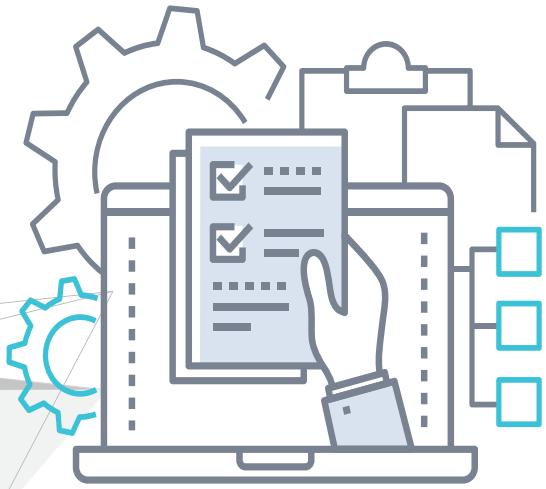
UNITRENDS

Deployment Guide for Unitrends Backup on Citrix XenServer

Release 10.5.2 | Document Version 5.08022023

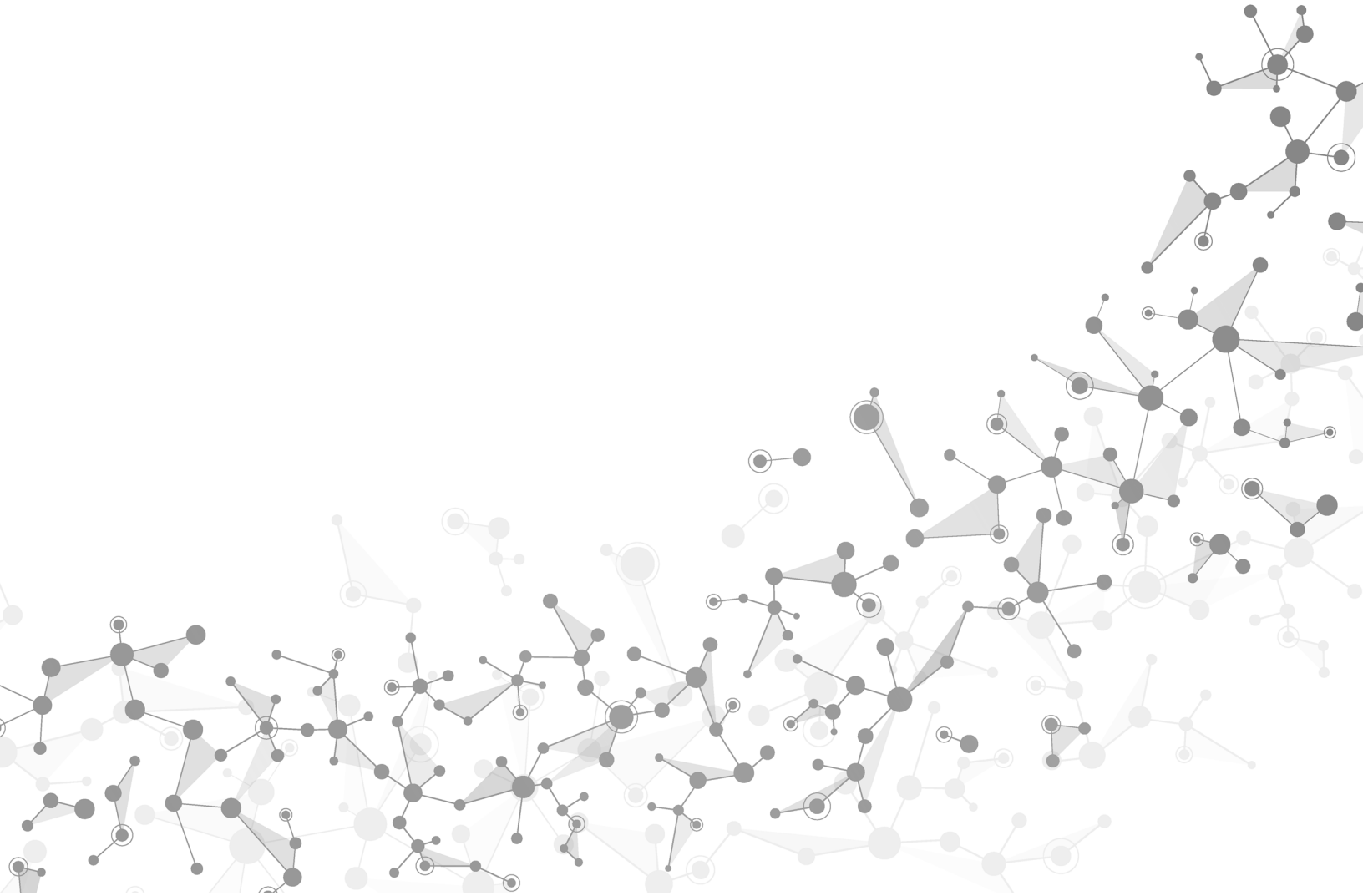


Copyright

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 Unitrends Backup appliance.

This deployment guide includes instructions for deploying using new storage and for deploying using storage that contains existing backup data from another Unitrends Backup 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.

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

Term	Definition
Added disk	VHD virtual disk storage created by deploying the Unitrends Backup XVA file or by using the XenServer host. A VHD can be created from direct attached storage (DAS) that is internal to the XenServer host, or from external SAN or NAS storage that is connected to the XenServer 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.
External storage	SAN or NAS storage that is connected directly to the Unitrends Backup VM over the iSCSI, CIFS, or NFS protocol.
Host	XenServer machine that houses the Unitrends Backup VM. Also called a *hypervisor*.
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 300GB - 64TB in size.
Initial disk	100GB disk used to create the Unitrends Backup VM. While installing the XVA, you select a Storage Repository on the XenServer host that the installer uses to create this disk.
XVA file	Unitrends XVA file used to deploy the Unitrends Backup VM on your XenServer host.

Term	Definition
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 by deploying the Unitrends Backup XVA file.

Chapter 2: Requirements and Considerations

Before deploying your Unitrends Backup appliance, verify that 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. Verify the following requirements for the hypervisor on which you are deploying the Unitrends Backup VM:

Requirement	Description
Hypervisor version	You can deploy Unitrends Backup on Citrix XenServer versions 6.5, 7.0, 7.1, 7.2, and 7.3.

Requirement	Description
Host-level protection	Host-level backups protect virtual machines by leveraging hypervisor snapshots. You do not need to install a Unitrends agent on a VM to run host-level backups. When you add a virtual host to the Unitrends Backup appliance, its VMs are discovered and available for host-level protection. The following requirements and limitations apply: • Host-level protection is supported for VMs hosted on the following: – Citrix XenServer versions 6.2, 6.5, 7.0, 7.1, 7.2, and 7.3. To protect VMs on older versions, you must either upgrade to a supported Citrix XenServer version or install the applicable agents on the VMs and run asset-level backups. – A Hyper-V host that is a supported version listed in the Compatibility and Interoperability Matrix. – A VMware vCenter or ESXi host that is a supported version listed in the Compatibility and Interoperability Matrix. • Only one XenServer host can be added to the Unitrends Backup appliance. • The XenServer host must be one of the following: – A XenServer pool master host meeting both of these criteria: – The Unitrends Backup VM resides either on the pool master host itself or on one of the pool master's slave hosts. – The Unitrends Backup VM has been granted access to the shared storage used by the pool master host. – A stand-alone XenServer host where the Unitrends Backup VM resides.

See the following for considerations by XenServer host type:

Host type	Description
XenServer pool master host	By adding the pool master host to the Unitrends Backup appliance, you can protect the following: • VMs on the host where the Unitrends Backup VM resides. This can be the pool master host itself or one of the pool master's slave hosts. • VMs that reside on shared storage in the resource pool.
Stand-alone XenServer host	By adding the XenServer host to the appliance, you can protect its hosted VMs.

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 if there is a firewall between your appliance and its protected assets, for connectivity to the Internet, and for connectivity to any hot backup copy target. See the following for details:

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

Connectivity between the appliance and its protected assets

Task	Port, Protocol, and Rule	Hostname and IP Address	Notes
Protect assets that are separated from the appliance by a firewall.	1743: • TCP • Outbound from appliance • Inbound from protected asset 1745: • TCP • Outbound from protected asset • Inbound from appliance	Appliance hostname and IP Asset hostname and IP	If a firewall exists between the appliance and the assets (machines) you wish to protect, open these ports to enable communication and data transfer between the appliance and assets. You must also enter 1745 in the appliance master ini file. To do this: 1 In the appliance UI, select **Configure > Appliances > Edit > Advanced > General Configuration**. 2 In the Configuration Options Section, select **data** in the Name column. 3 In the Edit Settings dialog, enter **1745** in the Value field and click **Save**.
Linux assets using the secure agent pairing feature (running agent version 10.7.5+)	888: • TCP • Inbound from protected asset • Outbound from appliance	Appliance hostname and IP Asset hostname and IP	888 is the port used for secure agent pairing. If a firewall exists between the appliance and the asset (machine) you wish to protect, you must open port 888 so that a secure pairing can be established between the appliance and Linux agent.

