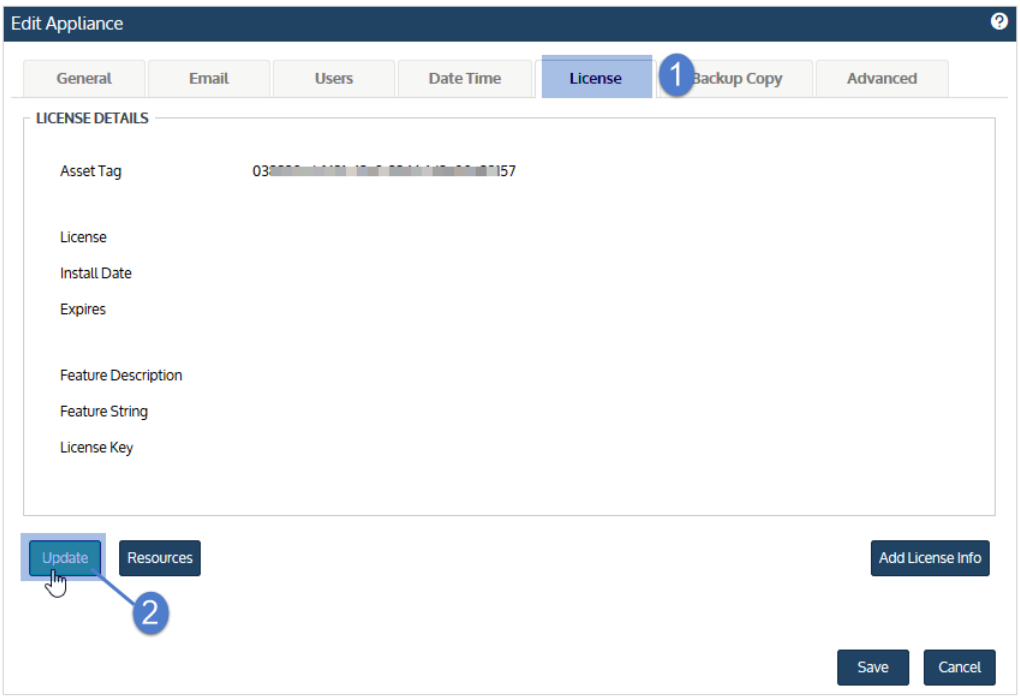
Each appliance requires an activation code and license key. Use the procedures below to register and license the appliance:

To register a Unitrends Backup appliance

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

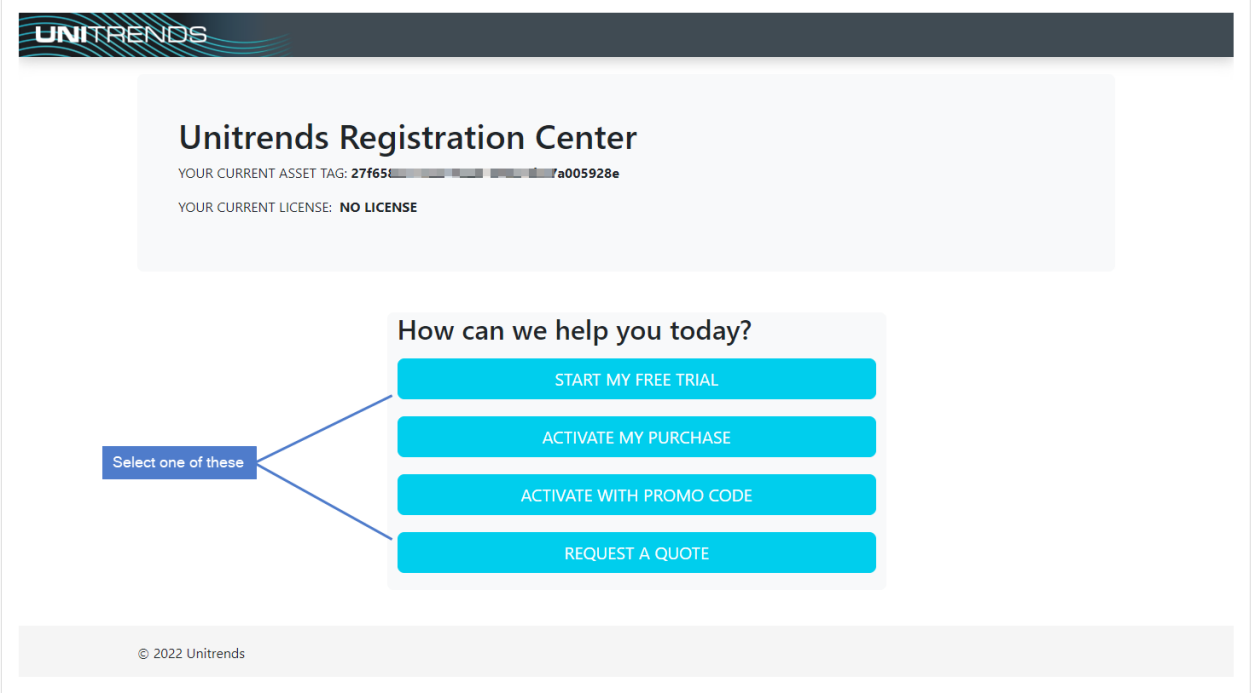


2 Select the **License** tab and click **Update**. The Registration Center displays.



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. You 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.



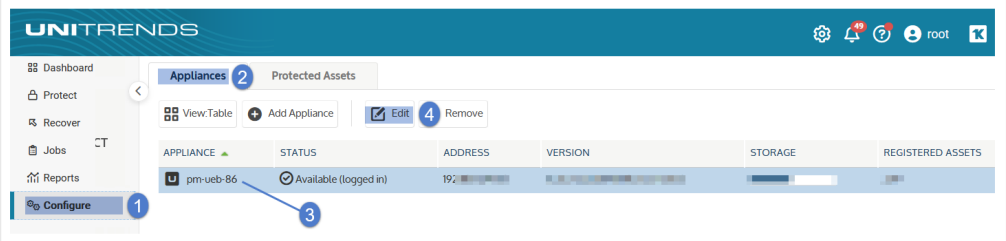
4 Complete and submit the applicable form.

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.

