



Archiware Pure

User Manual

software version 3.0



Content

1	Preface.....	3
1.1	About This Manual.....	3
1.2	Who Should Read This Document?.....	3
1.3	Software Description.....	4
1.4	Software Licensing.....	5
1.5	Registration.....	6
1.6	Technical Support.....	7
2	Installation.....	8
2.2	System Requirements.....	9
2.3	Deploying the Virtual Appliance.....	10
2.4	Deploying a Standalone Application.....	17
2.5	Deploying an Integrated NAS Application.....	18
3	Accessing the Archware Pure Web GUI.....	27
3.1	Initial Setup Wizard.....	28
4	Backing Up Virtual Machines.....	33
4.1	Automatic Backups.....	34
4.2	Verify.....	35
4.3	Manual Backup and Verify.....	36
5	Archware Pure Web GUI.....	37
5.1	Virtual Machines View.....	38
5.2	Event Log.....	45
5.3	App Configuration.....	46
5.4	System Settings.....	52

Document revision 01/21, Pure 3.0.0



1 Preface

1.1 About This Manual

This document describes the installation and configuration procedures for *Archware Pure*. You will also find examples and case studies for installing, managing and employing *Archware Pure* in a typical production environment.

1.2 Who Should Read This Document?

The information contained in this manual is intended for system administrators who will install and maintain *Archware Pure* as well as for users who will employ *Archware Pure* as a data protection system.



1.3 Software Description

Archware Pure is a software for protecting virtual machines by backing up the content of their virtual disks and allowing their easy recovery. Data is saved to a separate storage, preferably independent of the virtualization system, in order to increase the overall security and level of protection. *Archware Pure* can be deployed as a virtual appliance, running within the virtualization system being protected, it can be installed as a standalone software package on one of the supported Linux platforms or it can be installed on one of the supported NAS devices using the corresponding app marketplace. Regardless of the installation type, *Archware Pure* is designed to be replaceable at any time. In case of a failure within the virtualization system, a new *Archware Pure* instance can simply be downloaded and deployed. After importing the existing backup storage, previously protected virtual machines can easily be restored and work can be seamlessly continued.



1.4 Software Licensing

By default, *Archware Pure* is installed with a fully functional, 30-day trial license. At the end of the trial period, a license needs to be applied.

A free license offers full protection of your vSphere environment, without any limitations to the number of protected virtual machines, ESXi hosts or the total amount of backup data saved. It also grants access to all future *Archware Pure* updates.

Buying an *Archware Pure Support Package* will grant you access to our technical support. For details, please visit our webpage.



1.5 Registration

You can register your copy of *Archiware Pure* by navigating to the *System Settings > Software* menu, entering your *Archiware Portal* login credentials and applying the corresponding license.

Alternatively, you can register a license on Archiware's web site. Upon correctly completing the form, you will receive an activation code. You have to create a license and enter this activation code to enable the functionality that it provides.

You may find further information regarding licensing in section 5.4.2 Software Settings.



1.6 Technical Support

Contact information, software updates, technical documentation and information about the current support programs and options may be found on Archware's web site.



2 Installation

Deployment options

2.1.1. Virtual Appliance

Archiware Pure is delivered as a ready to use virtual appliance and does not require software installation beyond the deployment of the virtual machine template in your virtualization environment. For detailed instructions on how to deploy the *Archiware Pure* virtual appliance, please see 2.3 Deploying the Virtual Appliance.

2.1.2. Standalone Application

Archiware Pure can also be installed as a standalone application on a virtual or physical server. The officially supported operating system is Ubuntu Linux 18.04 LTS.

To install a standalone version, please download the current software version from Archiware's webpage, unpack it into a folder of your choice and run *start.sh* script from the same folder. If you need to change the default *Archiware Pure* port from 443, you can add the desired port number as argument to the start script. For example, the following commands would download and install *Archiware Pure* version 2.0.0 into a */usr/local/pure/vmsn* folder on port 4433:

```
$ sudo mkdir -p /usr/local/pure/vmsn/temp && cd /usr/local/pure/vmsn/  
$ sudo wget  
https://s3.eu-central-1.amazonaws.com/pure-distribution/release/vmsn.2.0.0.tgz  
$ sudo tar xzf temp/vmsn.2.0.0.tgz -C .  
$ sudo ./start.sh 4433
```

2.1.3. Integrated NAS Application

Archiware Pure is also available as an integrated application on supported NAS systems, such as Synology, QNAP and NETGEAR. To install *Archiware Pure* on those systems, simply find it in the respective app marketplace and click Install.

Alternatively, the latest version of *Archiware Pure* can always be downloaded from Archiware's web site and manually installed according to the instructions outlined in the respective NAS system user manual. For detailed instructions on how to install Pure on some of the NAS platforms, please see 2.5 Deploying an Integrated NAS Application.



2.2 System Requirements

2.2.1. Hardware Specification

- VMware vSphere 6.0 or later, any non-free edition¹
- VMware ESXi 6.0 Express Patch 4 (build number 3247720, 2015-11-25) or later
- vCenter Server 6.0 or later (optional)
- CPU: x86-64 processor
- Memory: 2 GB RAM
- Disk space (not including separate disk space used for the backup repository):
 - virtual appliance: 6 GB
 - standalone application: 1 GB
 - Integrated NAS application: 1 GB
- Supported NAS versions:
 - Synology DSM 6.0+ (Intel x86 64-bit)
 - QNAP QTS 4.3.0+ (Intel x86 64-bit)
 - NETGEAR ReadyNAS OS 6.9.1+ (Intel x86 64-bit)

The above are the minimum supported system requirements. Provisioning more processor power and memory to the *Archware Pure*'s virtual appliance will help increase performance when performing multiple parallel backups.

2.2.2. Supported Cloud Services

Archware Pure optionally supports cloning of the backup repository to a cloud based object storage. Supported cloud services are:

- Amazon S3
- Wasabi S3
- Generic S3
- Backblaze B2
- Microsoft Azure

2.2.3. Other Deployment Considerations

Archware Pure protects all types and versions of virtual machines supported by VMware. Because backup operations leverage VM snapshots and virtual disk hot-adding, virtual disks not supported by these mechanisms are automatically skipped from backup.²

In order for *Archware Pure* to be able to backup a virtual machine, it needs access to its virtual disks. Disk access can be achieved either directly or over a network connection. Direct access requires that *Archware Pure* be deployed as a Virtual Appliance and that the ESXi host managing *Archware Pure* has access to the VMware datastore where the virtual machines to be protected reside.

For the virtual disks that reside on inaccessible datastores or in case that *Archware Pure* is not deployed as a Virtual Appliance, backups will use network transfer instead.

¹ This limitation is imposed by VMware as necessary vSphere APIs are disabled in free ESXi

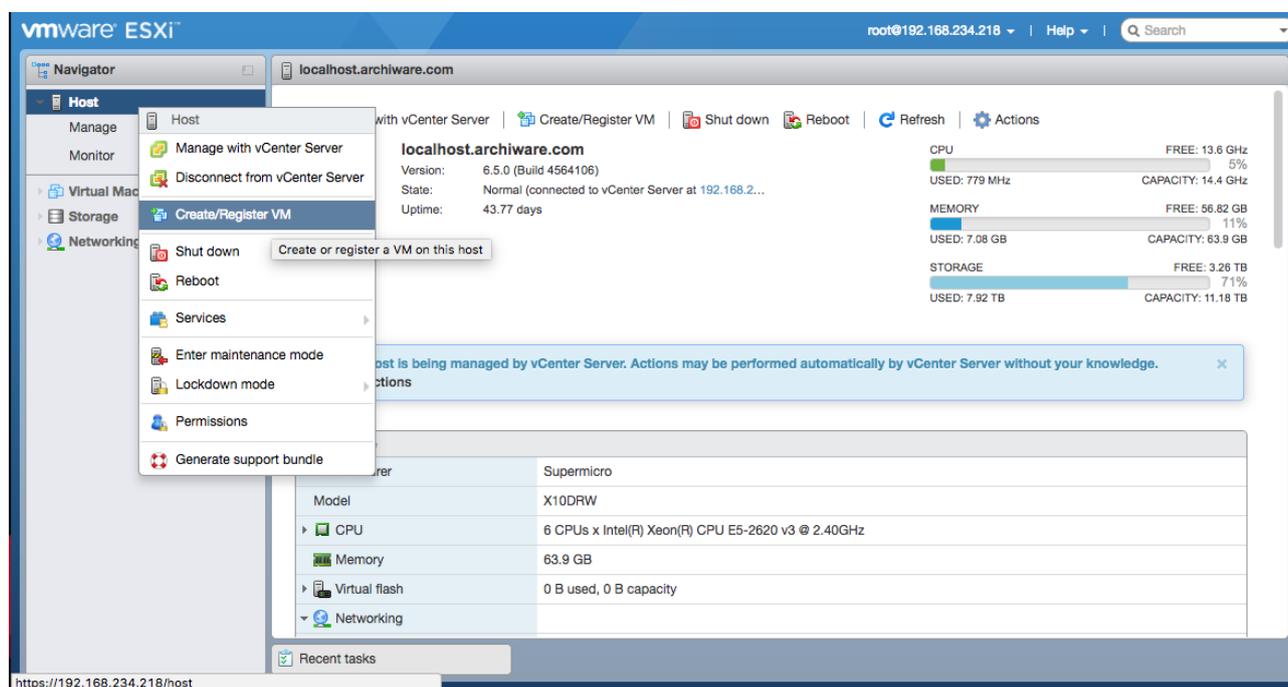
² VMware does not support snapshots of raw disks, RDM physical mode disks, independent disks, PCI vSphere Direct Path I/O devices, disks configured for bus sharing or disks that use an iSCSI initiator in the guest operating system.

2.3 Deploying the Virtual Appliance

The *Archware Pure Virtual Appliance* is preconfigured to meet the minimum hardware requirements for the CPU and RAM. However, disks to be used for the Backup Repository are not pre-configured and need to be configured after deploying the appliance.

To deploy the *Virtual Appliance* using the *VMware vSphere Web Client*, follow the steps illustrated below. For deployment through a vCenter server or on a standalone ESXi version 6.5 host, please follow the official VMware instructions for OVF and OVA Templates³. For standalone ESXi version 6.0 hosts, please follow the instructions for deployment using the *vSphere Client* (please note that *VMware* is phasing out the *vSphere Client* and as a result the latest instructions are for *vSphere 5.0*)⁴

1. Log in to the *VMware ESXi* web GUI, right click on the *Host* and select the *Create/Register VM* option from the context menu.

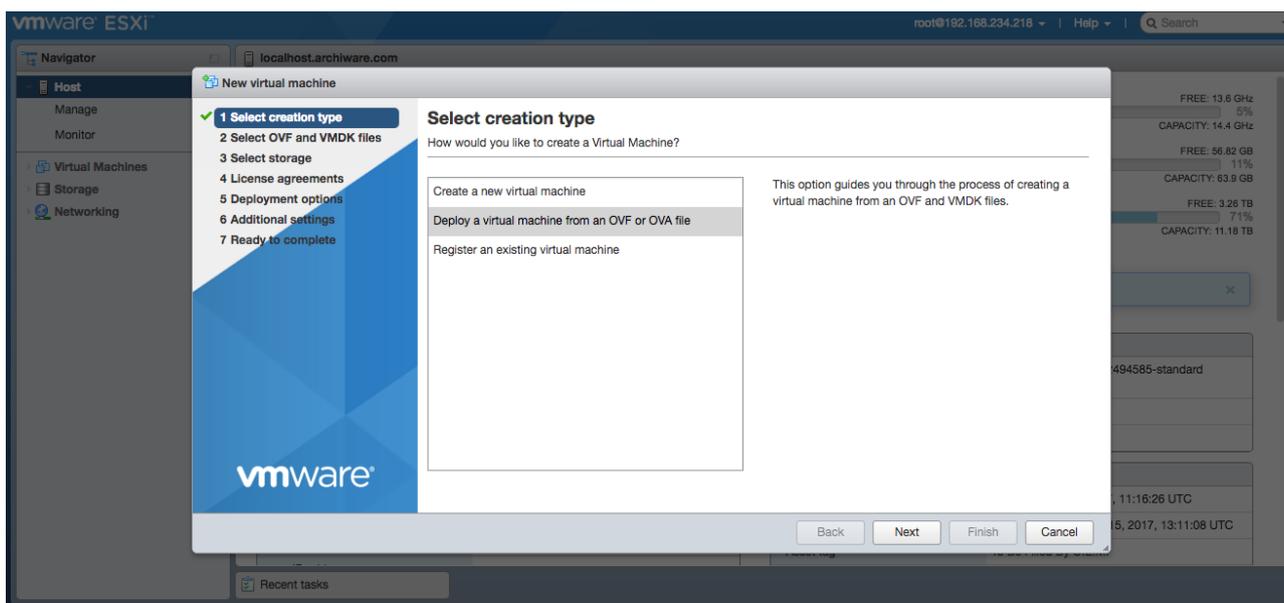


³ https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.vm_admin.doc/GUID-AFEDC48B-C96F-4088-9C1F-4F0A30E965DE.html

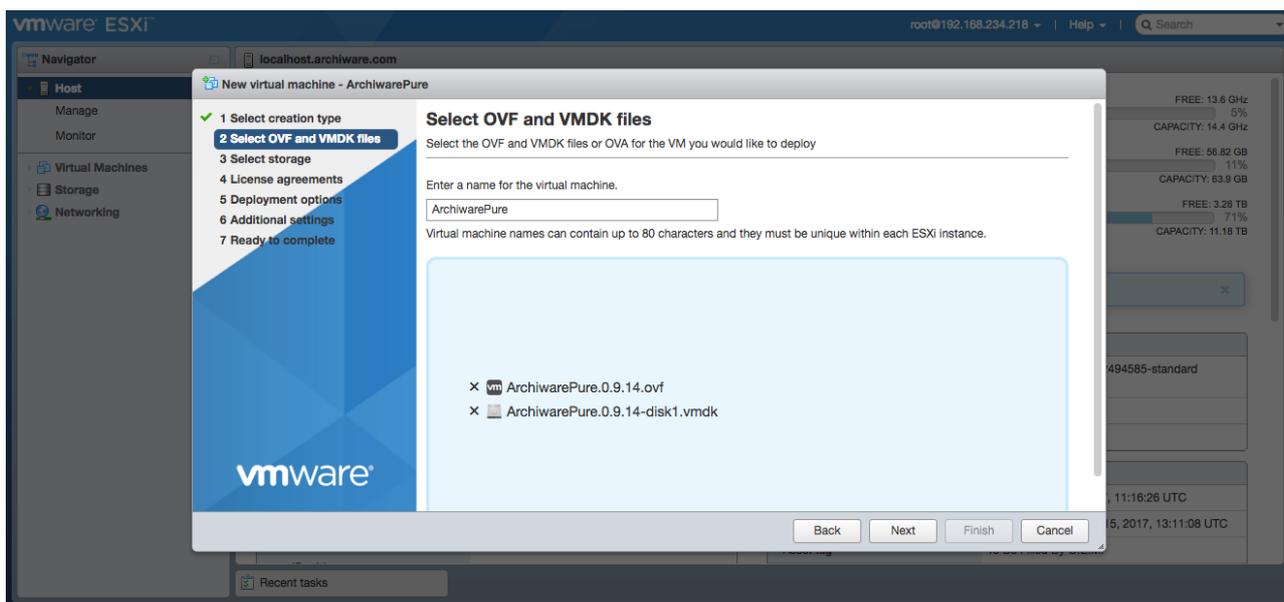
⁴ https://pubs.vmware.com/vsphere-50/index.jsp#com.vmware.vsphere.vm_admin.doc_50/GUID-AFEDC48B-C96F-4088-9C1F-4F0A30E965DE.html



2. Select the *Deploy a virtual machine from an OVF or OVA file* option and click *Next*.

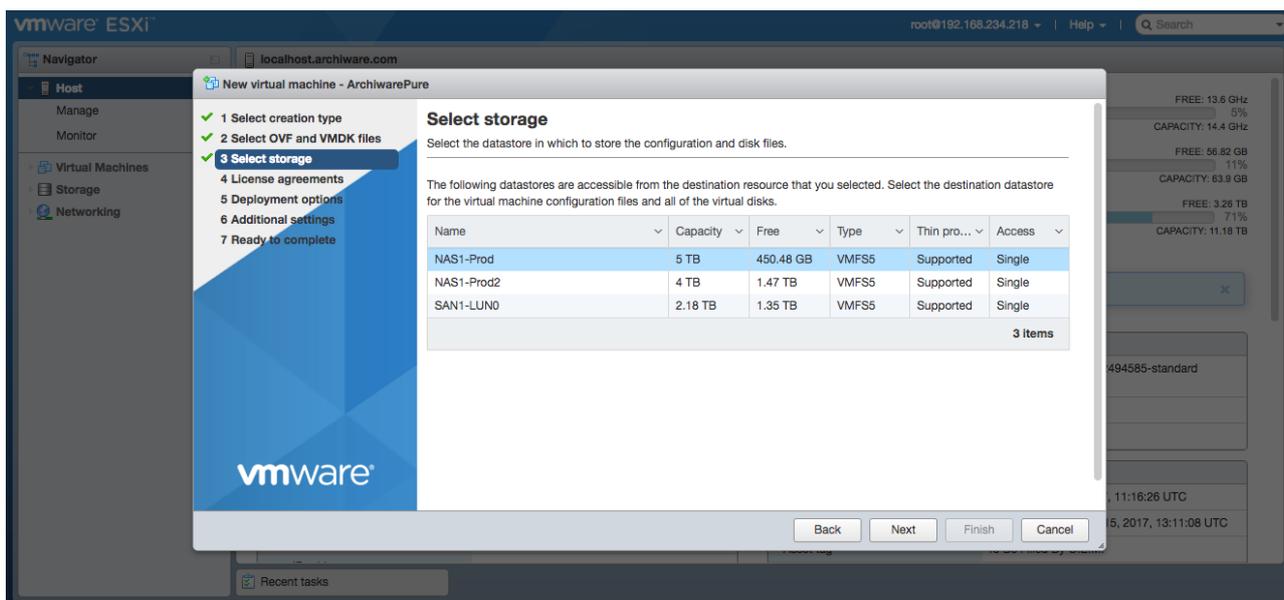


3. Enter a name for your *Archware Pure* virtual appliance. Click in the central area and select the previously downloaded *Archware Pure* template files. If you downloaded the appliance as a single zip archive, please extract the content first. Be sure to select all the included files (*ArchwarePure.x.y.z.ovf*, *ArchwarePure.x.y.z.mf*, *ArchwarePure.x.y.z-disk1.vmdk*). Click *Next* to continue. Note: the *ArchwarePure.x.y.z.mf* file will not be shown in the ESXi web GUI.

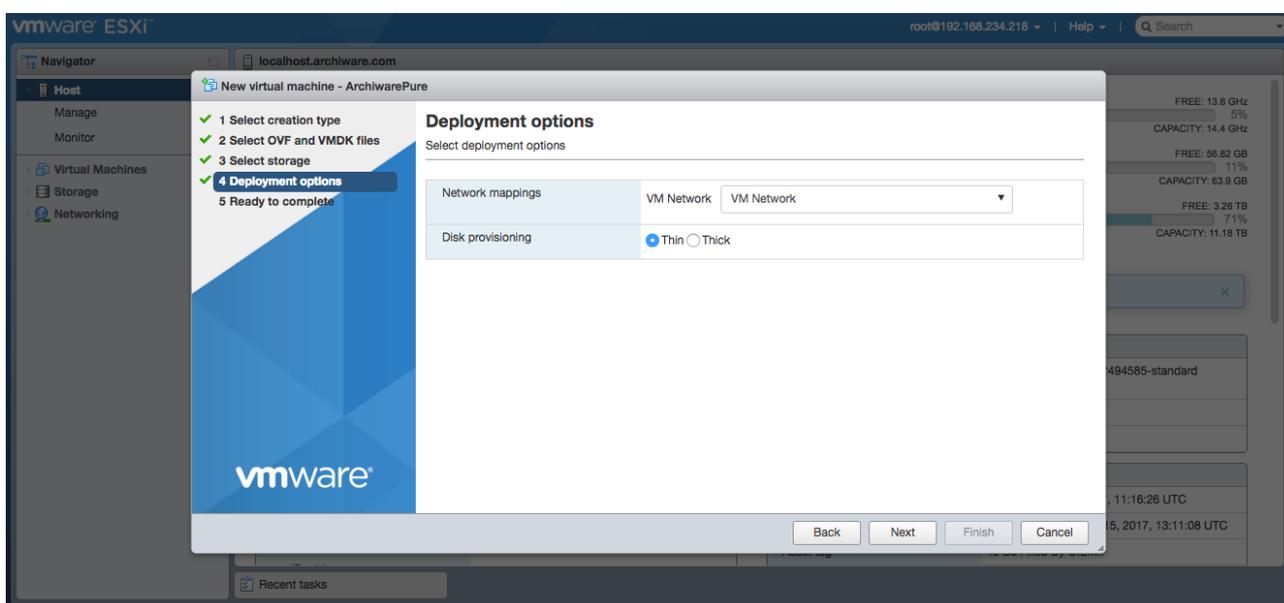




4. Select the datastore in which to store the *Archware Pure* virtual appliance's configuration and disk files and click *Next*.

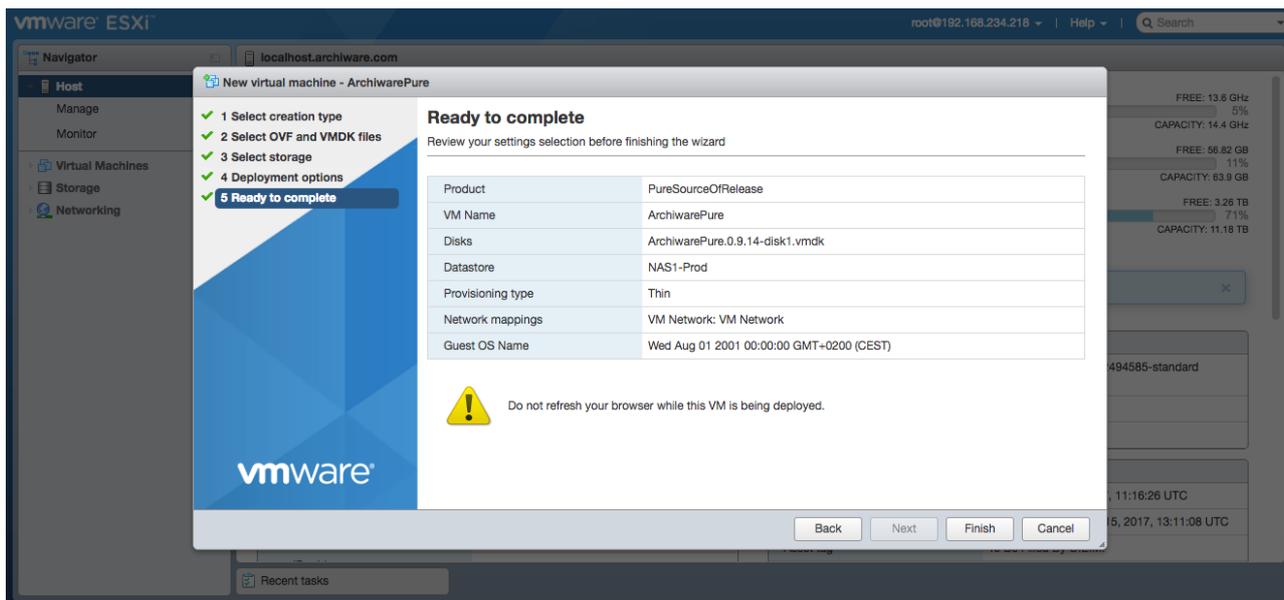


5. Choose the VM Network to which the appliance will be assigned as well as the disk provisioning type. The *Archware Pure* appliance comes with a thin disk with 6GB of provisioned size. Because this disk is not vital for performance, it can be deployed as thin in order to save storage file space. Click *Next* to proceed.





6. Review your settings and click *Finish* to start the deployment process.





2.3.1. Configuring Storage for the Virtual Appliance

Before *Archware Pure* can be used for virtual machine backups, it is necessary to configure at least one storage location as the *Backup Repository* where the backup data of the protected virtual machines will be saved. *Archware Pure* supports any storage option as long as the corresponding mount point is accessible from Virtual Appliance's OS, is formatted with one of the file systems supported by *Ubuntu Linux* and *Archware Pure* has write access to it.

Although *Archware Pure* supports all storage options supported by VMware, even configuring storage as a virtual disk residing on the same datastore where the VMs to be protected are deployed, we strongly suggest using a dedicated external storage for the added security. For best performance, we recommend configuring a SAN LUN in *raw device mapping mode*.

Due to VMware limitations, if the *Backup Repository* is configured as a VMware virtual disk attached to *Archware Pure's* Virtual Appliance, RDM disks must be configured on the SCSI controller 0 so as not to interfere with *Archware Pure* operations. When adding new virtual disks through the VMware GUI, controller 0 is selected by default. It is possible to configure up to 14 virtual disks as *Backup Repositories*.

Please consult the official VMware instructions on adding hard disks to a virtual machine.⁵

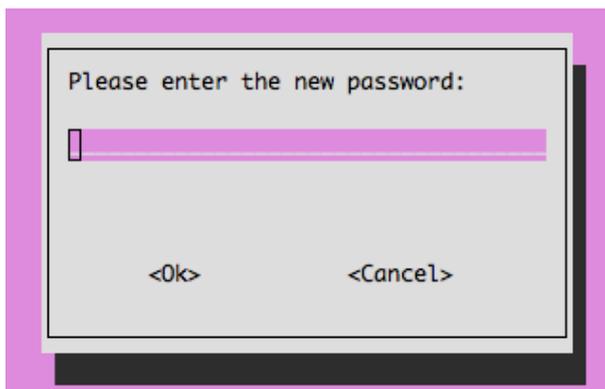
⁵ https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.vm_admin.doc/GUID-79116E5D-22B3-4E84-86DF-49A8D16E7AF2.html

2.3.2. Configuring the Virtual Appliance

Configuring the Access Password

For security reasons, the *Archware Pure* appliance does not have a preconfigured default password and does not accept external SSH connections until manually enabled.

After a successful deployment (and powering on the VM) it is necessary to configure the *Archware Pure* appliance using its console menu, accessing it through the VMware GUI⁶. On first access, a new password configuration prompt is shown. This password will be used as the *root* password for the *Virtual Appliance* and also as the login password for the *Archware Pure* web GUI. Please enter the desired password and confirm it by re-typing it again when prompted.



⁶ Right-click the *Archware Pure* VM in the VMware inventory and select *Open Console* option from the on-screen menu.



Using the Console Menu

After successfully configuring the password, the console menu is shown. It presents basic information about the appliance's version as well as the web address through which the *Archware Pure* GUI can be accessed.

Note: When accessing the *Archware Pure* GUI, make sure to enter the complete URL, including the `https://` part. Http access is disabled for security reasons.

```
Welcome to ARCHIWARE PURE Server Appliance

PURE Version: 2.0.0
OS Appliance: GNU/Linux 4.15.0-47-generic

To manage your appliance please browse to:
https://192.168.234.137:443

PURE Console Menu
-----
1) Reset Password
2) Configure Network
3) Date and Time Properties
4) Start SSH Server
5) Stop SSH Server

p) Restart Archiware Pure
r) Reboot Pure VM
s) Shut down Pure VM
x) Exit to shell
Enter a number: _
```

Through the console menu, you can perform the following actions:

- 1) Reset Password** – Sets the new password for the appliance and for the GUI.
- 2) Configure Network** – This option opens the Linux NetworkManager tool to allow configuring the appliance's network settings.
- 3) Date and Time Properties** – Allows changing Date, Time and Timezone.
- 4) Start SSH Server** – For security reasons, SSH access to the appliance is disabled by default. This option temporarily enables SSH access to the appliance and is automatically switched off when the appliance is rebooted.
- 5) Stop SSH Server** – Immediately disable SSH access to the appliance.
- p) Restart Archiware Pure** – Restarts *Archiware Pure* without rebooting the appliance.
- r) Reboot Pure VM** – Restarts the whole *Archiware Pure* virtual machine.
- s) Shut down Pure VM** – Powers off the *Archiware Pure* virtual machine.
- x) Exit to shell** – Exits the console menu into a Linux shell. To open the console menu again, run the console script again by executing the following command:

```
/usr/local/pure/vmsn/vmsn_console.sh
```



2.4 Deploying a Standalone Application

Archware Pure can also be installed as a standalone application on a virtual or physical server. The officially supported operating system is Ubuntu Linux 18.04 LTS.

To install a standalone version, please download the current software version from Archware's webpage, unpack it into a folder of your choice and run the *start.sh* script from the same folder. If you need to change the default *Archware Pure* port from 443, you can add the desired port number as argument to the start script. For example, the following commands would download and install *Archware Pure* version 2.0.0 into the `/usr/local/pure/vmsn` folder on port 4433:

```
$ sudo mkdir -p /usr/local/pure/vmsn/temp && cd /usr/local/pure/vmsn/  
$ sudo wget  
https://s3.eu-central-1.amazonaws.com/pure-distribution/release/vmsn.2.0.0.tgz  
$ sudo tar xzf temp/vmsn.2.0.0.tgz -C .  
$ sudo ./start.sh 4433
```

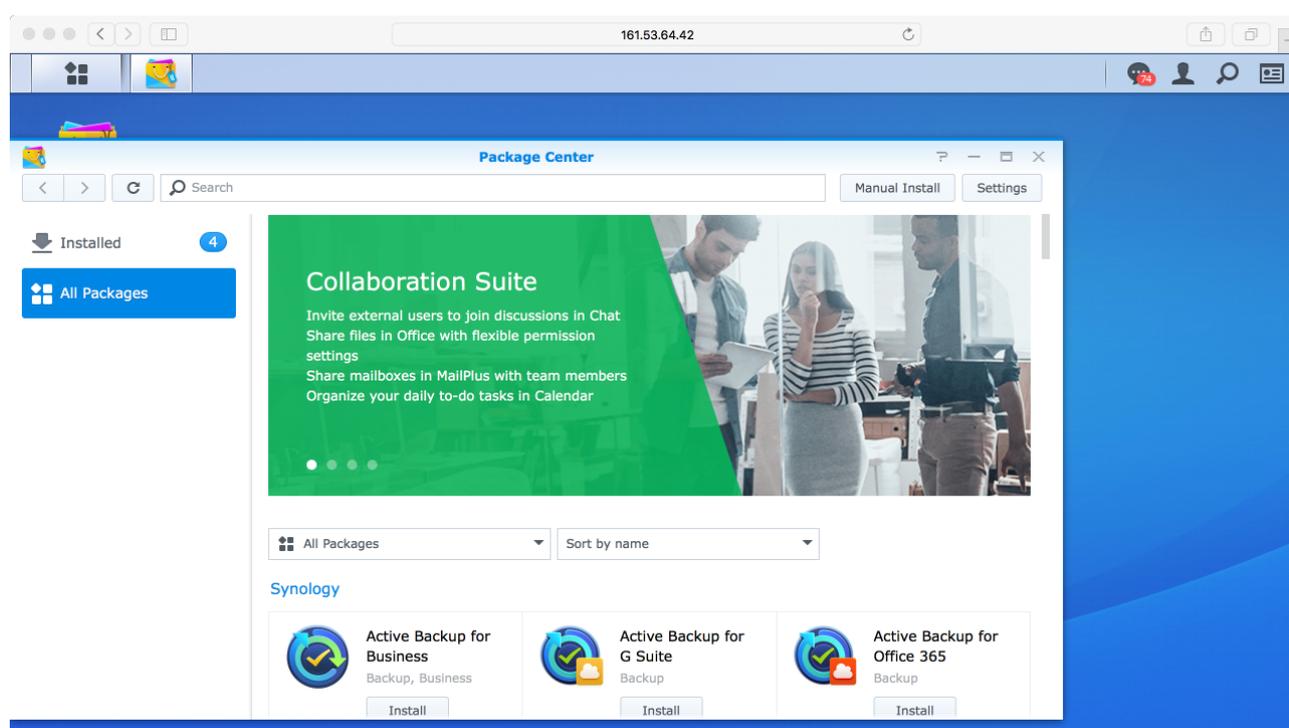
2.5 Deploying an Integrated NAS Application

The easiest way to deploy *Archware Pure* on one of the supported NAS hardware devices is to install it directly from each vendor's respective app marketplace. However, if the latest *Archware Pure* version is not available or if you prefer a manual installation, you can always download the latest software package for your NAS platform from *Archware's* website and follow the manual installation steps.

Note: *Archware Pure* requires a 64-bit x86 compatible processor. Devices not meeting these requirements are not supported.

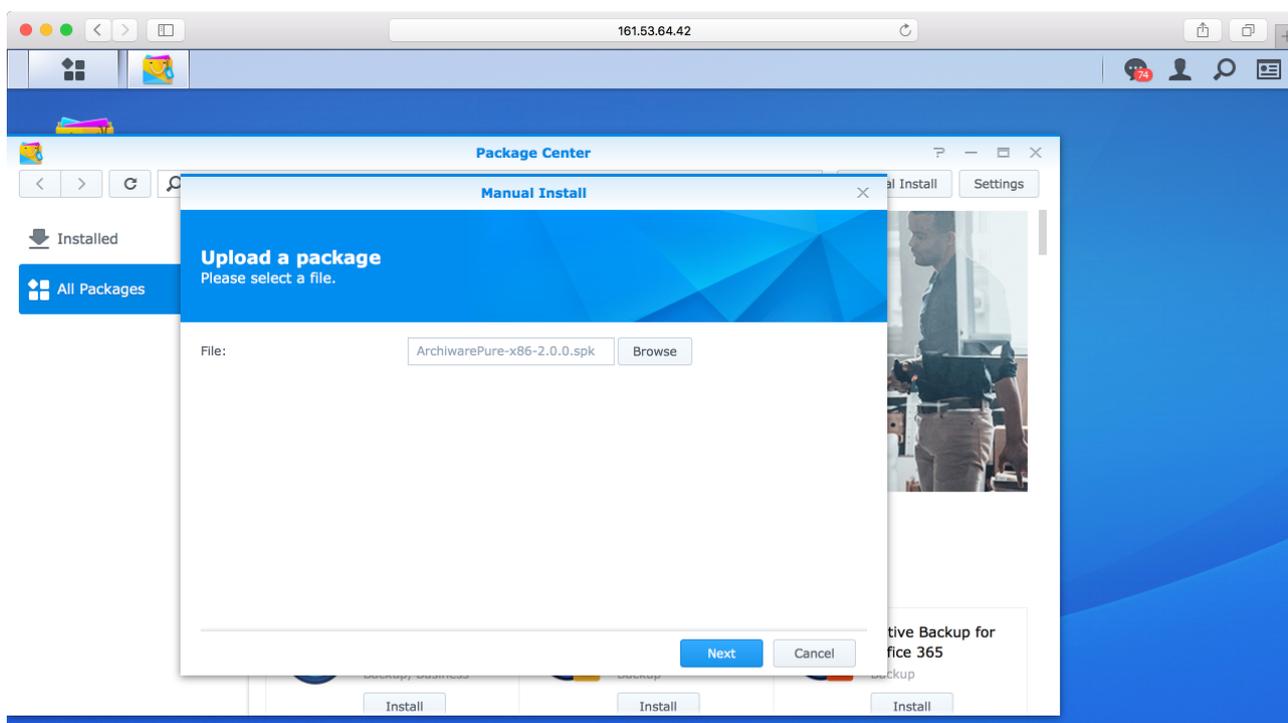
2.5.1. Deploying on Synology Devices

1. Log on to your *Synology* NAS system web interface and open the *Package Center*

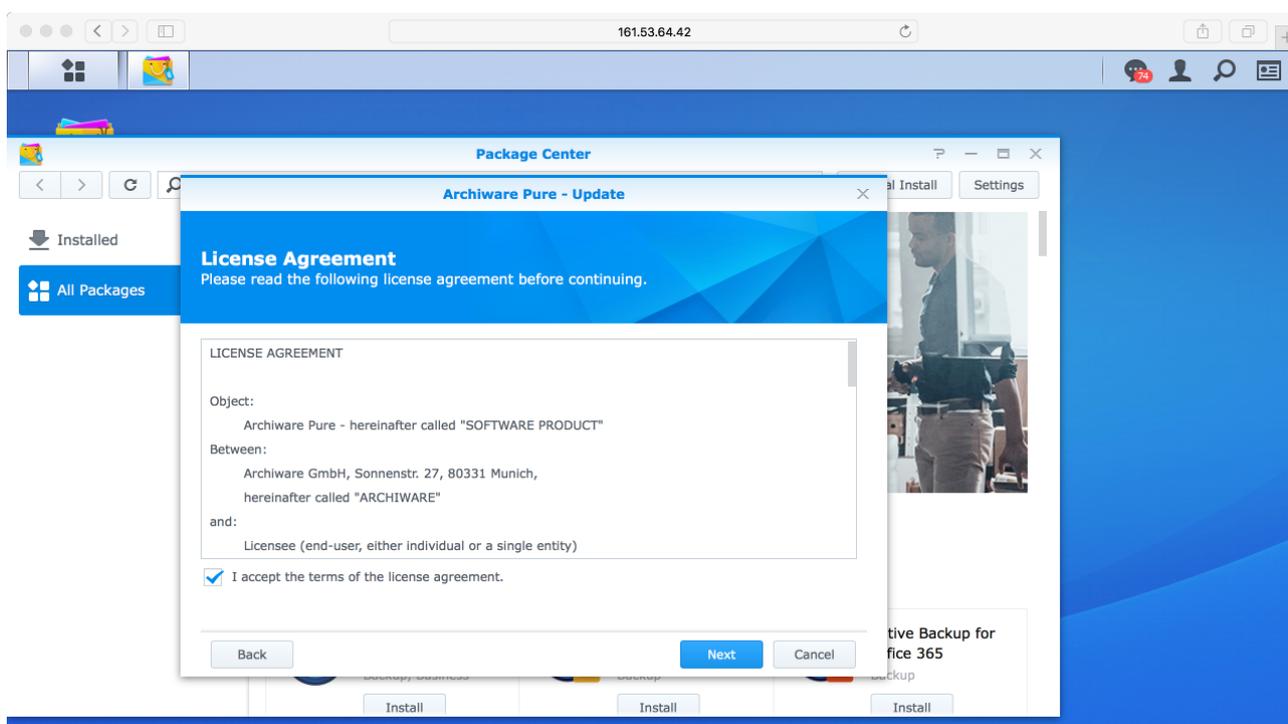




2. Select the *Manual Install* option, press *Browse* and navigate to the folder containing the downloaded *Archiware Pure Synology* package file. Select the .spk file and start the installation process by pressing *Next*.

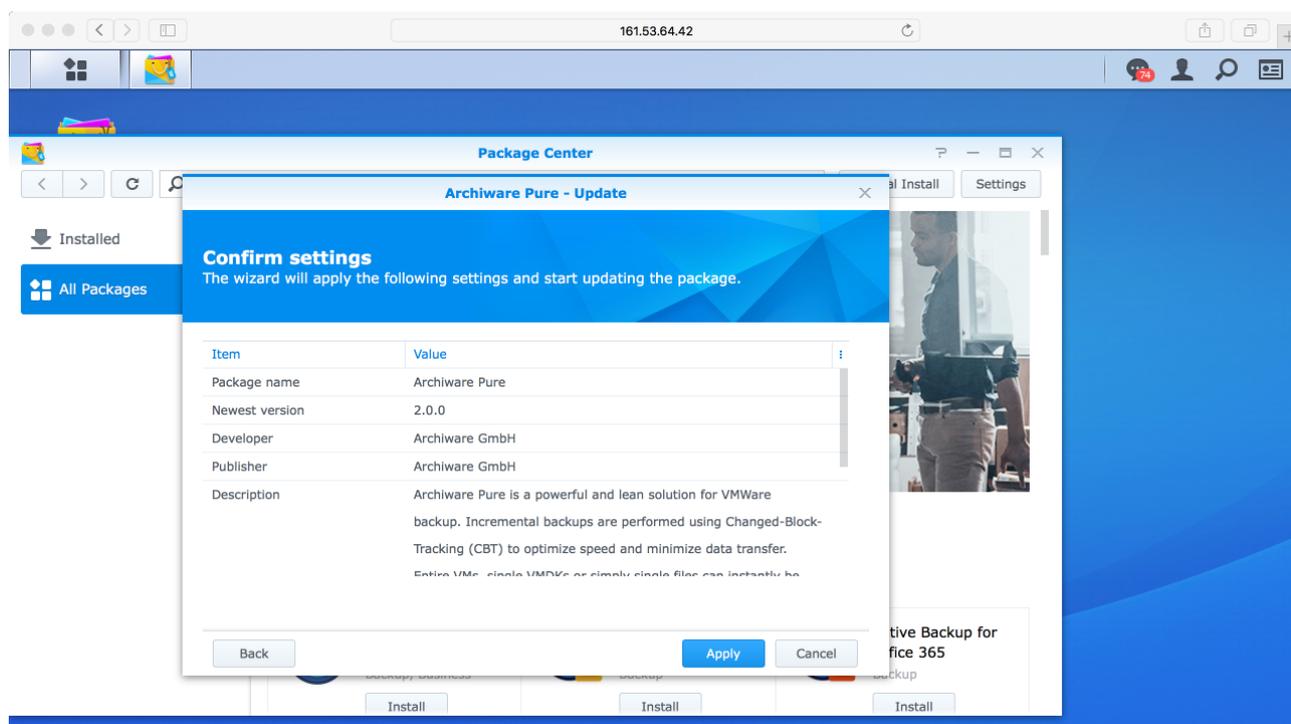


3. Carefully read and accept the license agreement by clicking *Next*.

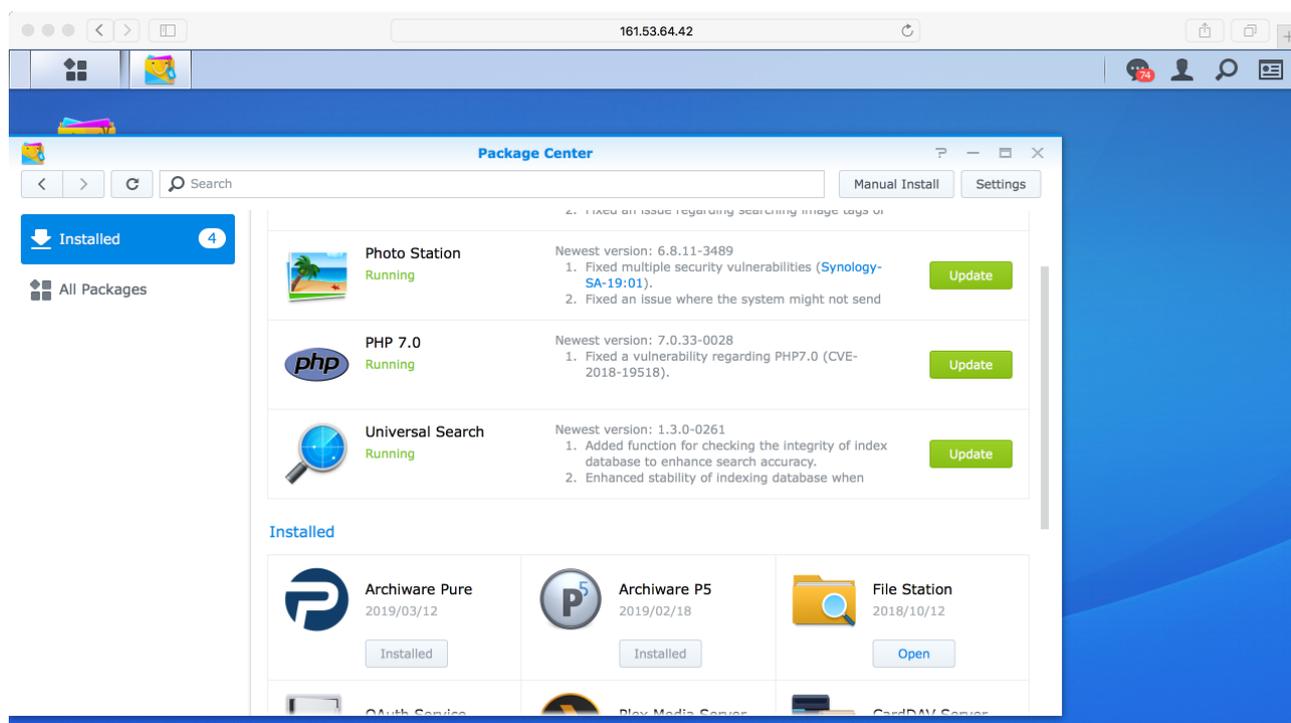




4. Confirm the application settings and start the installation by clicking *Apply*.



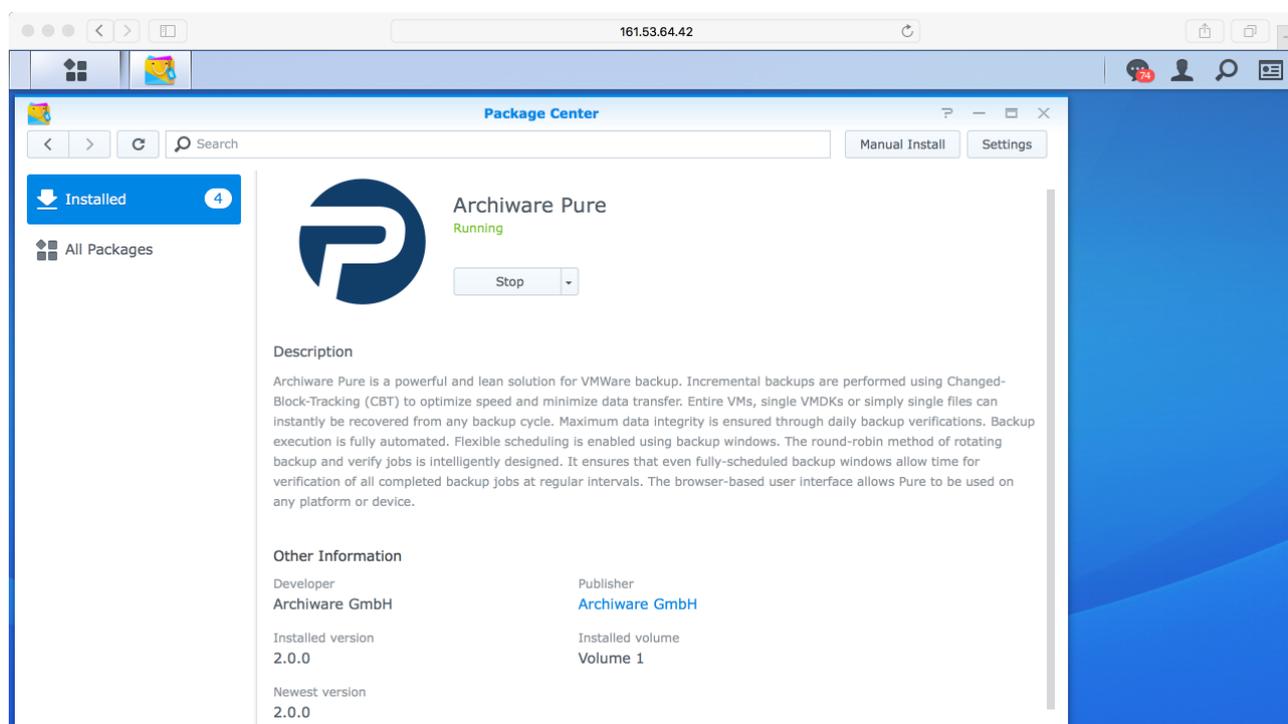
5. After the installation is finished, *Archiware Pure* is shown in the list of installed apps.





6. Selecting *Archiware Pure* in the list of the installed apps in *Package Center* gives you an overview of the app's status and its description. Here you can find options to start and stop *Archiware Pure*.

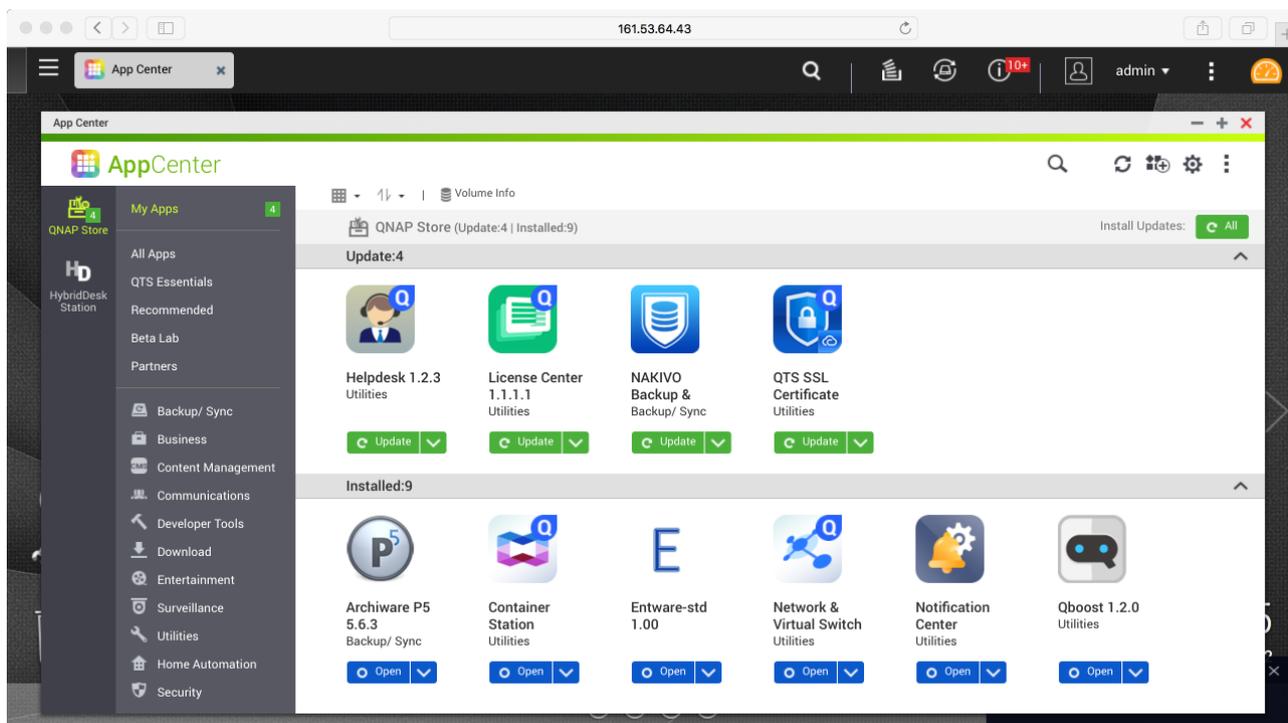
Note: If *Archiware Pure* is stopped before the *Synology* device is restarted, *Archiware Pure* will not be configured to automatically start on system boot.



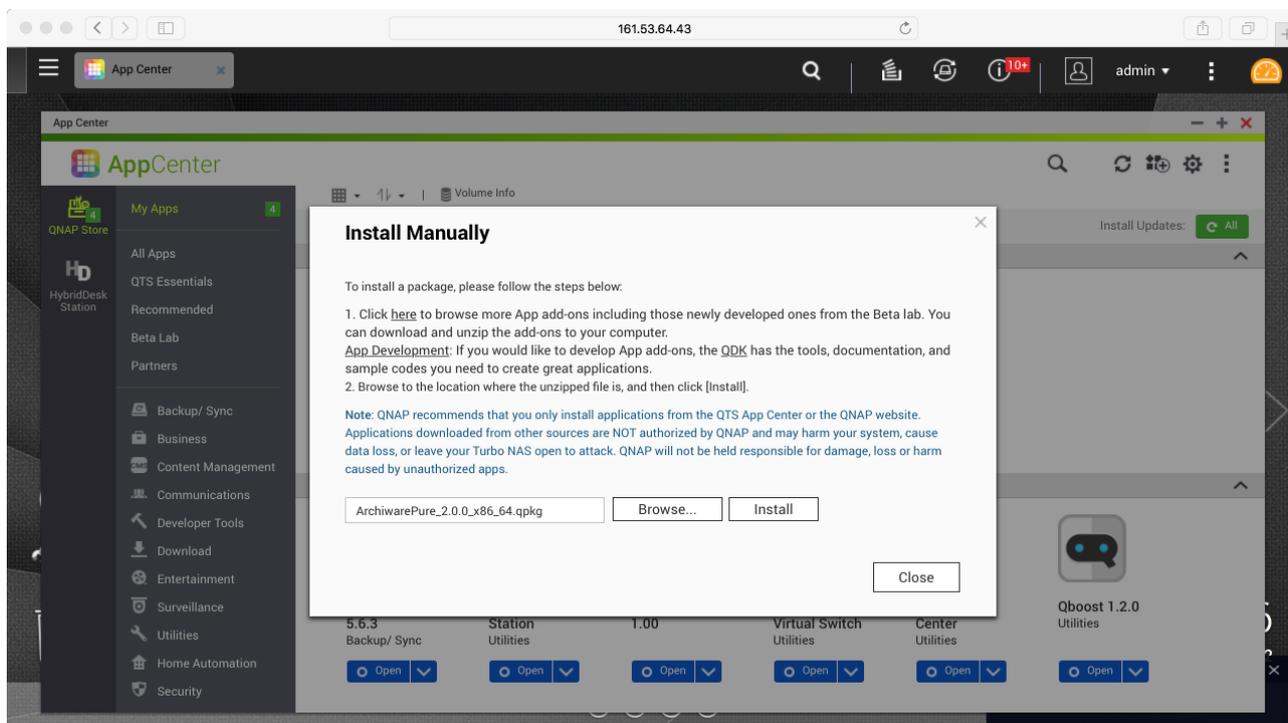


2.5.2. Deploying on QNAP Devices

1. Log on to your QNAP NAS device web interface and open *AppCenter*. Select the *Install Manually* option in the top right-hand-sides corner.

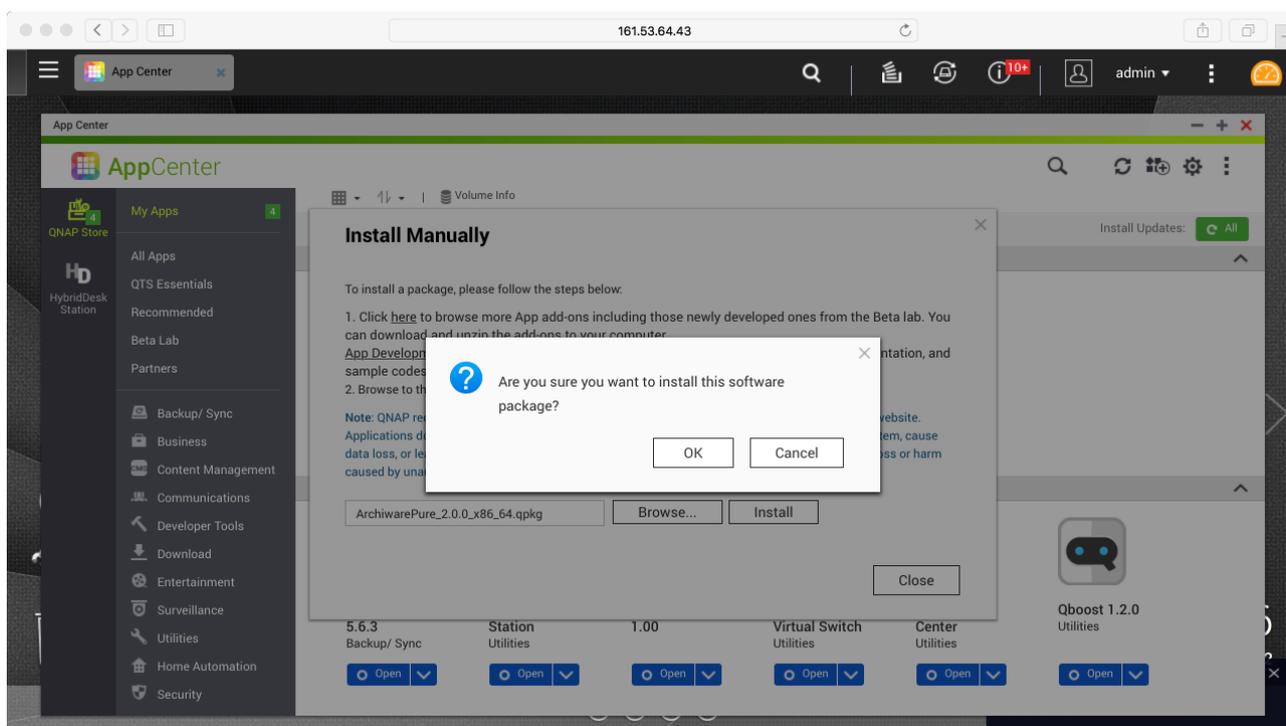


2. Select *Browse* and navigate to the folder containing the downloaded *Archiware Pure* QNAP package file. Select the *.qpkg* file and start the installation process by pressing *Install*.

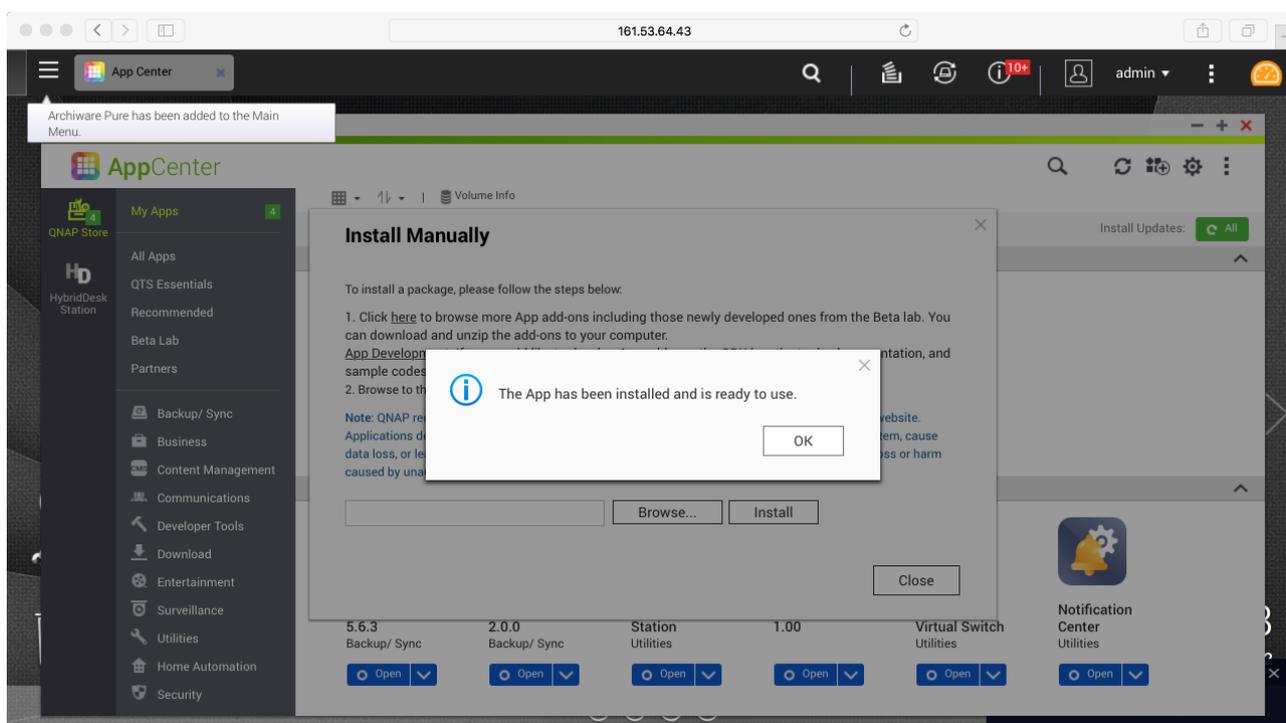




3. Select *Ok* to proceed with the installation.

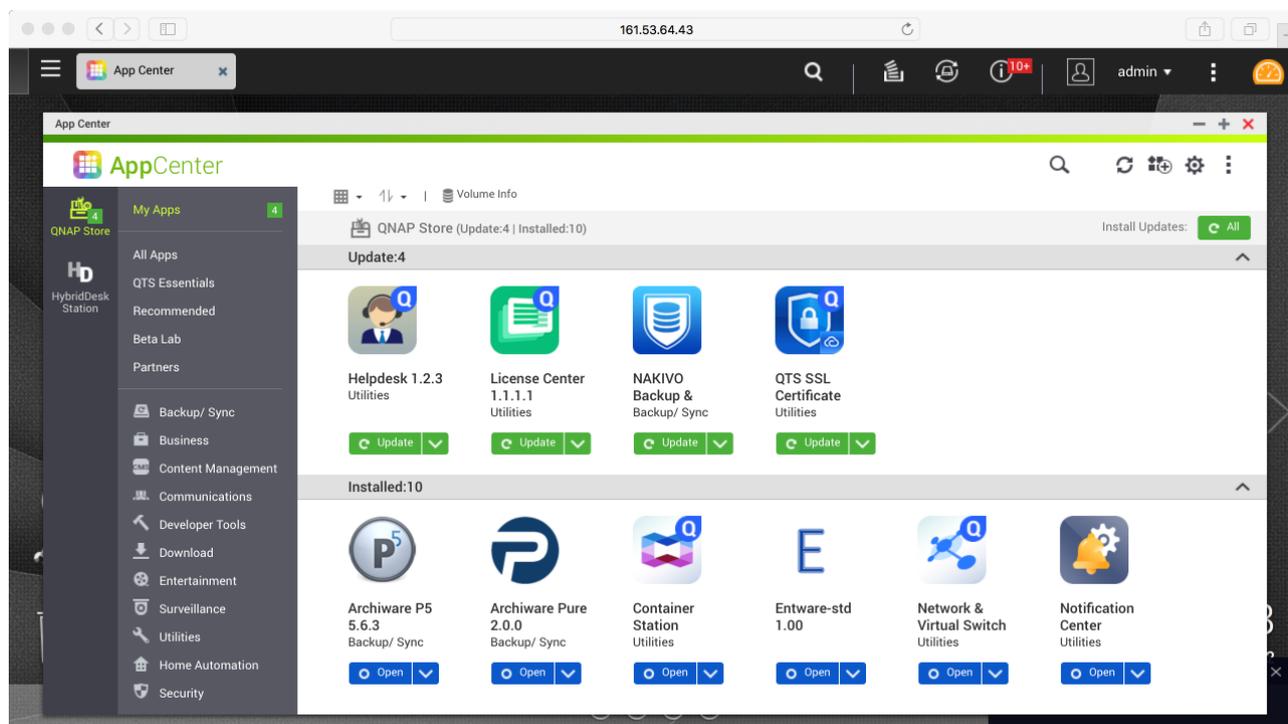


4. Select *Ok* to finish the installation process.



5. *Archware Pure* is shown in the list of installed applications. From there it can be opened, started, stopped or uninstalled.

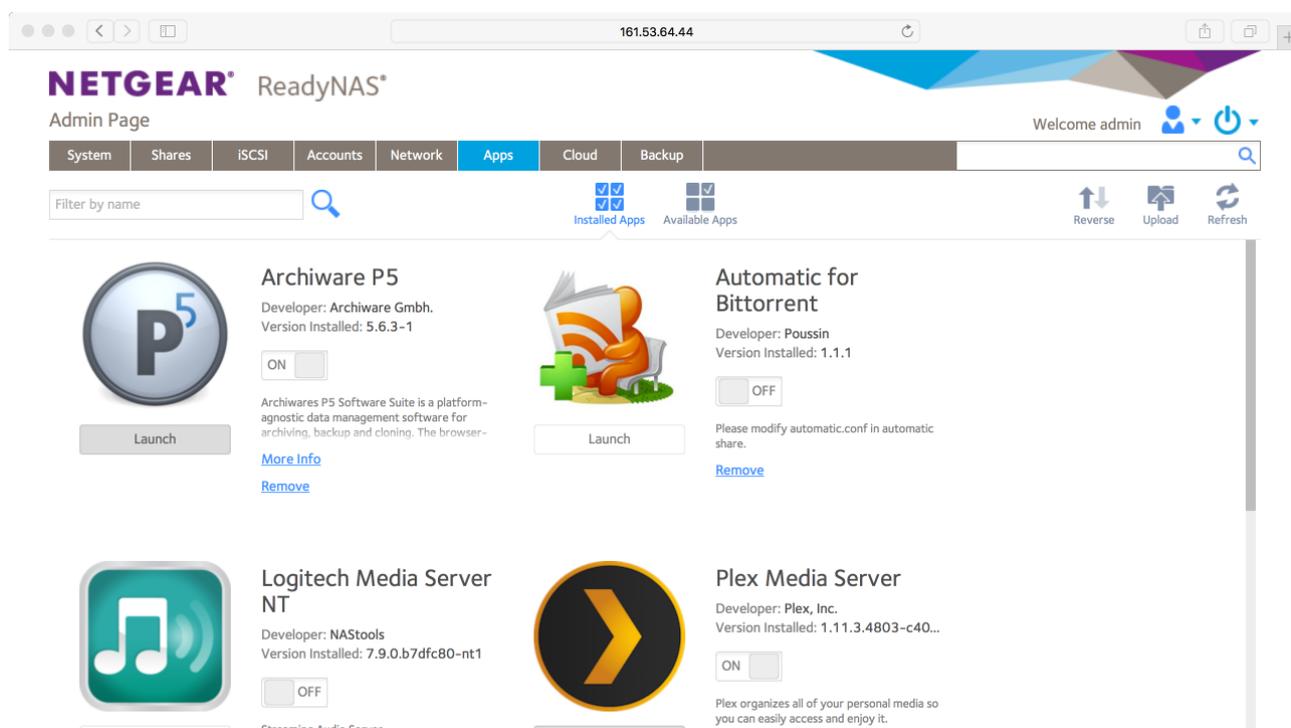
Note: If *Archware Pure* is stopped before the QNAP device is restarted, *Archware Pure* will not be configured to automatically start on system boot.



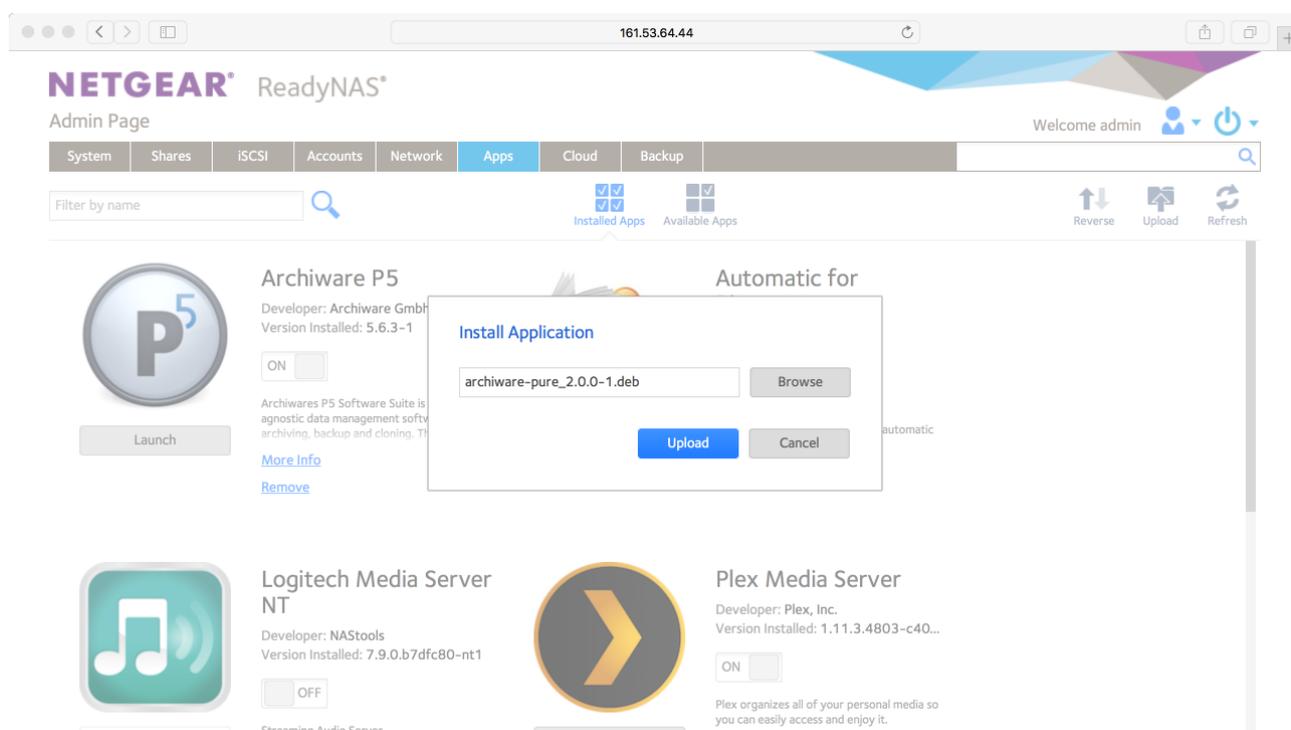


2.5.3. Deploying on ReadyNAS Devices

1. Log on to your *ReadyNAS* device's web interface and open the *Apps* menu. Select *Upload* in the top right-hand-side corner.

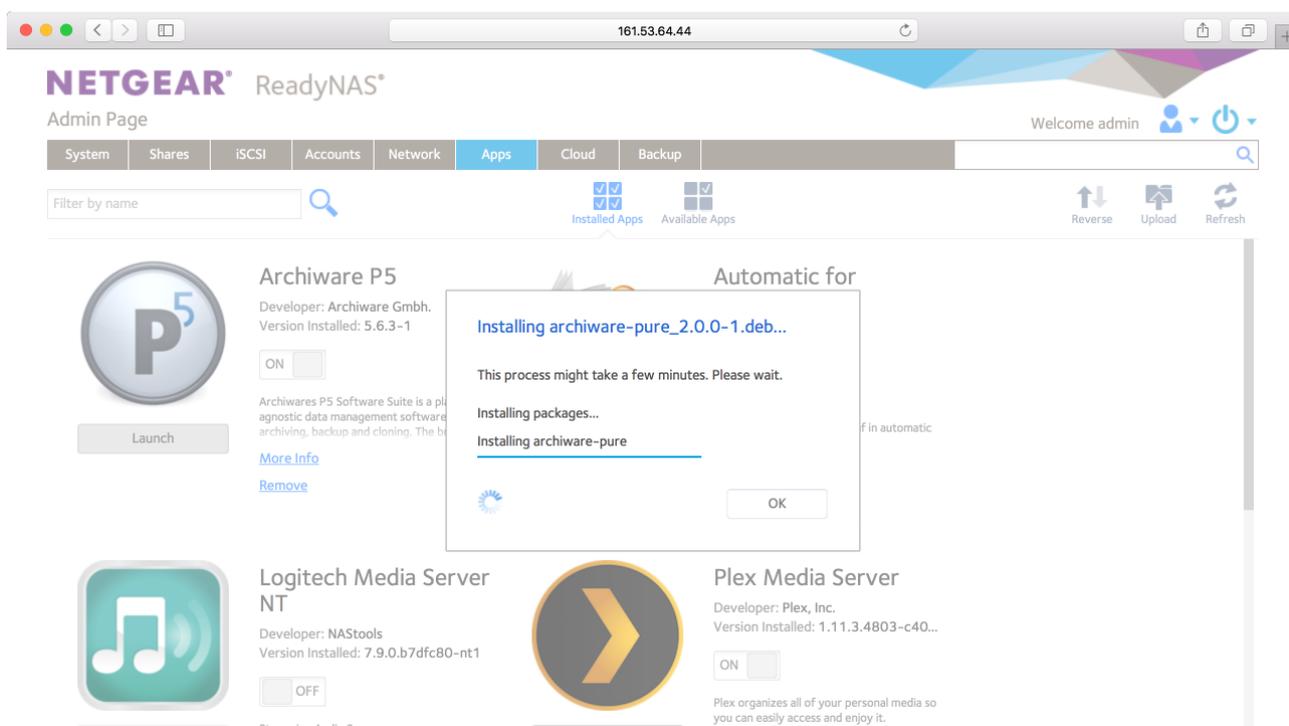


2. Select *Browse* and navigate to the folder containing the downloaded *Archiware Pure* ReadyNAS package. Choose the *.deb* file and start the installation process by pressing *Upload*.



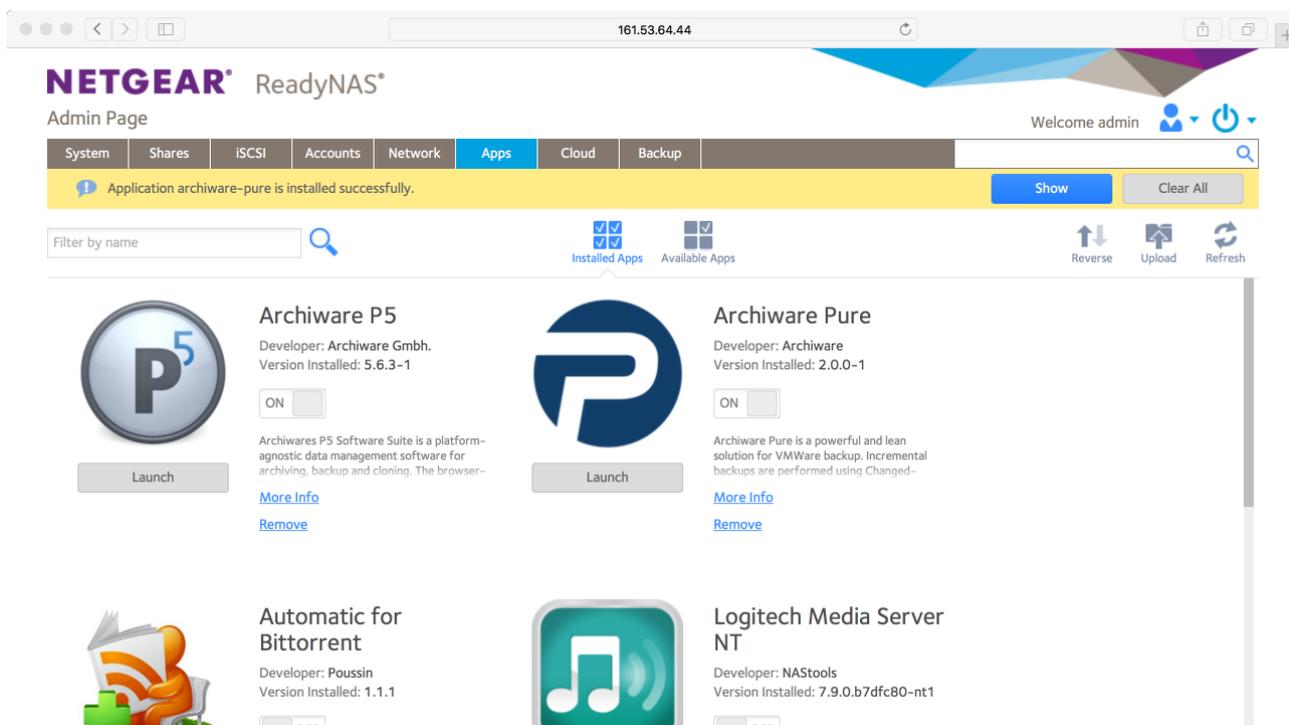


3. Wait for the installation to finish.



4. Archiware Pure is shown in the list of installed applications. From there it can be opened, started, stopped or uninstalled.

Note: If Archiware Pure is stopped before the ReadyNAS device is restarted, Archiware Pure will not be configured to automatically start on system boot.





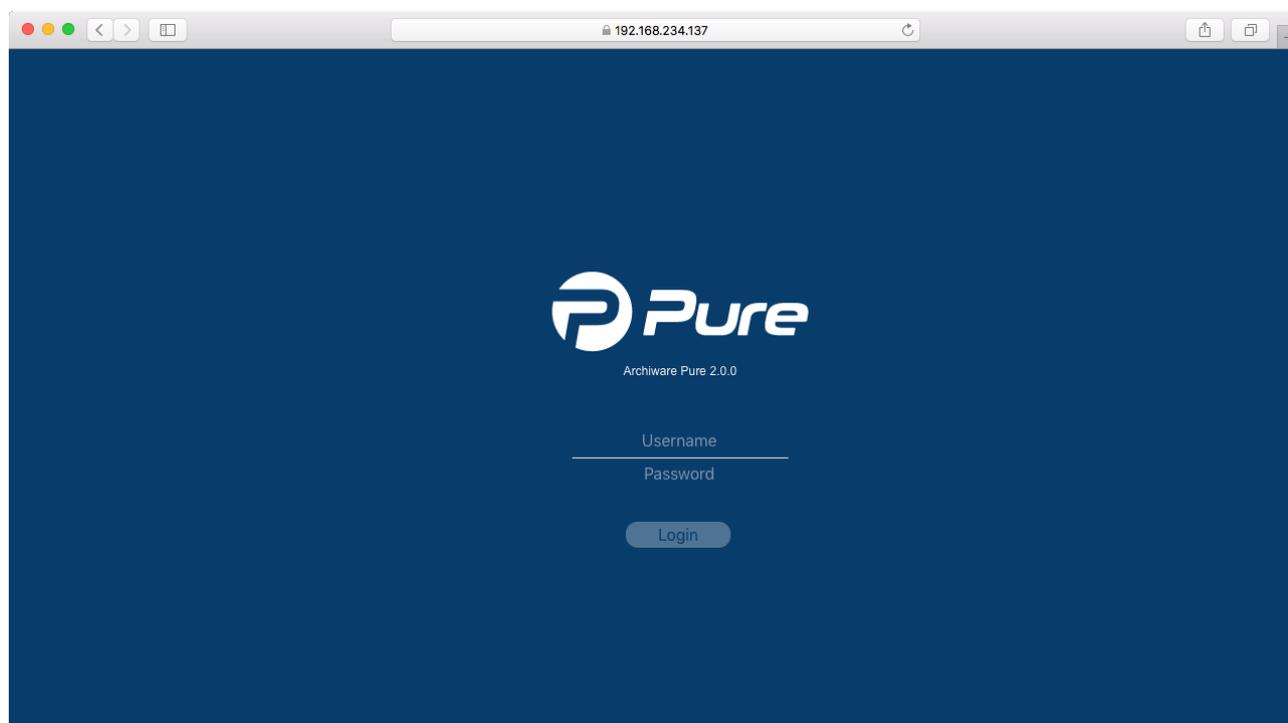
3 Accessing the Archiware Pure Web GUI

The *Archiware Pure* web GUI can be accessed by navigating to the URL indicated in the *Appliance's* console (“https://<Appliance IP address>:<port>”). For standalone installations, this URL corresponds to the IP address assigned to the host machine, followed by the port number configured when starting *Archiware Pure*.

Please find the default port numbers in the following table.

Deployment type	Port number
Virtual Appliance	443
Standalone Linux application	443
Synology	20500
QNAP	8060
ReadyNAS	8250

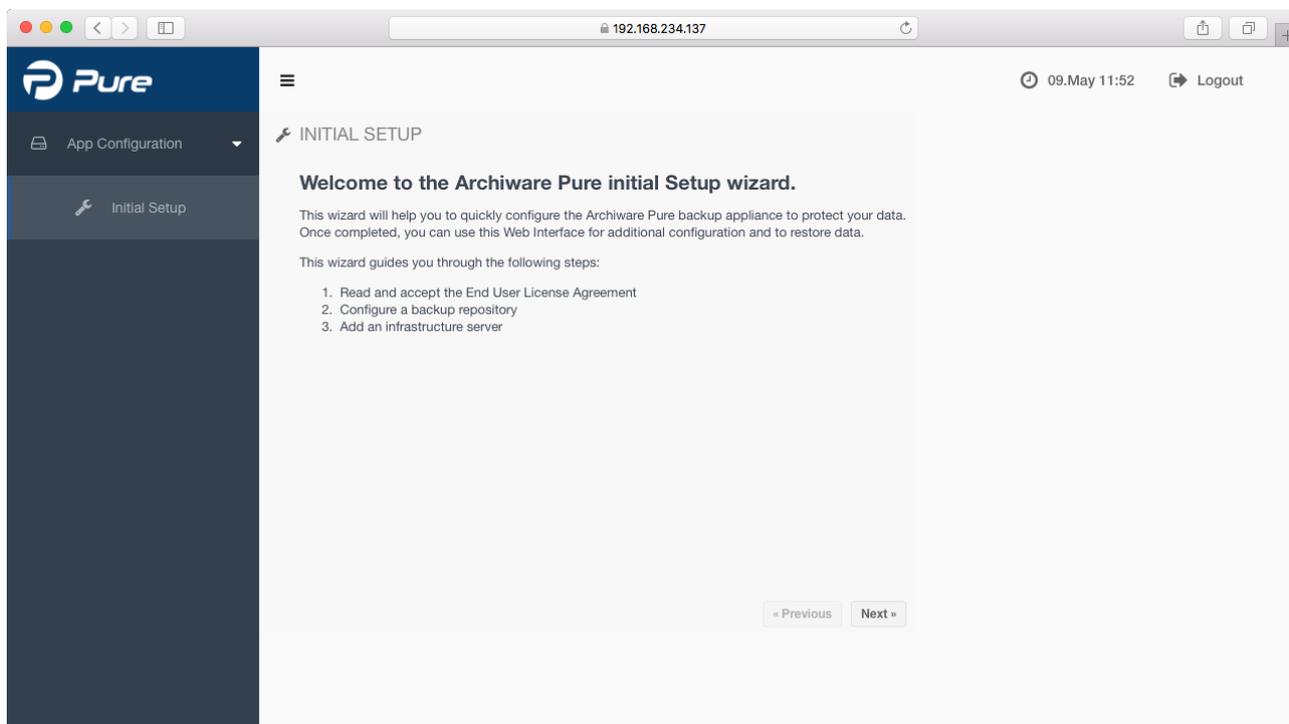
Please make sure to include the “https://” part of the address.





3.1 Initial Setup Wizard

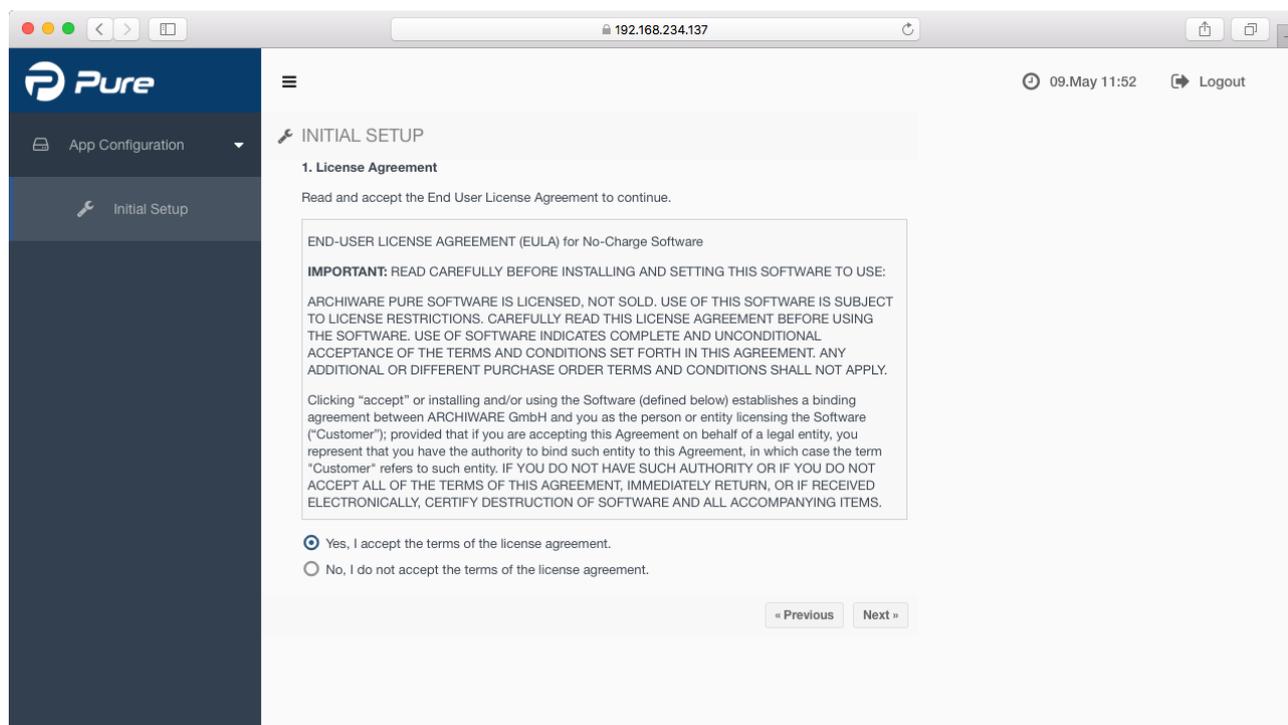
When starting the GUI for the first time, the *Initial Setup Wizard* will guide you through the initial configuration. The *Wizard* will allow you to review the *End User License Agreement*, enter the license key, configure a backup repository and add an infrastructure server to the configuration.





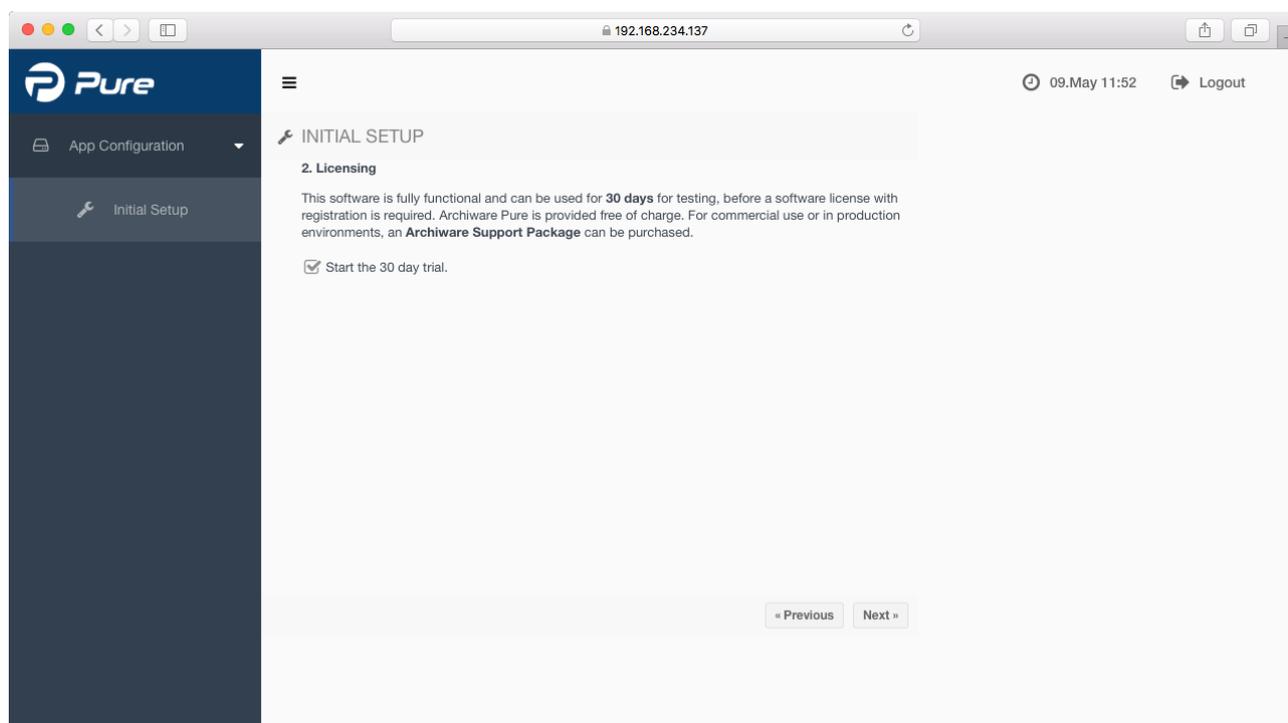
3.1.1. License Agreement

Please carefully read and accept the *End User License Agreement*.



3.1.2. Licensing

Please enter a valid license key or start your 90-day trial.



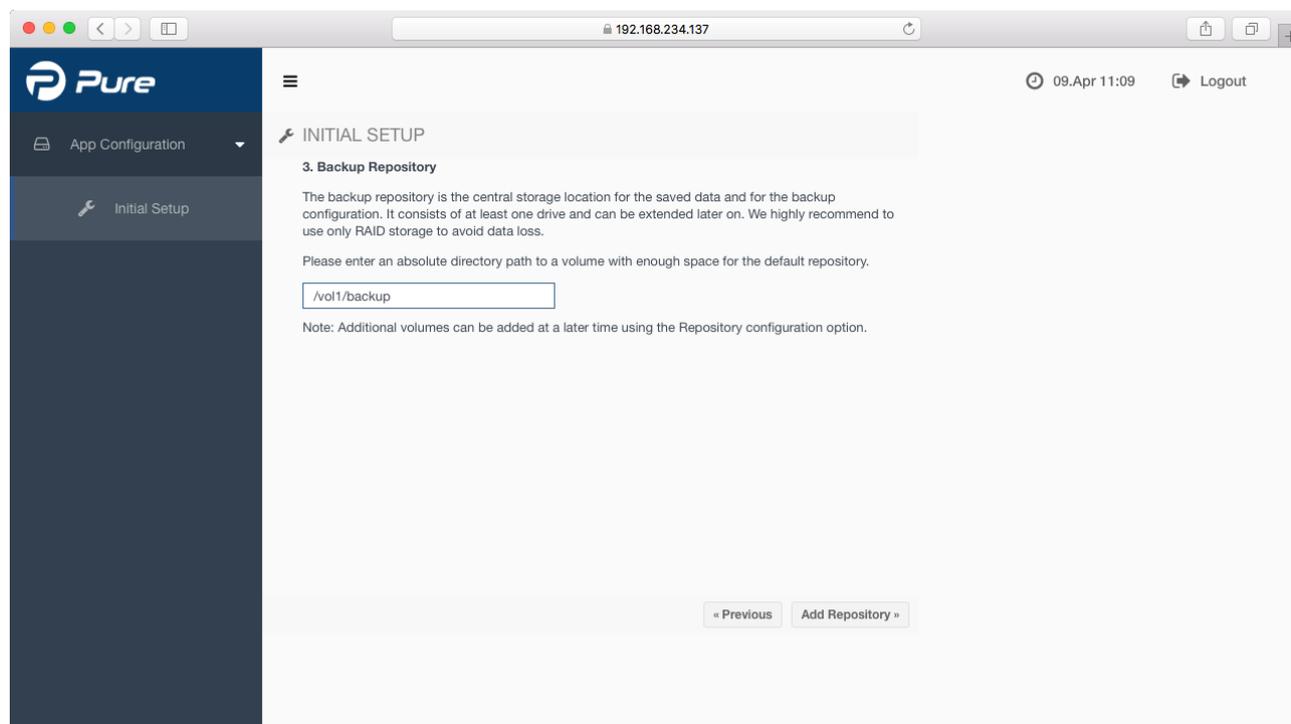


3.1.3. Backup Repository

The Backup Repository is the central storage location for the saved data and for the backup configuration. It consists of at least one mount point and can be extended later on. We highly recommend using only RAID storage to avoid data loss.

Archware Pure supports all filesystem types supported by the host OS and accessible from the host machine, including network shares.

Please select the path where you would like to store the Backup Repository.





3.1.4. Infrastructure Server

Please configure the connection parameters for your virtual infrastructure.

Archware Pure can protect a single vCenter environment with multiple ESXi servers. Adding a vCenter server as an Infrastructure server will allow *Archware Pure* to protect all the VMs it manages. For information on configuring additional vCenter or ESXi hosts, please see 5.3.2 Configuring Infrastructure Servers.

The screenshot shows the Archware Pure web interface. The browser address bar displays '192.168.234.137'. The interface has a dark blue sidebar on the left with the 'Pure' logo and navigation options: 'App Configuration' and 'Initial Setup'. The main content area is titled 'INITIAL SETUP' and contains a section for '4. Infrastructure server'. The text in this section reads: 'Prior to creating the first backup you need to add your virtual infrastructure to the backup configuration. You can add your VMware vCenter server or standalone ESXi hosts. Please enter the IP address or network name and the login credentials of the system administrator.' Below this text is a form with the following fields: 'Host name' (with a placeholder 'DNS name or IP address'), 'User name' (with a placeholder 'e.g. root for ESXi'), 'Password' (with a placeholder 'Password'), 'Description' (empty), and 'Protocol & Port' (with a dropdown menu set to 'https' and a port input field set to '443'). At the bottom of the form are two buttons: 'Previous' and 'Add Server'.

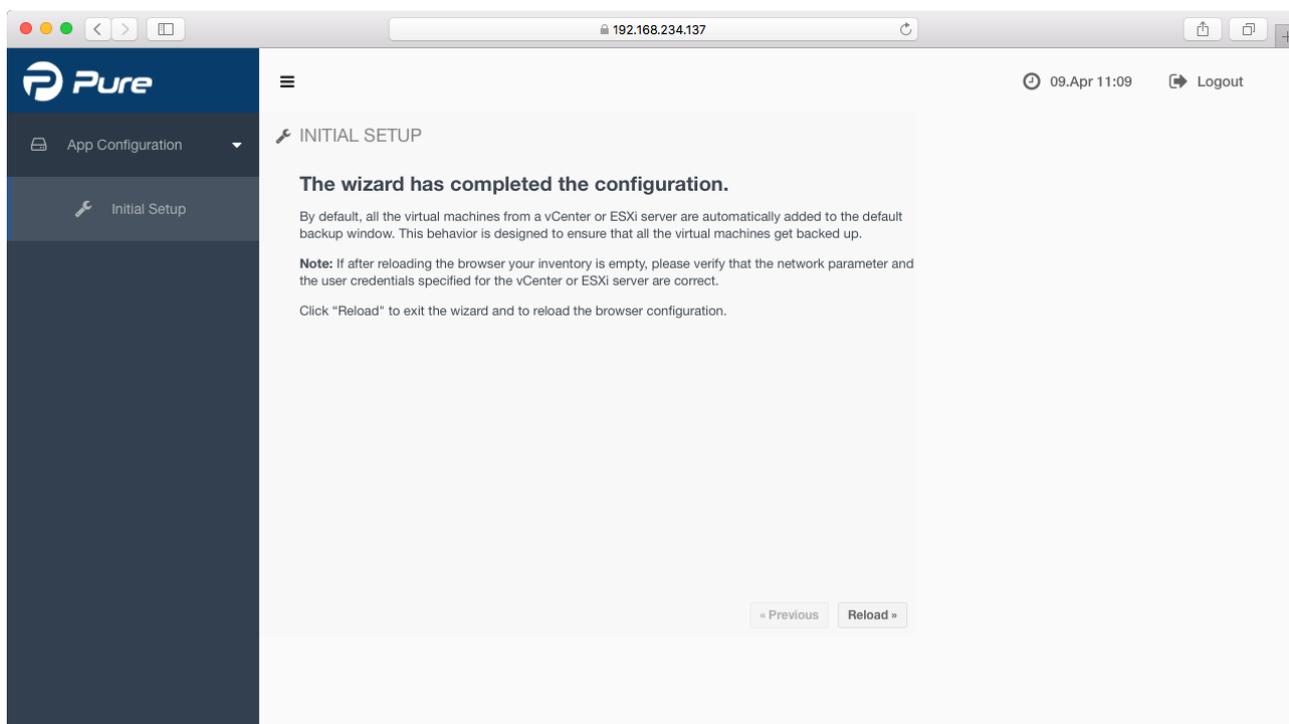
Note: When deployed as a virtual appliance, *Archware Pure* is able to use a faster transport method for backing up virtual machines residing on datastores accessible by the ESXi server managing the *Archware Pure Virtual Appliance*. In order to make use of this advantage, please make sure to configure the vCenter or ESXi server managing *Archware Pure Virtual Appliance* as one of the *Infrastructure servers*.

Note: In order to enable the backup of a vCenter virtual appliance, it is necessary to add both the vCenter server and its managing ESXi host to the list of configured servers. If the ESXi server is not configured, the vCenter virtual appliance VM will not be shown in the list of virtual machines. Please see 5.3.2 Configuring Infrastructure Servers on how to add additional infrastructure servers.



3.1.5. Completing the Initial Setup

After the *Initial Setup Wizard* has finished, please click *Reload* to exit the *Wizard* and reload the configuration.





4 Backing Up Virtual Machines

Archware Pure is designed with simplicity and ease of use in mind. It can be configured to automatically back up and keep all the discovered VMs protected.

The screenshot displays the Archware Pure web interface. The main content area shows a table of Virtual Machines (VMs) with columns for 'Virtual Machine', 'Backup/Verify', 'Backup Disk Usage', and 'Backup/Restore Job Progress'. The table is grouped by IP address (192.168.234.208 and 192.168.234.217). A 'Restore' button is visible at the bottom of the table.

Virtual Machine	Backup/Verify		Backup Disk Usage		Backup/Restore Job Progress
	Completed	Duration	Total	Last i..	
▼ 192.168.234.208					
OS X 10.11					
Kerio-Control	● 10.Apr 00:36	36 min 45 s	6.1 GB	6.1 GB	
OS X 10.9					Backing Up: 6.98 GB of 40.61 GB
OS X 10.6 234.26					
▼ 192.168.234.217					
Tiny Linux VM	● 10.Apr 00:37	0 min 39 s	0.0 GB	0.0 GB	
com.archiware.pure.builder					
APT_ubuntu					
Tiny Linux VM-1_1_7					
Tiny Linux VM-2					
Unitrends_test					
Ubuntu15					
W2016					
APT_solaris	● 09.Apr 13:44	1 min 31 s	3.6 GB	3.6 GB	
Synology Play	● 10.Apr 01:14	36 min 59 s	27.7 GB	27.7 GB	
Tiny Linux VM-3	● 09.Apr 13:41	0 min 08 s	0.0 GB	0.0 GB	
51 VMs			37.38 GB	37.38 GB	

Restore

Backup Administration

Basic Advanced Overview

VM: OS X 10.11

Automatic backup is enabled

Backup Windows:

Frequency	Start	Period
<input checked="" type="checkbox"/> Run weekly on Sat	00:00	48h
<input checked="" type="checkbox"/> Run weekly on Mon, Tue, Wed, Thu, Fri	00:00	6h

Tags:

Apply

Note: Create new label on enter



4.1 Automatic Backups

Each VM is assigned one or more backup windows – i.e. time slots when the automatic backup is allowed to be executed, typically during hours of lower demand on the resources. Each VM will enter the backup queue at the beginning of its backup window. Depending on various parameters, including when the last backup of the VM was done, how many VMs may concurrently be backed up, and how much load may be imposed on the storage, the VM may stay in the queue until its turn to actually be backed up arrives or until the backup window closes. No backup or verify operation will start outside of the backup window, even if the particular VM does not get backed up on that occasion. In a properly configured system with a sufficiently large backup window, all of the VMs configured to be backed up will be backed up or will alternate, rotate, and be backed up on consecutive occasions. Once a backup is started for a specific VM, it will be run to completion, even if the operation extends outside the allocated window.

Archware Pure comes preconfigured with two default backup windows: one set to last for 6 hours, starting every midnight Monday to Friday, and the other lasting the whole weekend (48 hours duration, starting on Saturday 00:00).

Note: Because the very first backup for each VM needs to transfer the entire content of all its virtual disks, it is possible that not all the VMs will fit inside the default backup window. Subsequent backups will use Changed Block Tracking information, which significantly decreases the backup time.

Additional backup windows may be configured by clicking on the “+” icon and selecting the desired start time and duration. Note that backup windows cannot overlap.

Frequency	Start
<input type="checkbox"/> Run weekly on Sat	00:00 48h
<input type="checkbox"/> Run weekly on Mon, Tue, Wed, Thu, Fri	00:00 6h
<input checked="" type="checkbox"/> Run weekly on Mon, Tue, Thu, Fri, Sun	18:00 8h



4.2 Verify

Backup consistency is ensured through an automatic *Verify* process where the backed up content is compared, byte by byte, with the actual virtual disk content of the VM. Verifications of the machines that are queued for backup are automatically queued to be run after all the backups are completed. The VM that has not been verified for the longest will be verified first. In the course of a verification, detected mismatches are corrected to render a consistent backup snapshot.

Note: Please ensure a sufficiently large backup window to enable verify to run for all the VMs scheduled in that window.

4.2.1. Quick verification

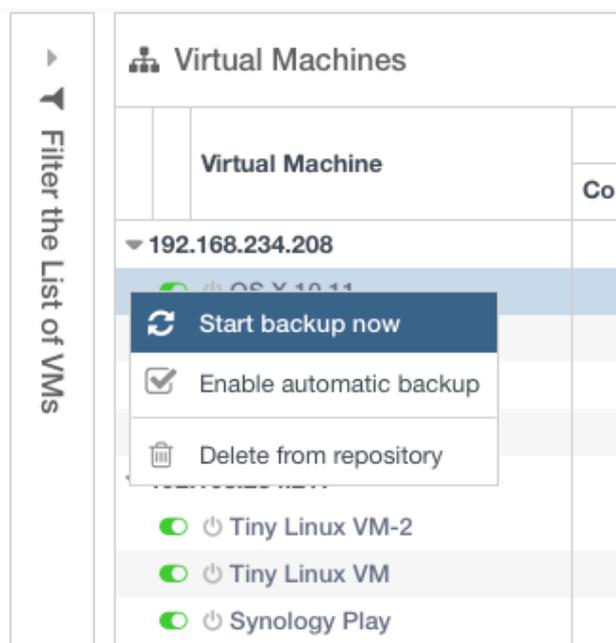
Because backup verification compares the entire virtual disk byte by byte, the process can take a long time to complete for very large or over-provisioned virtual disks. By enabling the *Quick verification* feature, *Pure* will skip unallocated disk areas and only perform backup verification of the allocated disk blocks, as reported by the ESXi host.

Quick verification is a property of a *Backup window* and is either enabled or disabled for all of the corresponding virtual machines. This allows for configurations where some of the backups use *Quick verification* feature to greatly decrease backup time and resource usage while still allowing for a thorough verification in a separate *Backup window* to be scheduled at the time of greater resource availability.

Warning: *Quick verification* limits the verification process only to the allocated disk areas. The list of allocated disk areas is obtained from the VMware ESXi host and cannot be independently verified by *Archware Pure*. External bugs or errors affecting the correct reporting of allocated disk areas may also impact the reliability of backup verification when *Quick verification* is used.

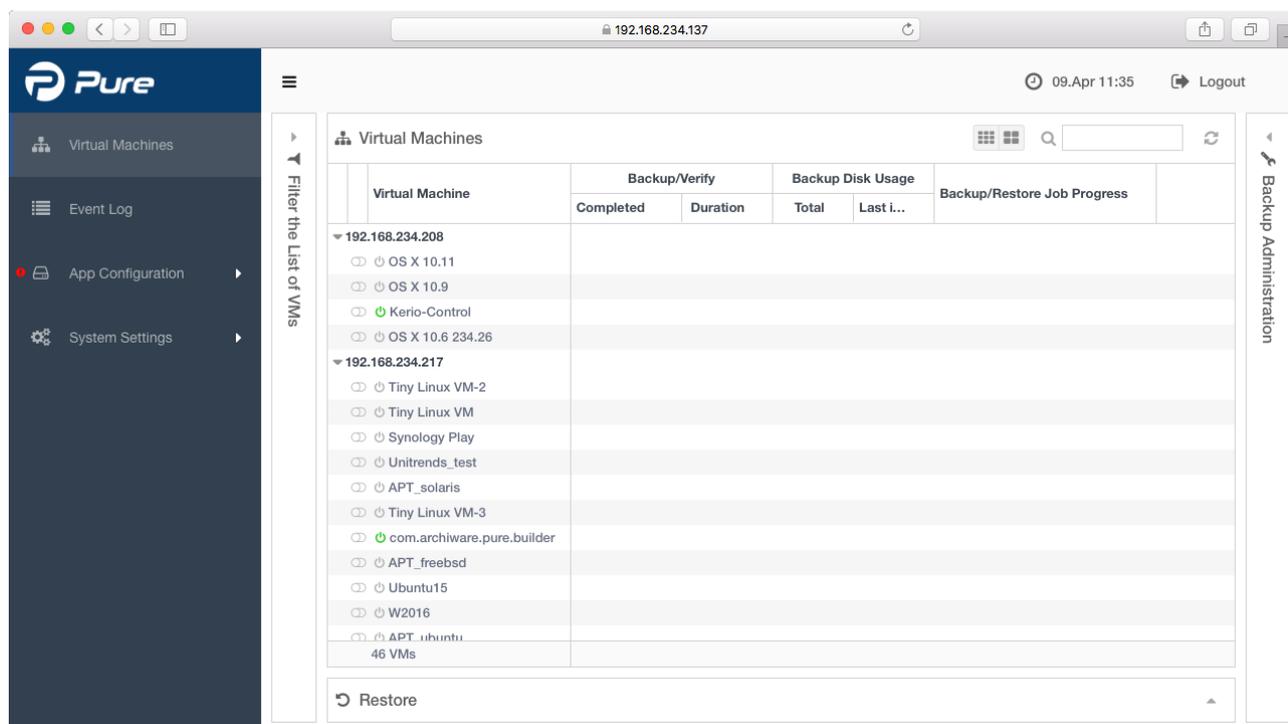
4.3 Manual Backup and Verify

Backup and verify operations can also be run on demand by clicking on the icon left of the desired VM and selecting the *Start Backup Now*.





5 Archiware Pure Web GUI



The *Archiware Pure* web GUI consists of four main views, accessible through a menu located at the left hand side:

Virtual Machines – this is the central area of interest as it handles backup and restore administration, shows the list of all discovered VMs with their current statuses and states of the backup/verify/restore operations

Event Log – this view shows the historical overview of all backup, verify and restore operations.

App Configuration – this section contains settings that manage the most important aspects of *Archiware Pure* operation, such as configuration of Backup repositories, Infrastructure servers, Daily reports and General backup preferences

System Settings – this section contains settings not directly related to backup and restore operations, such as the configuration of the email server, software updates and licensing.

Another point of interest is the top area, common for all four views, that contains the collapse/expand sidebar button, the current date and time information and the logout button.



5.1 Virtual Machines View

The Virtual Machines view shows a list of all the discovered virtual machines, their statuses and information on their backup/verification times and disk usage.

It consists of:

1. The Central area
2. A collapsible *Backup Administration* panel (right)
3. A collapsible *Filter the List of VMs* panel (left)
4. A collapsible *Restore* panel (bottom)

5.1.1. The Central Area

Virtual Machine	Backup/Verify		Verify		Backup Disk Usage			Next Backup Starts Between	
	Completed	Duration	Completed	Duration	Repository	Total	Last i...	Start	End
OS X 10.11					/vol1/backup			11.Apr 00:00	11.Apr 06:00
Kerio-Control	10.Apr 00:36	36 min 45 s			/vol1/backup	6.1 GB	6.1 GB	11.Apr 00:00	11.Apr 06:00
OS X 10.9	10.Apr 11:20	24 min 09 s			/vol1/backup	33.2 GB	33.2 GB	11.Apr 00:00	11.Apr 06:00
OS X 10.6 234.26					/vol1/backup			11.Apr 00:00	11.Apr 06:00
▼ 192.168.234.217									
Tiny Linux VM	10.Apr 00:37	0 min 39 s			/vol1/backup	0.0 GB	0.0 GB	11.Apr 00:00	11.Apr 06:00
com.archiware.pure.builder					/vol1/backup			11.Apr 00:00	11.Apr 06:00
APT_ubuntu					/vol1/backup			11.Apr 00:00	11.Apr 06:00
Tiny Linux VM-1_1_7					/vol1/backup			11.Apr 00:00	11.Apr 06:00
Tiny Linux VM-2					/vol1/backup			11.Apr 00:00	11.Apr 06:00
Unitrends_test					/vol1/backup			11.Apr 00:00	11.Apr 06:00
Ubuntu15					/vol1/backup			11.Apr 00:00	11.Apr 06:00
W2016					/vol1/backup			11.Apr 00:00	11.Apr 06:00
APT_solaris	09.Apr 13:44	1 min 31 s			/vol1/backup	3.6 GB	3.6 GB	11.Apr 00:00	11.Apr 06:00
Synology Play	10.Apr 01:14	36 min 59 s			/vol1/backup	27.7 GB	27.7 GB	11.Apr 00:00	11.Apr 06:00
Tiny Linux VM-3	09.Apr 13:41	0 min 08 s	09.Apr 13:41	0 min 08 s	/vol1/backup	0.0 GB	0.0 GB	11.Apr 00:00	11.Apr 06:00
APT_frebsd					/vol1/backup			11.Apr 00:00	11.Apr 06:00
51 VMs						70.56 GB			70.56 GB

The Central view lists all the discovered VMs per host and their status. The list is collapsible per host and can be searched by VM name (top right corner).

Clicking on *More details* and *Less details* buttons toggles between a detailed and a simplified information view. Detailed information displays backup and verify completion time and duration, backup disk usage, next backup window information and the progress of the current backup/verify/restore operation. The simplified information view omits the verify completion time and duration and the next backup window details.

The refresh button can be found in top right-hand-side corner, it is used to manually force a refresh of the VM list and information.



The status of each of the VMs is indicated by three icons – automatic backup enabled/disabled, VM powered on/off and the result of the latest backup or verify operation.

When a VM is selected, a button (...) appears immediately to the left of the VM status icons. When clicked, it opens a pop-up menu with the following options:

- **Start backup now:** to immediately execute backup or verify operation for this VM
- **Enable automatic backup:** to toggle the automatic backup setting for this VM
- **Delete from repository:** to delete all of the backup data for this VM from *Archware Pure* repository

5.1.2. Filter the List of VMs

This panel allows narrowing down the displayed list of the VMs using these categories:

Filter the List of VMs	
<input checked="" type="checkbox"/>	Backup Results
<input type="checkbox"/>	Backup completed
<input type="checkbox"/>	Backup & verify completed
<input type="checkbox"/>	Last backup failed
<input type="checkbox"/>	Backup completed with warning
<input type="checkbox"/>	Backup Status
<input type="checkbox"/>	Backup is enabled
<input type="checkbox"/>	Backup disabled
<input type="checkbox"/>	Backup running
<input type="checkbox"/>	Restore running
<input type="checkbox"/>	Job pending
<input type="checkbox"/>	VM is offline
<input type="checkbox"/>	Tags
<input type="checkbox"/>	Backup Volumes
<input type="checkbox"/>	/vol1/backup
<input type="checkbox"/>	Backup Windows
<input type="checkbox"/>	Run weekly on Sat 00:00 48h
<input type="checkbox"/>	Run weekly on Mon, Tue, 00:00 6h

- **Backup Results:** the result of the latest backup or verify operation
- **Backup Status:** based on backup settings and state of the backup or restore
- **Tags:** can be manually set (one or more) for each VM (see 5.1.3 Backup Administration for more info); selecting one or more tags lists only the VMs that have at least one matching tag assigned
- **Backup Volumes:** filters VMs based on their backup storage location
- **Backup Windows:** contains a list of all the defined Backup Windows (see 5.1.3 Backup Administration for more info)

5.1.3. Backup Administration

This panel allows configuring the parameters related to the VM backup. It consists of three tabs - Basic, Advanced and Job Logs.

Basic Tab

Enables/disables automatic backup for this and all the selected VMs

Shows a list of all the available backup windows with a checkbox to enable each for the selected VMs. New backup windows can be created by clicking the + button, deleted by clicking the - button and the existing backup windows can be modified by clicking the pen button. The backup window creation and modification screen also controls whether the verify is executed or not.

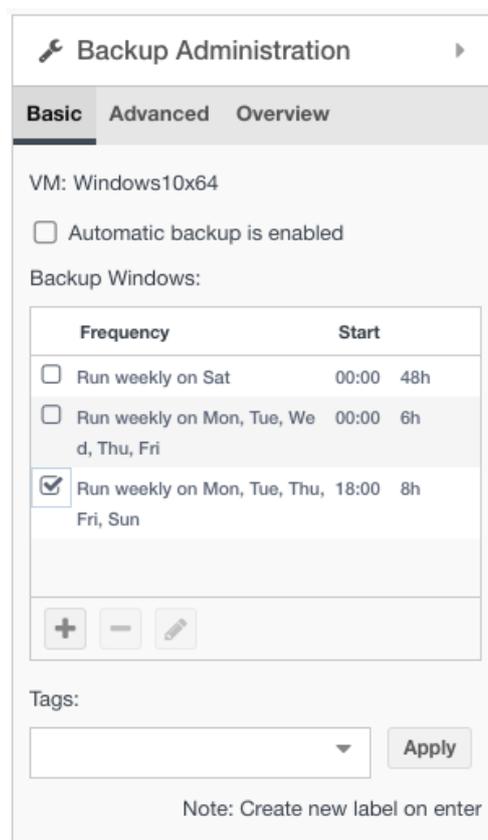
Note: newly created or modified backup windows will also become available for all the other VMs. If after deselecting a backup window, no VM is left using that particular window, it is automatically removed when Pure gets restarted.

Note: for Pure to optimally function, backup windows need to be sufficiently large to allow verify to be started for at least one of the VMs.

Note: The initial backup of a VM will take significantly more time since it needs to back up the whole VM data. Subsequent backups will be significantly faster, leaving more time for verify.

Note: When a backup window is modified or deleted, the changes are automatically applied to all VMs that are assigned to it, modifying their schedules accordingly.

Shows the tags assigned to this VM. Tags are an optional field and each VM can have an arbitrary number of custom tags to enable easier grouping and displaying of similar VMs. To create a new tag, simply enter the desired text and press Enter to finish. Click on the Apply button to save and assign defined tags. Tags are deleted by pressing 'x' icon on the right of each tag.



Frequency	Start
<input type="checkbox"/> Run weekly on Sat	00:00 48h
<input type="checkbox"/> Run weekly on Mon, Tue, Wed, Thu, Fri	00:00 6h
<input checked="" type="checkbox"/> Run weekly on Mon, Tue, Thu, Fri, Sun	18:00 8h



Advanced Tab

Shows the list of disks that are available for backup and allows including or excluding of particular disks from backup. Excluding a non crucial disk from backup will save storage space and backup time, both for the automatic and for the manual backups. However, keep in mind that disks that were not included for backup will not be available for restore.

Note: The list of virtual disks will show only those disks that are available for backup. Because backup operations leverage VM snapshots, virtual disks not supported by this mechanism will be omitted from the list.⁷

Shows the currently configured value and allows changing of the backup retention time. This settings determines the number of backup snapshots that will be retained in the repository before the space is reused for new backups.

Note: To change the default backup retention time automatically applied to newly discovered virtual machines, see 5.3.5 Preferences.

Shows the option to enable or disable cloning of backup snapshots to a configured cloud storage individually for the selected VM and optionally allows configuring a number of additional cloud based backup snapshots to keep.

Backup Administration

Basic **Advanced** Overview

Selected VM: APT_win7

Virtual disks to backup:

Label ↑	Size	File
<input checked="" type="checkbox"/> Hard disk 1	20.00 GB	[NAS1-Prod] APT_wi n7/APT_win7.vmdk
<input checked="" type="checkbox"/> Hard disk 2	32.00 GB	[NAS1-Prod] APT_wi n7/APT_win7_1.vmdk
		52.00 GB

Backup retention time:

Each backup run creates a snapshot. And each snapshot is a point in time to which a VM can be restored.

of local snapshots to keep: 7

The entire backup can be cloned as a copy on an object store.

clone to object store:

Additionally, older snapshots can be kept longer on the object store.

of remote snapshots to keep: 50

Backup Administration

Basic **Advanced** Overview

Started	Duration	Size
10.Apr 00:00	161 min 55 s	25.2 GB
09.Apr 00:00	99 min 59 s	18.4 GB
08.Apr 00:00	98 min 45 s	20.5 GB
06.Apr 00:00	99 min 03 s	18.8 GB
05.Apr 00:00	92 min 42 s	12.6 GB
04.Apr 14:30	94 min 36 s	18.3 GB
04.Apr 00:00	105 min 47 s	44.4 GB
		158.07 GB

Last 7 Backups

Date	Size
04-Apr	44.4 GB
04-Apr	18.3 GB
05-Apr	12.6 GB
06-Apr	18.8 GB
08-Apr	20.5 GB
09-Apr	18.4 GB
10-Apr	25.2 GB

Note: To change the default cloud retention policy applied to newly discovered virtual machines, see 5.3.5 Preferences.

Note: When backup snapshot cloning to an object store is enabled, all of the local snapshots will be copied to a cloud based storage. The configurable value for the number of remote snapshots to keep is in addition to the number of local snapshots that are copied by default.

Overview

Allows selecting a backup job from a drop-down menu and viewing its detailed log information. Job logs contain a step by step rundown of the backup process and will display such info as job statistics and possible backup errors.

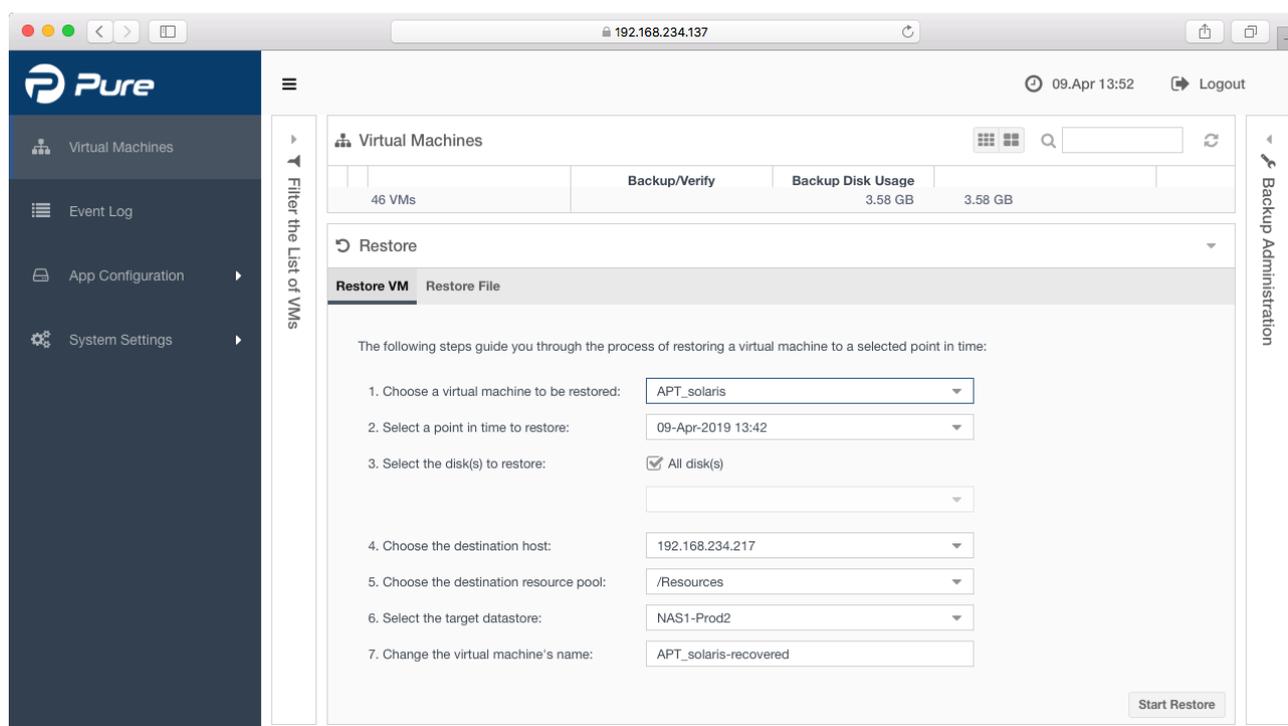
⁷ VMware does not support snapshots of raw disks, RDM physical mode disks, independent disks, PCI vSphere Direct Path I/O devices, disks configured for bus sharing or disks that use the iSCSI initiator in the guest operating system.

5.1.4. Restore

All the restore operations are accessible through the *Restore* panel. Depending on the desired operation, choose one of the available tabs:

- Restore VM – to restore an entire virtual machine from the backed up data
- Restore File – to select a single file from one of the backed up virtual disks and download it directly to your workstation

Restore VM



The *Restore VM* operation creates a new virtual machine on the chosen target host, with the same configuration and virtual disk content as that of the selected backed up VM at the selected point in time. In order to avoid possible configuration collisions, such as IP configuration, the newly restored virtual machine is not automatically powered on upon completion.

A restore VM operation can be started from the *Restore* tab. It consists of 7 steps:

1. Choose a virtual machine to be restored: the VM can be chosen from a drop-down menu or by selecting the desired VM in the main window.
2. Select a point in time to restore: after a VM is selected, this drop-down menu shows all the available points in time, i.e. backups from which the VM can be restored.
3. Select the disks to restore: by default, all the disks available at the point in time selected in step 2 will be restored. If some disks are not required to be restored, the *All disks* checkbox has to be deselected and the desired disks selected from the drop-down menu. Please note that that menu shows only the disks that were backed-up in step 2 at the



particular point in time selected. If the desired disk does not appear in the list, a different point in time must be selected in step 2.

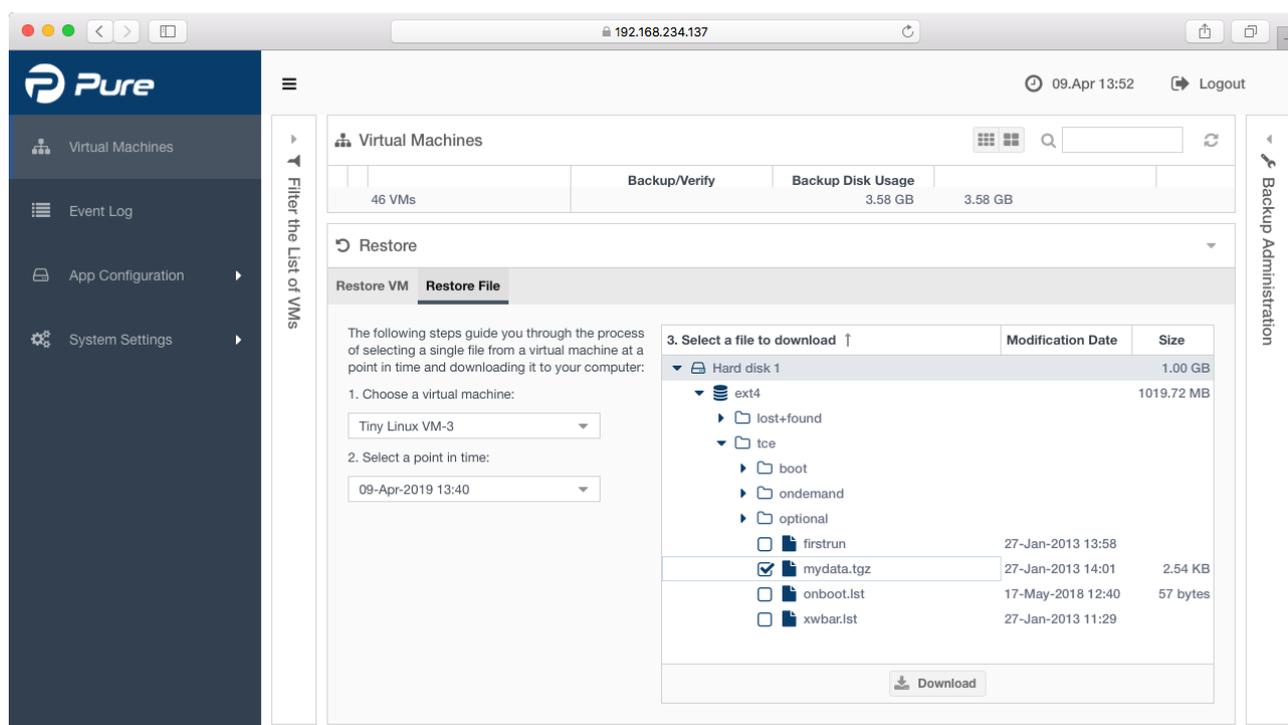
4. Choose the destination host: by default this is automatically set to the original host, but can be changed to any available host by selecting it from the drop-down menu.
5. Choose the destination resource pool: by default this is automatically set to the original resource pool, but can be changed to any available resource pool by selecting it from the drop-down menu.
6. Select the target datastore: by default this is automatically set to the original datastore, but can be changed to any available datastore by selecting it from the drop-down menu.
7. Change the virtual machine's name: by default this is automatically set to the original name with an added '-recovered' suffix, but can be changed to any desired name provided that a VM with the same name does not already exist on the selected host.

After following all these steps, click *Start Restore* to begin the restore operation. The progress of the restore can be tracked in the central view (depending on the browser window size, you may need to collapse the Restore panel first).

Note: *Archware Pure* can seamlessly restore virtual machines from cloud based backup snapshots by automatically downloading the required data files. Such restore operations could potentially require more time to complete, depending on the network transfer speed.



Restore File



Restore File operation allows browsing the content of backed up virtual disks and downloading a single file or a folder directly to your workstation.

Restoring a file is a straightforward operation: First select the VM that has the required file and then choose the desired point in time to browse for files.

Only the disks that were part of the backup at that point in time are shown. Expanding each disk shows its partitions and their sizes. Supported partitions can then be further expanded and browsed for the desired file to download. When the file or folder is located, mark it and press download to initiate the download process. The file will be downloaded to the download location determined by your web browser. If the entire folder is selected, it will be downloaded as a zip archive

Note: Archiware Pure supports the following file systems for *Restore File* operations: HFS+, NTFS, FAT32, ExFAT, UFS2, ext2, ext3, ext4, Btrfs.

Note: LVM managed partitions are supported only if their Volume groups consist of a single Physical volume. Multi disk volumes are currently not supported.

Note: When Archiware Pure is not deployed from the official Virtual Appliance template, file system support may be limited by the host operating system. Please consult your OS or NAS device documentation on how to enable support for the additional file systems.



5.2 Event Log

The screenshot shows the Pure Event Log interface. The left sidebar contains navigation options: Virtual Machines, Event Log (selected), App Configuration, and System Settings. The main area displays an 'Event Log Query' section with filters for Period (Today, Yesterday, Past week, Past month, Overall), Result (Any, Completed, Warning, Error), and Type (Any, Backup, Verify, Restore). The main table lists the following entries:

Name	Type	Start ↓	End	Size	Summary
● APT_solaris	Backup	09.Apr 13:42	09.Apr 13:44	8.0 GB	Operation completed successfully
● Tiny Linux VM-3	Verify	09.Apr 13:41	09.Apr 13:41		Operation completed successfully
● Tiny Linux VM-3	Backup	09.Apr 13:40	09.Apr 13:40	0.0 GB	Operation completed successfully
● Tiny Linux VM-3	Verify	09.Apr 13:39	09.Apr 13:39		Verify not possible because no backup snapshots exist yet.

At the bottom, there is a pagination control showing 'Page 1 of 1' and a 'Page size' dropdown set to 50.

The Event Log shows the historical overview of all the backup, verify, restore and snapshot upload operations. Entries can be filtered according to their start time, result and type.

Clicking on the icon that appears immediately to the left of the status icon for each entry will bring up the detailed view window listing all the steps performed during the selected operation.



5.3 App Configuration

5.3.1. Configuring the Backup Repository

The screenshot shows the Archware Pure Backup Repository configuration page. The left sidebar contains navigation options: Virtual Machines, Event Log, App Configuration (selected), Repository, Servers, Object store, Reporting, Preferences, and System Settings. The main content area is titled 'BACKUP REPOSITORY' and contains the following text:

The Archiware Pure backup repository is the central storage location for the saved data and the backup configuration. It consists of at least one volume and can be extended later on. We highly recommend using only RAID storage in order to avoid backup failure. The primary volume is the default target for storing newly discovered virtual machines. Already saved virtual machines remain stored on the volume disk. The repository consists of one or more volume. For each volume, a limit on the number of simultaneous backup jobs can be set.

Volume	Path	Total Size	Free Size	Parallelism	Primary
vol-20201109141949	/vol1/cloudtest	2.69 TB	1.91 TB	1	<input checked="" type="checkbox"/>

Below the table, there are summary statistics: 2.69 TB Total Size, 1.91 TB Free Size. There are '+' and '-' buttons to add or remove volumes.

The configuration form below the table includes:

- Directory path:
- Number of simultaneous backup jobs:
- Primary backup disk
-

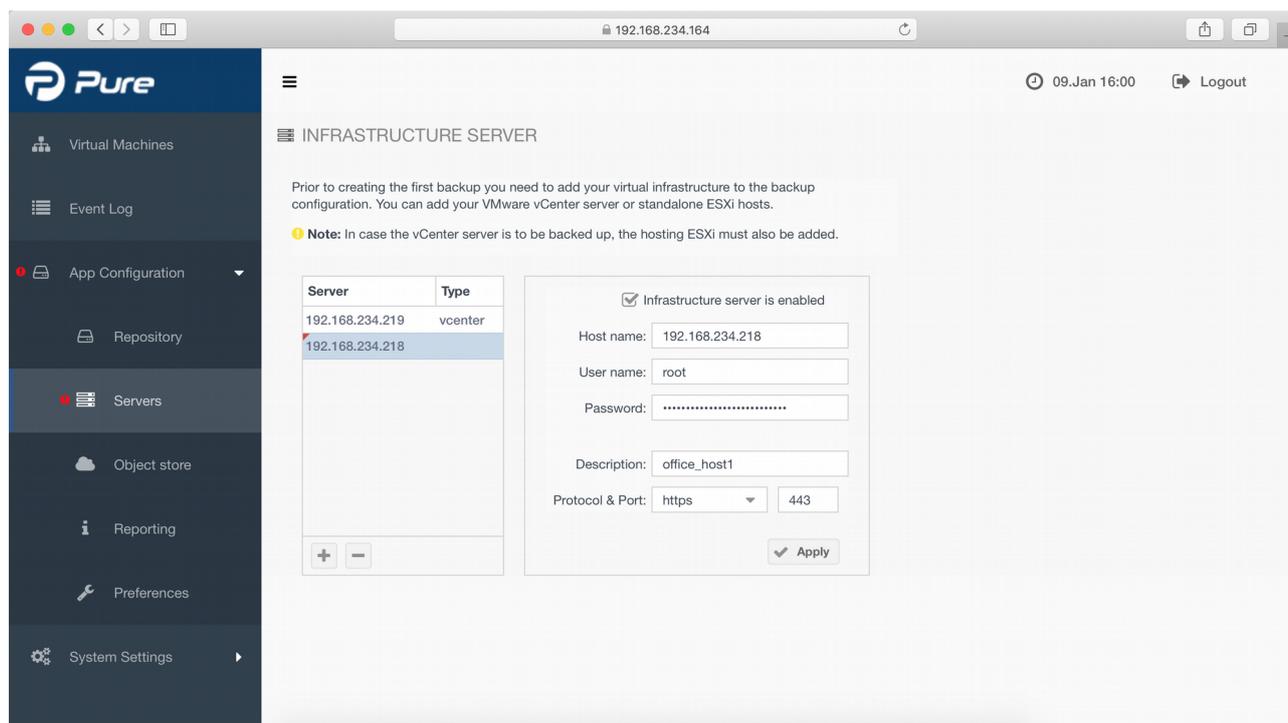
Additional backup volumes can be configured by selecting the *Repository* tab in the left side menu. By adding additional mount paths to the *Volumes* list and clicking *Apply*, that path will be configured as part of a *Backup Repository*.

Note: Newly discovered *Virtual Machines* will automatically be assigned to the primary backup volume. You can change the primary volume by toggling the corresponding checkbox in the *Volumes* list. Already discovered *Virtual Machines* will always be backed up to their assigned backup volume.

Note: The number of simultaneous backup jobs can be separately configured for each volume. This overrides the default number of simultaneous backup jobs that is defined in 5.3.5 Preferences.



5.3.2. Configuring Infrastructure Servers



Archiware Pure can be configured to protect virtual machines managed by multiple ESXi servers, with or without a vCenter. A new Infrastructure server can be added by clicking the “+” button and entering the corresponding connection parameters:

Host name: FQDN or IP address of the vCenter or the ESXi

User name and password: of the account used to connect to the vCenter or the ESXi

Protocol and port: used for connection (https or http)

Description: optional parameter

After all the required fields are entered, click the *Apply* button to save the configuration.

Note: For vSphere installations managed by a vCenter server, it is strongly recommended that Archiware Pure be configured to connect to this vCenter server. Additional connections to managed ESXi hosts can also be configured, but they will not be employed as long as the vCenter connection is available. The exception is the ESXi host where the vCenter virtual appliance resides, which has to be configured in order to enable backups of the vCenter virtual machine itself.

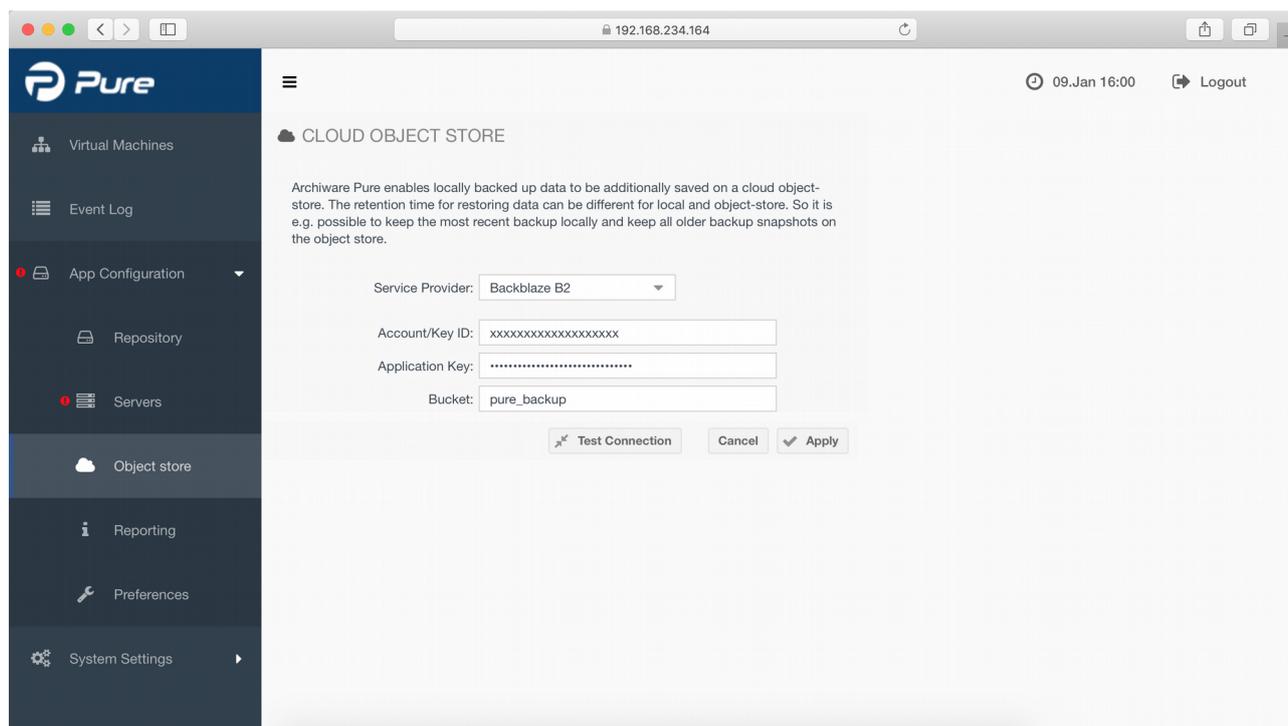
Note: When configuring an *Infrastructure Server*, if the given user belongs to a vSphere role other than *Administrators*, please ensure that the corresponding user has sufficient vSphere privileges to execute all the operations required for backup.

Note: In order to enable normal operation in environments with vSphere lockdown mode enabled, user names configured for access to ESXi servers will automatically be added to the VMWare's *Exception Users List*.⁸

⁸ <https://docs.vmware.com/en/VMware-vSphere/6.0/com.vmware.vsphere.security.doc/GUID->



5.3.3. Configuring Object Store

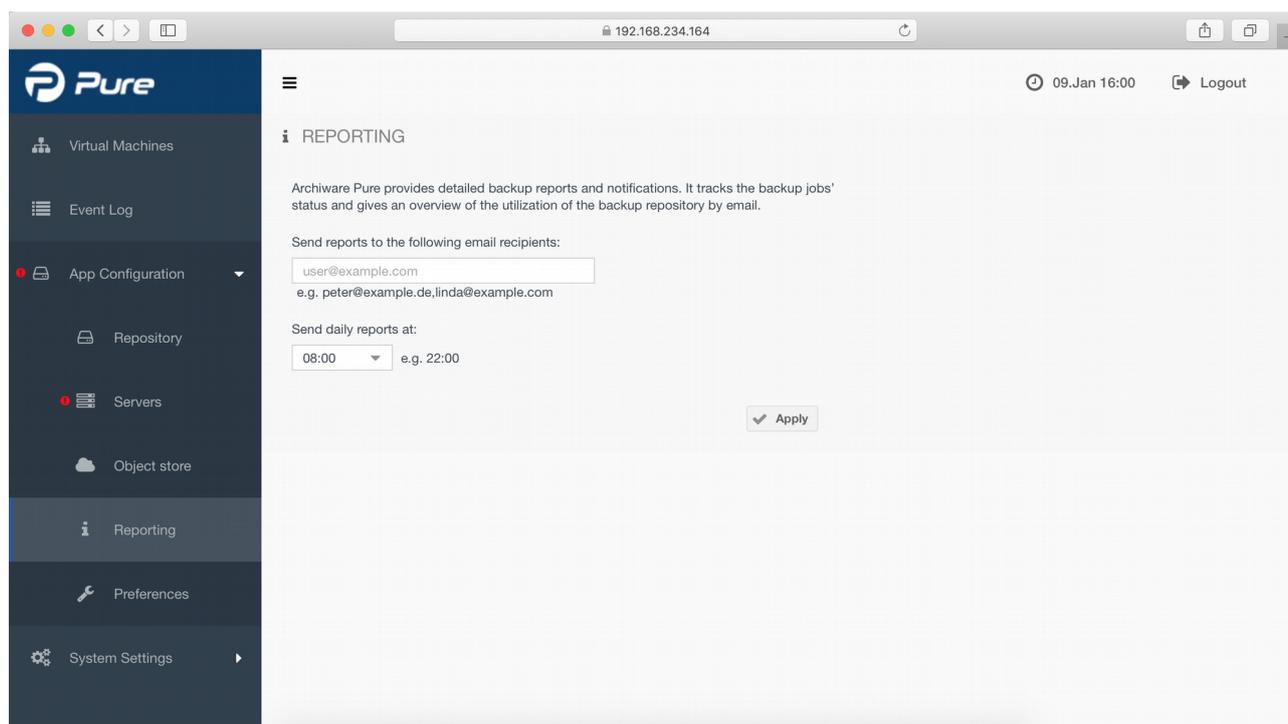


Archware Pure can be configured to clone the local backup repository to a cloud based object storage in order to increase data security and allow for longer retention times. In order to enable cloud object store, please select your storage provider and configure relevant access details.

Note: Archware Pure will autonomously maintain and manage the content of the configured cloud storage bucket. New snapshots will be scheduled for upload following a successful backups and Archware Pure will also periodically reschedule any snapshots that have not been upload in the previous runs. Please do not manually delete content from the cloud storage. To remove unwanted backup snapshots, modify the number of cloud based snapshots to be kept. Please see 5.1.3 Backup Administration for more details.



5.3.4. Reporting

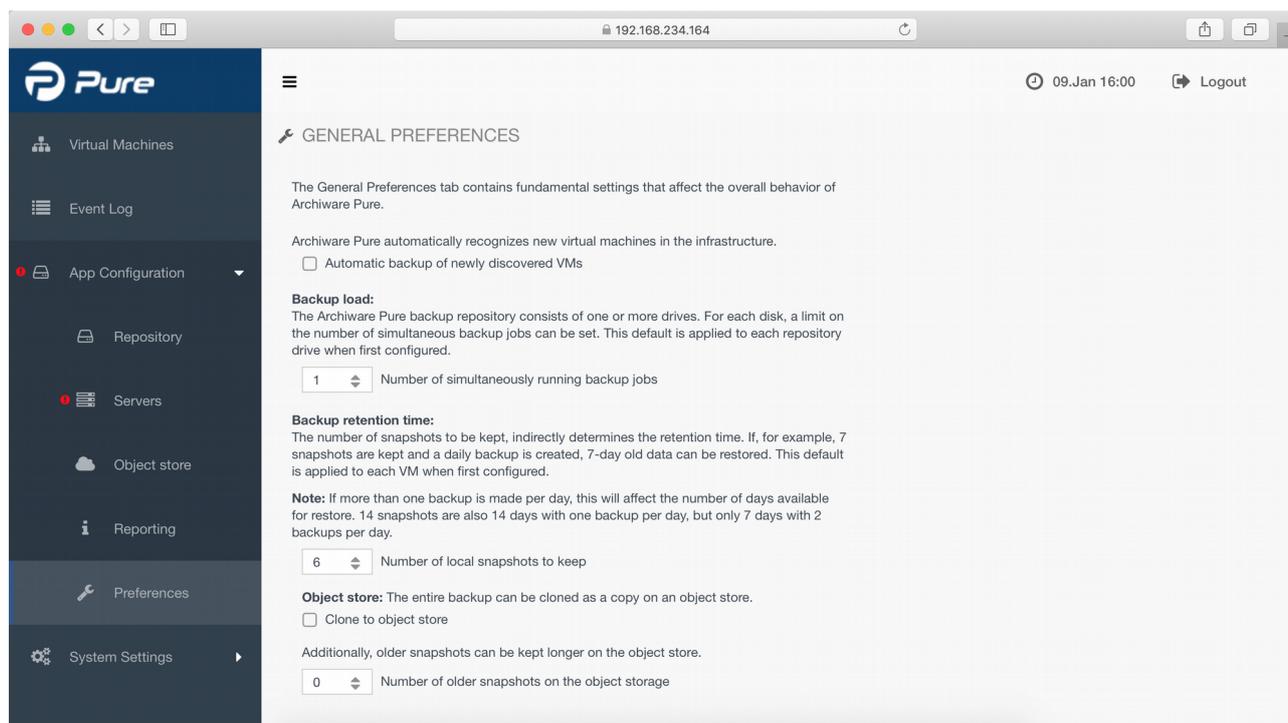


Archware Pure can be configured to automatically email a detailed daily backup report. If you wish to receive daily reports, please configure the email recipients and the required report generation time. In case of the multiple recipients, please separate the individual email addresses with commas and without spaces.

Note: In order for *Archware Pure* to be able to send daily reports, the *Email server* settings need to be configured. Please see 5.4 System Settings.



5.3.5. Preferences



The *Preferences* tab contains fundamental settings that affect the overall behavior of *Archware Pure*. Each of these settings can be individually overridden for selected virtual machines or backup volumes, allowing you to fine tune the configuration to your specific needs.

The settings that can be adjusted are:

Automatic backup of newly discovered VMs

This setting determines whether *Archware Pure* should automatically schedule newly discovered virtual machines for backup. Each new VM will be assigned to the primary backup volume and assigned the default backup window schedule.

Number of simultaneously running backup jobs

This setting determines how many backup jobs will concurrently be run for each backup volume. If there are multiple virtual machines to be backed up within a backup window, only this number of backups will be executed at the same time. All the other jobs remain in the queue until the next job slot becomes available.

Note: This setting is applied to newly added backup volumes only. To change this setting for an existing volume, please see 5.3.1 Configuring the Backup Repository.

Backup retention

This settings determines the number of backup snapshots to be retained in the repository before reusing the space for new backups.

Cloning to object storage and cloud retention

These settings enable cloning the entire backup repository to a configured cloud based object



store and determine the number of backup snapshots to be retained in cloud in addition to the copies of local snapshots that are uploaded by default. Cloud based backup snapshots are used completely transparently and *Archware Pure* will automatically download the required data files to perform the desired operation.



5.4 System Settings

5.4.1. Email

The screenshot shows the Archware Pure web interface. The top navigation bar includes the Pure logo, a menu icon, the IP address 192.168.234.137, and the date/time 09.Apr 13:49 along with a Logout button. The left sidebar contains the following menu items: Virtual Machines, Event Log, App Configuration, System Settings (expanded), Email (selected), and Software. The main content area is titled 'EMAIL SERVER' and contains the following configuration fields:

- Sender (Reply To) email:
- Outgoing mail server:
- Use SMTP Authentication:
- Port to connect to:
- For the authentication optional username and password:
 - Username:
 - Password:

At the bottom of the form, there are two buttons: 'Send Test Mail' and 'Apply'.

In order to enable *Archware Pure* to send daily email reports, the email server settings need to be configured first. Please provide the following parameters:

Sender email – the email address to be used as a sender

Outgoing mail server – the FQDN or IP address of your mail server. In case a FQDN name is entered, please make sure the name can be resolved to an IP address.

Use SMTP Authentication – enter the desired type of encryption TLS/SSL/NONE

Port to connect to – by default this port is related to the encryption type and is preset to the default port for each encryption type. If required, it can be manually set to a desired value.

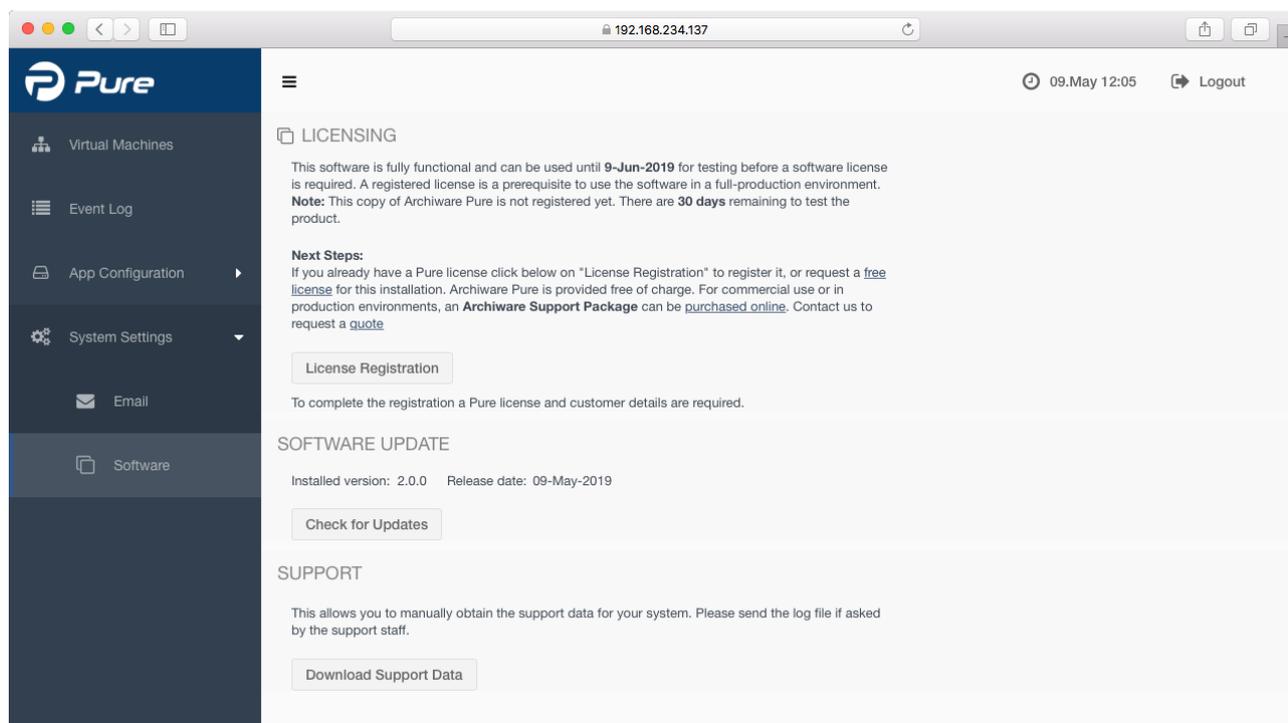
Username & Password – enter valid login credentials for the selected email server

After configuring the email server settings click *Apply* to save the configuration.

To ensure that the entered email settings are correct and that emails can be sent, use the *Send Test Mail* function and fill in the email recipient when prompted.



5.4.2. Software Settings



The *Software settings* view allows you to register and license *Archiware Pure*, perform software updates and download the support data.

Licensing

To allow testing the product, *Archiware Pure* will run for 30 days before a software license is required. Once a license is obtained, click on the *License Registration* button to start the *License Registration Wizard* and register your copy of the software.

Update

The *Update* section displays information about the currently installed *Archiware Pure* version and allows checking for new updates online. Because the *Archiware Pure* could be placed behind a firewall, without direct Internet access, the update process is separated into several steps:

1. Using the *Download* button, the *update package* can be downloaded to your PC
2. With the *Select* button, select the downloaded *update package*. With the *Upload* button, transfer the package to the *Archiware Pure*
3. Start the update process and let *Archiware Pure* restart in order to finish the update

Note: The update process will restart *Archiware Pure* and any active backup or restore tasks will consequently be interrupted. Please make sure that there are no active jobs at the time of the update.

Note: The update button will be disabled when *Archiware Pure* is deployed on a NAS appliance. Please use the respective vendor's app marketplace to perform update. The corresponding software update package can also always be downloaded from Archiware's web site.



Support

In order to aid customer support, *Archware Pure* can collect and pack the necessary support data to be forwarded to the support staff if requested. The support package contains the *Archware Pure's* log files, configuration, selected OS logs and the *vSphere's* inventory and configuration. Click on the *Download Support Data* button to prepare and download a zip archive to be attached to your support ticket, if requested by the *Archware* support staff.