Task	Port, Protocol, and Rule	Hostname and IP Address	Notes
Windows assets using the secure agent pairing feature (running agent version 10.6.6+)			888 is the port used for secure agent pairing. If a firewall exists between the appliance and the asset (machine) you wish to protect, firewall rules are created automatically. Ensure that port 888 is not in use on your protected Windows asset.
Windows assets protected with image-level backups	443: • TCP • Inbound from protected asset	Appliance hostname and IP Asset hostname and IP	

Connectivity between the appliance and the Internet

Task	Port, Protocol, and Rule	Hostname and IP Address	Notes
Product Updates	20 and 21: • FTP • Outbound 80: • HTTP • Outbound	repo.unitrends.com ftp.unitrends.com	• repo.unitrends.com is used by the Unitrends appliance to perform software updates. • ftp.unitrends.com is used by Support to install patches and updates.
Remote Support	443: • HTTPS • Outbound	support-itivity.unitrends.com 74.202.224.68	Used for opening a remote tunnel to the Unitrends support team.
Proactive Monitoring	161 and 162: • TCP and UDP • Outbound	notifications.unitrends.com 104.130.228.89	Used for SNMP trap collection for all proactive monitoring.

Connectivity between the appliance and a hot backup copy target

Task	Port, Protocol, and Rule	Hostname and IP Address	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. • TCP and UDP • Outbound 443: • TCP • Outbound	Target appliance hostname and IP For Unitrends Cloud, the public-facing IP address provided by Unitrends.	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:

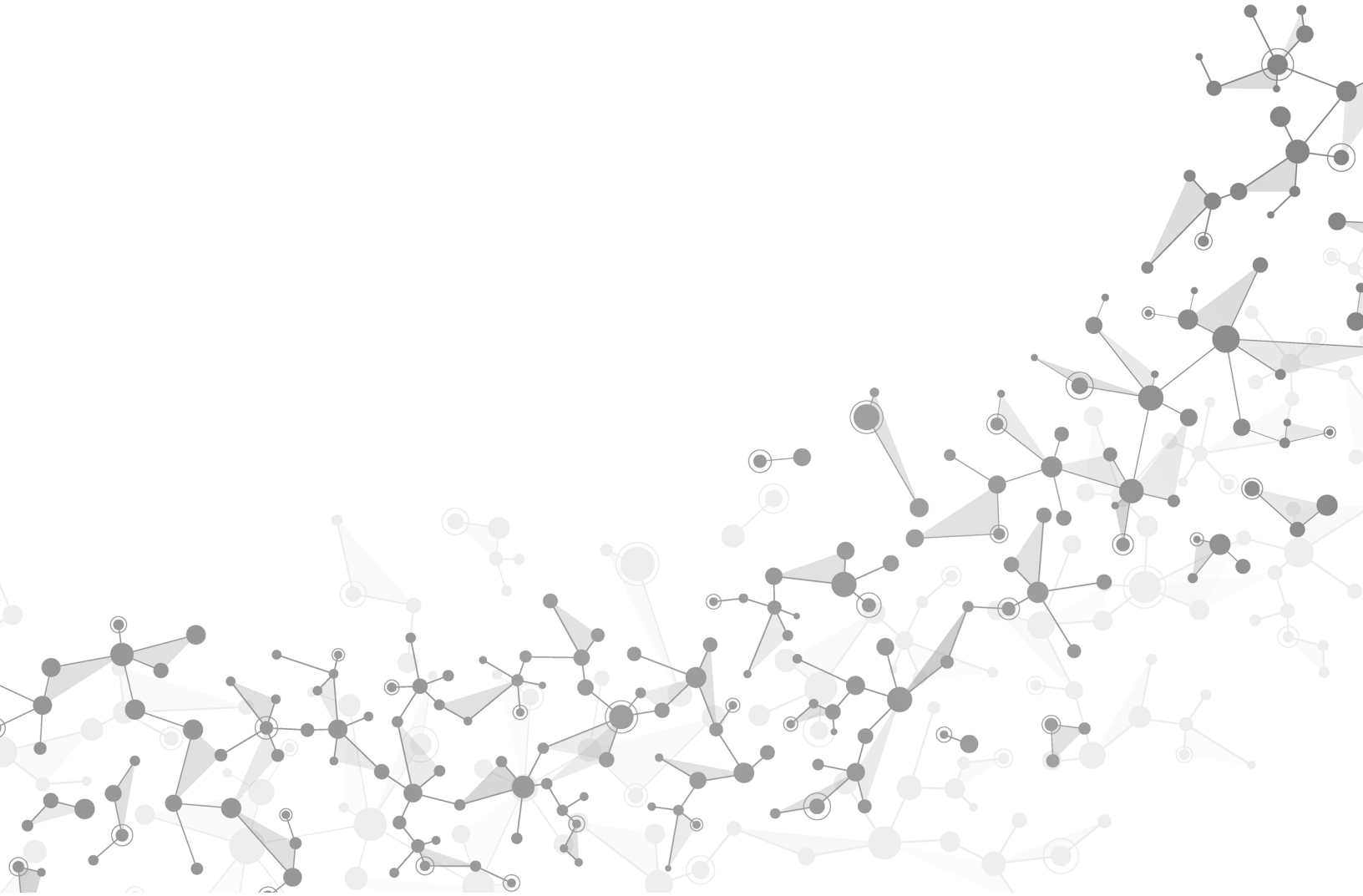
Note: These are the minimum resources required to deploy and begin using the Unitrends Backup appliance. As you add jobs and storage, be sure to monitor the system and add resources as needed over the lifetime of the appliance.

- A minimum of two virtual processors (CPUs).
- A minimum of 8GB of RAM.
- 100GB of space for the VM's initial disk.
- At least 300GB for the VM image and the initial backup storage.

Note: The VHD disk used for the initial backup storage also houses the Unitrends Backup VM image. This image consumes approximately 100GB of space. If you add a 300GB VHD, roughly 200GB will be available for backup storage. Be sure to account for this when adding the initial backup storage.

- VM disks cannot be attached as *Read Only*. Be sure to use the *Read Only* = *No* setting when attaching disks.

This page is intentionally left blank.



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 disks created by using the XenServer host. 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. Added disks cannot be attached as *Read Only*. Be sure to use the *Read Only* = *No* setting when attaching disks.
- 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 300GB for the VM image and 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.

Note: The VHD disk used for the initial backup storage also houses the Unitrends Backup VM image. This image consumes approximately 100GB of space. If you add a 300GB VHD, roughly 200GB will be available for backup storage. Be sure to account for this when adding the initial backup storage.

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.

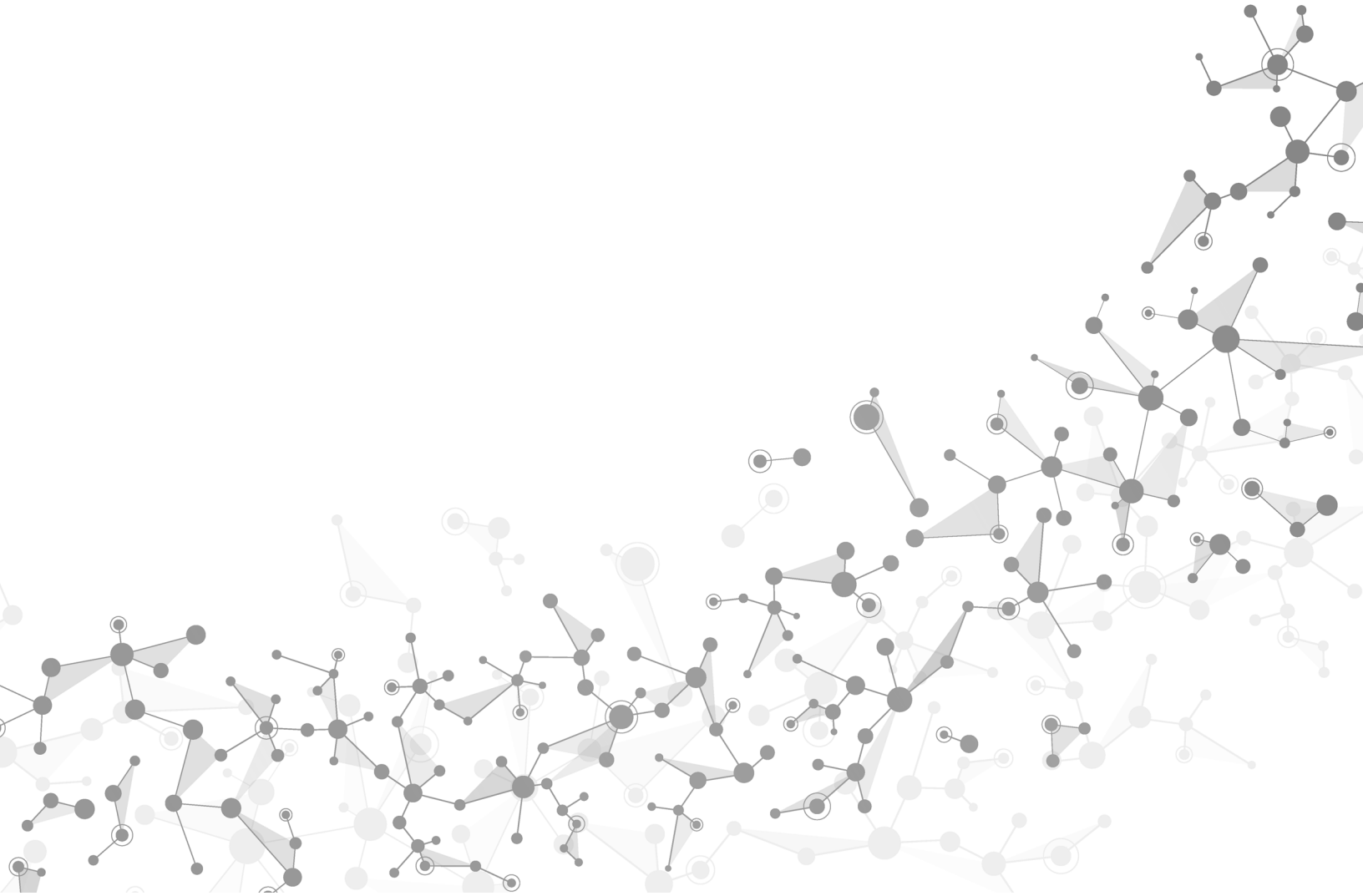
Unitrends Backup Storage Component	Recommendations
All	These recommendations apply to all Unitrends Backup storage (initial disk, initial backup storage, and additional backup storage): • Unitrends strongly recommends using hypervisor-certified storage arrays on Citrix XenServer's hardware certified 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. • Unitrends recommends using DAS, internal to the hypervisor, or to leverage SAN or NAS storage that you expose to the hypervisor. – You can create VHDs on storage internal to the hypervisor (DAS). – You can expose a SAN or NAS to the hypervisor and use the hypervisor to create a Storage Repository from this storage. You can then select this Storage Repository to create VHDs. – For optimal performance and scalability, add VHD 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.

Unitrends Backup Storage Component	Recommendations
Initial disk	You create the Unitrends Backup VM by deploying the XVA file. During deployment (in "Step 3: Deploy the Unitrends Backup VM" on page 23), you make various selections within your hypervisor, including the Storage Repository 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 300GB for the VM image and the initial backup storage (see "Step 4: Attach backup storage" on page 28). The following requirements and recommendations apply: **Note:** The VHD disk used for the initial backup storage also houses the Unitrends Backup VM image. This image consumes approximately 100GB of space. If you add a 300GB VHD, roughly 200GB will be available for backup storage. Be sure to account for this when adding the initial backup storage. • For disaster recovery, it is important to know which VHD, 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.

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 VHDs, 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 300GB 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 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 that uses the same Storage Repository 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 Storage Repository that was used for the initial backup storage and create a VHD using this Storage Repository. Once the VHD 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 Storage Repository and VHD 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 deploy an XVA file. 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. Step 6: is required only if you are using external storage that is connected directly to the Unitrends Backup VM.

Step 1: Set up storage on the hypervisor

You will select a Storage Repository to create the Unitrends Backup VM's initial VHD disk (in "Step 3: Deploy the Unitrends Backup VM" on page 23) and select a Storage Repository to add the initial backup storage (in "Step 4: Attach backup storage" on page 28). Verify that the hypervisor has enough storage available:

- 100GB for the Unitrends Backup VM's initial disk.
- At least 300GB for the VM image and the initial backup storage.

Note: The VHD disk used for the initial backup storage also houses the Unitrends Backup VM image. This image consumes approximately 100GB of space. If you add a 300GB VHD, roughly 200GB will be available for backup storage. Be sure to account for this when adding the initial backup storage.

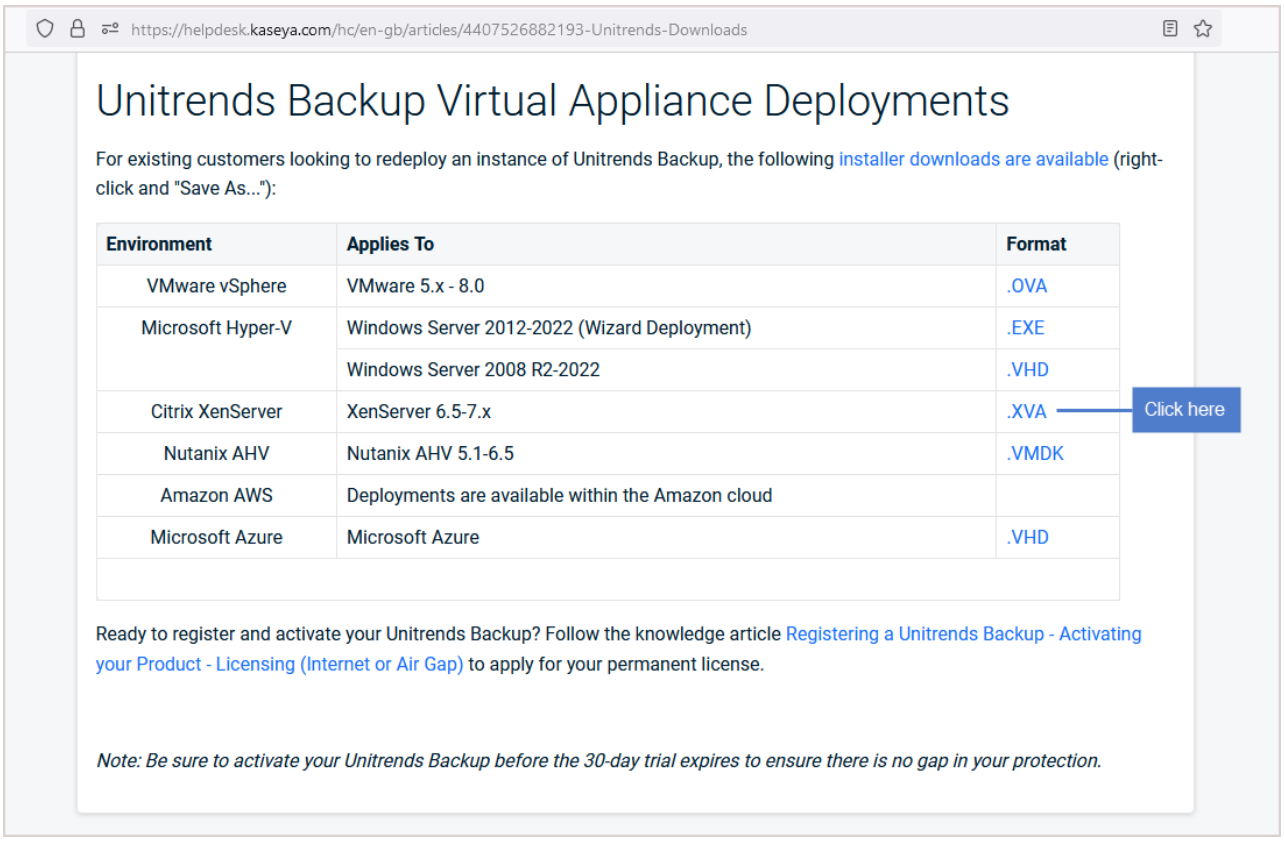
If necessary, add storage. Storage options are described in the following table. For more on storage, see "Determining your Storage Strategy" on page 15.

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 initial backup storage. VM disks cannot be attached as *Read Only*. Be sure to use the *Read Only* = *No* setting when attaching disks. To use external storage (rather than DAS), use the hypervisor to add the SAN or NAS and to create the associated Storage Repository.
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 Storage Repository.
Deploy using storage containing backups from another Unitrends Backup appliance	Verify that the hypervisor has enough storage to create the initial disk. You will add the storage that contains backups in "Step 4: Attach backup storage" on page 28.

Step 2: Download the Unitrends Backup XVA

An XVA file deploys the Unitrends Backup VM. To download the XVA:

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 **.XVA** link in the Citrix XenServer row.



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.

To deploy the Unitrends Backup VM on a Citrix XenServer

1. From the machine on which you saved the Unitrends Backup OVA file, access your XenServer host using XenCenter.
2. Select **File > Import...**.
3. Browse to the extraction location, select **Xen-UB-*version*.xva** and click **Open**. Click **Next**.
4. Select the XenServer host on which the Unitrends Backup VM will be created. Click **Next**.
5. Select the Storage Repository that will be used to create the Unitrends Backup VM. Click **Import**.
6. On the Networking screen, select the virtual network you want to use to connect to the Unitrends Backup VM. Click **Next**.
7. Check the **Start VM(s) after import** box. Click **Next**.
8. When deployment completes, click **Finish** to exit the wizard.

Note: To validate the integrity of the download, a checksum match is performed. If you see a message indicating this verification failed, delete any files that were created by the install process, download the XVA file again, and start a fresh installation.

9 Do one of the following:

- If the VM's virtual network has DHCP available, proceed to "Step 4: Attach backup storage" on page 28.
- 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".

Note: If you will be using the appliance as a hot backup copy target, you must assign a static IP address. Use the procedure "To set up the appliance with a static IP address" on page 24.

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 In XenCenter, access the console interface for the Unitrends Backup VM.

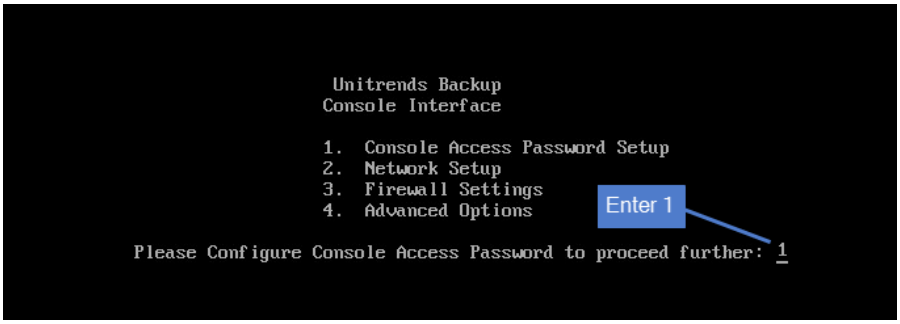
Note: The Unitrends Backup VM must be turned on. If necessary, right-click the VM and select **Start**.

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.



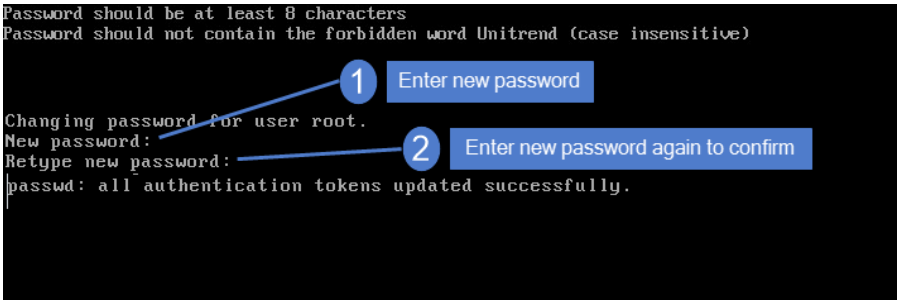
3 To change the direct console password, enter a new password, then enter the password again to confirm.

Notes:

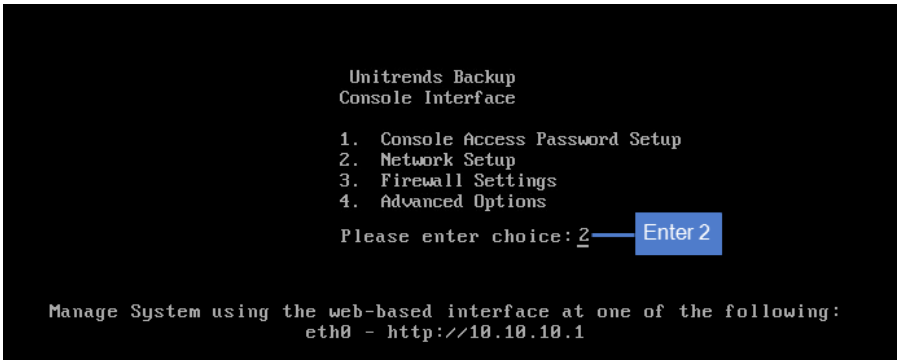
- This is the root operating system password that accesses the console. This password does not access the UI. (You will change the UI password in "Step 5: Set up the appliance using the Quick Setup Wizard" on

page 30.)

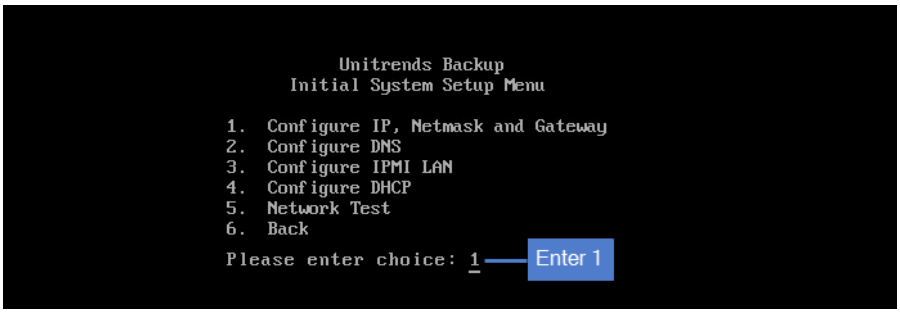
- All appliances are deployed with these default operating systems credentials: user *root*, password *unitrends1*. For appliance security, you must change this password.



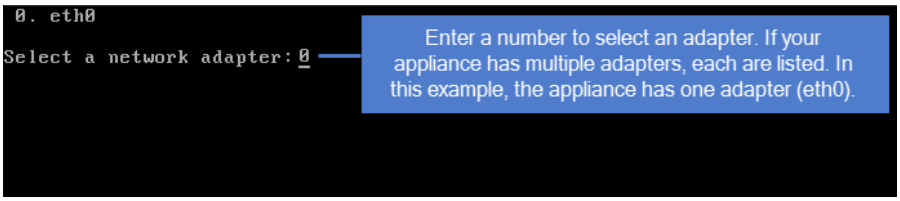
4 On the Console Interface screen, enter **2** in the **Please enter choice** field.



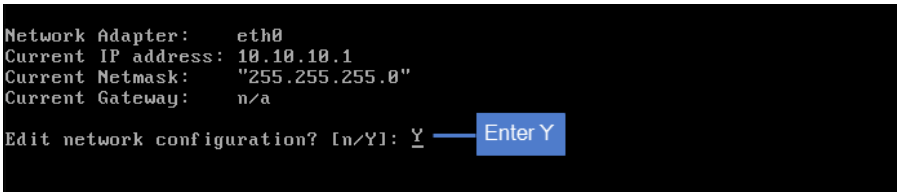
5 On the Initial System Setup Menu screen, enter **1** in the **Please enter choice** field.

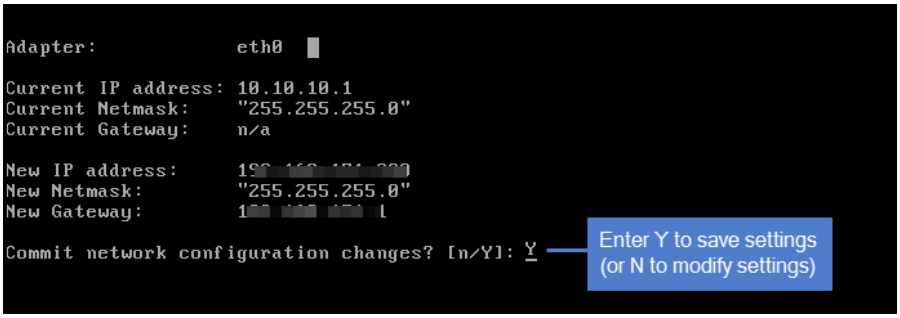


6 Enter a number in the **Select a network adapter** field. For example, enter **0** to select *eth0*.

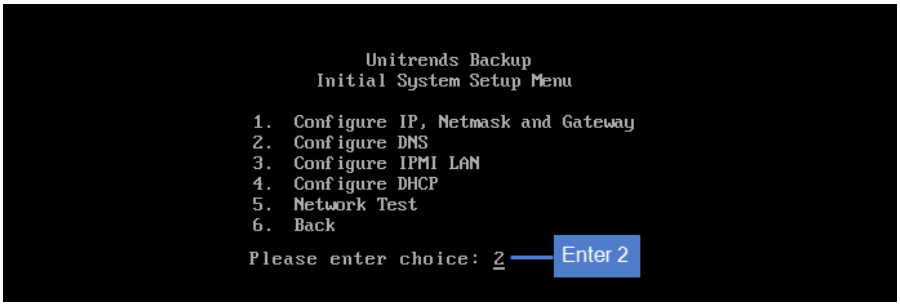


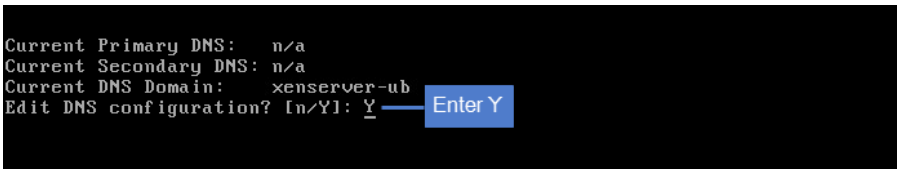
7 Enter **Y** in the **Edit network configuration** field. Then enter an **IP address**, **Netmask**, and **Gateway**. Review the settings and enter **Y** to save.

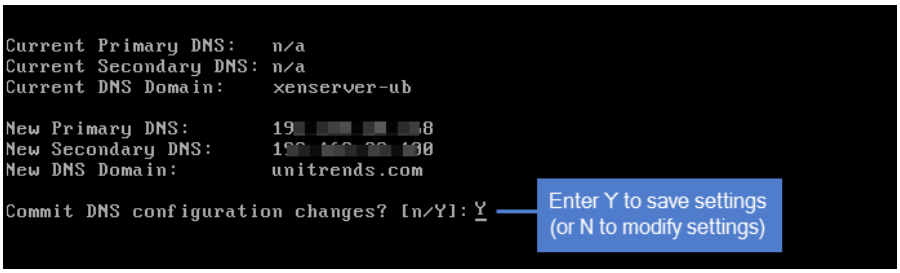




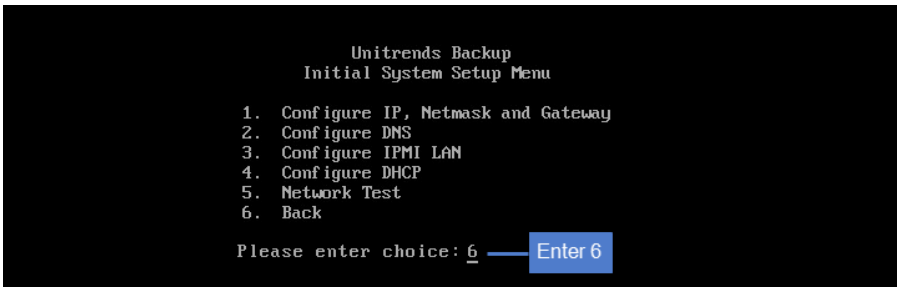
8 To configure DNS settings, enter **2**, then enter **Y** to edit. Enter the **Primary DNS** IP address, a **Secondary DNS** IP (optional), and a **DNS Domain**. Review the settings and enter **Y** to save.







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



10 Exit the VM console.

11 Proceed to "Step 4: Attach backup storage".

Step 4: Attach backup storage

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.

Instructions for attaching storage vary depending on 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" on page 28
- "Attaching storage that contains backups from another appliance" on page 28

Attaching new backup storage

For new backup storage, you can use added disk storage (DAS or external storage attached to the host) or external storage attached directly to the Unitrends Backup VM. VM disks cannot be attached as *Read Only*. Be sure to use the *Read Only* = *No* setting when attaching disks. The initial disk is added to an IDE controller, but for optimal performance and scalability, you should add all additional disks to SCSI controllers. Do one of the following:

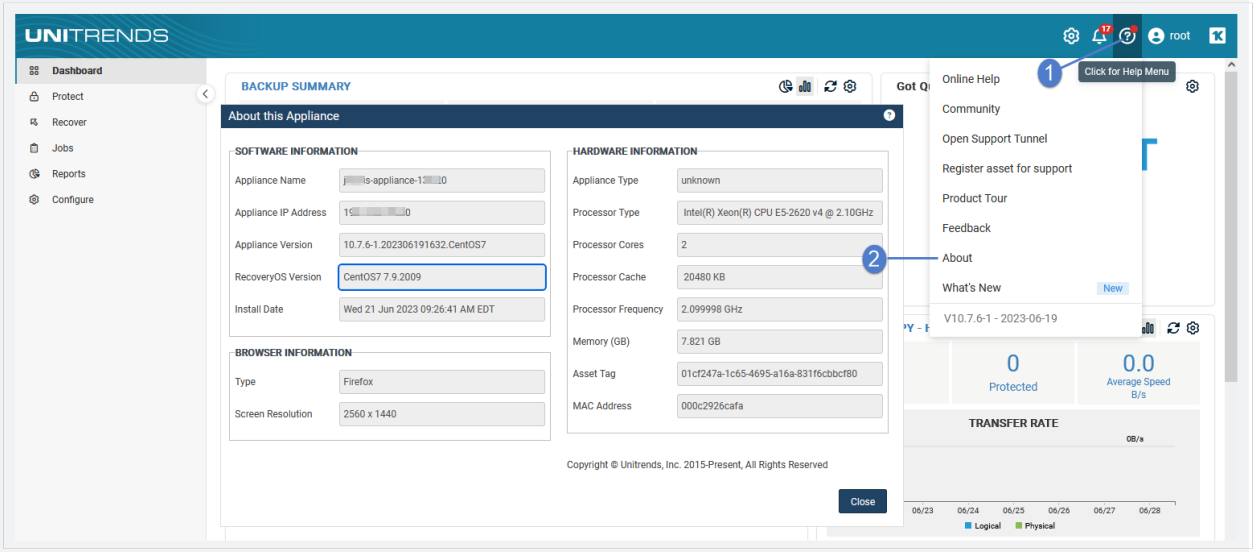
- **Added disk storage attached to the host** — Add a VHD to the Unitrends Backup VM by using the XenServer host. The appliance automatically uses the first VHD disk added to the Unitrends Backup VM as the initial backup storage. Once you have added the VHD, proceed to "Step 5: Set up the appliance using the Quick Setup Wizard" on page 30.
- **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 30.

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" on page 30. If you add 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. To check the appliance Recovery OS version, click on **? > About**:



Instructions for attaching storage that contains Unitrends backups vary by whether the storage is attached directly to the original VM or attached through the hypervisor. Do one of the following:

- **Backup data on disks that are attached to the original Unitrends Backup VM through the hypervisor** — If your backup data resides on VHD disks, you must attach the VHD disks to the new Unitrends Backup VM by using the XenServer host before setting up the appliance.

  IMPORTANT!

  - Be sure to attach the VHD disk that was used as the initial backup storage first (before adding any other VHD disks). Adding the wrong VHD disk first yields undesirable results. The appliance automatically uses the first VHD disk you attach as the initial backup storage. The appliance then recognizes all other attached disks and can access all existing backup data.
  - When adding the disk through the hypervisor, be sure that the newly added disk has read/write access. For details, see Mount errors when doing stateless recovery on a Xen UB.

  After attaching all disks that contain existing backup data, proceed to "Step 5: Set up the appliance using the Quick Setup Wizard" on page 30.

- **Backup data on external storage that is connected directly to the 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".

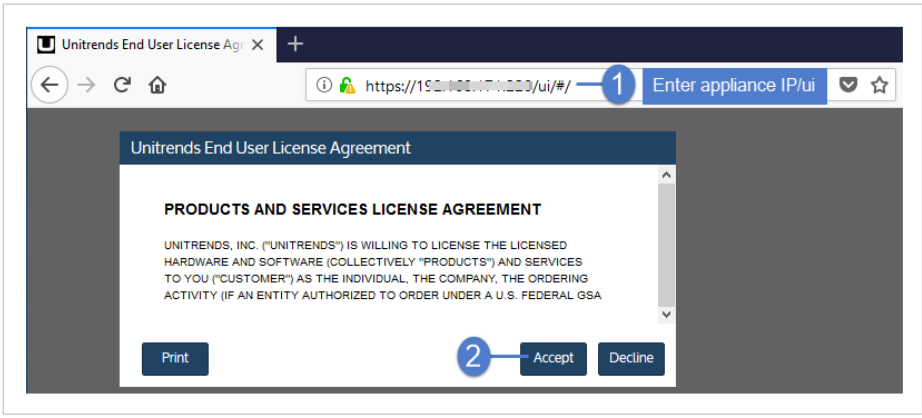
Step 5: Set up the appliance using the Quick Setup Wizard

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:

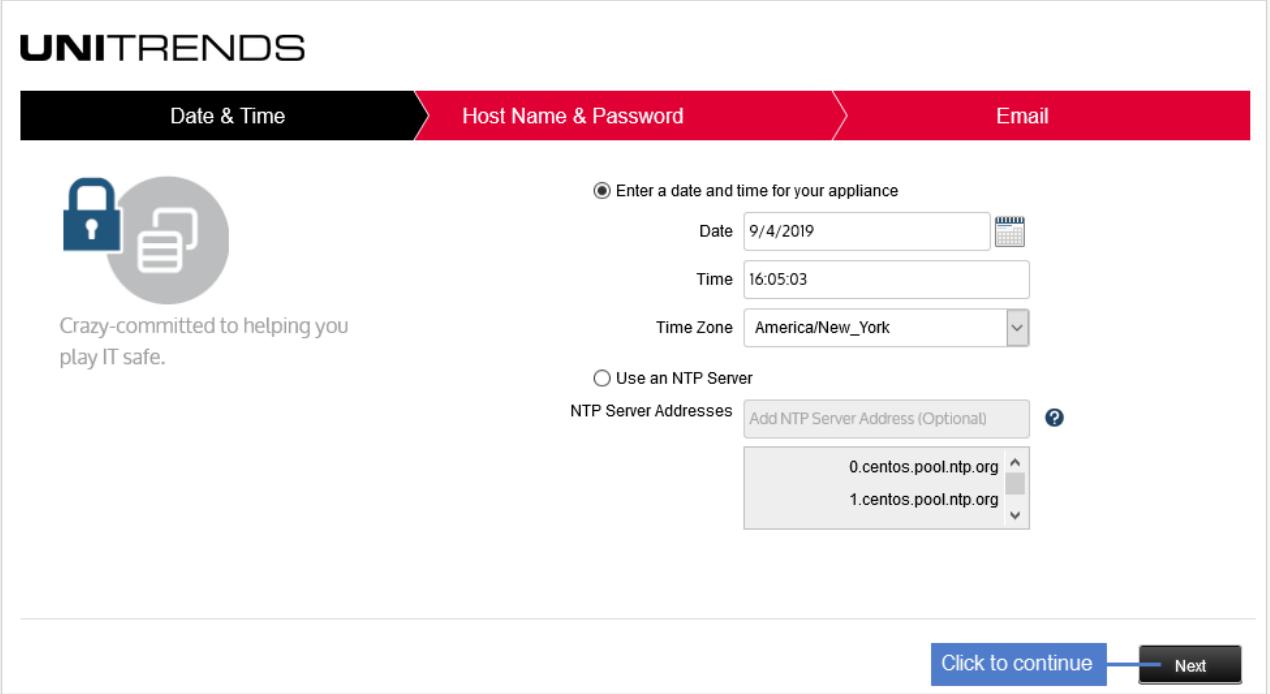
1. Open a browser and connect to your appliance by entering: ***https://<applianceIP>/ui***. For example: *https://10.10.10.1/ui*.
2. Click **Accept** to accept the license agreement.



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

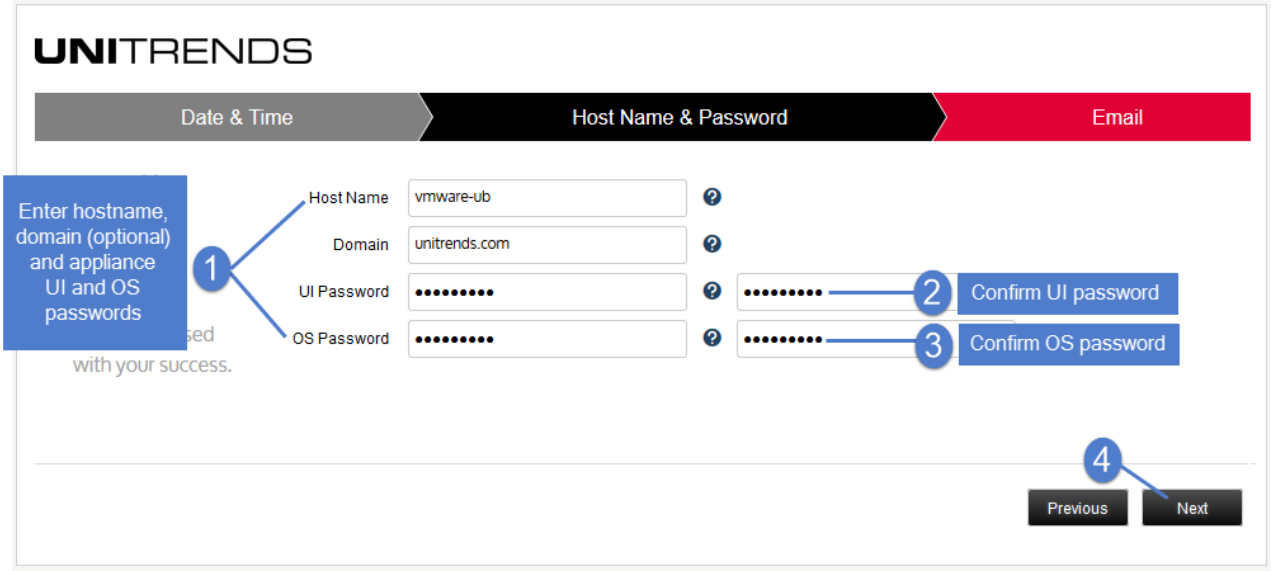
   - Check the **Use an NTP Server** box to sync to an NTP server. (Optional) Enter your preferred NTP server address.



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:

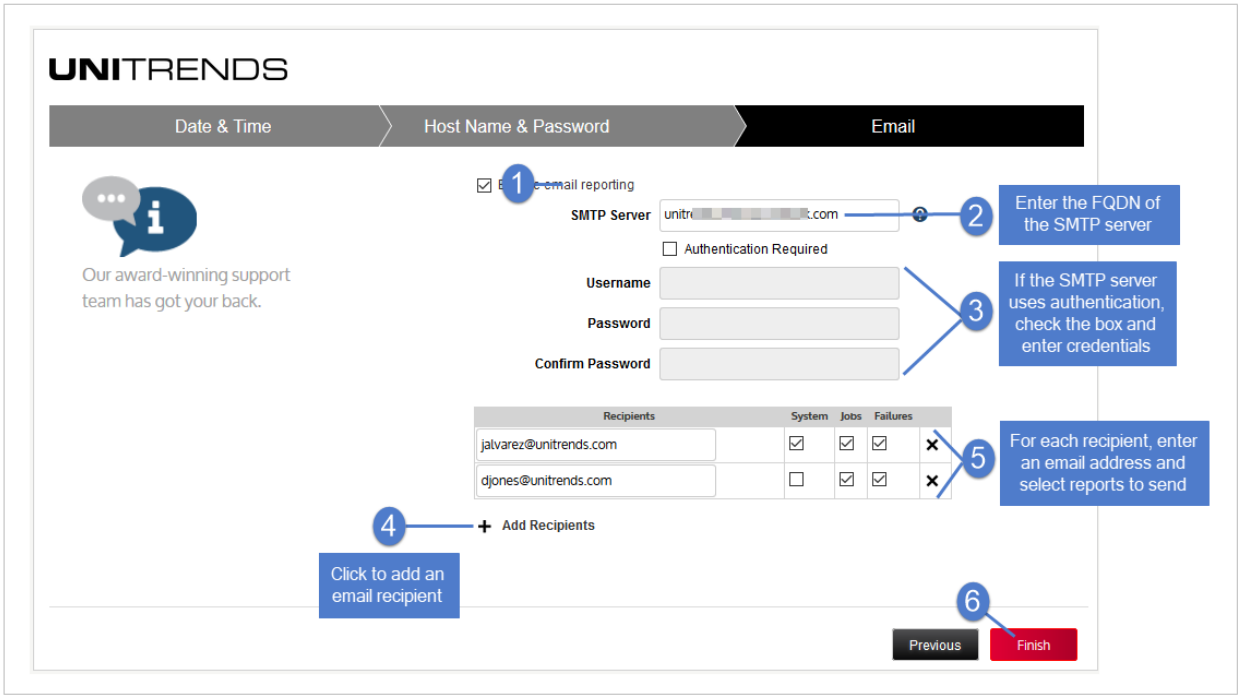
- The hostname can contain only alphanumeric characters, dashes, and underscores.
- The appliance has a UI root user and an OS root user. These are separate accounts. Changing the password of one root user account does NOT change the password of the other root user account. The UI root user is used to 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:

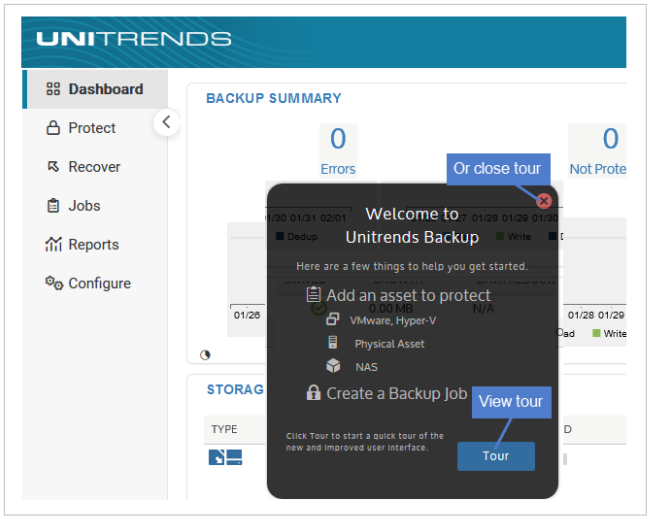
- The fully qualified domain name of the **SMTP server**.
- (If needed) If the SMTP server requires authentication, select **Authentication required** and enter a **Username** and **Password**.
- Click **+ Add Recipients** to add a an email recipient. Enter an email address in the **Recipient** field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



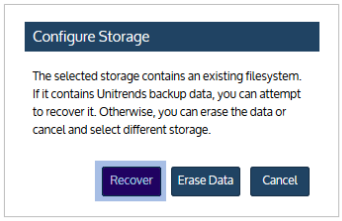
7 Do one of the following:

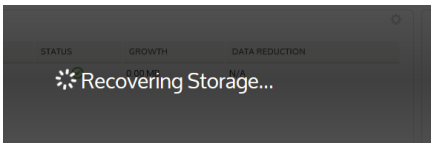
- If you deployed by using new storage for the initial backup storage, the Welcome to Unitrends Backup dialog displays. Click **Tour** to view the product tour (or **X** to exit).



OR

- If you deployed by using storage that contains backups from another Unitrends Backup appliance, click **Recover** to add the backups to the appliance.





8 Do one of the following:

- If you deployed using added VHD disk storage, proceed to "Step 7: (Optional) Modify deduplication settings" on page 37.

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 are 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 36
- "To add the initial backup storage device if using an external CIFS share" on page 36

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.

Use these steps to add an external LUN as the initial backup storage:

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 37.

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 "Step 7: (Optional) Modify deduplication settings" on page 37.

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.

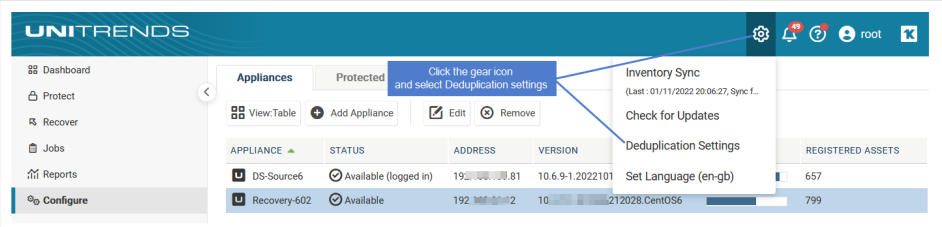
6. Proceed to "Step 7: (Optional) Modify deduplication settings".

Step 7: (Optional) Modify deduplication settings

Deduplication is a data compression technique that eliminates duplicate data blocks. Because only full backup are supported for XenServer VMs, the appliance is configured to use the Level 3 setting for maximum backup retention. You can opt to modify this setting for increased job performance. Keep in mind that decreasing the deduplication level decreases on-appliance retention.

To modify the deduplication level

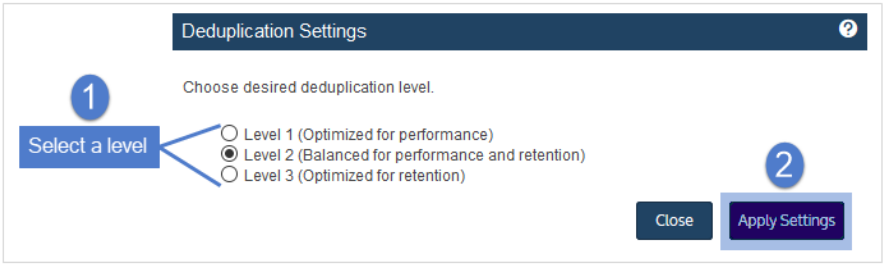
1. From the Global options at the top of the UI, select **Options > Deduplication Settings**.



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

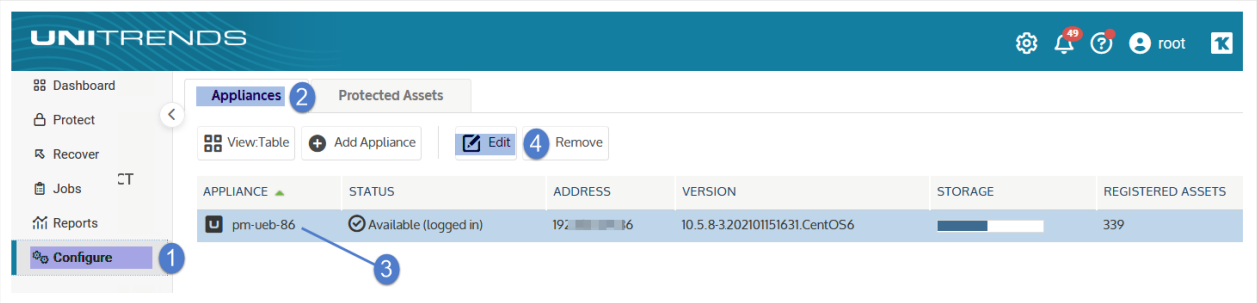
Your appliance is now configured and you can begin using it to protect your environment. For details, see the Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup.

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

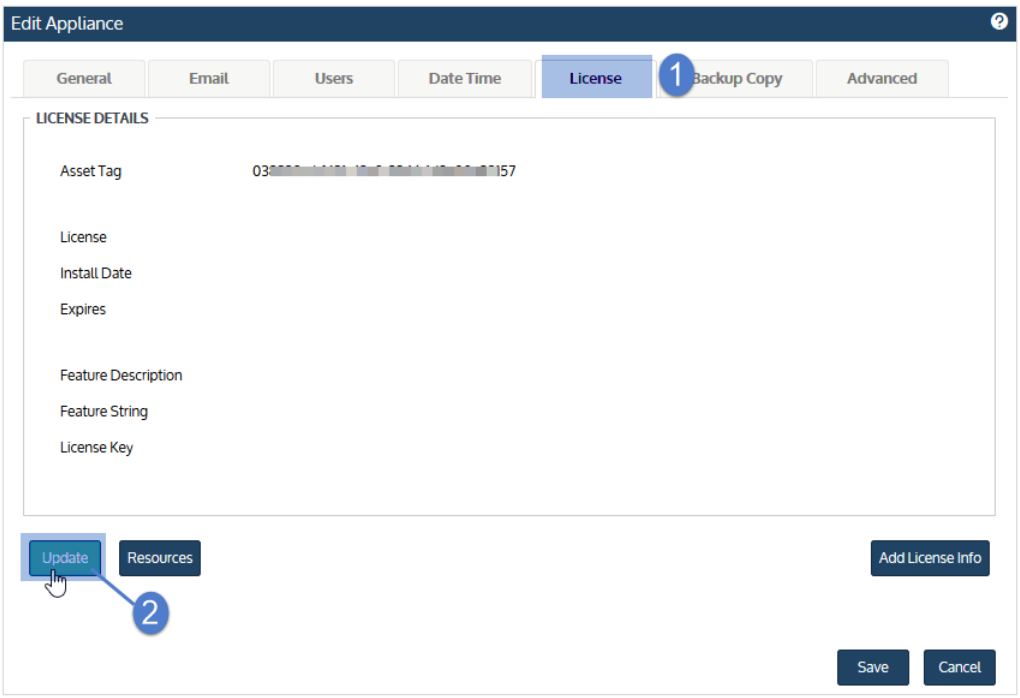
Each appliance requires an activation code and license key. Use the procedures below to register and license the appliance:

To register a Unitrends Backup appliance

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

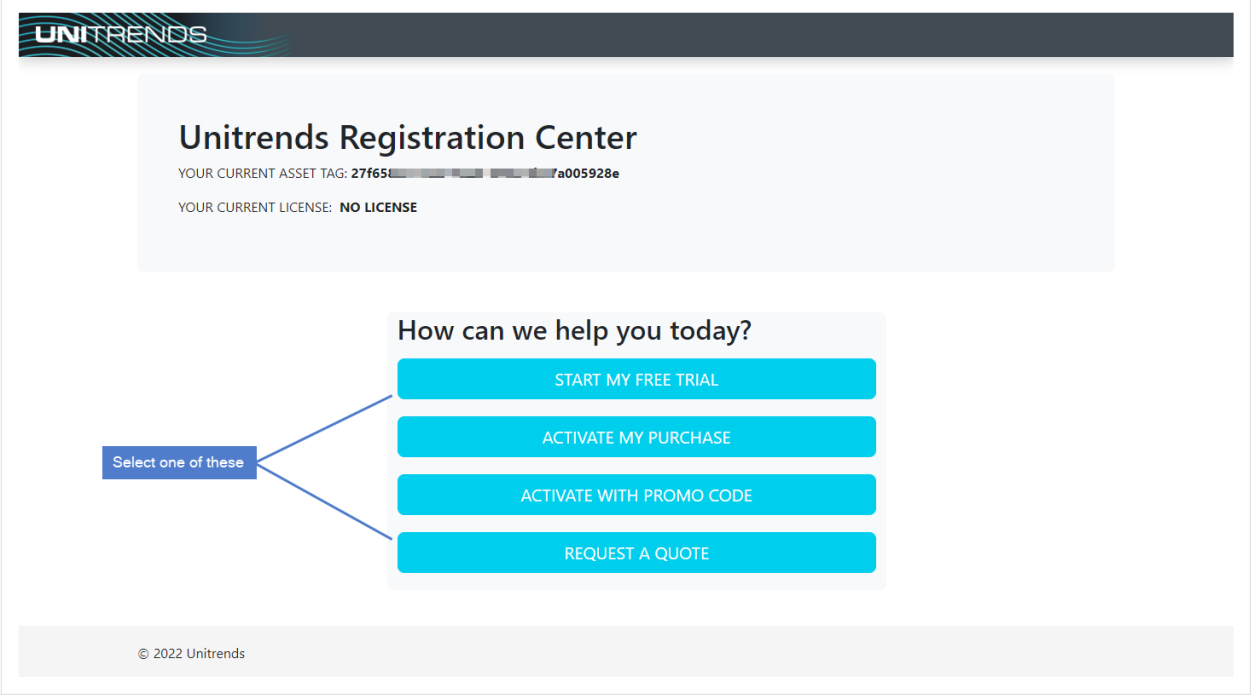


2 Select the **License** tab and click **Update**. The Registration Center displays.



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.



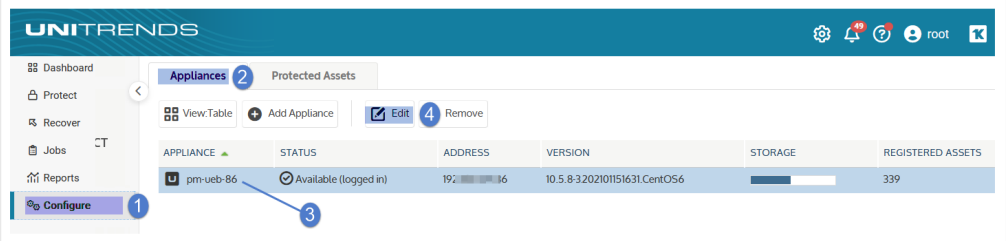
4 Complete and submit the applicable form.

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.

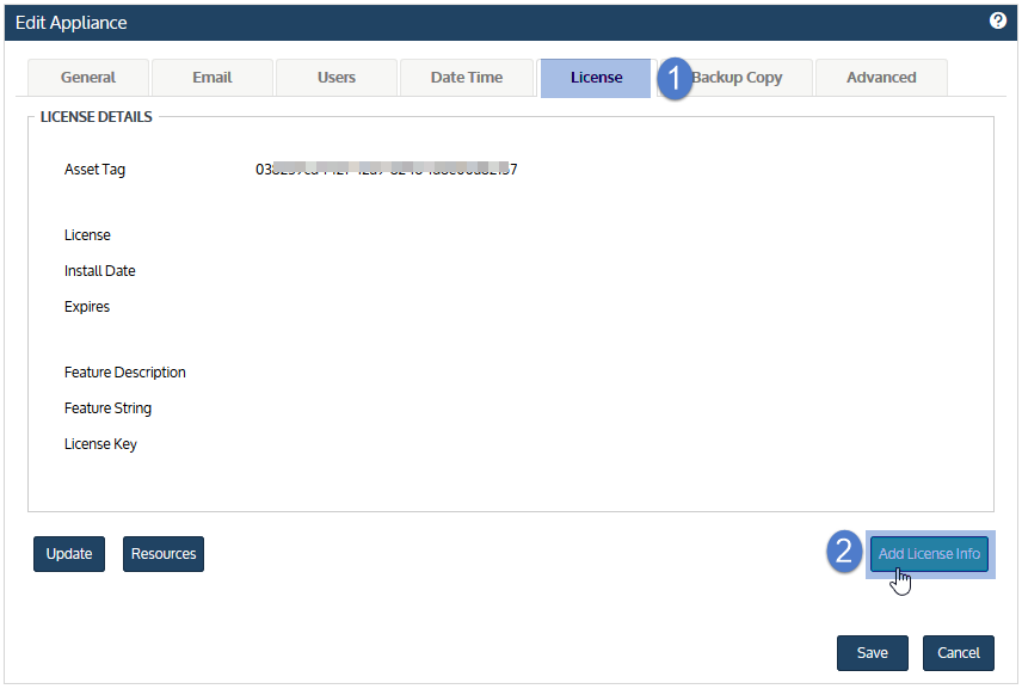
To license a Unitrends Backup appliance

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

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

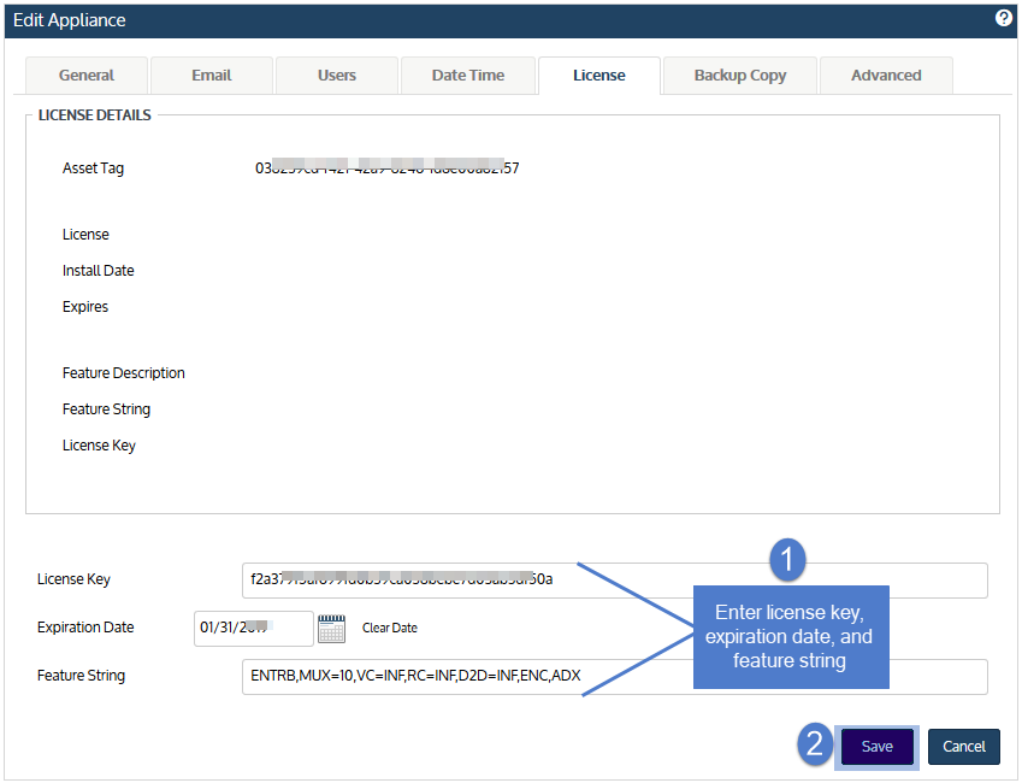


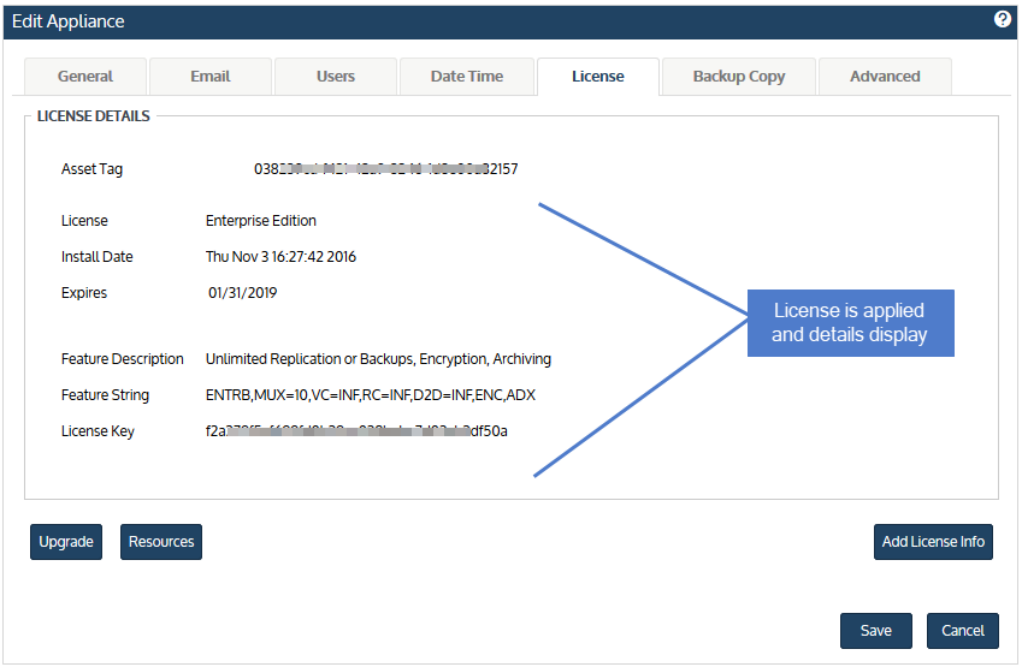
2 Select the **License** tab and click **Add License Info**.



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.