

# Deployment Guide for Unitrends Backup on Citrix XenServer

Release 10.5.2 | Document Version 7.11212023



# Copyright

Copyright © 2023 Unitrends Incorporated. All rights reserved.

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

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

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

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

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 Unpublished-rights reserved under the copyright laws of the United States.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

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

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

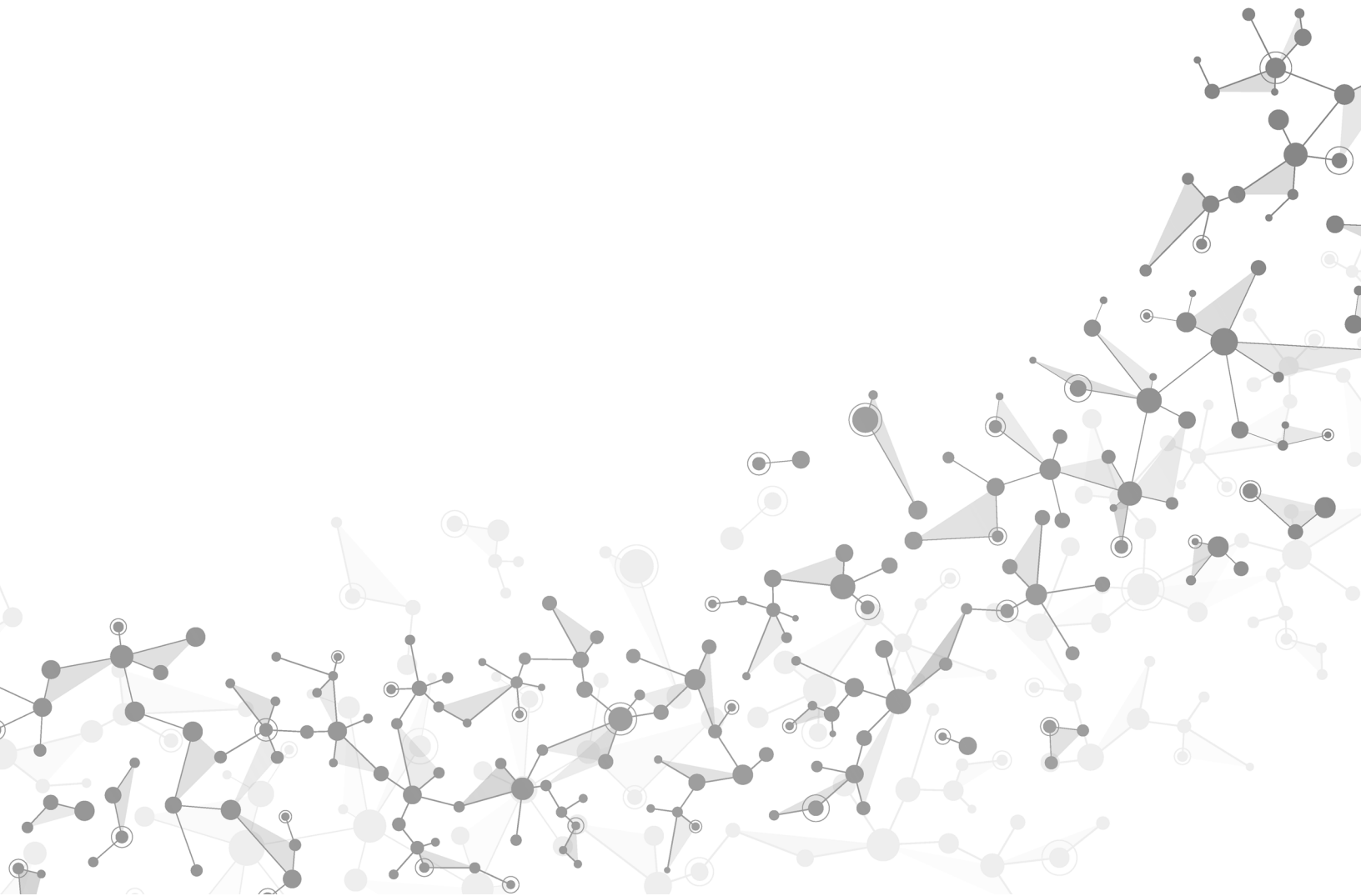
Unitrends, Inc  
200 Wheeler Road  
North Tower, 2nd Floor  
Burlington, MA 01803, USA  
Phone: 1.866.359.5411

# Contents

---

<b>Chapter 1: Introduction</b>	<b>5</b>
<b>Chapter 2: Requirements and Considerations</b>	<b>7</b>
Hypervisor requirements and considerations	7
Network requirements	9
Port requirements	10
Web access	11
Virtual machine resource requirements	11
<b>Chapter 3: Determining your Storage Strategy</b>	<b>13</b>
How Unitrends Backup storage works	13
Storage recommendations	13
<b>Chapter 4: Deploying a Unitrends Backup appliance</b>	<b>19</b>
Step 1: Set up storage on the hypervisor	19
Step 2: Download the Unitrends Backup XVA	20
Step 3: Deploy the Unitrends Backup VM	21
Step 4: Attach backup storage	26
Attaching new backup storage	26
Attaching storage that contains backups from another appliance	26
Step 5: Set up the appliance using the Quick Setup Wizard	28
To set up the appliance	28
Step 6: Add the initial backup storage device if using external storage directly attached to the Unitrends Backup VM	32
Step 7: (Optional) Modify deduplication settings	35
Step 8: Register and license the Unitrends Backup appliance	36
Step 9: Start protecting your environment	40

*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 <i>attached disk storage</i> .
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 <i>hypervisor</i> .
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"](#)
- ["Network requirements" on page 9](#)
- ["Port requirements" on page 10](#)
- ["Web access" on page 11](#)
- ["Virtual machine resource requirements" on page 11](#)

### 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	<p>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:</p> <ul style="list-style-type: none"> <li>• Host-level protection is supported for VMs hosted on the following: <ul style="list-style-type: none"> <li>– 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.</li> <li>– A Hyper-V host that is a supported version listed in the <a href="#">Compatibility and Interoperability Matrix</a>.</li> <li>– A VMware vCenter or ESXi host that is a supported version listed in the <a href="#">Compatibility and Interoperability Matrix</a>.</li> </ul> </li> <li>• Only one XenServer host can be added to the Unitrends Backup appliance.</li> <li>• The XenServer host must be one of the following: <ul style="list-style-type: none"> <li>– A XenServer pool master host meeting both of these criteria: <ul style="list-style-type: none"> <li>– The Unitrends Backup VM resides either on the pool master host itself or on one of the pool master's slave hosts.</li> <li>– The Unitrends Backup VM has been granted access to the shared storage used by the pool master host.</li> </ul> </li> <li>– A stand-alone XenServer host where the Unitrends Backup VM resides.</li> </ul> </li> </ul>

See the following for considerations by XenServer host type:

Host type	Description
XenServer pool master host	<p>By adding the pool master host to the Unitrends Backup appliance, you can protect the following:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• VMs that reside on shared storage in the resource pool.</li> </ul>
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 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"
- "Connectivity between the appliance and a hot backup copy target"

### Connectivity between the appliance and the Internet

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

Task	Port, Protocol, and Rule	Destination	Notes
Proactive Monitoring	161/UDP Outbound from the Unitrends appliance  161/TCP Outbound from the Unitrends appliance  162/UDP Outbound from the Unitrends appliance  162/TCP Outbound from the Unitrends appliance	notifications.unitrends.com	Used for SNMP trap collection for all proactive monitoring.
Task	Port, Protocol, and Rule	Destination	Notes

### 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 Outbound 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 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.

## 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	<p>These recommendations apply to all Unitrends Backup storage (initial disk, initial backup storage, and additional backup storage):</p> <ul style="list-style-type: none"> <li>• Unitrends strongly recommends using hypervisor-certified storage arrays on Citrix XenServer's hardware certified list for deploying Unitrends Backup appliances.</li> <li>• 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.</li> <li>• Unitrends recommends using DAS, internal to the hypervisor, or to leverage SAN or NAS storage that you expose to the hypervisor. <ul style="list-style-type: none"> <li>– You can create VHDs on storage internal to the hypervisor (DAS).</li> <li>– 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.</li> <li>– For optimal performance and scalability, add VHD disks to SCSI controllers.</li> </ul> </li> <li>• To use external SAN or NAS storage that is directly attached to the Unitrends Backup VM, follow these recommendations: <div data-bbox="407 1058 1458 1224" style="background-color: #f0f8ff; padding: 10px; margin: 10px 0;"> <p><b>Note:</b> 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 <a href="#">Supported external storage vendors for use with Unitrends Backup appliances</a>.</p> </div> <ul style="list-style-type: none"> <li>– 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.</li> <li>– 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.</li> <li>– For best performance with SAN storage, use a thick-provisioned LUN.</li> </ul> </li> </ul>

Unitrends Backup Storage Component	Recommendations
Initial disk	<p>You create the Unitrends Backup VM by deploying the XVA file. During deployment (in <a href="#">"Step 3: Deploy the Unitrends Backup VM" on page 21</a>), 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.</p> <p>The initial disk can reside on DAS, internal to the hypervisor, or on external storage attached to the hypervisor.</p> <hr/> <p><b>Note:</b> 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.</p> <hr/>
Initial backup storage	<p>You must add a minimum of 300GB for the VM image and the initial backup storage (see <a href="#">"Step 4: Attach backup storage" on page 26</a>). The following requirements and recommendations apply:</p> <hr/> <p><b>Note:</b> 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.</p> <hr/> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> <li>• 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 <a href="#">Special Configuration for NFS or CIFS with UB Initial Deployment Storage</a>.</li> </ul>

Unitrends Backup Storage Component	Recommendations
Additional backup storage	<p>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.</p> <p>When you add attached disk or external NAS or SAN storage, the VHDs, LUNs, or shares display in the Unitrends Backup UI as <code>/dev/sdx/</code>. The x indicates alphabetically the order in which the storage was added.</p> <p>For example, the initial disk is always <code>/dev/sda/</code>, the initial backup storage is <code>/dev/sdb/</code>, the next would be <code>/dev/sdc/</code>, and so forth.</p> <p>The following requirements apply to additional backup storage:</p> <ul style="list-style-type: none"> <li>• Your backup storage devices must be at least 300GB to enable deduplication or to use the device as a backup copy target.</li> <li>• As you add more storage, be sure to add resources to the Unitrends Backup VM, such as CPU and memory.</li> <li>• 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.</li> </ul>
Examples of expanding storage	<p>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.</p> <div style="border: 1px solid #00a0e3; padding: 5px; margin: 10px 0;"> <p><b>Note:</b> Expanding storage is only supported for added disk storage (DAS or external storage attached to the hypervisor).</p> </div> <p>See the following examples:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> <li>• For details on expanding storage, see <a href="#">Procedures for adding attached disk backup storage</a> in the <a href="#">Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup</a>.</li> </ul>



Unitrends Backup Storage Component	Recommendations
Examples of adding storage	<p>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.</p> <p>See the following examples:</p> <ul style="list-style-type: none"> <li>• DAS or external storage attached to the hypervisor -           <p>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 <b>Create a separate storage area for an alternate backup device</b> and select the type <b>Added Disk</b>. Select the disk to add.</p> </li> <li>• External storage attached to the Unitrends Backup VM -           <div> <p><b>Note:</b> 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.</p> <hr/> <ul style="list-style-type: none"> <li>– 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 <b>Create a separate storage area for an alternate backup device</b> and select the type <b>CIFS or NFS</b>. Enter the IP address of the NAS and other required information.</li> <li>– 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 <b>Create a separate storage area for an alternate backup device</b> and select the type <b>iSCSI</b>. Enter the IP address of the SAN and other required information.</li> </ul> </div> </li> <li>• For details on adding storage, see <a href="#">Procedures for adding attached disk backup storage</a> and <a href="#">Procedures for adding external storage</a> in the <a href="#">Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup</a>.</li> </ul>

*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"](#)
- ["Step 2: Download the Unitrends Backup XVA" on page 20](#)
- ["Step 3: Deploy the Unitrends Backup VM" on page 21](#)
- ["Step 4: Attach backup storage" on page 26](#)
- ["Step 5: Set up the appliance using the Quick Setup Wizard" on page 28](#)
- ["Step 6: Add the initial backup storage device if using external storage directly attached to the Unitrends Backup VM" on page 32](#)
- ["Step 7: \(Optional\) Modify deduplication settings" on page 35](#)
- ["Step 8: Register and license the Unitrends Backup appliance" on page 36](#)
- ["Step 9: Start protecting your environment" on page 40](#)

## 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 21](#)) and select a Storage Repository to add the initial backup storage (in ["Step 4: Attach backup storage" on page 26](#)). 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 13.

Storage option	Requirements
Use added disk (DAS or external) storage for both the initial disk and initial backup storage (recommended)	<p>Verify that the hypervisor has enough storage to create the initial disk and initial backup storage. VM disks cannot be attached as <i>Read Only</i>. Be sure to use the <i>Read Only = No</i> setting when attaching disks.</p> <p>To use external storage (rather than DAS), use the hypervisor to add the SAN or NAS and to create the associated Storage Repository.</p>
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)	<p>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.</p> <p>Use the hypervisor to add the SAN or NAS and to create the associated Storage Repository.</p>
Deploy using storage containing backups from another Unitrends Backup appliance	<p>Verify that the hypervisor has enough storage to create the initial disk. You will add the storage that contains backups in "<a href="#">Step 4: Attach backup storage</a>" on page 26.</p>

## 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.

Unitrends Backup Virtual Appliance Deployments

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

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

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

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

## Step 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 26](#).
- 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 22](#).

### 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.

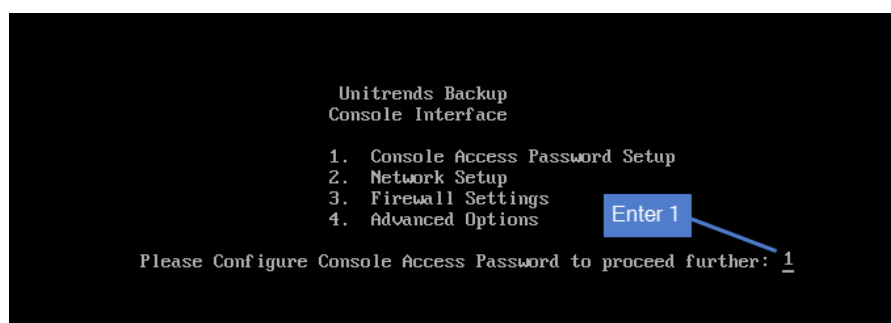
**Note:** The Unitrends Backup VM must be turned on. If necessary, right-click the VM and select **Start**.

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 28.)

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

```
Password should be at least 8 characters
Password should not contain the forbidden word Unitrend (case insensitive)

1 Enter new password

Changing password for user root.
New password:
Retype new password: 2 Enter new password again to confirm
passwd: all authentication tokens updated successfully.
```

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

```
Unitrends Backup
Console Interface

1. Console Access Password Setup
2. Network Setup
3. Firewall Settings
4. Advanced Options

Please enter choice: 2 Enter 2

Manage System using the web-based interface at one of the following:
eth0 - http://10.10.10.1
```

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

```
Unitrends Backup
Initial System Setup Menu

1. Configure IP, Netmask and Gateway
2. Configure DNS
3. Configure IPMI LAN
4. Configure DHCP
5. Network Test
6. Back

Please enter choice: 1 Enter 1
```

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

```
0. eth0
Select a network adapter: 0
```

Enter a number to select an adapter. If your appliance has multiple adapters, each are listed. In this example, the appliance has one adapter (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.

```
Network Adapter:   eth0
Current IP address: 10.10.10.1
Current Netmask:   "255.255.255.0"
Current Gateway:   n/a
```

```
Edit network configuration? [n/Y]: Y
```

Enter Y

```
Current IP address: 10.10.10.1
Enter new System IP Address: 192.168.1.10
```

Enter an IP address for the  
Unitrends appliance

```
Current Netmask: "255.255.255.0"
Enter new System Netmask:
```

Enter new netmask or press  
Enter to accept the default

```
Current Gateway: n/a
Enter new Network Gateway: 192.168.1.1
```

Enter gateway IP address

```
Adapter:           eth0
Current IP address: 10.10.10.1
Current Netmask:   "255.255.255.0"
Current Gateway:   n/a
```

```
New IP address:    192.168.1.10
New Netmask:       "255.255.255.0"
New Gateway:       192.168.1.1
```

```
Commit network configuration changes? [n/Y]: Y
```

Enter Y to save settings  
(or N to modify settings)

- 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.

#### Unitrends Backup Initial System Setup Menu

1. Configure IP, Netmask and Gateway
2. Configure DNS
3. Configure IPMI LAN
4. Configure DHCP
5. Network Test
6. Back

```
Please enter choice: 2
```

Enter 2



```
Current Primary DNS:  n/a
Current Secondary DNS: n/a
Current DNS Domain:  xenserver-ub
Edit DNS configuration? [n/Y]: Y
```

Enter Y

```
Current Primary DNS: n/a
Enter new Primary DNS: 192.168.1.108
```

Enter IP of primary DNS server

```
Current Secondary DNS: n/a
Enter new Secondary DNS: 192.168.1.108
(Leave blank if no secondary DNS desired)
```

(Optional) Enter IP of  
secondary DNS server

```
Current DNS Domain:  xenserver-ub
Enter new DNS Search Domain: unitrends.com
```

Enter domain

```
Current Primary DNS:  n/a
Current Secondary DNS: n/a
Current DNS Domain:  xenserver-ub

New Primary DNS:      192.168.1.108
New Secondary DNS:    192.168.1.108
New DNS Domain:       unitrends.com
```

```
Commit DNS configuration changes? [n/Y]: Y
```

Enter Y to save settings  
(or N to modify settings)

- 9 To exit network setup, enter 6.

```
Unitrends Backup
Initial System Setup Menu

1. Configure IP, Netmask and Gateway
2. Configure DNS
3. Configure IPMI LAN
4. Configure DHCP
5. Network Test
6. Back
```

```
Please enter choice: 6
```

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 26](#)
- ["Attaching storage that contains backups from another appliance" on page 26](#)

### 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:

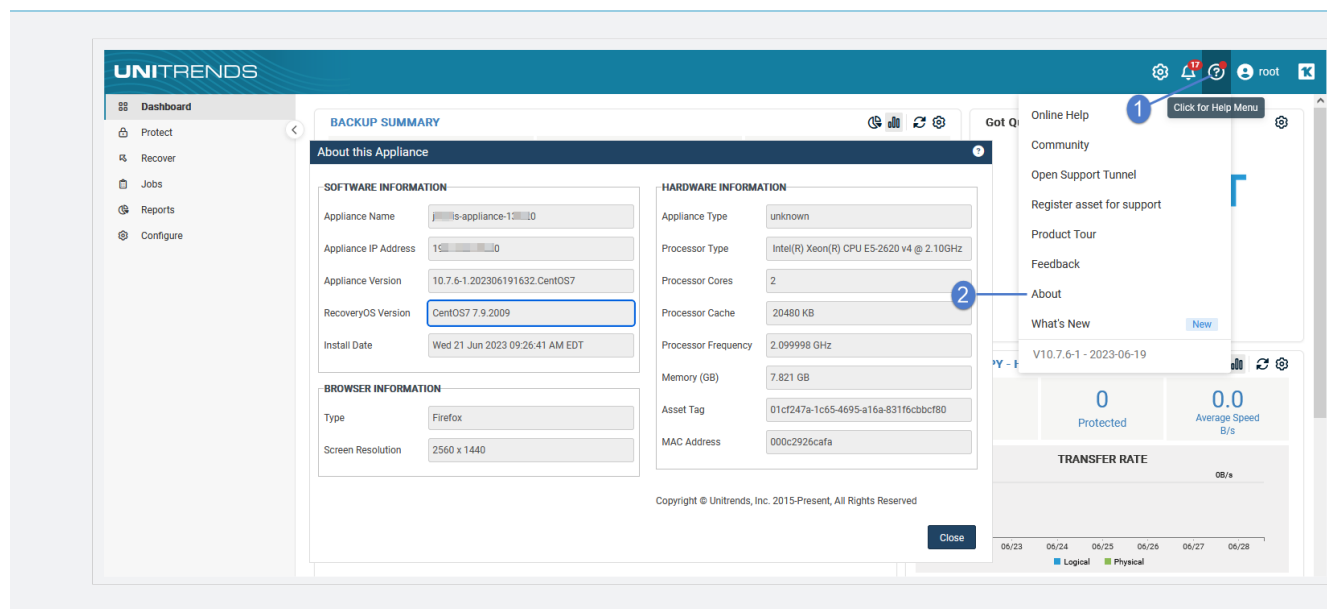
- **Added disk storage attached to the host** — Add a VHD to the Unitrends Backup VM by using the XenServer host. The appliance automatically uses the first VHD disk added to the Unitrends Backup VM as the initial backup storage. Once you have added the VHD, proceed to ["Step 5: Set up the appliance using the Quick Setup Wizard" on page 28](#).
- **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 28](#).

### 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 28](#). 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 28.

- **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".

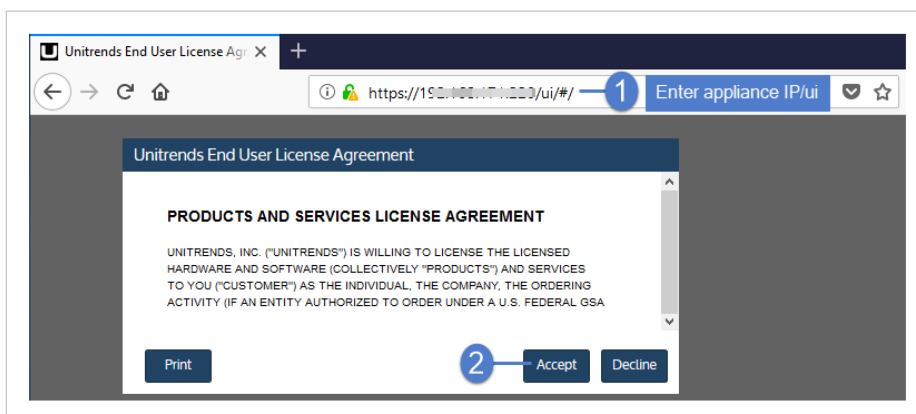
## Step 5: Set up the appliance using the Quick Setup Wizard

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.

**UNITRENDS**

**Date & Time** | **Host Name & Password** | **Email**

 Crazy-committed to helping you play IT safe.

☒ Enter a date and time for your appliance

Date:

Time:

Time Zone:

☐ Use an NTP Server

NTP Server Addresses:

0.centos.pool.ntp.org

1.centos.pool.ntp.org

[Click to continue](#) [Next](#)

- 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.

**UNITRENDS**

Date & Time    Host Name & Password    Email

1 Enter hostname, domain (optional) and appliance UI and OS passwords

Host Name: vmware-ub ?

Domain: unitrends.com ?

UI Password: ..... ?    2 Confirm UI password

OS Password: ..... ?    3 Confirm OS password

with your success.

4 Previous Next

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

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

6 Click **Finish**.

**UNITRENDS**

Date & Time | Host Name & Password | **Email**

1 ☒ Enable email reporting

SMTP Server: unitrends.com 2 Enter the FQDN of the SMTP server

☐ Authentication Required

Username: 3 If the SMTP server uses authentication, check the box and enter credentials

Password:

Confirm Password:

Recipients	System	Jobs	Failures
jalvarez@unitrends.com	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
djones@unitrends.com	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

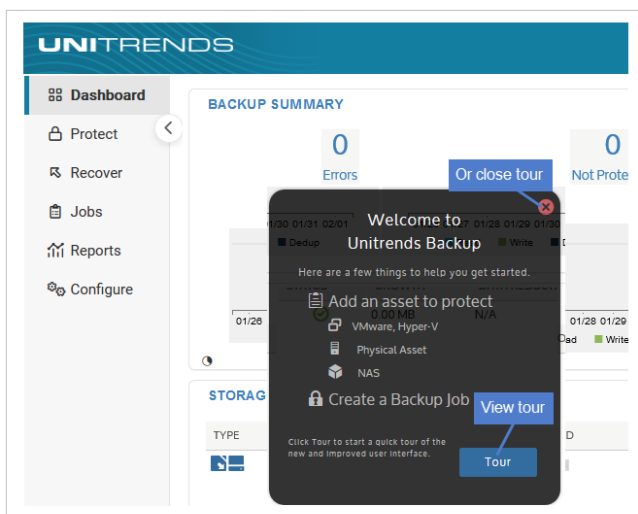
4 + Add Recipients Click to add an email recipient

5 For each recipient, enter an email address and select reports to send

6 Previous Finish

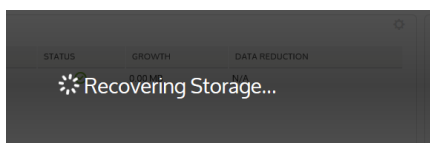
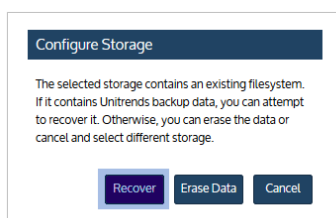
7 Do one of the following:

- 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 35.](#)

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 34](#)
- ["To add the initial backup storage device if using an external CIFS share" on page 34](#)

### 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 35](#).

#### 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.

- 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"](#).
- On the **Configure > Appliances** page, select your appliance.
- Click the **Storage** tab below.
- Select **Add Storage > NFS**.
- 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 35](#).

#### 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.

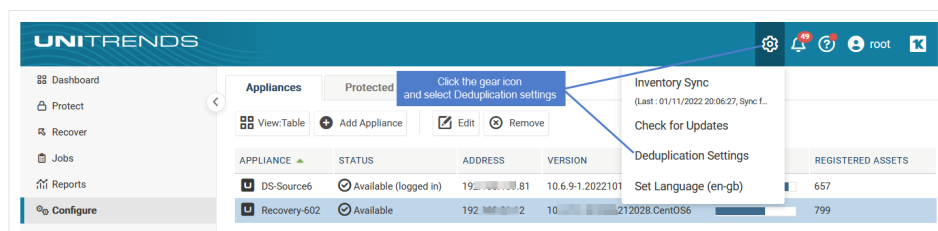
- 6 Proceed to ["Step 7: \(Optional\) Modify deduplication settings"](#).

## Step 7: (Optional) Modify deduplication settings

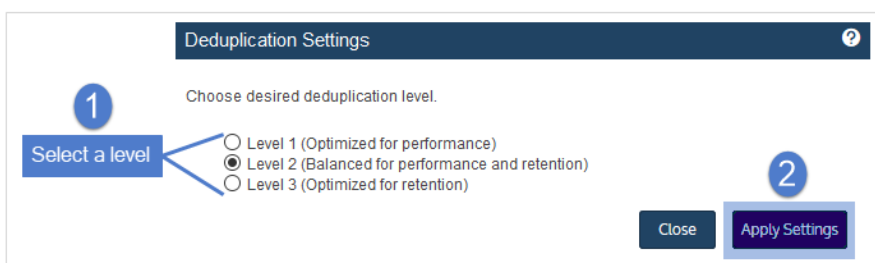
Deduplication is a data compression technique that eliminates duplicate data blocks. Because only full backup are supported for XenServer VMs, the appliance is configured to use the Level 3 setting for maximum backup retention. You can opt to modify this setting for increased job performance. Keep in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

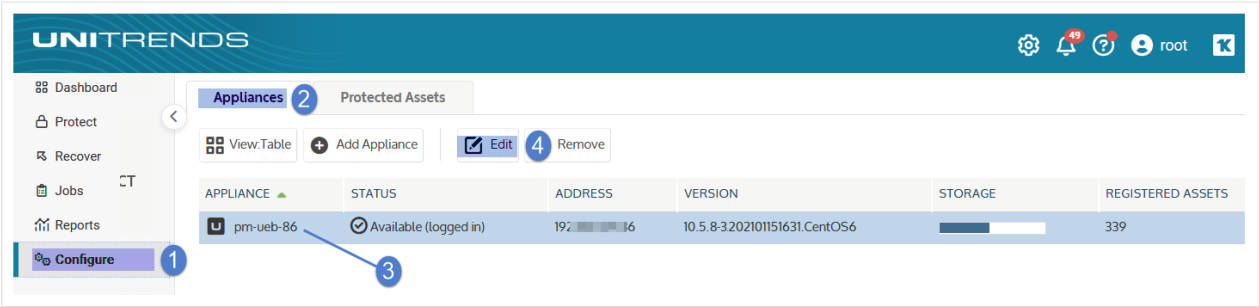
Your appliance is now configured and you can begin using it to protect your environment. For details, see the [Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup](#).

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

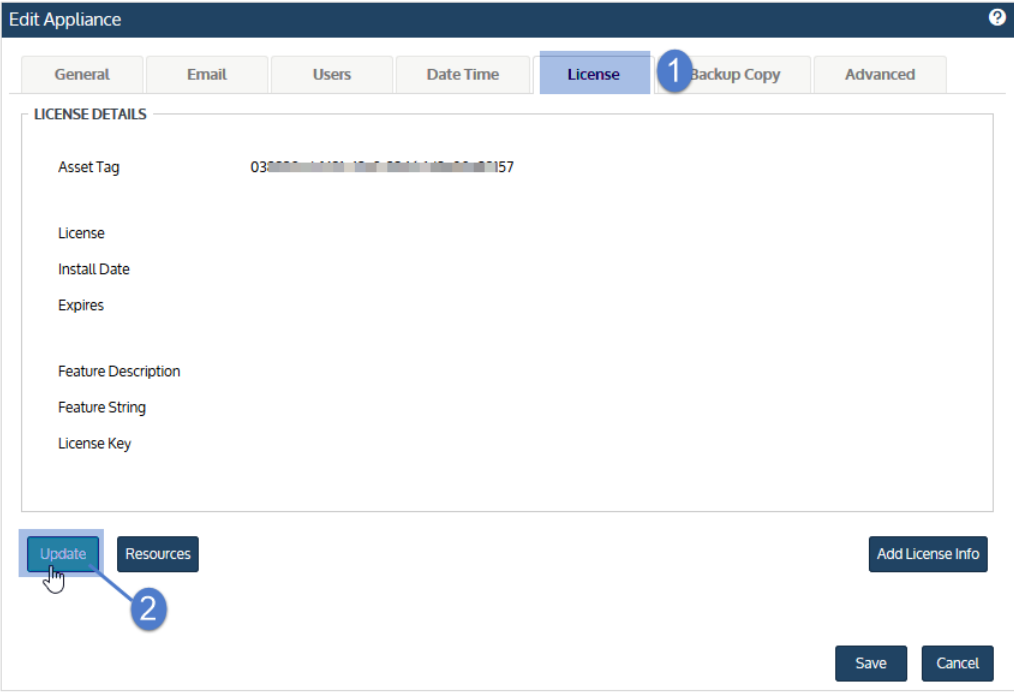
Each appliance requires an activation code and license key. Use the procedures below to register and license the appliance:

### To register a Unitrends Backup appliance

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

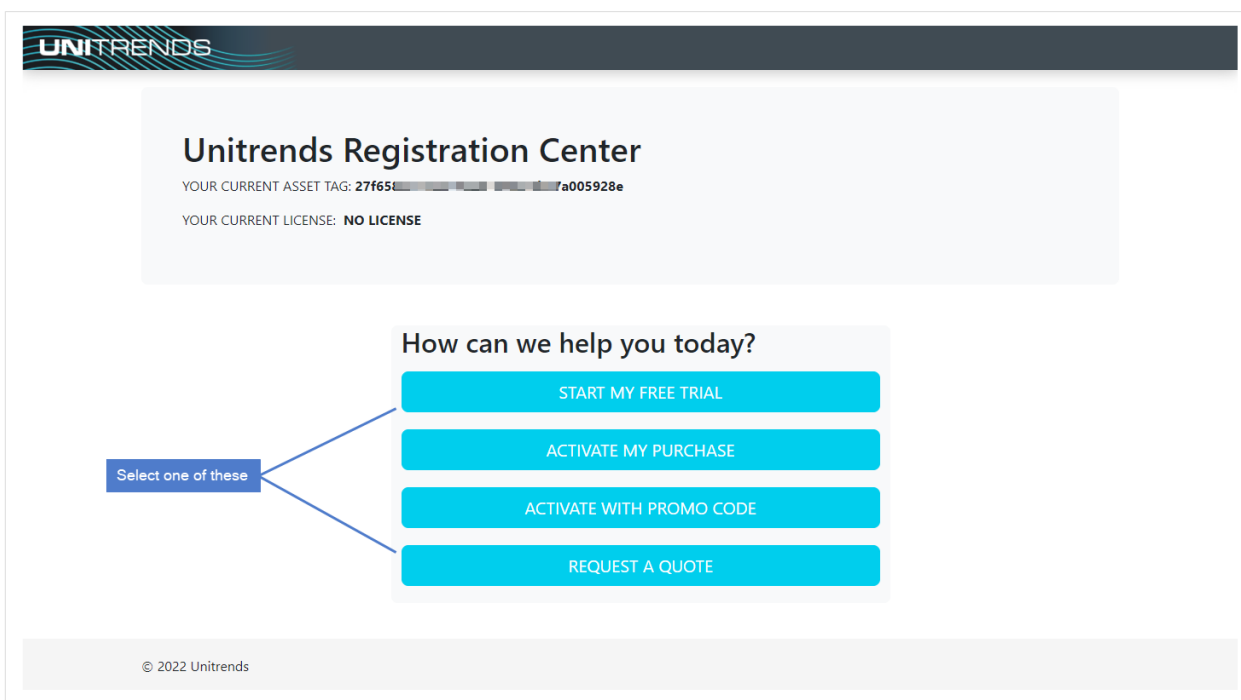


2 Select the **License** tab and click **Update**. The Registration Center displays.



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.



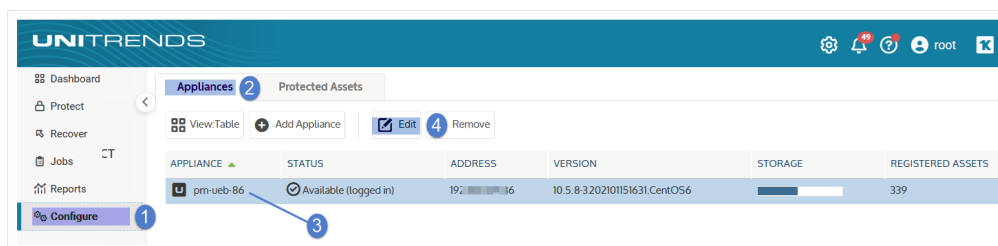
#### 4 Complete and submit the applicable form.

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**.

Edit Appliance

General

Email

Users

Date Time

**License**

Backup Copy

Advanced

LICENSE DETAILS

Asset Tag

030257C3-74E7-42E7-8240-1800000002157

License

Install Date

Expires

Feature Description

Feature String

License Key

Update

Resources

2

Add License Info

Save

Cancel

- 3 Enter the **License Key**, **Expiration Date**, and **Feature String**.
- 4 Click **Save**. The license is applied.

**Edit Appliance**

General Email Users Date Time **License** Backup Copy Advanced

**LICENSE DETAILS**

Asset Tag 0302373d4742f42d70e4b100e00062157

License

Install Date

Expires

Feature Description

Feature String

License Key

License Key f2a37715d0771d0b77ca0506c0c7005a05a30a

Expiration Date 01/31/2019 Clear Date

Feature String ENTRB,MUX=10,VC=INF,RC=INF,D2D=INF,ENC,ADX

1 Enter license key, expiration date, and feature string

2 Save Cancel

**Edit Appliance**

General | Email | Users | Date Time | **License** | Backup Copy | Advanced

**LICENSE DETAILS**

Asset Tag	03820000-MC1-1007-0014-10000002157
License	Enterprise Edition
Install Date	Thu Nov 3 16:27:42 2016
Expires	01/31/2019
Feature Description	Unlimited Replication or Backups, Encryption, Archiving
Feature String	ENTRB,MUX=10,VC=INF,RC=INF,D2D=INF,ENC,ADX
License Key	f2a370f5-4606401d-0001-1174631d3df50a

Upgrade | Resources | Add License Info

Save | Cancel

License is applied and details display

## 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](#).