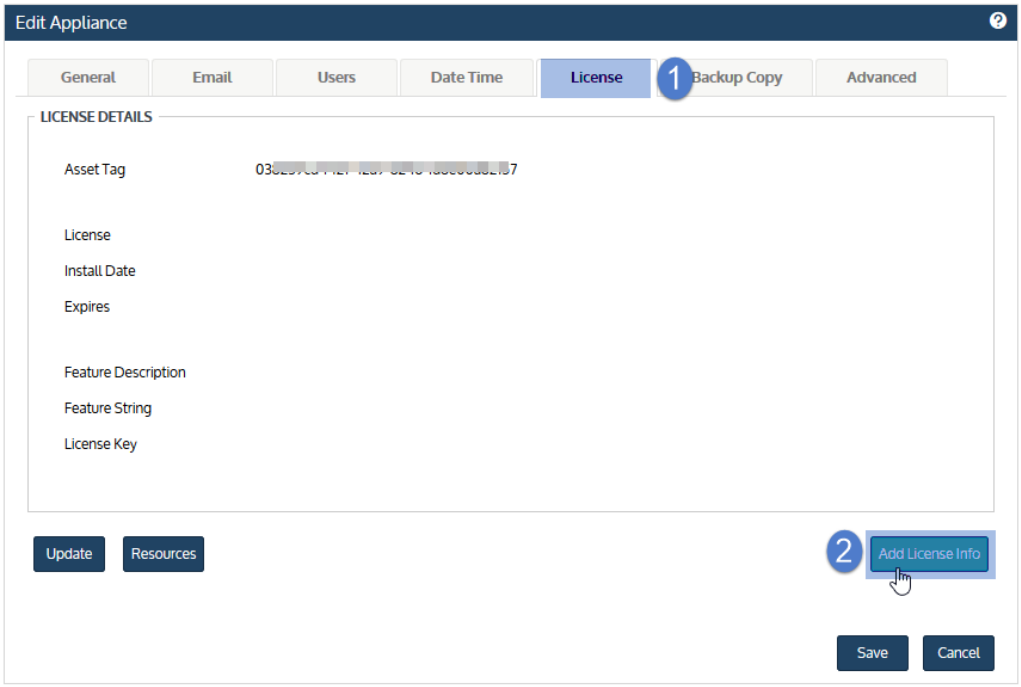
To license a Unitrends Backup appliance

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

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

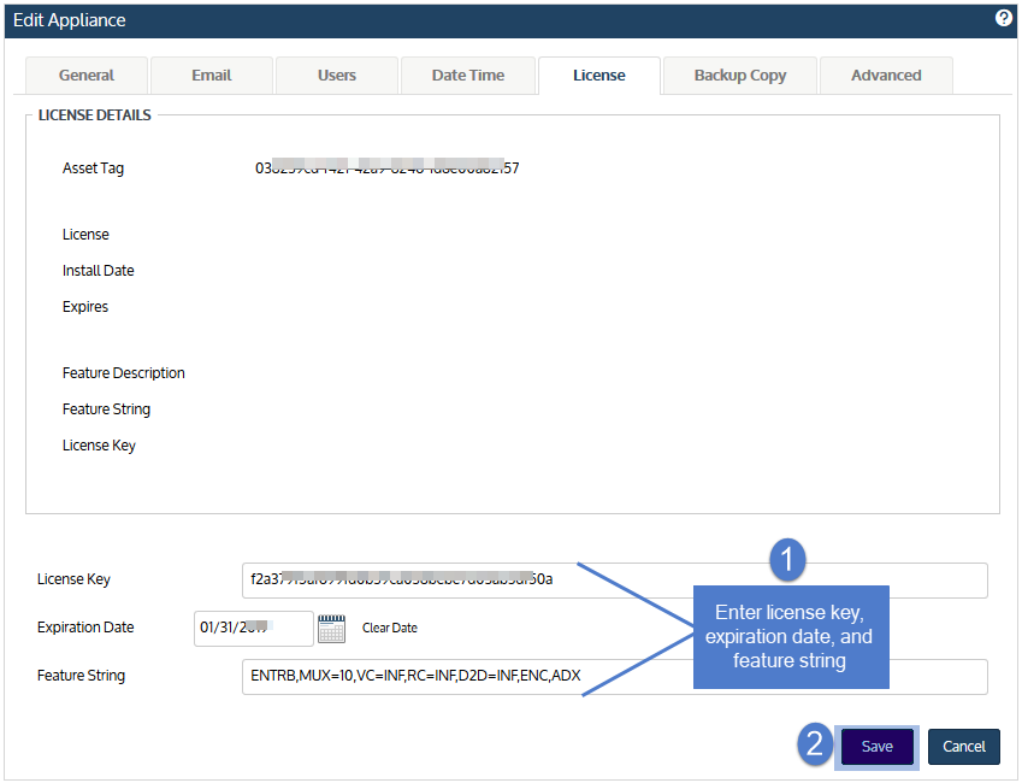


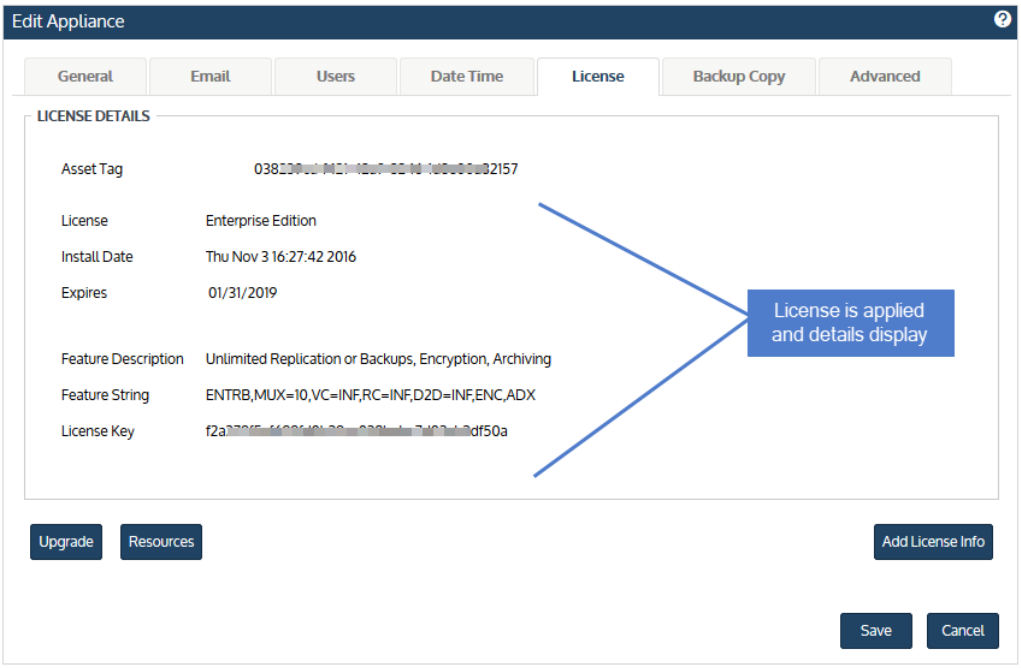
2 Select the **License** tab and click **Add License Info**.



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

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





Step 9: Start protecting your environment

Deployment is complete and you can get started protecting your environment. For details, see the Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup.