

CentOS 6 to CentOS 7 Migration Guide for VMware

Release 10.6 | Document Version 1.02082022



Copyright

Copyright © 2022 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 Unpublished-rights reserved under the copyright laws of the United States.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

Chapter 1: Introduction	5
Migration considerations	5
Migration procedures checklist	5
Chapter 2: Migration Requirements	7
Requirements for CentOS 6 Unitrends Backup virtual appliance	7
Deployment requirements for CentOS 7 Unitrends Backup virtual appliance	13
Chapter 3: Migration Procedures	17
Step 1: Migrate data on the CentOS 6 appliance	17
Step 2: Deploy the CentOS 7 Unitrends Backup VM	20
Step 3: Attach backup storage	26
Step 4: Configure network settings	33
Step 5: Set up the CentOS 7 appliance using the Quick Setup Wizard	38
Step 6: (If needed) Configure encryption with the CentOS 6 passphrase	41
Step 7: (If needed) Add data copy access profiles	44
Step 8: Register and license the CentOS 7 appliance	44

This page is intentionally left blank.



Chapter 1: Introduction

This guide provides instructions for migrating your Unitrends Backup virtual appliance from the CentOS 6 platform to CentOS 7. Migration consists of preparing the CentOS 6 appliance, deploying the CentOS 7 Unitrends Backup virtual machine (VM), attaching backup storage from the original CentOS 6 VM, and configuring settings on the new appliance.

To get started, review the ["Migration considerations"](#). Then use the ["Migration procedures checklist"](#) as a guide for performing the migration. Or, if you prefer more detail, review the complete ["Migration Requirements"](#), then perform the step-by-step ["Migration Procedures"](#).

Migration considerations

Review these considerations before you start:

- Once you migrate the CentOS 6 data, the CentOS 6 appliance is no longer usable. You must recover the data to the newly deployed CentOS 7 VM. ESXi version 5.5 or higher is required to deploy the CentOS 7 VM. Do not migrate data until you are ready to deploy the CentOS 7 VM.
- Before you migrate the CentOS 6 data, you must use your ESXi server to consolidate any snapshots on the CentOS 6 VM. Snapshots must be consolidated for a successful migration.
- Before you migrate, check these tabs for any active recovery objects: Recover > File Level Recovery, Instant Recovery, and Replicas. Tear down any objects before starting the migration. You will need to recreate these objects on the CentOS 7 appliance.
- If you are encrypting backups, save the CentOS 6 encryption passphrase in a safe place. You must manually configure encryption with this same passphrase on the new CentOS 7 appliance. If you migrate and are not able to configure encryption with the CentOS 6 passphrase, any encrypted backups that were migrated cannot be recovered.
- Data copy access lab profiles are not migrated. If you are using this feature, you need to manually recreate lab profiles on the CentOS 7 appliance.
- Push install of the Windows agent is not supported on migrated appliances. After migrating to CentOS 7, the Windows agent must be installed manually on its protected assets.
- The migration tool verifies all requirements other than encryption, snapshot consolidation, and whether there are any active recovery objects. If a requirement has not been met, the migration does not proceed and you receive a message describing each issue that must be addressed. You can opt to simply run the migration tool without checking these CentOS 6 requirements, then address any issues if found. For detailed requirements, see ["Requirements for CentOS 6 Unitrends Backup virtual appliance"](#).

Migration procedures checklist

- ["Step 1: Migrate data on the CentOS 6 appliance"](#) – To migrate the data, upgrade the CentOS 6 appliance to release 10.5.0-3 or higher, then select **Migrate from CentOS 6 to CentOS 7** in the Support Toolbox (**Configure > Appliances > Edit > Advanced > Support Toolbox**).

IMPORTANT! Migration time varies by database size. Do not manually close the user interface while the migration is running. It is safe to close the UI after the Results Migration message displays.

- "Step 2: Deploy the CentOS 7 Unitrends Backup VM" – Download the CentOS 7 OVA file from <https://www.unitrends.com/download/enterprise-backup-software> and deploy it on your ESXi server (**File > Deploy OVF Template**). Ensure that the memory and CPU settings match or exceed those of the CentOS 6 VM.
- "Step 3: Attach backup storage" – Edit the CentOS 7 VM to attach the all backup storage disks from the original CentOS 6 VM.

IMPORTANT!

- You must add all backup storage disks from the original CentOS 6 VM.
 - Do not add Hard Disk 1. This 100GB disk was created during VM deployment and is NOT used to store backups.
 - You must add the first backup storage disk (typically Hard Disk 2) before you add any other backup storage disks.
- "Step 4: Configure network settings" – Access the VM console and configure these settings to match those of the CentOS 6 VM: Console Access Password, Network Settings, and DNS Settings.
 - "Step 5: Set up the CentOS 7 appliance using the Quick Setup Wizard" – Log in to the appliance UI. Use the Setup Wizard to configure appliance settings. When prompted to configure storage, click **Recover** to add the migrated backups to the appliance.
 - "Step 6: (If needed) Configure encryption with the CentOS 6 passphrase" – If backups were being encrypted on the CentOS 6 appliance, you must configure encryption with the passphrase that was used by the CentOS 6 appliance. If you do not use the original passphrase, any encrypted backups that were migrated cannot be recovered. To configure encryption settings, select **Configure > Appliances > Edit > Advanced**.
 - "Step 7: (If needed) Add data copy access profiles" – Data copy access profiles are not migrated from the CentOS 6 appliance. If you were using the copy data management feature, you need to recreate your data copy access profiles. For details, see [Copy Data Management](#) in the [Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup](#).
 - "Step 8: Register and license the CentOS 7 appliance" – You must register and license the appliance within 30 days of deploying the CentOS 7 VM. Go to **Configure > Appliances > Edit > License**. Click **Update** and select **I need to activate my purchase**.

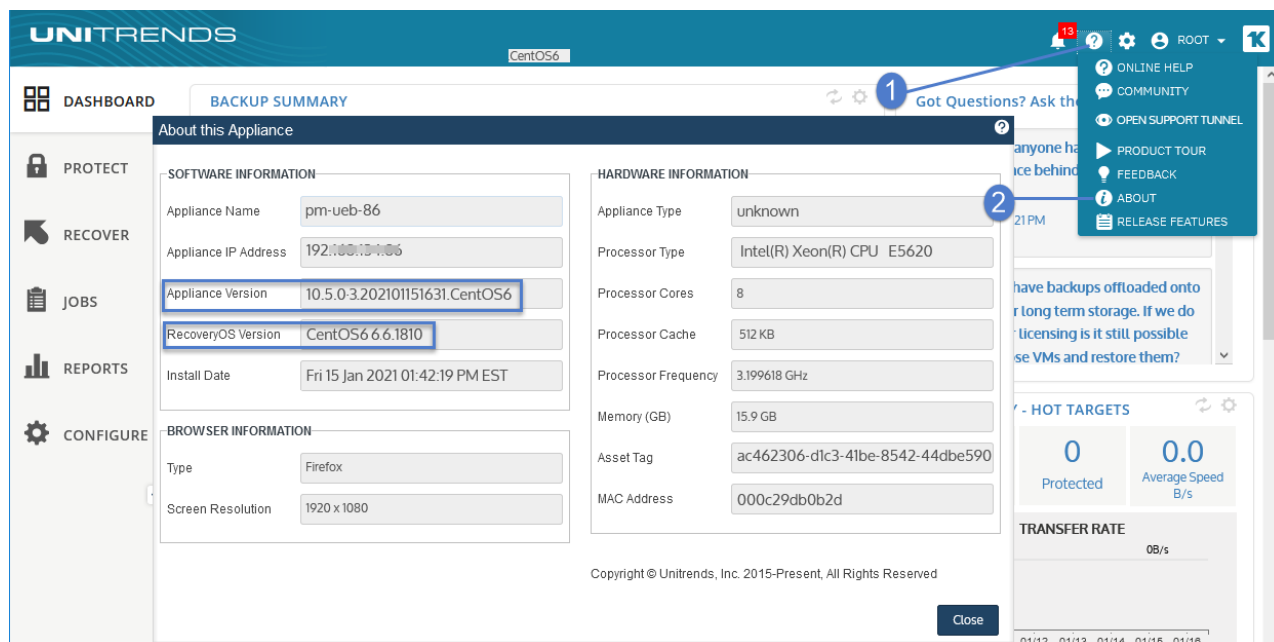
Chapter 2: Migration Requirements

Migration requirements for the CentOS 6 and CentOS 7 Unitrends Backup virtual appliances are described below.

Requirements for CentOS 6 Unitrends Backup virtual appliance

Your CentOS 6 Unitrends Backup appliance must meet these prerequisites:

- Snapshot consolidation – Use your ESXi server to consolidate any snapshots on the CentOS 6 VM.
- Manager appliances – The CentOS 6 appliance must not be managing another appliance. Migration is not supported for manager appliances.
- Appliance version and platform – The appliance is running release 10.5.0-3 or higher on the CentOS 6 platform. To check, select ? > About:



- License and asset tag – The appliance has a valid license, support contract, and asset tag (**Configure > Appliance > Edit Appliance > License**):

The screenshot displays the Unitrends web interface. On the left sidebar, the 'CONFIGURE' option is selected, indicated by a blue circle with the number 1. The main content area shows the 'Appliances' section, with the 'Edit Appliance' modal open for the appliance 'pm-ueb-86'. The modal has tabs for General, Email, Users, Date Time, License, Backup Copy, and Advanced. The 'License' tab is active, showing the following details:

LICENSE DETAILS	
Asset Tag	ac46c908-0f6b-4b7c-9b7c-7400e590ca0e
License	Enterprise Plus
Install Date	Fri Feb 28 09:49:19 2020
Expires	never
Feature Description	Unlimited Hot Backup Copies and Backups, Encryption, Cold Backup Copy, Copy Data Management
Feature String	ENTRB,MUX=10,VC=INF,RC=300G,D2D=INF,ENC,ADX,NDMP=1,MKT=4
License Key	1f60a000-0000-0000-0000-000000000000:559b

At the bottom of the modal, there are buttons for 'Update', 'Resources', 'Add License Info', 'Save', and 'Cancel'. The 'pm-ueb-86' appliance entry in the table above the modal is highlighted with a blue circle and the number 3. The 'Appliances' header and the 'Edit Appliance' modal title are highlighted with blue circles and the number 4.

- Internet access – The appliance has access to the Internet.
- Email – Email is configured on the appliance so you can receive email notifications related to platform migration (**Configure > Appliance > Edit Appliance > Email**):

Edit Appliance

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

SMTP SETTINGS

Enable email reporting
Reporting is enabled

SMTP Server: unit@outlook.com
SMTP server is configured

Server requires credentials

Username:

Password:

Send a Test Email

EMAIL RECIPIENTS

RECIPIENTS	APPLIANCE JOBS	FAILURES
ds@outlook.com	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> ✘
ash@outlook.com	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> ✘ +

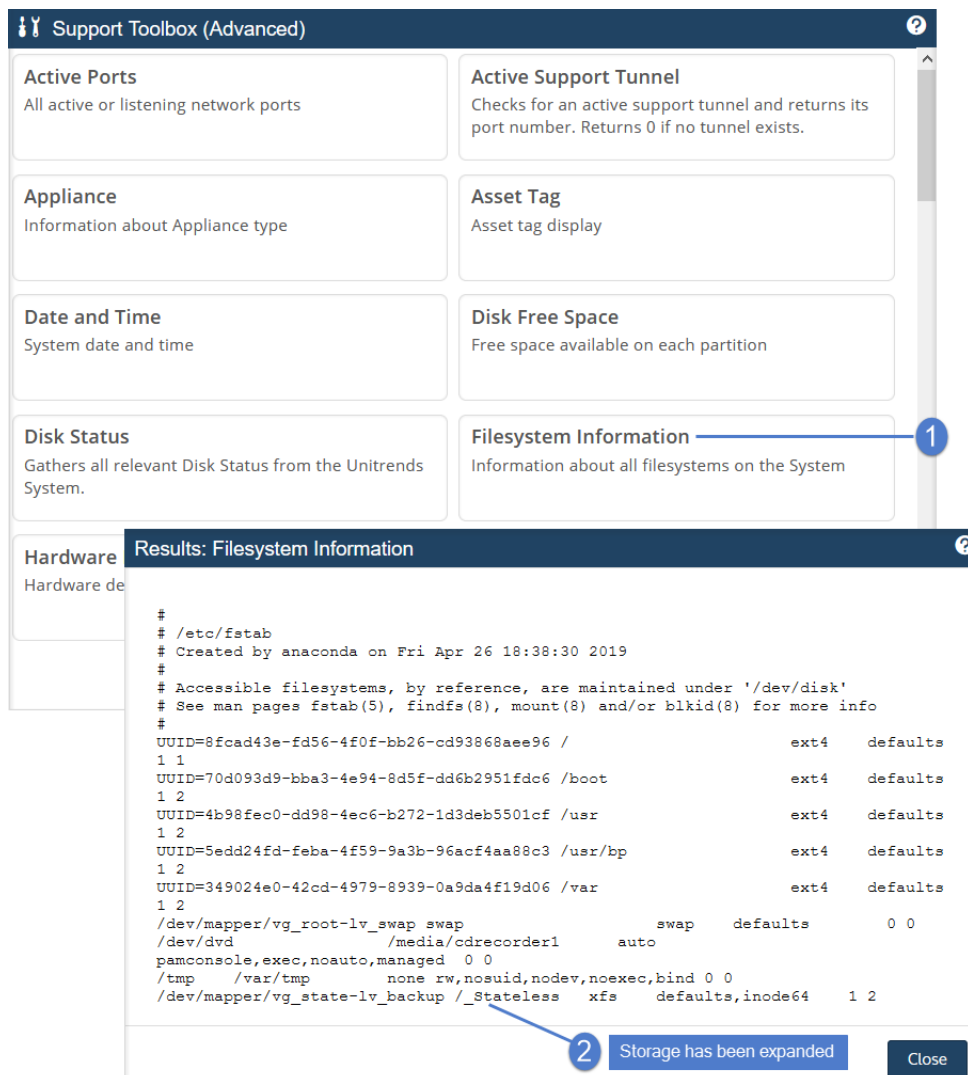
Recipients are set up to receive Appliance notifications

Save Cancel

- Filesystem configuration – The database resides on the storage partition. This is the default configuration. If your database was moved to a separate partition, migration is not supported. The migration tool detects this and no data is migrated.
- Filesystem configuration – The appliance is configured with expanded storage. To verify that storage has been expanded:
 - On the **Configure > Appliances** page, select the appliance and click **Edit**. Click **Advanced** and select **Support Toolbox**.

The screenshot displays the UNITRENDS web interface. On the left is a sidebar with navigation icons and labels: DASHBOARD, PROTECT, RECOVER, JOBS, REPORTS, and CONFIGURE (1). The main content area shows a table of appliances under the 'Appliances' (2) section. The table has columns for APPLIANCE and STATUS. One appliance is listed with ID 'pm-ueb-86' and status 'Available' (3). Above the table are buttons for 'View:Table', '+ Add Appliance', 'Edit' (4), and 'Remove'. An 'Edit Appliance' dialog box is open, showing tabs for General, Email, Users, Date Time, License, Backup Copy, and Advanced (5). The Advanced tab is active, displaying 'ENCRYPTION SETTINGS' with options to 'Enable Encryption' (checked), 'Change Passphrase', and 'Save Master Key File'. Below this is a 'SAN DIRECT DETAILS' table with columns for Name, Host, Port, Target, and LUN. At the bottom of the dialog, a 'Support Toolbox' button (6) is highlighted, along with other configuration buttons like 'General Configuration', 'OS Password', 'iSCSI CHAP', 'SNMP', 'VM Replica Configuration', 'Save', and 'Cancel'.

- In the Support Toolbox (Advanced) dialog, click **Filesystem Information**. If you see `/_Stateless`, storage has been expanded.



- Available space – The `/_Stateless` partition must have adequate available space to accommodate the database migration. To check the space available, select **Disk Free Space** in the Support Toolbox (Advanced) dialog:

The screenshot shows the 'Support Toolbox (Advanced)' interface. The 'Disk Free Space' section is highlighted with a blue circle and a callout box. The callout box contains the following text: 'Available space is 105G'.

Filesystem	Size	Used	Avail	Use%	Mounted on
devtmpfs	1.9G	0	1.9G	0%	/dev
tmpfs	1.9G	32K	1.9G	1%	/dev/shm
tmpfs	1.9G	186M	1.7G	10%	/run
tmpfs	1.9G	0	1.9G	0%	/sys/fs/cgroup
/dev/sda2	976M	227M	683M	25%	/
/dev/sda5	5.8G	2.7G	2.9G	49%	/usr
/dev/sda1	239M	194M	29M	88%	/boot
/dev/sda6	3.9G	676M	3.0G	19%	/var
/dev/sda3	50G	6.0G	41G	13%	/usr/krp
/dev/mapper/vg_state-lv_backup	200G	96G	105G	48%	/_Stateless
overlay	200G	96G	105G	48%	/_Stateless/backup
/overlay2/760d154544					fe7eaab1253f271dcb7a135
shm	64M	0	64M	0%	/_Stateless/backup
/containers/771cc5					7b500c2026/3nm
tmpfs	379M	0	379M	0%	/run/user/0
//19	932G	855G	78G	92%	/mnt/nas/nas92public2
//19	932G	855G	78G	92%	/mnt/nas/nas92public

- Encryption – If backups are being encrypted, save the encryption passphrase in a safe place. You must manually configure encryption with this same passphrase on the new CentOS 7 appliance.

IMPORTANT! If you are not able to configure encryption on the CentOS 7 appliance using the original passphrase, there is no way to recover the encrypted backups that were migrated from the CentOS 6 appliance.

- Cold backup copy devices – Any cold backup copy target devices have been disconnected.
- Backup and cold backup copy jobs – There are no active backup and cold backup copy jobs. If jobs are running, wait for them to complete or cancel them before starting the migration.
- Recovery objects – Check these tabs for any active recovery objects: Recover > File Level Recovery, Instant Recovery, and Replicas. Tear down any objects before starting the migration. You will need to recreate these objects on the CentOS 7 appliance.



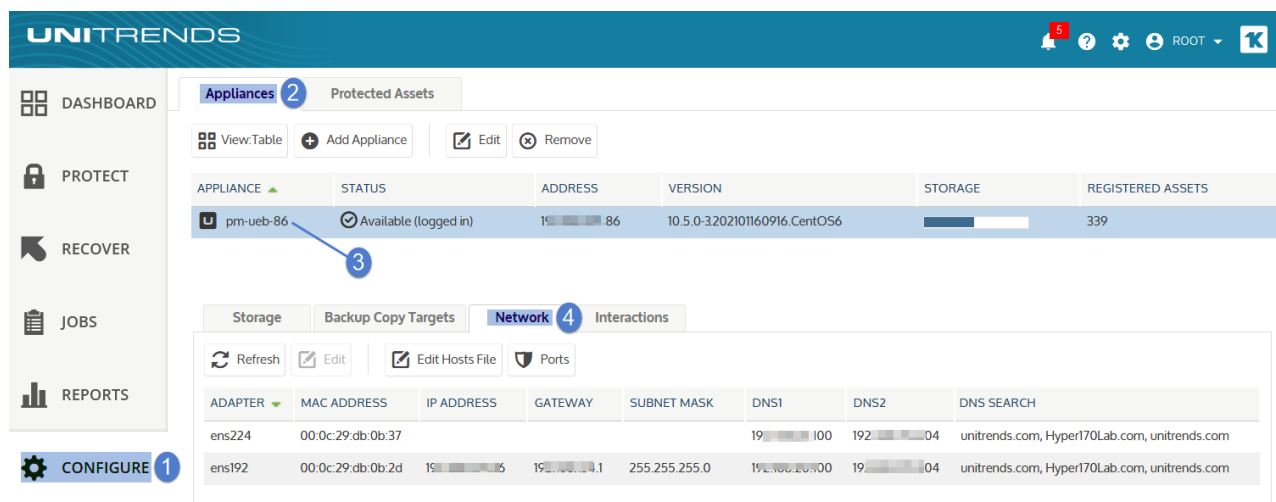
Deployment requirements for CentOS 7 Unitrends Backup virtual appliance

You will deploy a new CentOS 7 Unitrends Backup appliance that will be used to replace your original CentOS 6 appliance. Before deploying your Unitrends Backup appliance, verify that the following requirements have been met:

- Hypervisor requirements – You can deploy Unitrends Backup to these free or paid versions of ESXi: 5.5, 6.0, 6.5, 6.7, or 7.0.
- Network requirements – During deployment, you will configure these network settings: IP address and subnet, gateway, and DNS. Be sure to use the same network configuration as the original CentOS 6 appliance. To view the network settings of the CentOS 6 appliance, select **Configure > Appliances > Network**:

Notes:

- 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.
- 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. For details, see [Appliance network settings > Additional ports](#) in the [Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup](#)

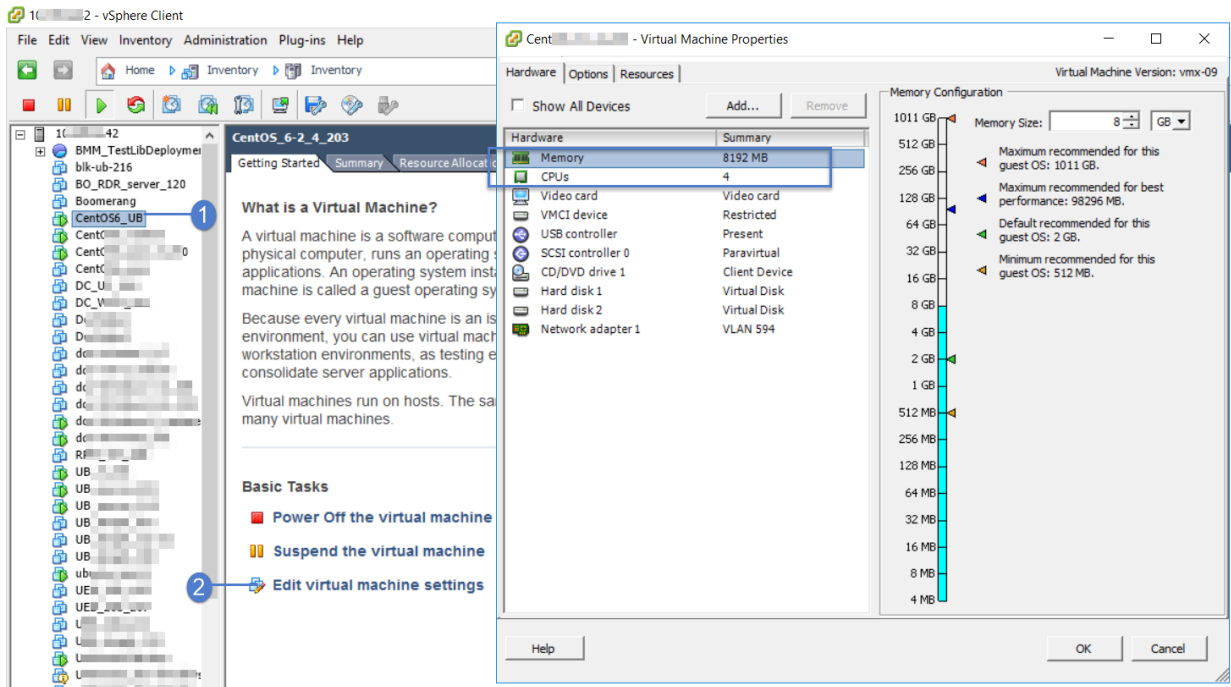


- Virtual machine resource requirements – The following minimum resources are required:
 - 100GB of space for the VM's initial disk.
 - A minimum of 2 virtual processors (CPUs) or the number of virtual processors (CPUs) on the original CentOS 6 appliance, whichever is greater.
 - A minimum of 8GB of RAM or the amount of RAM on the original CentOS 6 appliance, whichever is greater.

To Check the CPU and RAM of the CentOS 6 appliance in the appliance UI (? > About):

The screenshot displays the Unitrends backup summary interface for a CentOS 6 appliance. The 'About this Appliance' window is open, showing hardware information. The 'Processor Cores' field is highlighted with a blue box and a '2' callout, showing a value of 8. The 'Memory (GB)' field is also highlighted with a blue box and a '2' callout, showing a value of 15.9 GB. A '1' callout points to the 'Got Questions? Ask the' link in the top right corner. The left sidebar shows navigation options: DASHBOARD, PROTECT, RECOVER, JOBS, REPORTS, and CONFIGURE. The top right corner shows user information (ROOT) and a notification bell with 13 alerts. A dropdown menu is open, showing options: ONLINE HELP, COMMUNITY, OPEN SUPPORT TUNNEL, PRODUCT TOUR, FEEDBACK, ABOUT, and RELEASE FEATURES.

To check the CPU and RAM of the CentOS 6 appliance by using the ESXi server, use Edit Virtual Machine Settings:



This page is intentionally left blank.



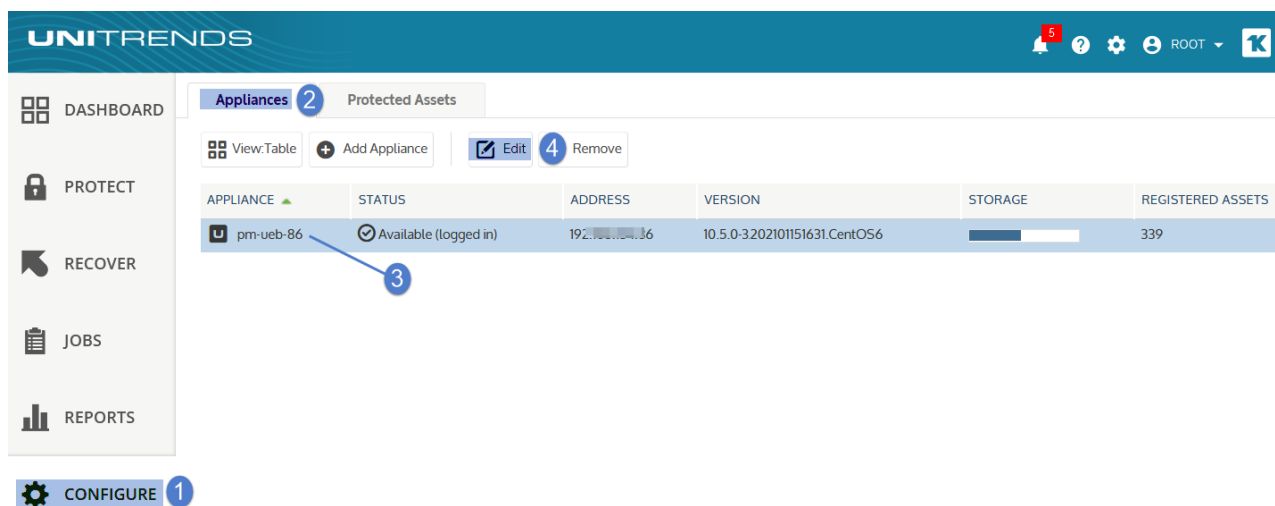
Chapter 3: Migration Procedures

Use these procedures to migrate your CentOS 6 appliance to CentOS 7.

Step 1: Migrate data on the CentOS 6 appliance

IMPORTANT! Before running this procedure, use your ESXi server to consolidate snapshots on the CentOS 6 VM. If your backups are encrypted, be sure you can access the passphrase that was configured on the CentOS 6 appliance. Once data has been migrated, the original CentOS 6 appliance is no longer usable. Any encrypted backups can only be recovered by configuring encryption on the CentOS 7 appliance using the CentOS 6 passphrase.

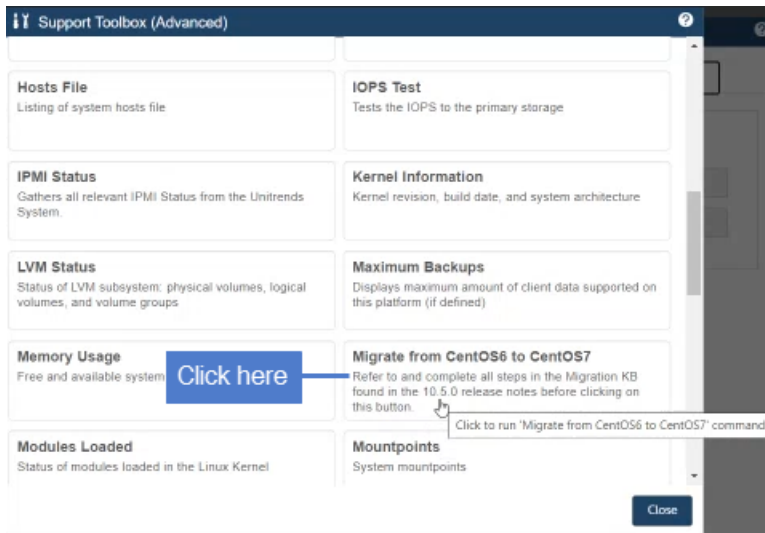
- 1 Log in to the CentOS 6 appliance UI.
You must log in directly to the appliance. You cannot access the Support Toolbox of a managed appliance.
- 2 On the **Configure > Appliances** page, select the appliance and click **Edit**.



- 3 Click **Advanced** and select **Support Toolbox**.

- 4 In the Support Toolbox (Advanced) dialog, scroll down and click **Migrate from CentOS 6 to CentOS 7**.

IMPORTANT! Migration time varies by database size. Do not manually close the user interface while the migration is running. It is safe to close the UI after the Results Migration message displays.



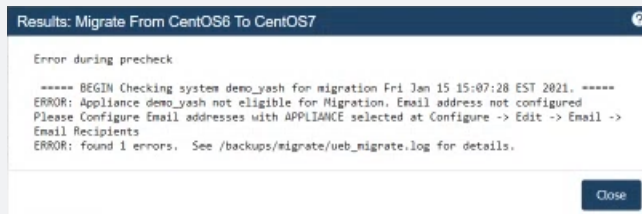
- 5 The migration tool does the following:

- Verifies that all appliance requirements have been met.

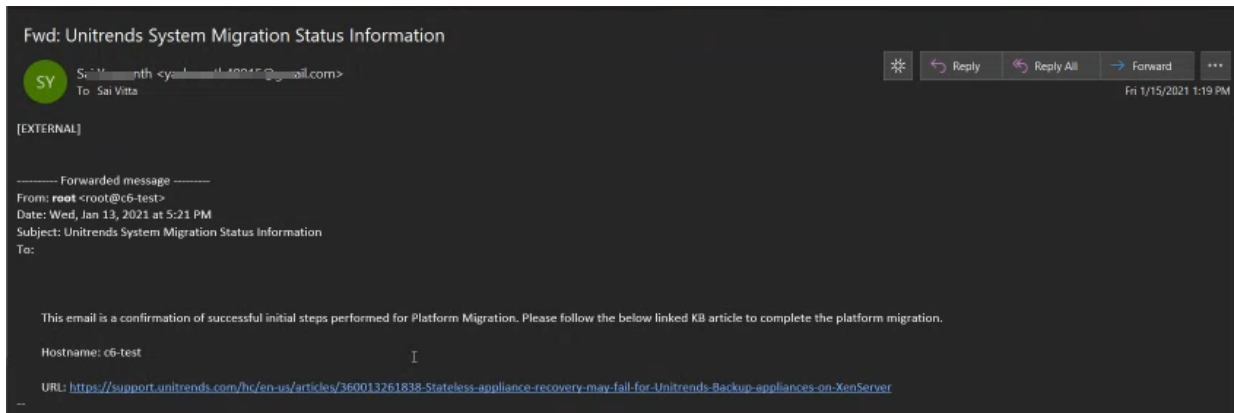
Notes:

- If requirements have not been met, a message displays describing the issue.

- Click **Close** to exit the message, then address the requirement.



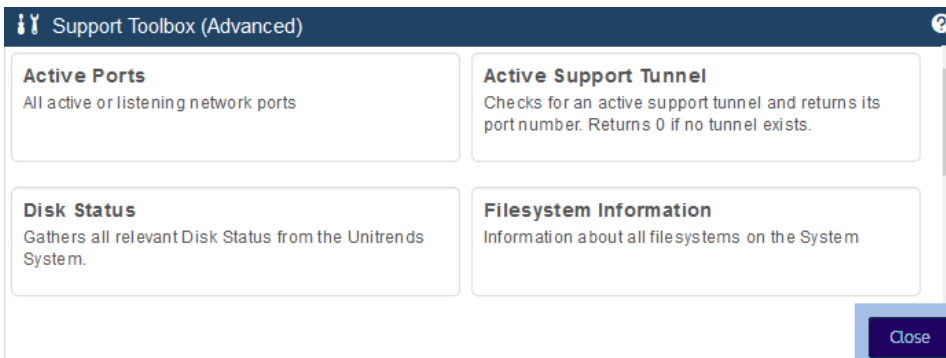
- Migrates the database, sends a confirmation message to the Appliance email recipients, then powers off the CentOS 6 VM. Sample confirmation email:



- 6 A confirmation message displays. Click **Close** to exit the message.



- 7 Click **Close** to exit the Support Toolbox.



Step 2: Deploy the CentOS 7 Unitrends Backup VM

Use the following procedure to deploy the Unitrends Backup VM by using the OVA file.

1 Download the Unitrends Backup OVA:

- Go to <https://www.unitrends.com/download/enterprise-backup-software>, complete the form under Try Unitrends Backup, and click **Download Now**.



The screenshot shows a registration form titled "Unitrends Backup Software Free Trial". Below the title is the text "Try Unitrends Backup Software Free For 30 Days". The form contains two input fields: "Email*" with the value "dbarrett@unitrends.com" and "Industry*" with the value "Business Services". A blue button labeled "Enter details" with a circled "1" is positioned to the right of the input fields. Below the form is a red button labeled "Download Now" with a circled "2".

- Select **VMware vSphere**. Click to download the OVA and save it on the machine you will use to access your ESXi server for the deployment.

Unitrends Backup Software Free Trial

Here's Your Download

VMware vSphere | Microsoft Hyper-V | Citrix XenServer
Nutanix AHV | System Requirements

1 Click VMware vSphere

Download and Deploy on vSphere

This free trial of Unitrends Backup software deploys as a virtual appliance on VMware vSphere. You have 30 days to test drive this fully-featured, Enterprise Plus version of Unitrends Backup. Be sure to register your installation to qualify for free expert help from our Evaluations team.

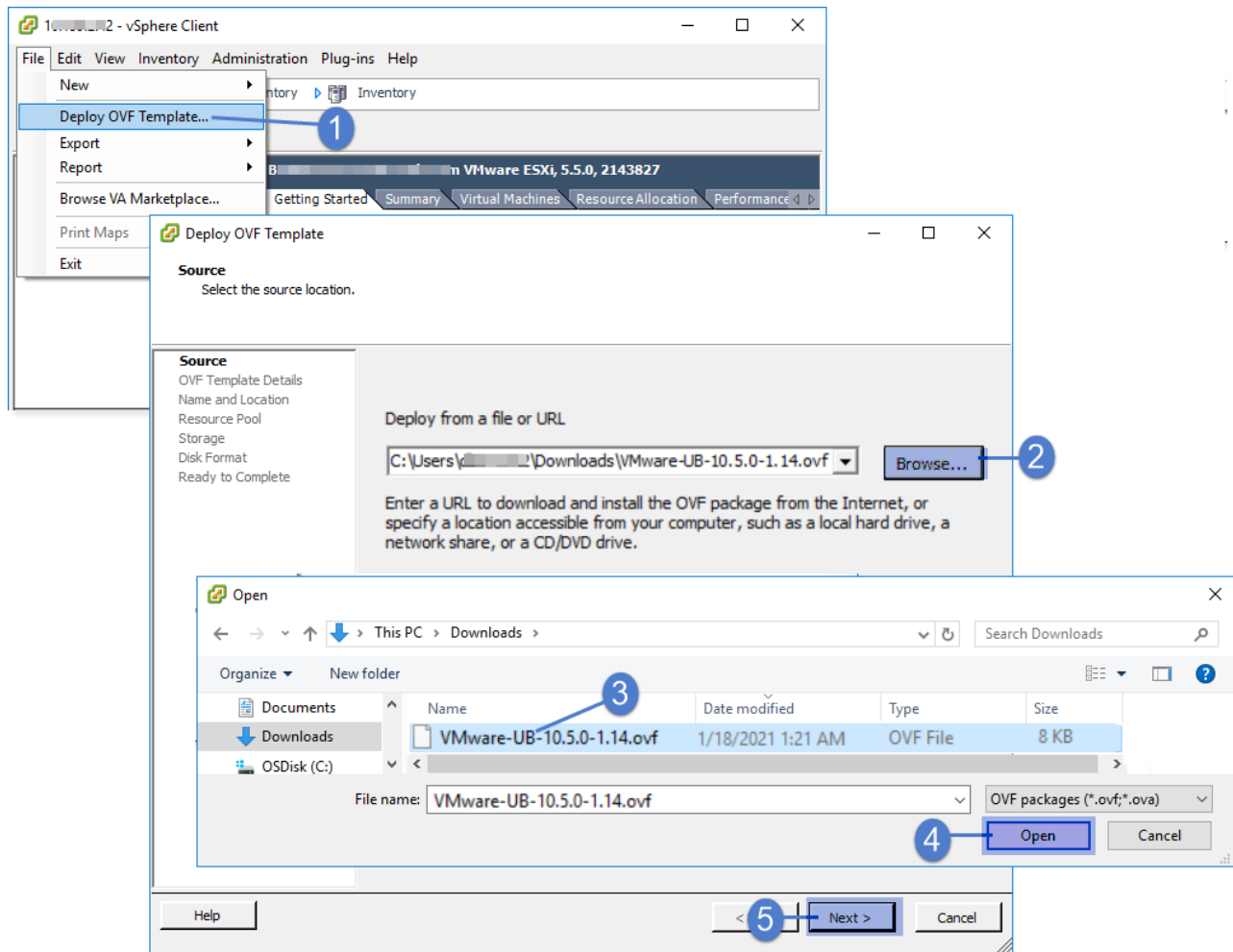
Need help getting started? Read [this post in the Unitrends Community](#).

NOTE: If you are running ESXi Free, you MUST use [the OVA here](#).

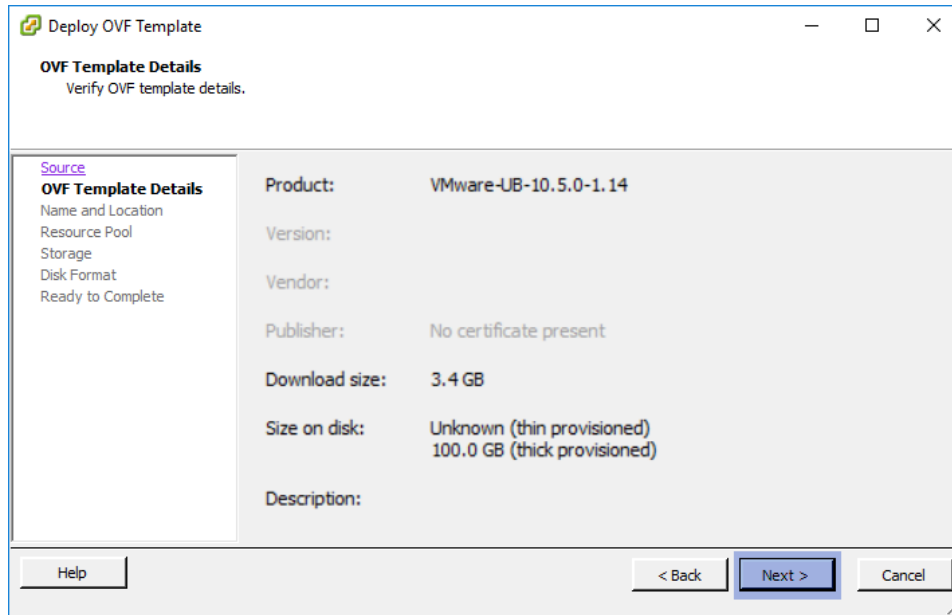
2 Click to download the OVA

Download EXE Now

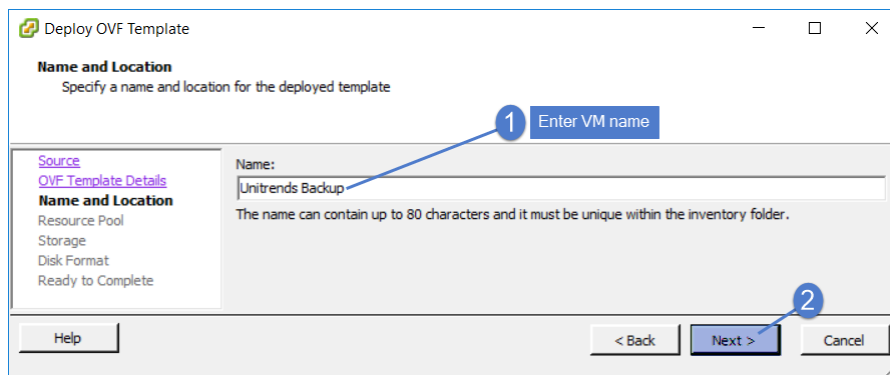
- 2 From the machine on which you saved the Unitrends Backup OVA file, access your ESXi server using vSphere Client.
- 3 Select **File > Deploy OVF template**.
- 4 Browse to the extraction location, select **VMware-UB-version.ovf**, click **Open**, then click **Next**.



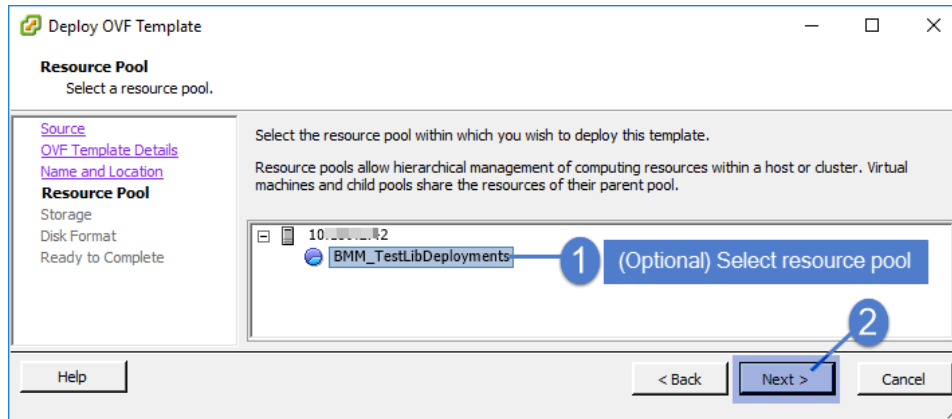
- 5 Verify details and click **Next**.



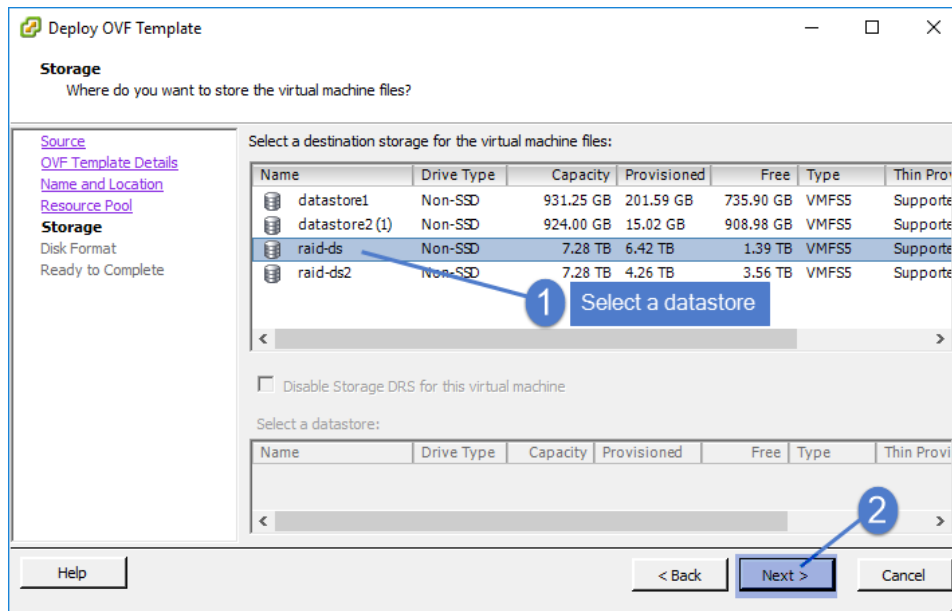
- 6 Enter a display name for the Unitrends Backup VM. The name can contain only alphanumeric characters, dashes, and underscores. This is the name that will display for the VM in your hypervisor. Click **Next**.



- 7 (Optional) If your environment has resource pools, you can opt to choose one for the Unitrends Backup VM. If your environment does not have resource pools, you do not see this step. Click **Next** to continue.

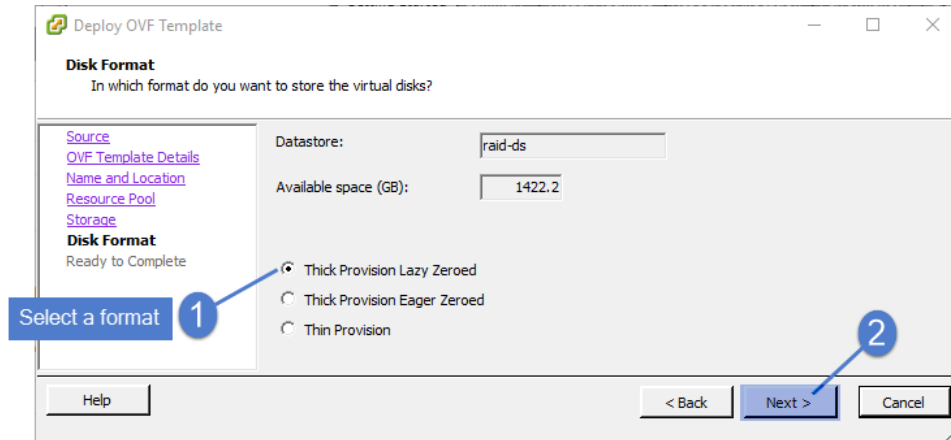


- 8 Select the datastore that will be used to create the Unitrends Backup VM. Click **Next**.

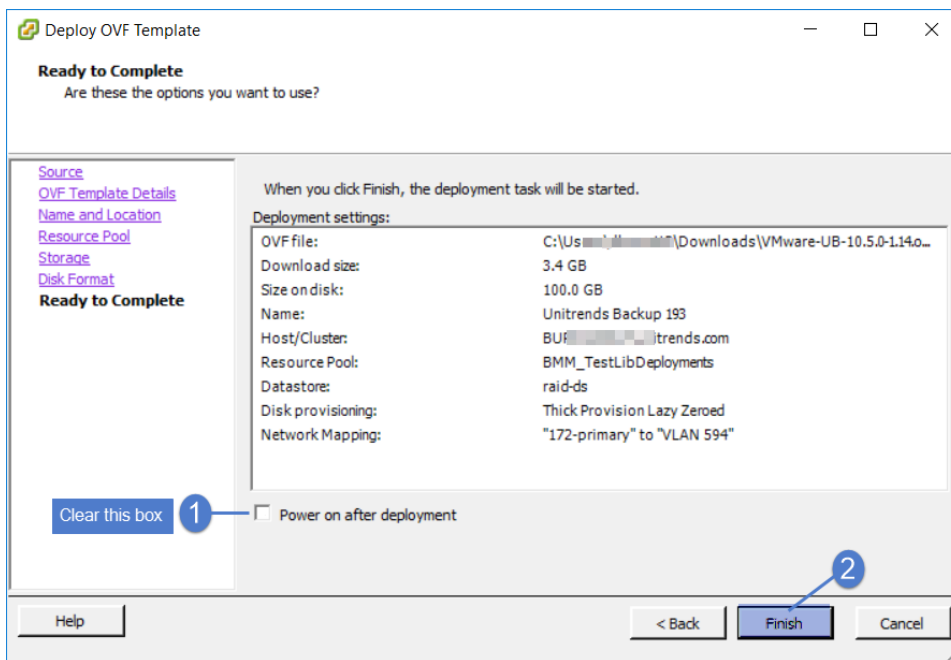


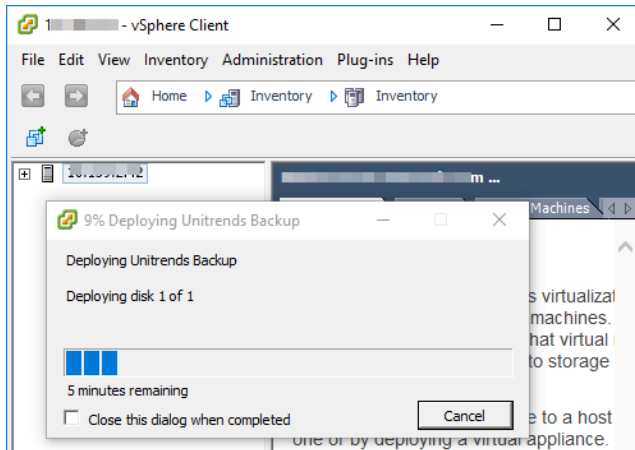
- 9 Select the disk format. Click **Next**.

For best performance, use a thick provisioned format.

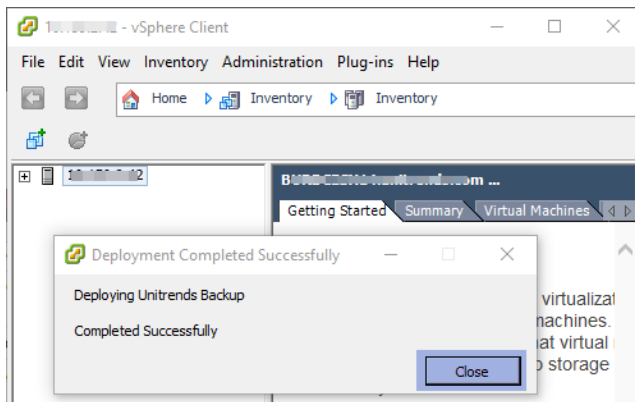


- 10 If the server has multiple virtual networks, select one from the list and click **Next**. If the server has only one virtual network, you are not prompted for a selection.
- 11 On the Ready to Complete screen, do not select **Power on after deployment**.
- 12 Click **Finish** to deploy.

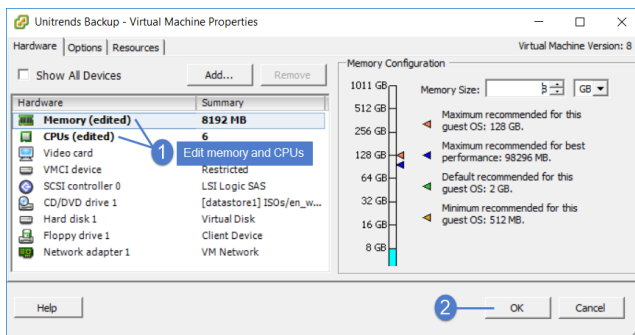




- 13 When deployment is complete, close the confirmation message.



- 14 Edit the virtual machine settings to adjust the CPU and memory to meet or exceed the settings of the CentOS 6 appliance. Click **OK**.



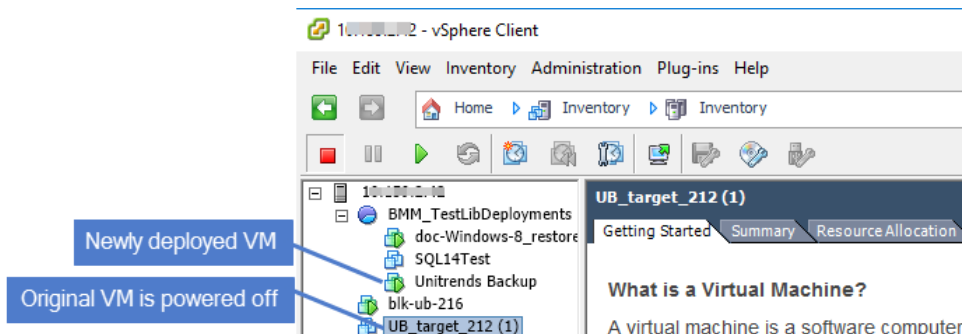
Step 3: Attach backup storage

In this step you will attach the storage that contains backups from the CentOS 6 Unitrends Backup appliance.

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

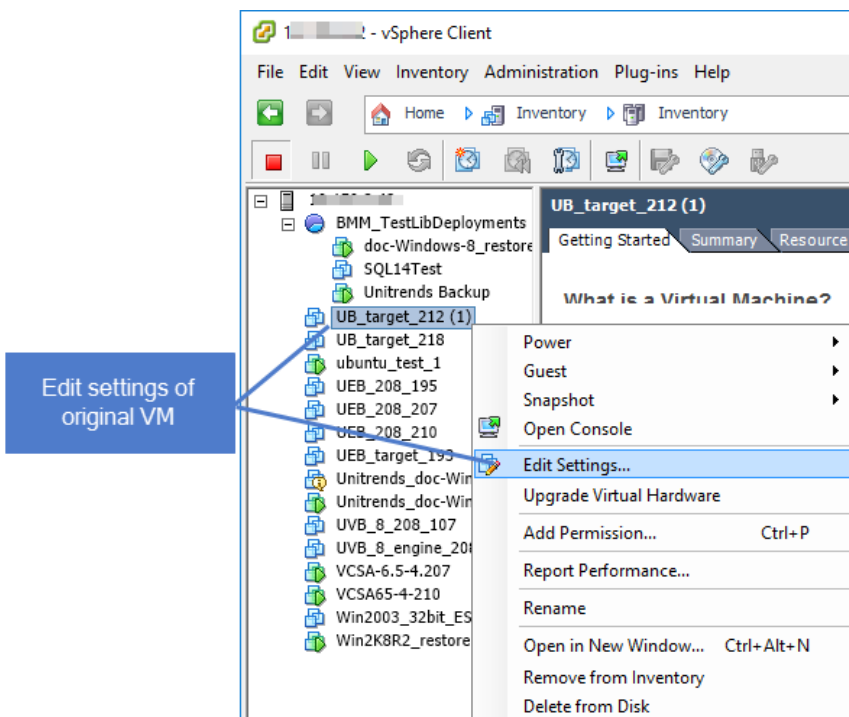
To add a VMDK that contains backups from the CentOS 6 Unitrends Backup appliance:

- 1 Access your ESXi server using vSphere Client.
- 2 Ensure that the CentOS 6 VM is powered off.



3 Identify the disk(s) that you want to add to the CentOS 7 VM by doing these steps:

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



- Select each hard disk to view details. Note the disk file details of the one(s) you will add to the CentOS 7 VM. (You will need the datastore and disk name to locate the disk in vSphere Client).

Notes:

- You must add all backup storage disks from the original CentOS 6 VM.
- Do not add Hard Disk 1. This 100GB disk was created during VM deployment and is NOT used to store backups.
- You must add the first backup storage disk (typically Hard Disk 2) before you add any other backup storage disks.

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

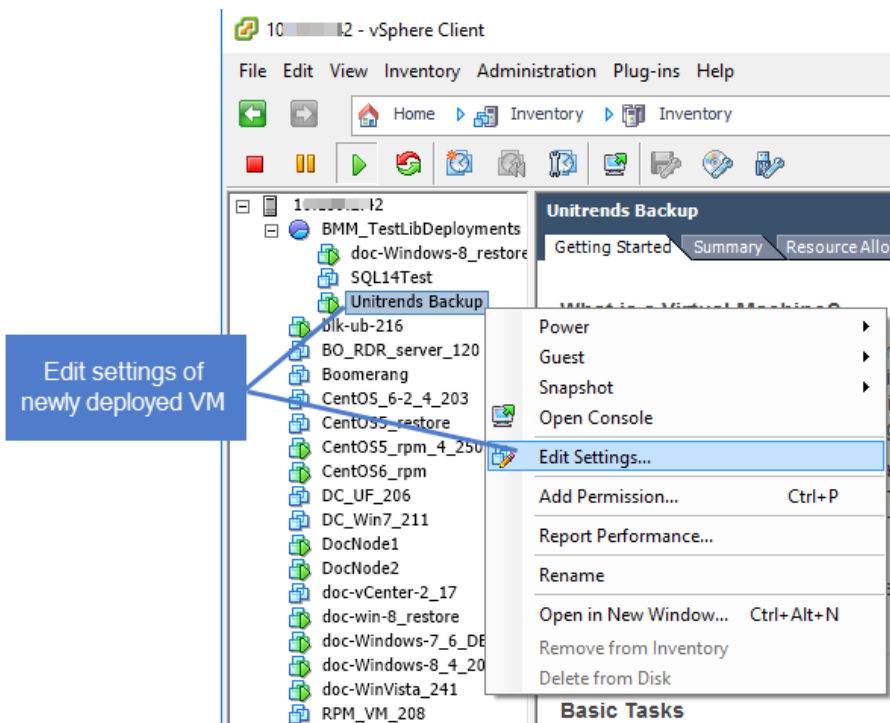
Hard disk 1 is the VM's initial disk and is not used for backup storage. Do NOT add this disk to the newly deployed VM.

Hard disk 2 is the VM's first backup storage disk. Add this disk to the newly deployed VM.

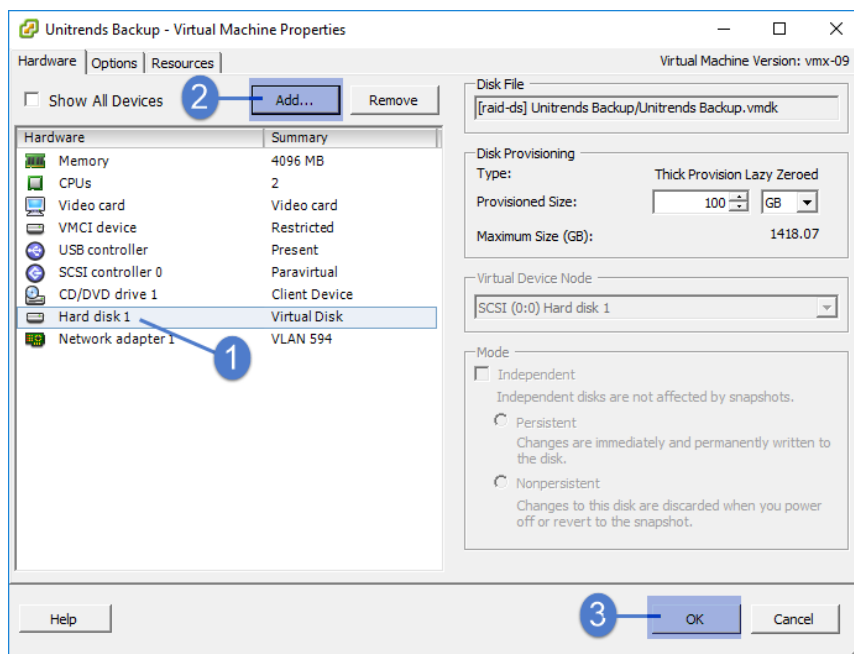
This Unitrends Backup VM has only one backup storage disk (hard disk 2). If there were other hard disks, you would add them after hard disk 2 had been added.

4 Add the disk(s) to the CentOS 7 VM by doing these steps:

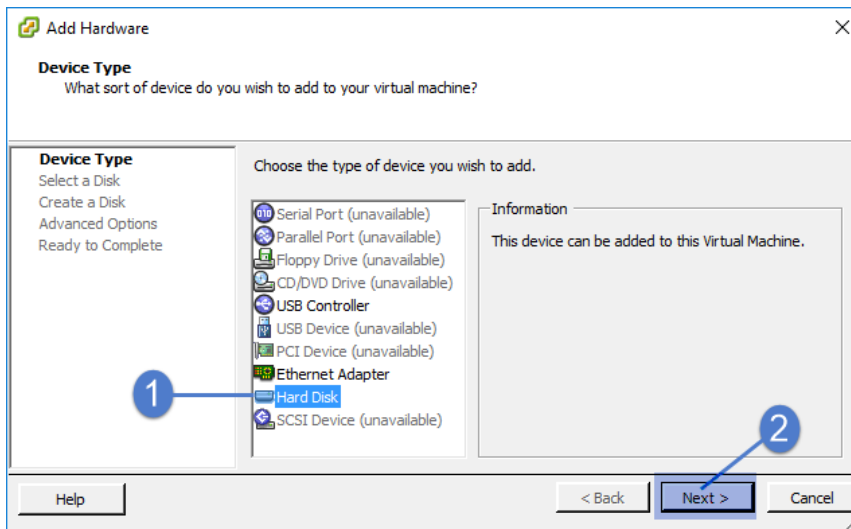
- Right-click the CentOS 7 VM and select **Edit Settings**.



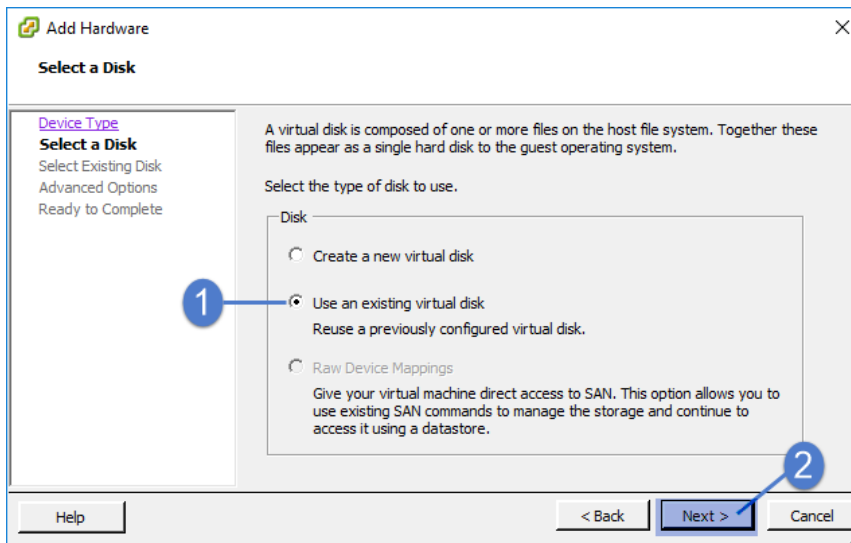
- Select **Hard disk 1**, click **Add**, then **OK**.



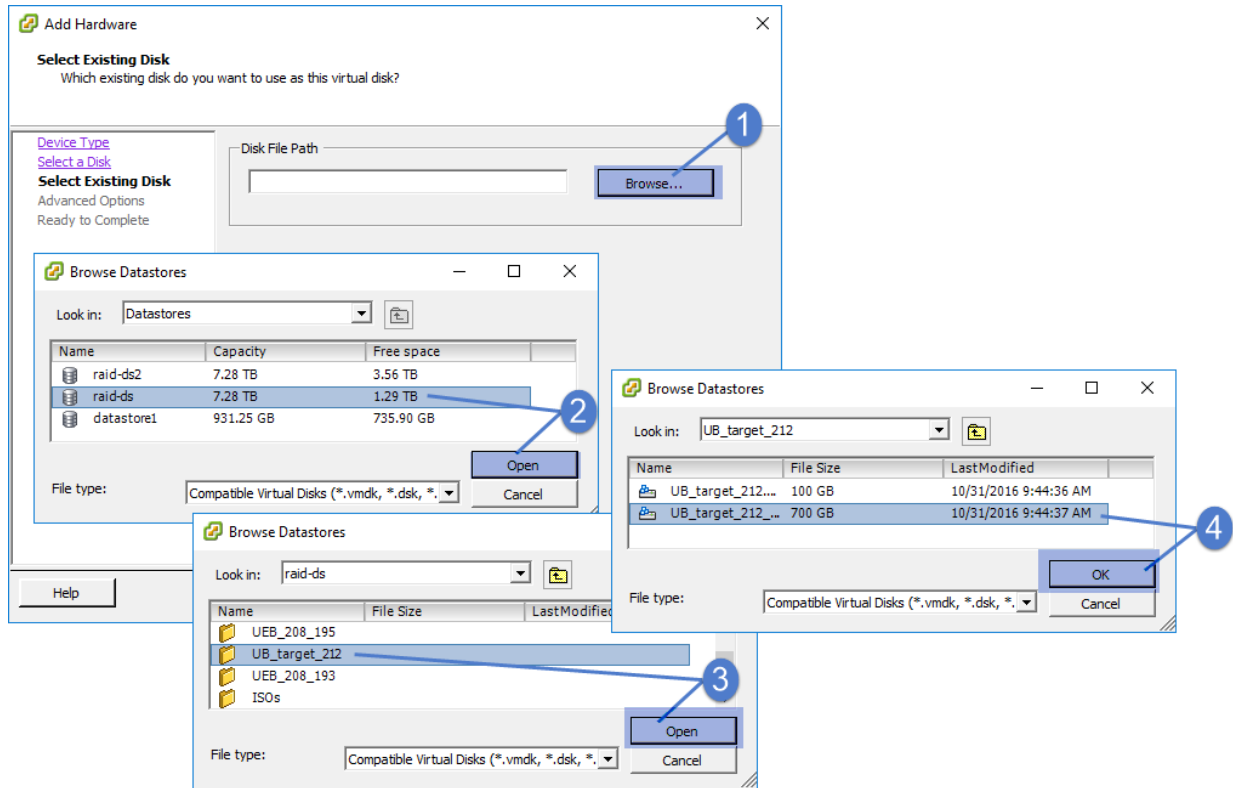
- Select **Hard Disk** and click **Next**.



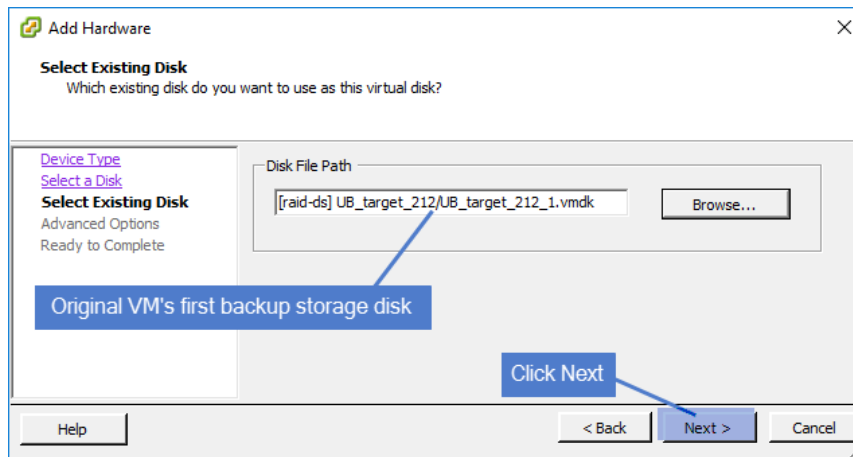
- Select **Use an existing virtual disk** and click **Next**.



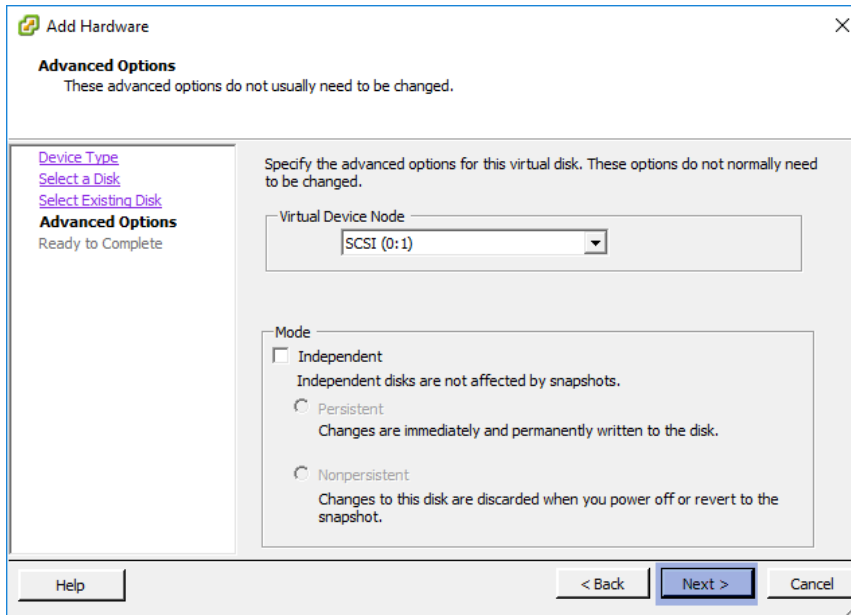
- Click **Browse**. Browse to the CentOS 6 VM's first backup storage disk and click **OK**.



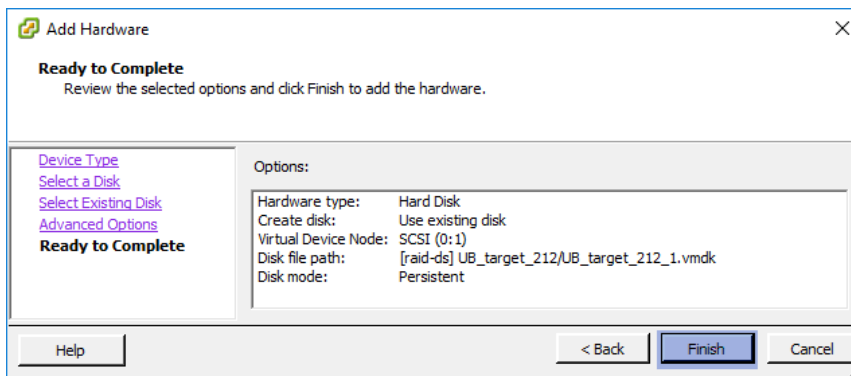
- Click **Next** to continue.



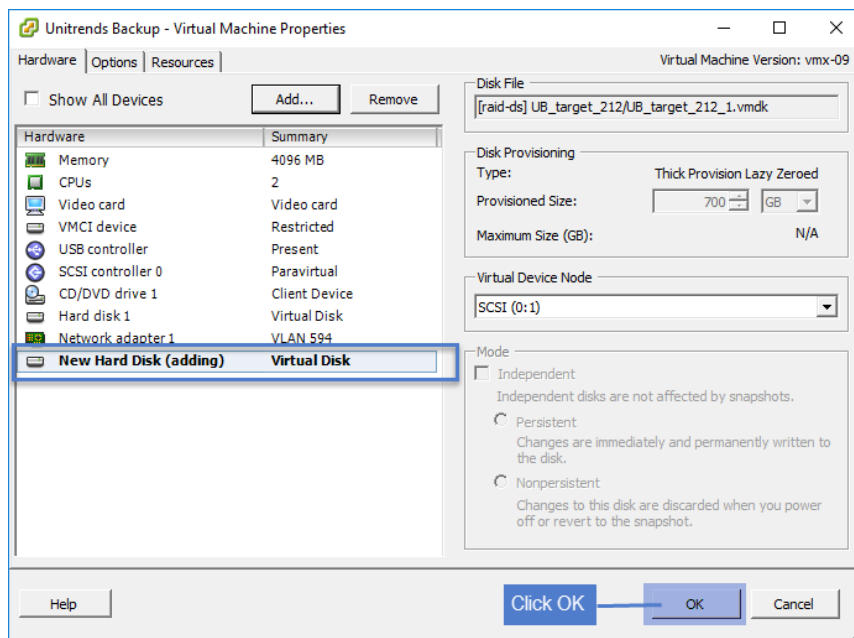
- Click **Next** to accept the default Advanced Options.



- Click **Finish**.



- Click **OK**.



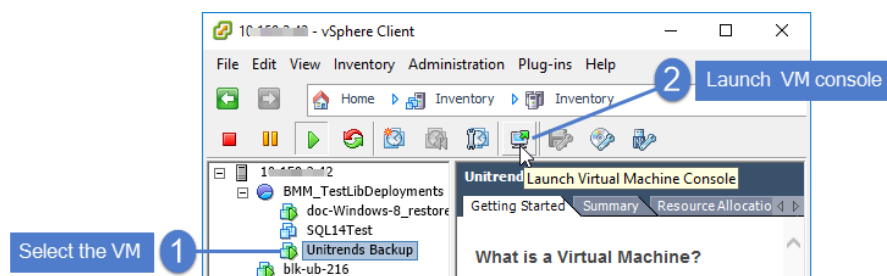
- 5 (If needed) If the CentOS 6 VM has multiple backup storage disks, repeat [step 4](#) to add those disks.
- 6 After attaching all backup storage disks, proceed to "[Step 5: Set up the CentOS 7 appliance using the Quick Setup Wizard](#)".

Step 4: Configure network settings

IMPORTANT! Be sure to enter settings that match those of the original CentOS 6 appliance.

- 1 From vSphere Client, access the Unitrends Backup VM's console interface by clicking the **Launch Virtual Machine Console** icon.

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

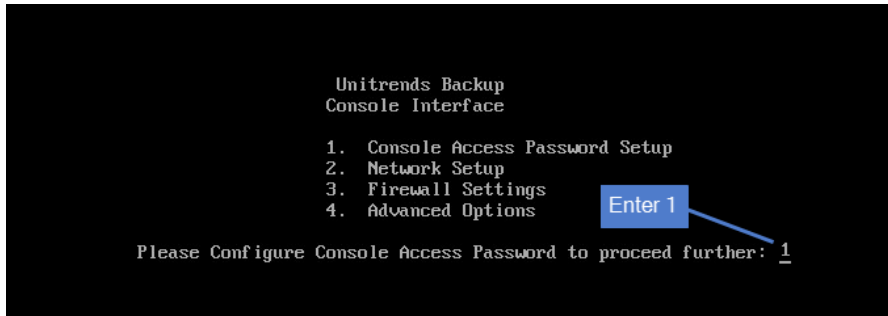


The remaining steps are run from the Unitrends Backup Console Interface. On these screens, you select a menu option by entering a number in the **Please enter choice** field.

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.

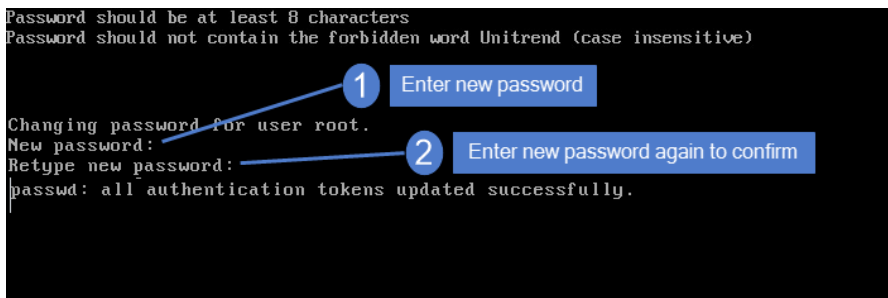
- 2 On the Console Interface screen, enter **1** in the **Please Configure Console Access Password...** field.



- 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 CentOS 7 appliance using the Quick Setup Wizard](#)" on page 38.)
- 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**.

```
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 the **IP address**, **Netmask**, and **Gateway** of the CentOS 6 appliance. 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: 192.168.1.20 — 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:   192.168.1.1
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:  vmware-ub
Edit DNS configuration? [n/Y]: Y Enter Y
```

```
Current Primary DNS: n/a
Enter new Primary DNS: 192.168.1.138 Enter IP of primary DNS server
```

```
Current Secondary DNS: n/a
Enter new Secondary DNS: 192.168.1.100 (Optional) Enter IP of secondary DNS server
(Leave blank if no secondary DNS desired)
```

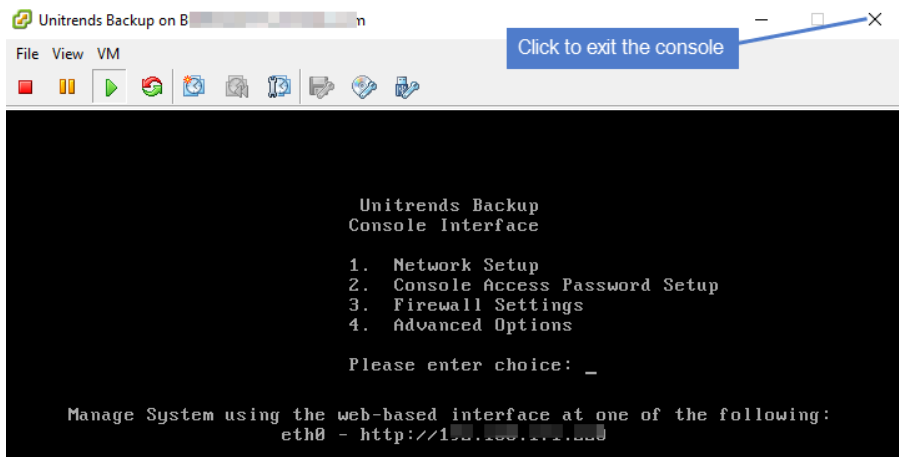
```
Current DNS Domain: vmware-ub
Enter new DNS Search Domain: unitrends.com Enter domain
```

```
Current Primary DNS: n/a
Current Secondary DNS: n/a
Current DNS Domain: vmware-ub
New Primary DNS: 192.168.1.100
New Secondary DNS: 192.168.1.100
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
```

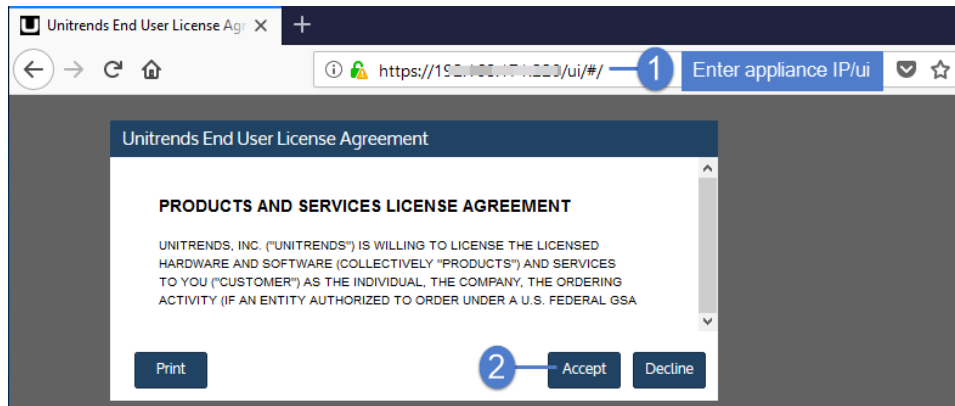
10 Exit the VM console.



Step 5: Set up the CentOS 7 appliance using the Quick Setup Wizard

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: 9/4/2019

Time: 16:05:03

Time Zone: America/New_York

Use an NTP Server

NTP Server Addresses: Add NTP Server Address (Optional) ?

- 0.centos.pool.ntp.org
- 1.centos.pool.ntp.org

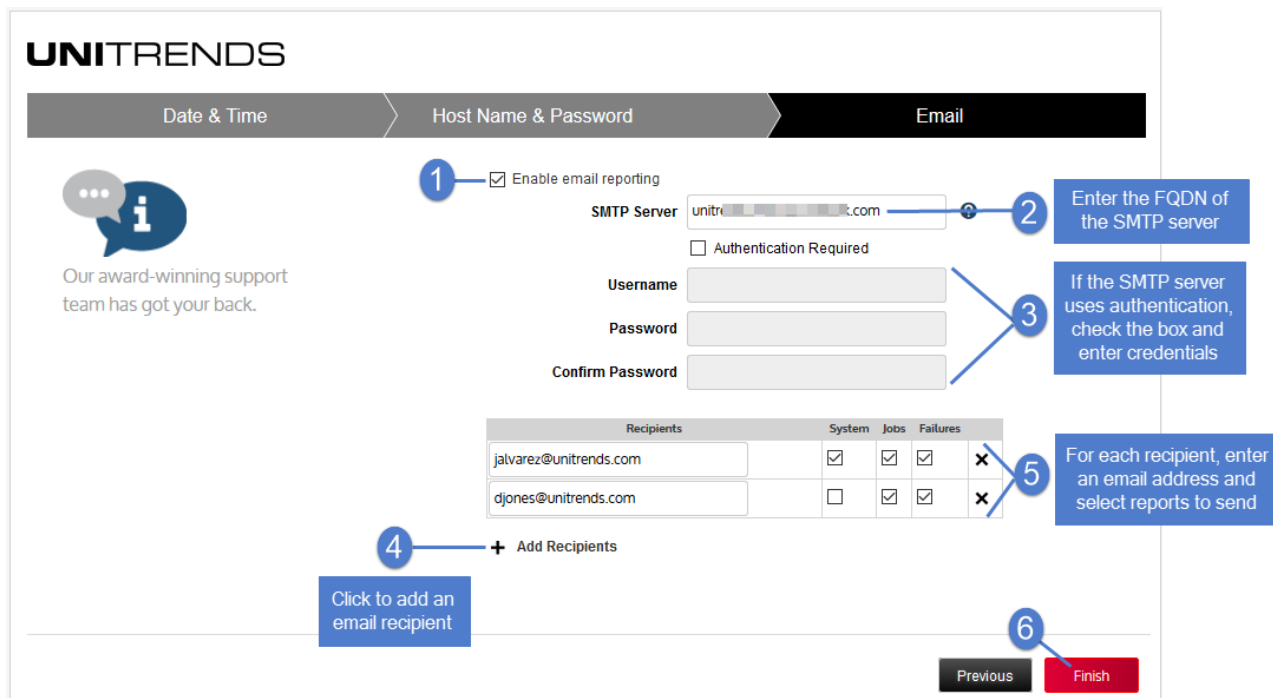
Click to continue Next

- 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**.

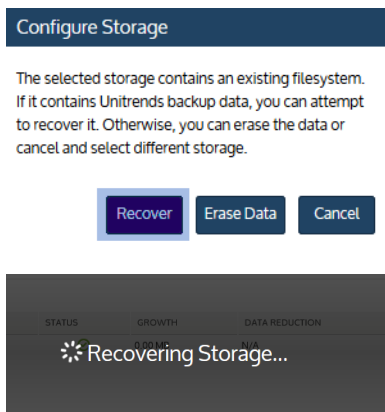
Notes:

- 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.

- 5 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**.



7 Click **Recover** to add the migrated backups to the appliance:



Step 6: (If needed) Configure encryption with the CentOS 6 passphrase

If backups were being encrypted on the CentOS 6 appliance, you must configure encryption with the passphrase that was used by the CentOS 6 appliance. If you do not use the original passphrase, any encrypted backups that were migrated cannot be recovered.

Use this procedure to configure encryption:

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

The screenshot shows the UNITRENDS dashboard. On the left is a navigation menu with options: DASHBOARD, PROTECT, RECOVER, JOBS, and REPORTS. At the bottom left is a 'CONFIGURE' button with a gear icon and a circled '1'. The main area is titled 'Appliances' with a circled '2'. Below this are buttons for 'View Table', 'Add Appliance', 'Edit' (circled with '4'), and 'Remove'. A table displays appliance information:

APPLIANCE	STATUS	ADDRESS	VERSION	STORAGE	REGISTERED ASSETS
pm-ueb-86	Available (logged in)	192.168.1.16	10.5.0-3.202101151631.CentOS6	<div style="width: 100%;"></div>	339

The 'pm-ueb-86' appliance name is circled with a '3'.

- 2 Select the **Advanced** tab.
- 3 Check **Enable Encryption**.
- 4 Enter the passphrase used by the CentOS 6 appliance in the **Passphrase** and **Confirm Passphrase** fields.

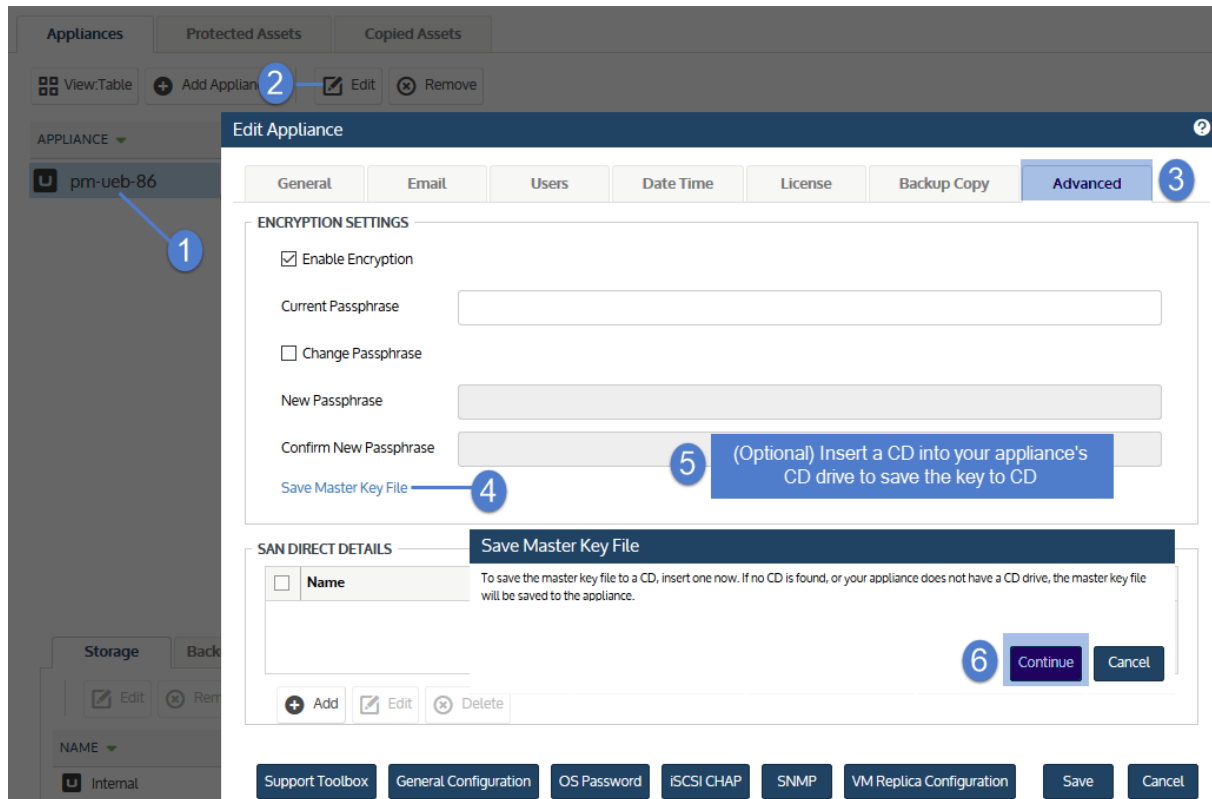
IMPORTANT! Be sure to keep the passphrase secure. If you forget the passphrase there is no way to recover it.

- 5 Click **Save**.

The screenshot shows the 'Edit Appliance' dialog box. At the top, there are tabs: 'General', 'Email', 'Users', 'Date Time', 'License', 'Backup Copy', and 'Advanced' (circled with '1'). Below the tabs is the 'ENCRYPTION SETTINGS' section. The 'Enable Encryption' checkbox is checked and circled with a '2'. Below it are two text input fields: 'Passphrase' and 'Confirm Passphrase', both containing masked characters and circled with a '3'. A blue callout box points to these fields with the text 'Enter and confirm the encryption passphrase'. At the bottom of the dialog, there are several buttons: 'Support Toolbox', 'General Configuration', 'OS Password', 'iSCSI CHAP', 'SNMP', 'VM Replica Configuration', 'Save' (circled with '4'), and 'Cancel'.

- 6 Return to the Edit Appliance dialog.
- 7 Select the **Advanced** tab and click **Save Master Key File**.

- 8 (Optional) If your appliance has a CD drive, you can save the key file directly to a CD. Insert a CD into your appliance's CD drive. (If no CD is inserted, the key file is saved to the appliance's samba share.)
- 9 Click **Continue**.



- 10 You receive a message indicating the master key file was saved to the appliance's samba share or to CD. Click **OK**.

Notice

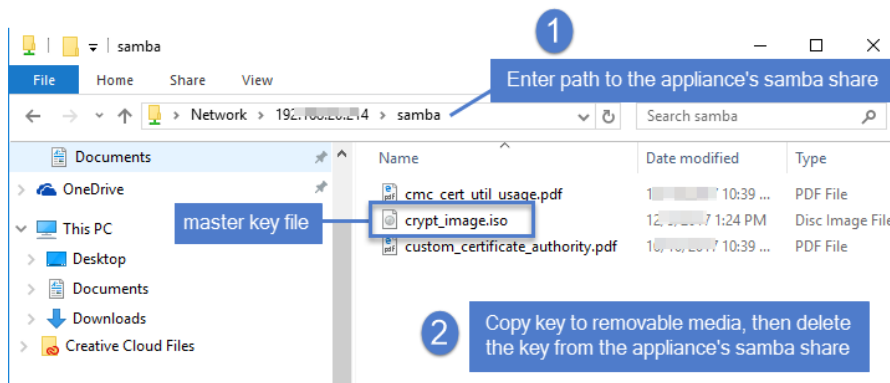
Master key file was saved to the samba share as `crypt_image.iso`. Please delete this when you have copied it to media.

OK

IMPORTANT! Be sure to keep the master key file secure. If you ever need to perform disaster recovery of the appliance, you will need this key to access any encrypted backups.

- 11 If you saved the key to the appliance's samba share, do these steps:
 - Log in to a Windows workstation as an administrator with full system access.
 - Launch File Explorer and enter the following path to access the master key file on the Unitrends appliance:
`\\ApplianceIP\samba`
 - Copy the master key file, called `crypt_image.iso`, to removable media and store it in a safe location.

- Once you have copied the key to removable media, delete *crypt_image.iso* from `\\ApplianceIP\samba` for increased security.



Step 7: (If needed) Add data copy access profiles

Data copy access profiles are not migrated from the CentOS 6 appliance. If you were using the copy data management feature, you need to recreate your data copy access profiles. For details, see [Copy Data Management](#) in the [Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup](#).

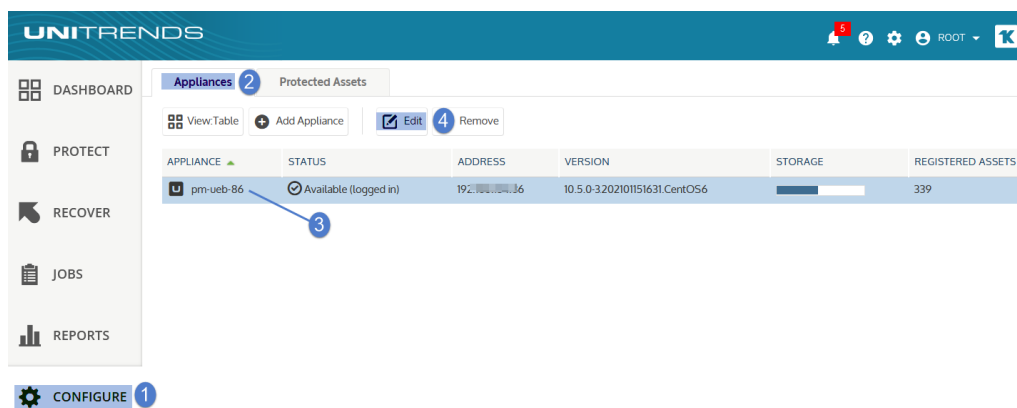
Step 8: Register and license the CentOS 7 appliance

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

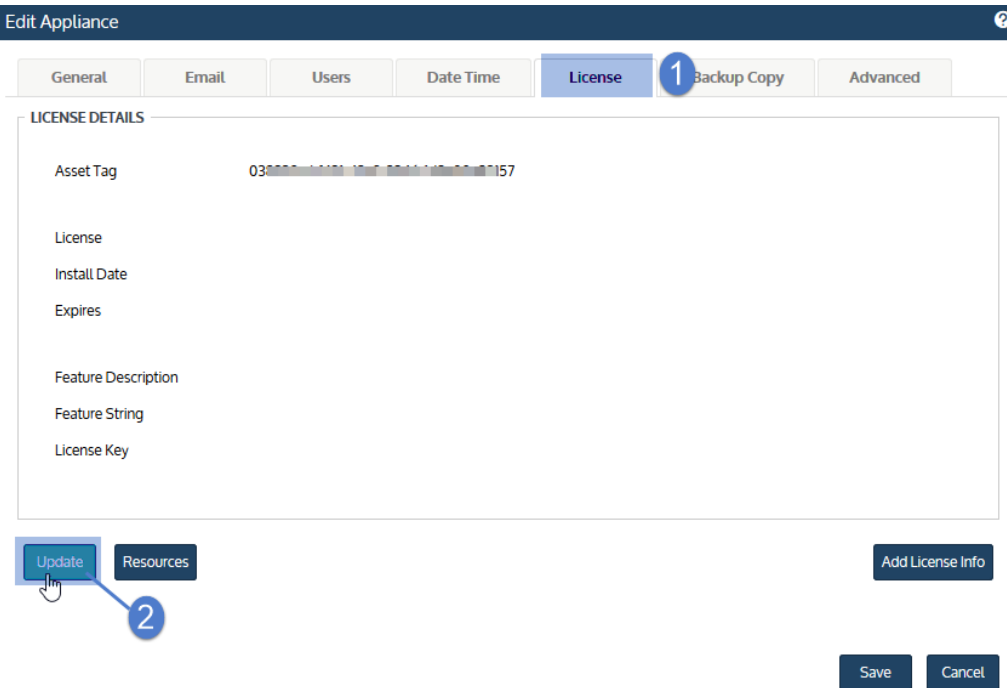
Each appliance requires an activation code and license key. Use the procedures below to register and license the appliance:

To register a Unitrends Backup appliance

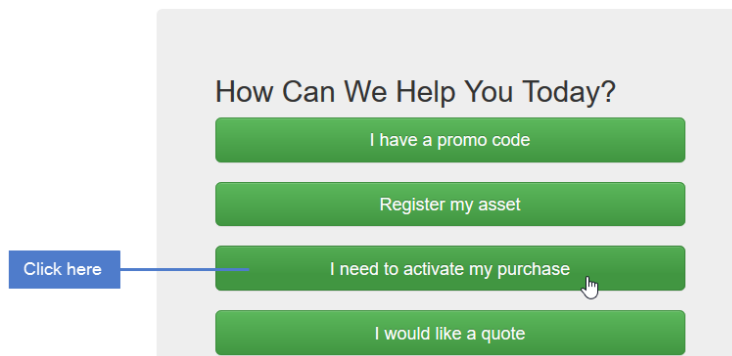
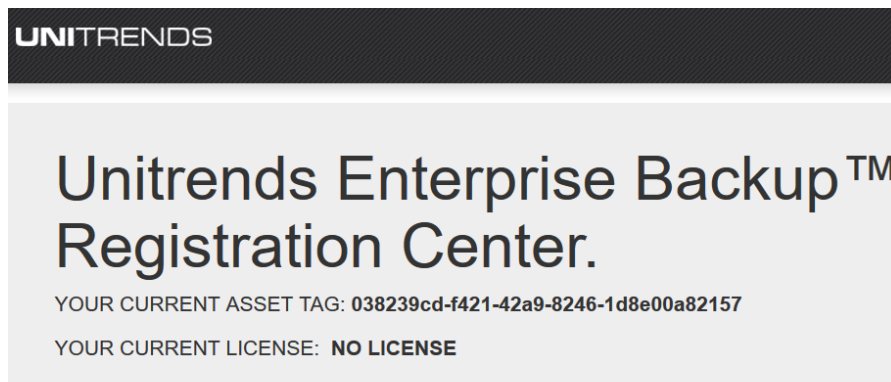
- On the **Configure > Appliances** page, select the appliance and click **Edit**.



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



- 3 Select **I need to activate my purchase**:



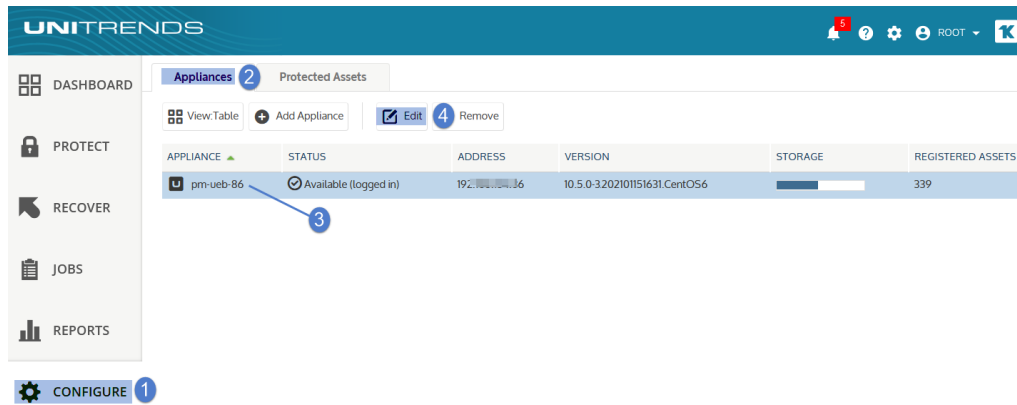
- 4 Complete and submit the applicable form.

Unitrends sends an email containing license details. Use the next procedure to apply this license information to the appliance.

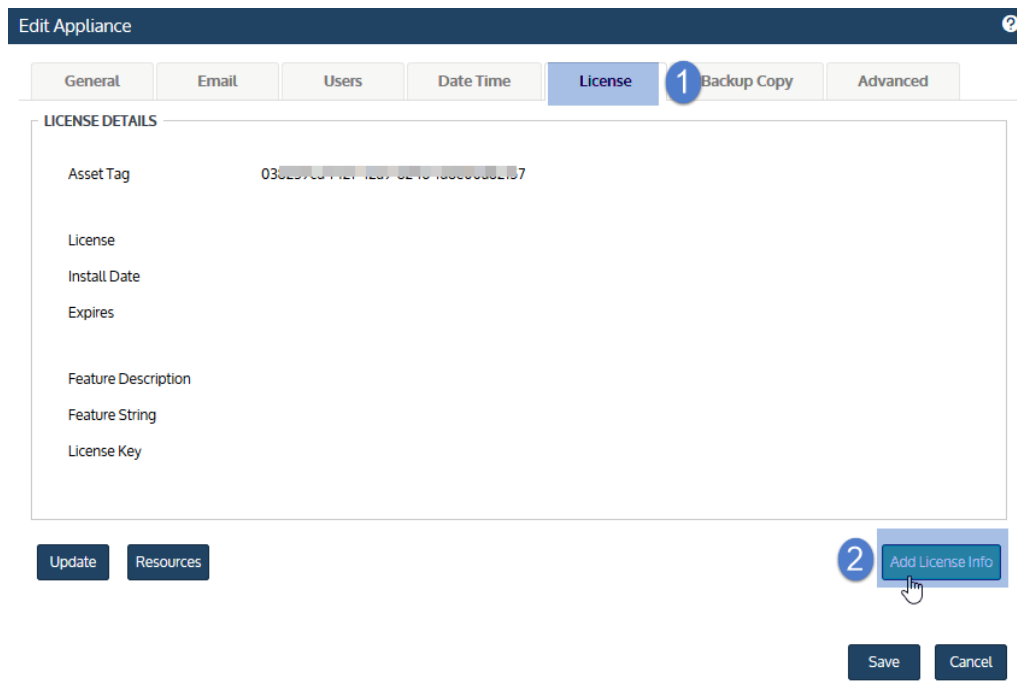
To license a Unitrends Backup appliance

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.

Edit Appliance

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

LICENSE DETAILS

Asset Tag: 038130...82157

License:

Install Date:

Expires:

Feature Description:

Feature String:

License Key:

License Key: f2a37...50a

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: 038130...82157

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: f2a37...50a

License is applied and details display

Upgrade | Resources | Add License Info

Save | Cancel

This page is intentionally left blank.

