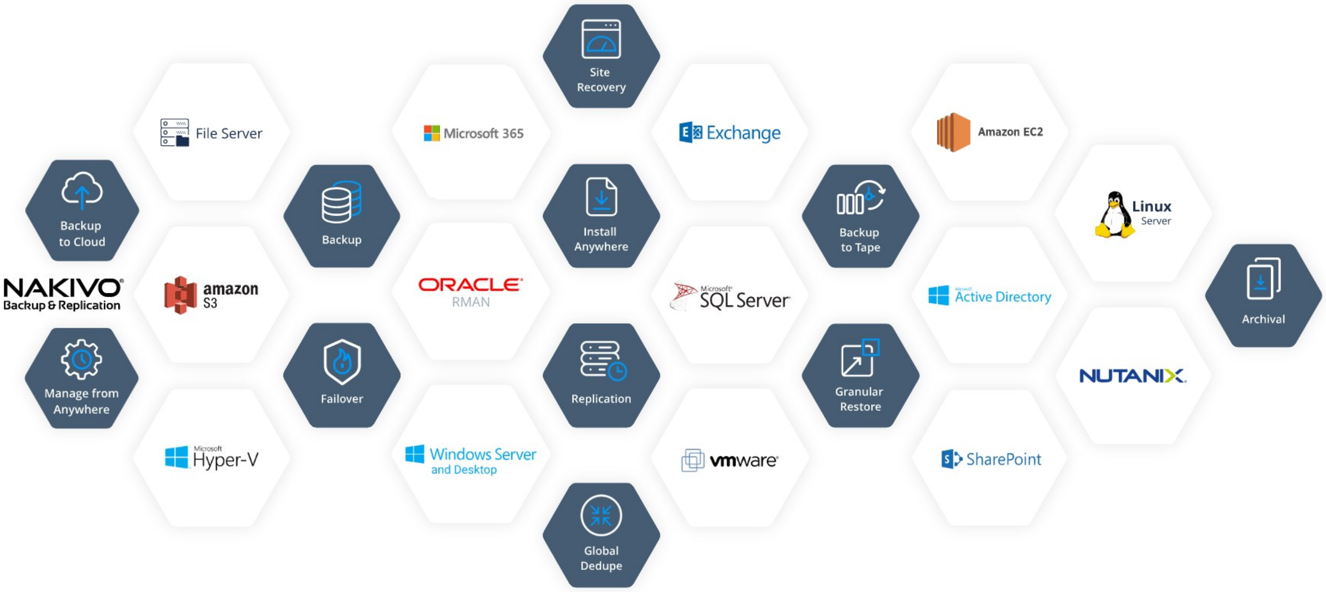
NAKIVO Backup & Replication v10.4

User Guide for Microsoft 365

Table of Contents

NAKIVO Backup & Replication Overview

NAKIVO Backup & Replication offers backup, replication, failover, backup to cloud, backup to tape, backup copy, backup data reduction, instant verification, granular restore and disaster recovery orchestration for virtual, physical, cloud and SaaS environments - all in one convenient web interface.



The product provides image-based, application-aware, incremental backup and replication. You can easily schedule jobs using the calendar in the product's web interface and save up to 1,000 recovery points for each backup, rotating them on a GFS basis. You can also protect your VMs and instances more efficiently by taking advantage of Changed Block Tracking (for VMware), Resilient Change Tracking (for Hyper-V), or Changed Regions Tracking (for Nutanix), LAN-Free Data Transfer, Network Acceleration, and other product features.

The solution includes an advanced disaster recovery (DR) functionality. It allows you to automate and orchestrate DR activities across multiple sites. Build advanced site recovery workflows to failover an entire site in just a few clicks, perform non-disruptive recoverability testing, and make sure you have a workable DR plan in place to help minimize downtime and prevent loss of revenue or data.

NAKIVO Backup & Replication allows you to simplify data protection management through the automation of core tasks such as backup, replication, and backup copy. Instead of tracking every change in your environment and manually adding VMs or physical machines to jobs, you can set up policies based on a VM/physical machine name, tag, size, location, power state, configuration, or other parameters. NAKIVO Backup & Replication can regularly scan your infrastructure and automatically protect VMs, physical machines, and Amazon EC2 instances that match policy rules.

With NAKIVO Backup & Replication, you can also ensure the safety and integrity of your Microsoft Office 365 data. The product allows you to reliably protect Microsoft Exchange mailboxes, OneDrives for Business, and SharePoint Online sites.

Deployment Options

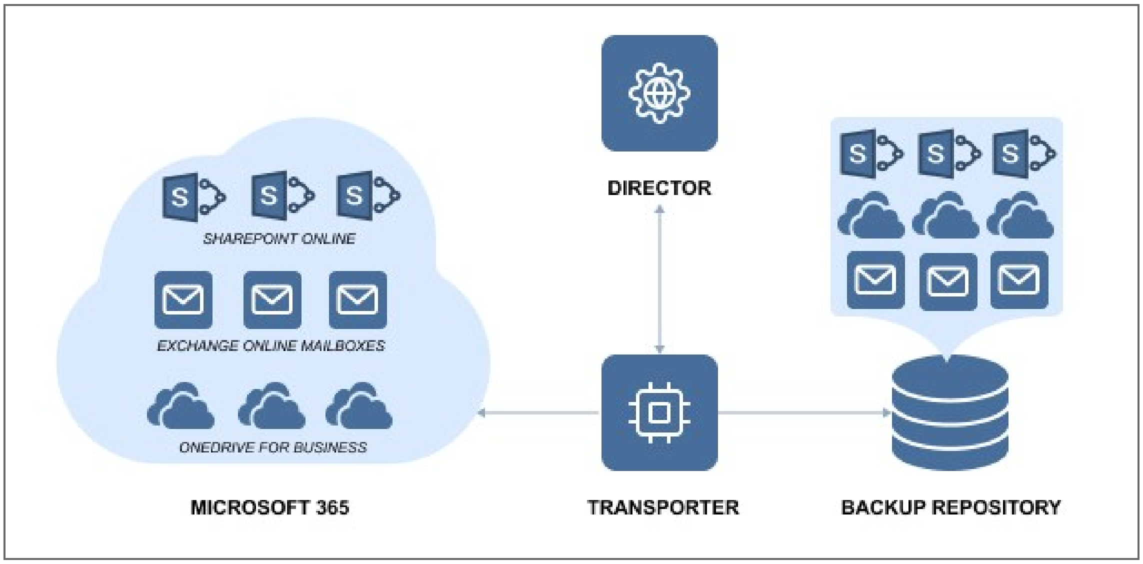
NAKIVO Backup & Replication is a versatile solution that can be installed on most modern operating systems and hardware solutions. For details, refer to the following topics:

- "Installing on Windows" on page 116
- "Installing on Linux" on page 127
- "Deploying Amazon Machine Image in Amazon EC2" on page 115
- "Installing on Synology NAS" on page 136
- "Installing on QNAP NAS" on page 143
- "Installing on Western Digital NAS" on page 153
- "Installing on ASUSTOR NAS" on page 148
- "Installing on NETGEAR ReadyNAS" on page 155

For the full list of supported systems and devices, refer to "Deployment Requirements" on page 70.

Microsoft 365 Backup

With NAKIVO Backup & Replication, you can back up your organization's entire Microsoft 365 account or individual users that have access to the following services: Exchange Online, OneDrive for Business, and SharePoint Online. The backups are stored in a SaaS Backup Repository for further recovery of Exchange Online, OneDrive for Business, and SharePoint Online data including mailboxes, contacts, calendars, emails, OneDrives, sites, subsites, document libraries, lists, list items, and individual files and folders.



A common misconception among SaaS users is that data stored in the cloud is safe and that it is not necessary to back it up. However, under Microsoft’s “shared responsibility model”, Microsoft is responsible for reliable uptime and the physical and virtual infrastructure. Beyond simple geo-redundancy – which is not the same as a backup – ensuring data safety is the responsibility of users. To address this gap, NAKIVO Backup & Replication offers Microsoft 365 Backup & Recovery to ensure that data is accessible and recoverable at all times. By backing up Microsoft 365 application data, you ensure that if data loss occurs, the necessary items can be easily recovered to the original or a custom location.

To start using this feature, the following preliminary steps need to be taken:

- Add your Microsoft 365 accounts to the inventory.
- Create a SaaS Backup Repository.
- Create a Microsoft 365 job .

Microsoft 365 Object Recovery

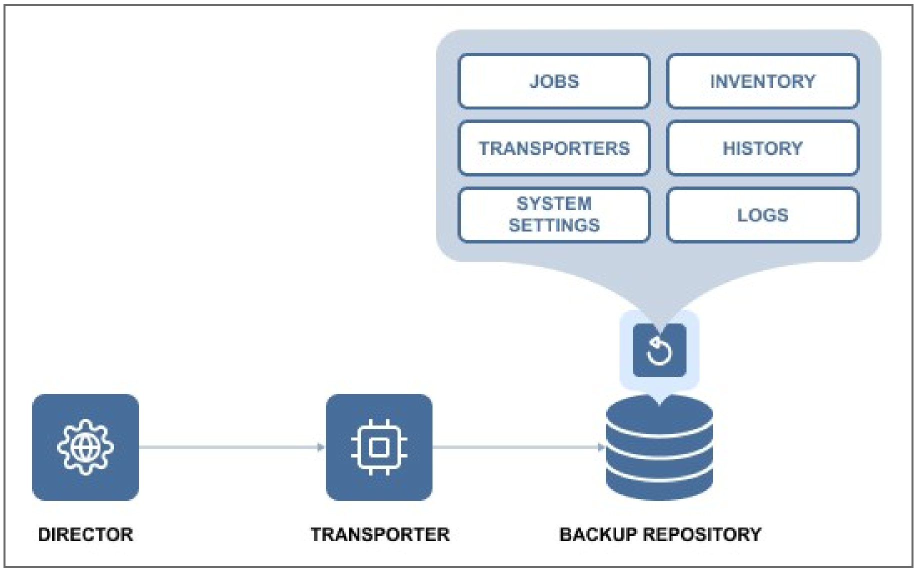
NAKIVO Backup & Replication provides you with the ability to instantly browse, search, and recover Microsoft 365 objects directly from compressed backups. The Microsoft 365 objects can be restored to their original location, or to a certain Exchange Online mailbox, OneDrive for Business instance or SharePoint Online site. The feature streamlines, automates, and speeds up the process of restoring your data, and is available out-of-the-box in NAKIVO Backup & Replication. For more details, refer to "Object Recovery for Microsoft 365" on page 332.

Self-Backup Feature

The Self-Backup feature provides automated protection of everything you have configured in NAKIVO Backup & Replication.

A truly complete data protection solution needs to back up not only your VMs, but also itself. There are good reasons for that. For example, the VM running the product may become corrupted, struck by a virus attack, or accidentally deleted. Regardless of the cause, you will need to restore the disrupted product as quickly as possible. Fortunately, a new instance of NAKIVO Backup & Replication can be installed in less than one minute. However, you will still need to restore the product configuration (such as jobs). Also, you do not want to lose the backup history. To save you time, NAKIVO Backup & Replication automatically backs up the entire configuration, including all jobs, inventory, information about connected Transporters, Backup Repositories and other.

The Self-Backup feature is enabled by default, and NAKIVO Backup & Replication sends daily self-backups to the first five backup repositories available in the product. Each self-backup is kept for five days, by default. Should you like to, you can fine-tune the backup targets, schedule, and retention policy.



If you accidentally make some undesired changes in the product, you can easily roll back to a previous system state from the backup. Migrating the system configuration to a new product instance is simple: just install a new copy of NAKIVO Backup & Replication, import a Backup Repository that contains a self-backup, and select a recovery point. The previous product configuration is restored along with all settings.

The Self-Backup feature saves you time and brings you peace of mind, ensuring reliable protection of everything you configure in NAKIVO Backup & Replication.

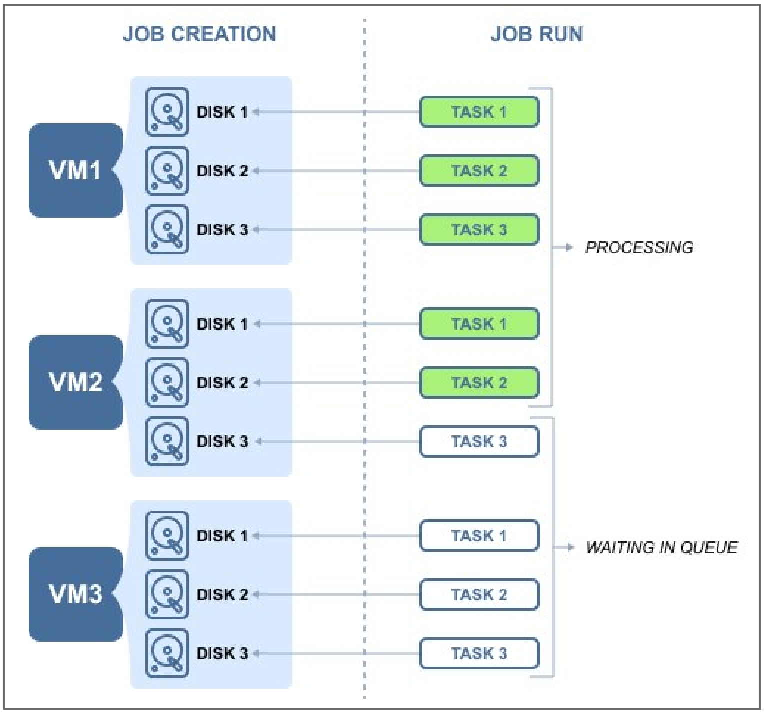
For information on the Self-Backup configuration, refer to “Self-Backup Configuration” on page 199.

Jobs and Concurrent Tasks

Job is a data protection activity that is performed by NAKIVO Backup & Replication in accordance with a distinct configuration. These are the main types of NAKIVO Backup & Replication jobs:

- Backup jobs
- Replication jobs
- Recovery Jobs

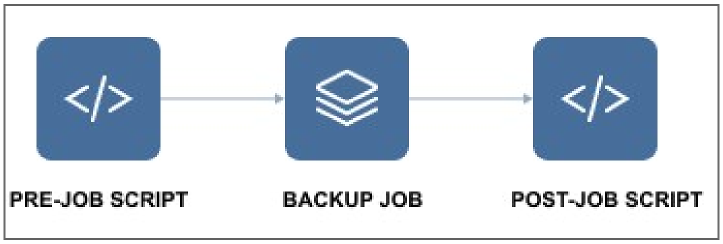
In NAKIVO Backup & Replication, a job can have one or more job objects to process. Depending on your preferences, job objects may be reordered for processing within a job. See the example below.



Each job object may consist of one or more machine disks, Oracle databases, Exchange Online mailboxes, OneDrive for Business instances or SharePoint Online sites that have to be processed within a job run. Data processing that is related to a specific VM disk or service constitutes a single task, in the scope of the corresponding job. Such tasks are processed by a Transporter. For the sake of managing the load over the infrastructure, any Transporter is configured to process a limited number of concurrent tasks. When a task is processed, the Transporter starts processing another task if available. A task can be one disk, file or recovery session, Oracle database, Exchange Online mailbox, OneDrive instance, or a SharePoint Online site. By default, NAKIVO Backup & Replication is set to process 6 concurrent tasks per one Transporter. Refer to "Editing Transporters" on page 269 to learn how to change the Transporter maximum load.

Pre and Post Job Scripts

NAKIVO Backup & Replication provides you with the ability to run a script before a job begins (a pre-job script) and after the job has been completed (a post-job script).



By running your pre- and post- job scripts, you can do just about anything: start custom pre-freeze and post-thaw scripts on Linux systems to wake servers, establish connections, mount volumes, start and stop services, send commands to 3rd-party reporting, monitoring and automation tools, and etc.

Amazon EC2 Concepts

Instance

An *Amazon EC2 Instance* is a virtual server in Amazon's Elastic Compute Cloud (EC2). Amazon EC2 provides different Instance types so you can choose the CPU, memory, storage, and networking capacity you need.

EBS Volume

An *Amazon EBS Volume* is a virtual disk that can be attached to any Amazon EC2 Instance that is in the same Availability Zone. Amazon EBS volumes persist independently from the life of the instance, i.e. deleting an Amazon EC2 Instance does not delete EBS Volumes that were connected to it.

Region

An *Amazon EC2 Region* is a geographic area where an Amazon EC2 Instance is hosted. Amazon EC2 provides multiple Regions so you can create and run your Amazon EC2 Instances in locations that meet your requirements. Each Region is completely independent and isolated from others.

Availability Zone

An *Amazon EC2 Availability Zone* is a location within an Amazon EC2 Region. Each Availability Zone is isolated from failures in other Availability Zones, yet all Availability Zones within the same region are connected with low-latency network connectivity to others in the same Region.

VPC

A *virtual private cloud* (VPC) is a virtual network in Amazon EC2. A VPC is dedicated to your AWS Account and is logically isolated from other virtual networks in the AWS cloud. Similar to regular networks, you can configure your VPCs: select IP address ranges, create subnets, configure route tables, network gateways, and security settings. After you have created and configured a VPC, you can connect your Amazon EC2 Instances to the VPC.

Subnet

A *subnet* is a range of IP addresses in a VPC. You can connect Amazon EC2 Instances to a subnet that you select: public subnets provide access to the Internet, while private subnets don't.

Security Group

A *security group* is a virtual firewall that controls the traffic for one or more instances. When you create an Amazon EC2 Instance, you associate one or more security groups with the Instance. You add rules to each security group that allows traffic to or from its associated instances. You can modify the rules for a security group at any time; the new rules are automatically applied to all instances that are associated with the security group. When we decide whether to allow traffic to reach an instance, we evaluate all the rules from all the security groups that are associated with the instance.

Key Pair

Amazon EC2 uses *key pairs* to encrypt and decrypt login information. A key pair consists of a Public Key that is used to encrypt passwords, and a Private Key is used to decrypt them. When creating a new Amazon EC2 Instance, you need to either create a new Key Pair for it or assign an existing key pair for the Instance. To log in to your Amazon EC2 Instance, you must provide the private key for it. Note that Linux instances have no password, and you use a key pair to log in using SSH. With Windows instances, you use a key pair to obtain the administrator password and then log in using RDP.

Elastic Network Adapter

Elastic Network Adapter (ENA) is a custom network interface with accompanying drivers providing Enhanced Networking on EC2 instances. ENA is optimized to deliver high throughput and packet per second performance and consistently low latencies on EC2 instances. Depending on the type of EC2 instance, you can utilize up to 20 Gbit/s of network bandwidth with ENA. For more information, refer to the corresponding article on the AWS website.

BaaS

NAKIVO Backup & Replication allows for creating and managing multiple isolated tenants within one product instance.

This section contains the following topics:

- "Branding" on page 14
- "License Delegation" on page 15
- "Multi-Tenancy" on page 16
- "Self-Service" on page 17

Branding

Whether you plan to use NAKIVO Backup & Replication internally or provide backup/DR-as-a-Service to external customers, you may find it beneficial to align the product's look and feel with your company's brand. NAKIVO Backup & Replication provides a simple way to customize your product's interface so that it looks like an integral part of your organization. You can customize:

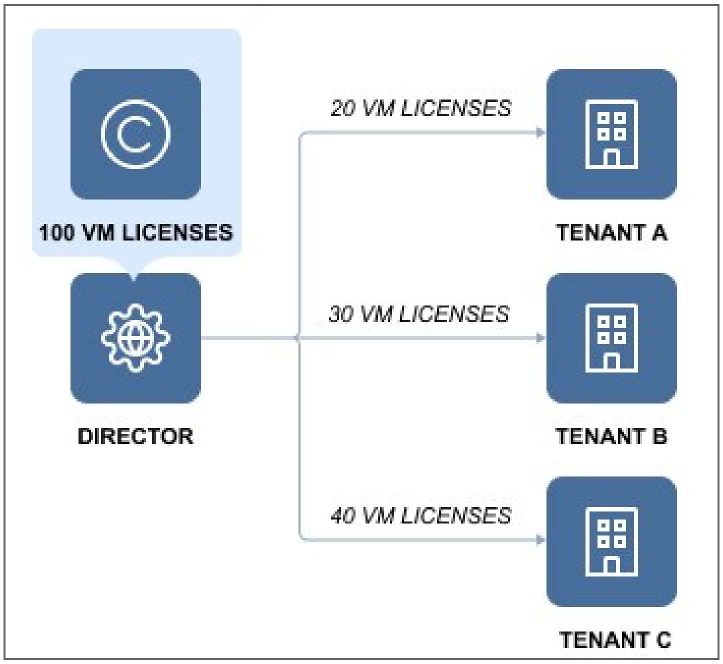
- **Product**: Product title and product logo.
- **Company information**: Company name and website URL.
- **Contact information**: Email, support email, and contact phone.
- **Look and feel**: Bookmark icon and page background.

For information on branding configuration, refer to “Branding Configuration” on page 192.

License Delegation

In Multi-tenant mode, NAKIVO Backup & Replication enables you to create multiple isolated tenants in a single copy of the product. The tenants can represent branch offices/departments in enterprise environments or clients in Cloud Provider environments.

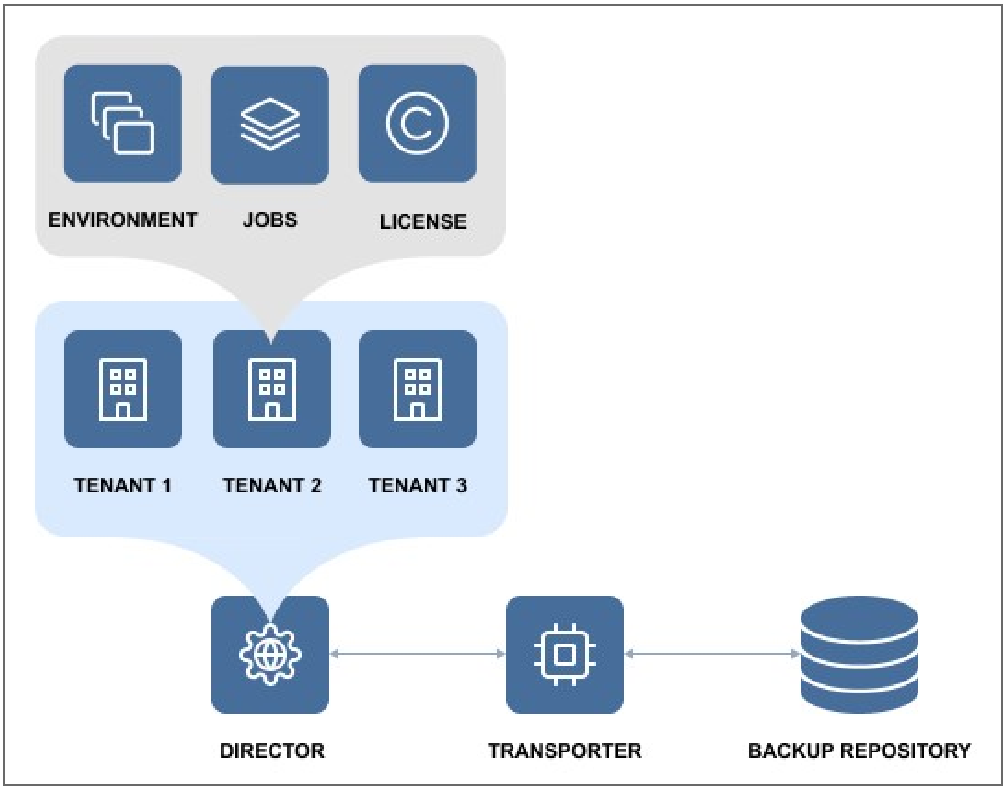
Since tenants are isolated and need to have a limit as to how many licenses each of them can use, NAKIVO Backup & Replication has provided the License Delegation feature. In Multi-tenant mode, a Master Admin (tenant manager) can install one multi-socket license in the product and then assign or delegate a specific number of licenses to each tenant. For example, the Master Admin can install a 20-socket license in the Multi-tenant mode of NAKIVO Backup & Replication, and assign 3 licenses to Tenant A, 2 licenses to Tenant B, and 4 licenses to Tenant C, and let 11 licenses remain unused.



At any moment, the Master Admin can redistribute licenses: revoke any number of licenses from any tenant, which will return them to the Master License Pool, and add licenses to another tenant. The License Delegation feature makes license management simple and manageable in large and distributed environments.

Multi-Tenancy

Multi-tenancy enables you to create and manage up to 1,000 isolated tenants within a single copy of the product. Tenants can represent business units, branch offices, departments, customers, and any other entities.



In Multi-tenant mode, each tenant can access their own environment through a self-service portal, and perform all data protection and recovery tasks. At the same time, tenants are isolated from each other and cannot access the environment and jobs of other tenants.

With Multi-tenancy, you can:

- Deliver Backup-as-a-Service, Replication-as-a-Service, and Disaster-Recovery-as-a-Service more efficiently and cost-effectively.
- Reduce complexity by managing multiple tenants in a single pane of glass.
- Offload data protection and recovery tasks to tenants.
- Reduce footprint by managing tenants in a single instance of the product.

Self-Service

In the multi-tenant mode, you can provide tenants with access to their dashboards. By default, a tenant admin account is automatically created when you create a new tenant. If you assign the **Self-service administrator** role to the tenant admin, the tenant admin has full control over all product features inside the tenant dashboard. This includes editing and updating tenant inventory, Transporters, and Backup Repositories, creating and managing jobs and groups, as well as managing local users and user roles. For each tenant, one guest account can be created. The tenant guest usually has limited permissions inside the tenant.

To provide a tenant with access to the self-service interface, send them the following information:

- Link to NAKIVO Backup & Replication Director
- Tenant login
- Tenant password

Licensing

Choose the licensing type that best suits your business needs. For details, refer to the topics below:

- Licensing Types
    - Perpetual Licensing
    - Per-Workload Licensing
    - Subscription Licensing for Microsoft 365
- Licensing Rules
- NAKIVO Support

Licensing Types

NAKIVO Backup & Replication offers the following licensing types:

Perpetual Licensing

For VMware, Hyper-V, and Nutanix AHV infrastructures, NAKIVO Backup & Replication can be licensed on a per-socket basis. A license is required for each socket on a host where you plan to back up or replicate VMs. Licenses are required only for the source side of backup and replication, that is, you do not need to license target servers for your replicas or the servers on which you want to recover VMs.

Perpetual licenses are also available for physical machines on a per server or workstation basis and Oracle databases (Enterprise Plus edition only) on a per Oracle database basis.

Notes

- Perpetual licenses for physical servers can't be applied for physical workstations and vice versa.
- Physical machines with unsupported OS are treated as physical servers.

Per-workload Subscription Licensing

NAKIVO Backup & Replication can be licensed on a per-workload basis. A workload can be a VMware VM, Microsoft Hyper-V VM, Nutanix AHV VM, physical machine (1 physical server or 3 workstations), Oracle database (Enterprise Plus edition only), or Amazon EC2 instance that you plan to back up or replicate. Regardless of the type, each item is counted as one workload. Licenses are required only for the source side of backup and replication, that is, you do not need to license target servers for your replicas or the servers on which you want to recover workloads. Subscription licenses include 24/7 Support.

Subscription Licensing for Microsoft 365

Backup and Recovery for Microsoft 365 is licensed on a per-user, per-month basis. The license can be purchased together with any edition (Basic, Pro Essentials, Enterprise Essentials, Pro, Enterprise, or Enterprise Plus) and combined with any license type (Perpetual or Subscription). Subscription licenses for Backup and Recovery for Microsoft 365 include 24/7 Support. The minimum number of licenses per order is 10.

When combined with a perpetual license, the support end date of the perpetual license and subscription license for Backup and Recovery for Microsoft 365 must be aligned. The support level may be Standard for perpetual sockets and 24/7 for Microsoft 365 subscription. Optionally, the support level for perpetual sockets can be upgraded to 24/7 Support.

The table below provides information on licensing options.

License Type	VMware	Hyper-V	Nutanix AHV	Amazon EC2	Physical Machine	Microsoft 365	Oracle Database
Perpetual	+	+	+	-	+	-	+
Subscription	+	+	+	+	+	+	+

Licensing Rules

- Perpetual and subscription licenses cannot be combined in one license.
- Subscription license for Backup and Recovery for Microsoft 365 can be combined with both perpetual and subscription (per-workload) licenses.
- Shared mailboxes do not require a license for backup and recovery.

Note

For the most recent information about licensing, refer to the NAKIVO's pricing page.

NAKIVO Support

NAKIVO Backup & Replication offers two levels of technical support:

- Standard Support
- 24/7 Support

Standard Support provides coverage from Monday to Friday during business hours as defined in the Customer Support Policy. One year of Standard Support is included in all new perpetual license purchases.

24/7 Support provides 24/7/365 coverage via phone, chat or email. To switch from Standard to 24/7 Support, you need to purchase a support Upgrade. Customers who upgrade to a higher-tier edition and have purchased additional years of support are required to upgrade their support too.

If a support agreement has been expired for more than 1 month, it can be extended with Expired Support Renewal.

For more information about the terms and conditions of using NAKIVO Customer Support services, refer to the following resources:

- NAKIVO Customer Support Policy
- NAKIVO Customer Support Agreement
- End-User License Agreement

Getting Started

When deployed, NAKIVO Backup & Replication is ready for use. The topics below will provide you with information on how to start working with the application.

Logging in to NAKIVO Backup & Replication

Getting to the Login Page

To go to the NAKIVO Backup & Replication login page, open the following URL in your web browser: https://machine_IP_or_DNS:4443.

Note

If you selected a custom HTTPS port during installation, replace 4443 with the custom value.

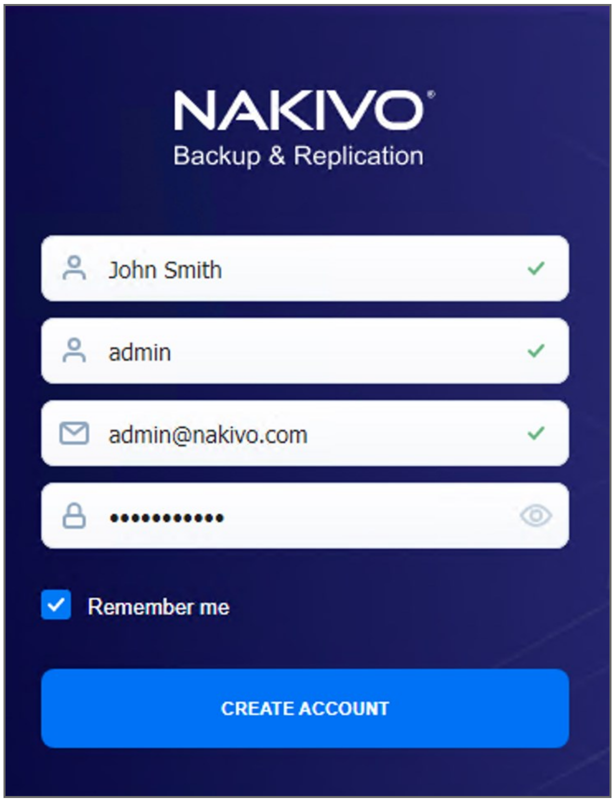
Creating a User Account

When you open the NAKIVO Backup & Replication login page for the first time, you are prompted to create a new user account. This user account is the admin account to be used to access your instance of NAKIVO Backup & Replication. Fill out the fields in the form:

1. **Name**: Provide your real name.
2. **Username**: Enter an admin username to log in to NAKIVO Backup & Replication.
3. **Email**: Provide an email.
4. **Password**: Enter a password.
5. Optionally, you can select **Remember me** to save your credentials.
6. Click **CREATE ACCOUNT**.

   Note

   If NAKIVO Backup & Replication is deployed in an Amazon EC2 instance, you will first be prompted to enter the Amazon EC2 instance ID.



John Smith ✓

admin ✓

admin@nakivo.com ✓

•••••••••••

☑ Remember me

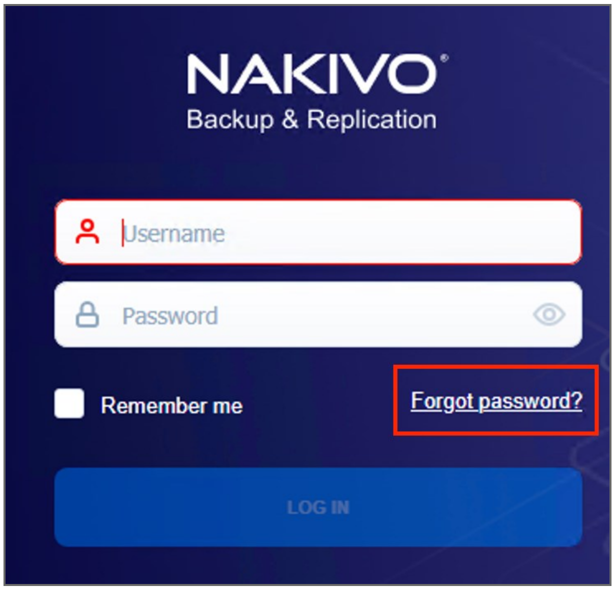
NAKIVO Backup & Replication opens in your browser displaying the configuration wizard. Refer to First Steps with NAKIVO Backup & Replication to learn how to start using NAKIVO Backup & Replication.

To log out, click **Logout** in the bottom left corner.

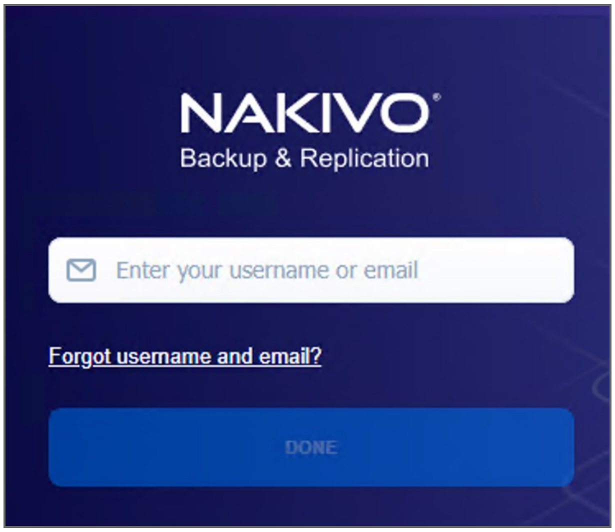
Changing Password

If you forget the password used to log in to NAKIVO Backup & Replication, you can restore it by following the steps below:

1. Go to NAKIVO Backup & Replication login page.
2. Click the **Forgot password** link.



3. Do one of the following:
   - If you have set up email settings in NAKIVO Backup & Replication, enter your email address and click **Done**.



A temporary password, which is a security string, is sent to your inbox. Enter this password the next time you log in to your NAKIVO Backup & Replication instance. Once you are logged in, it's recommended that you change the temporary password for your user account. To change the temporary password:

a. Click **Logout** in the bottom left corner.

b. Select **Profile**.

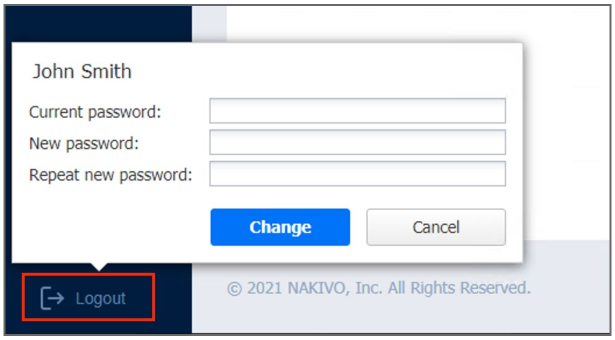
c. Click **Change password**.

d. In the dialog box that opens, fill out the following fields:

   - **Current password**: Enter the temporary password that you received to your inbox.
   - **New password**: Enter a new password.

- **Repeat new password**: Enter the new password again.

e. Click **Change**.



You can also change your temporary password in **Settings**>**General**>**Users and Roles**

- If you have not set up email settings in NAKIVO Backup & Replication:

  a. Enter your username and click **Done**.

  b. Go to the product installation folder and locate the “forgot_password.txt” file.

  Important

  For security reasons, only a root user (Linux) or a member of the Administrators group (Windows) is allowed to access the installation folder and the "forgot_password.txt" file.

  c. Paste the security string from the file in the appropriate field.

  d. Click **Done**.

  Notes

  - If you are using a Virtual Appliance (VA), go to the VA console, then go to the command line and enter: `cat /opt/nakivo/director/forgot_password.txt` The security string will be displayed on the screen. You can copy and paste it into the web interface.
  - If you are using a NAS, open an SSH connection to your device and read the forgot_password.txt file in the following folders:
    - For ASUSTOR NAS: `/usr/local/AppCentral/NBR`
    - For FreeNAS (inside the jail): `/usr/local/nakivo/director`
    - For NETGEAR NAS: `/apps/nbr`
    - For QNAP NAS: `/share/CACHEDEV1_DATA/.qpkg/NBR`
    - For Raspberry PI: `/opt/nakivo/director`
    - For Synology NAS: `/volume1/@appstore/NBR`
    - For Western Digital NAS: `/mnt/HD/HD_a2/Nas_Prog/NBR`
  - To learn how to open an `SSH` connection to your NAS device and read text files, refer to the NAS vendor documentation.

Default Password in Amazon EC2

If you have deployed NAKIVO Backup & Replication as an Amazon machine image in Amazon EC2, use the following default credentials to log in:

- **Username**: admin
- **Password**: The password is the ID of the NAKIVO Backup & Replication instance in Amazon EC2.

Passing Verification

If two-factor authentication was configured, verification needs to be passed after entering the credentials to access your NAKIVO Backup & Replication instance. This can be done in one of the following ways:

- Google Authenticator code from the mobile app
- A code sent to the specified email address
- One of the single-use backup codes

If Two-factor authentication was enabled but never configured, it must be configured now. Do the following:

1. Click **Continue**.
2. Optionally, click on the **change your email** link to enter the new email address for the user. Select **Continue** to proceed.
3. Enter the verification code that was sent to the specified email and click **Continue**. Optionally, click **Resend email** in case you did not receive it.
4. Optionally, enter the alternative email address that can be used in case the primary one becomes unavailable, and select **Continue**. Alternatively, select **Skip this step**.
5. If you have entered the alternative email address for the previous step, enter the verification code that was sent to the specified email, and click **Continue**. Optionally, click **Resend email** in case you did not receive it.
6. Follow instructions on screen to download and install Google Authenticator, and click **Continue**.
7. Add your NAKIVO Backup & Replication user account to Google Authenticator. Use one of the following methods:
   - Select **Scan QR Code** option and scan the QR code in the popup window.
   - Select **Enter a Code** option and follow the instructions to enter the shown code into the Google Authenticator app.
8. Enter the 6-digit verification code from Google Authenticator into the field. Note that the verification code is time-based. Click **Continue** to proceed.
9. A pairing key is displayed which can be used to add multiple devices to your account.

   Important

It is highly recommended that you save the pairing key or write it down.

You have the following options:

- Optionally, click on the **Copy the key** link to copy your key and save it for future use.
- Optionally, click on the **Download pairing information** link to download and save instructions on how to use the pairing key.
- Click **Continue** when you're done.

10. Four backup codes are displayed on the next page. These one-time codes can be used to log in when you are unable to provide a verification code. Click on the **Save as PDF** link to download and save these codes in PDF format or write them down. Click **Continue**.
11. Enter one of the backup codes in the next popup window to confirm that you have saved them, and click **Finish**.

Google Authenticator Verification

If you have selected the **Google Authenticator** verification method on the Managing Two-Factor Authentication page, do one of the following:

- Enter the verification code from Google Authenticator into the field, and click **Proceed**.
- Enter one of the one-time backup codes.
- Click **More verification options** to use email verification.

Email Verification

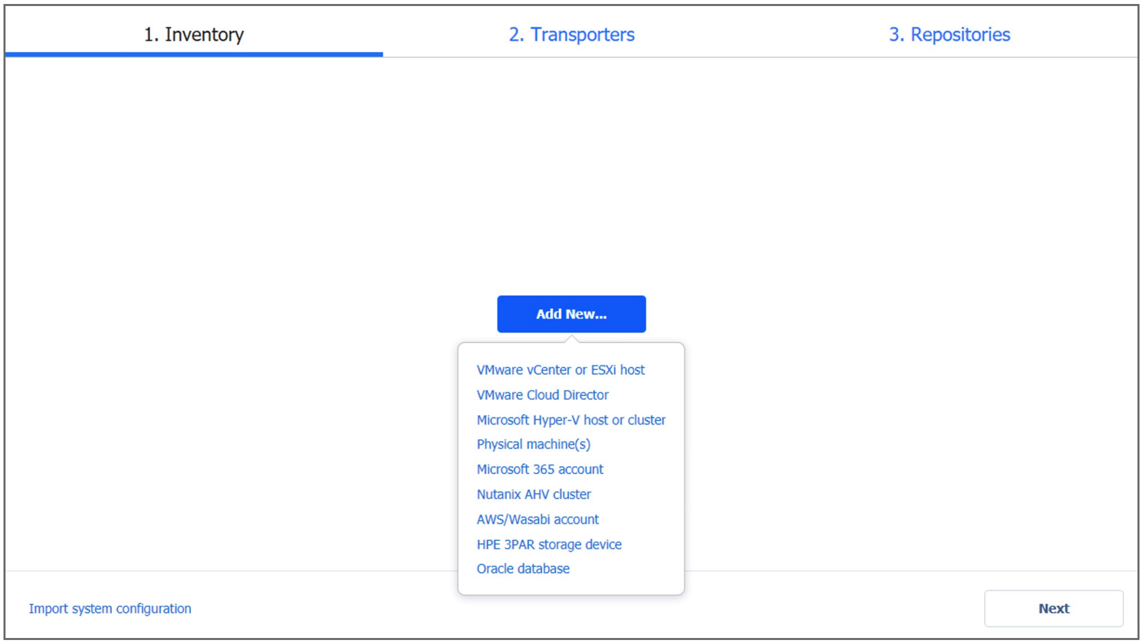
If you have selected the **Email** verification method on the Managing Two-Factor Authentication page, do one of the following:

- Select one of the email addresses verified previously, and click **SEND VERIFICATION CODE**. Then click **OK**.
- Enter one of the one-time backup codes.
- Alternatively, click **More verification options** to choose a different email for verification.

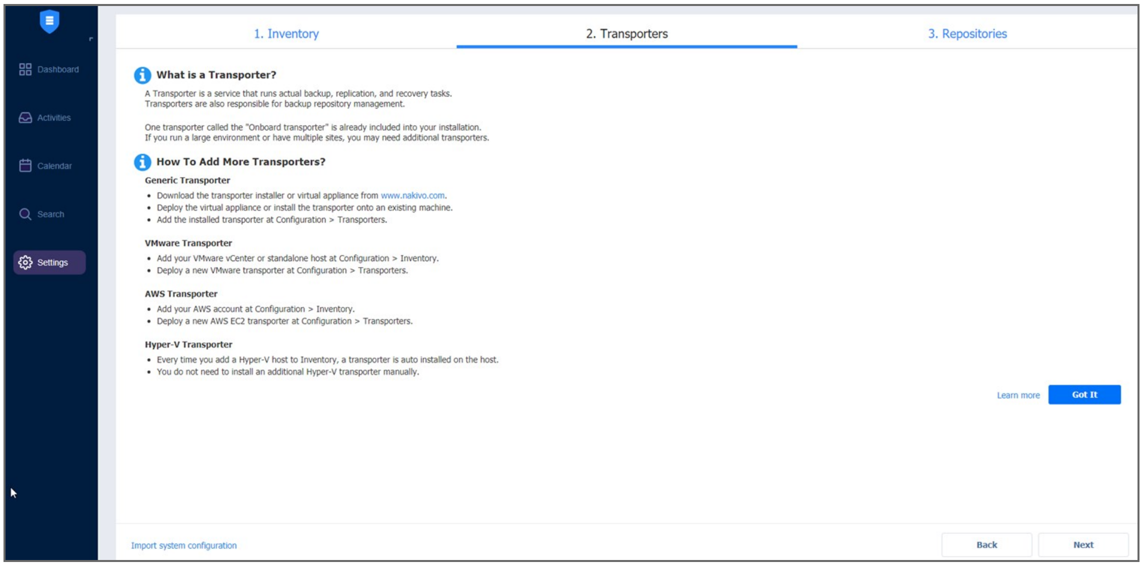
First Steps with NAKIVO Backup & Replication

When you log in to NAKIVO Backup & Replication for the first time, the initial configuration wizard opens. Proceed as follows:

1. On the **Inventory** page of the wizard, click **Add New**.
2. Select one of the options below:
   - VMware vCenter or ESXi host
   - VMware Cloud Director
   - Microsoft Hyper-V host or cluster
   - Physical machine(s)
   - Microsoft 365 account
   - Nutanix AHV cluster
   - AWS/Wasabi account
   - HPE 3PAR storage device
   - Oracle database



3. Proceed with adding items as described in the Inventory article.
4. On the **Transporters** page of the wizard, you will find information about the Transporter component of the NAKIVO Backup & Replication.
5. To deploy a new Transporter or add an existing one, click **Got it** and proceed as described in the Transporters article.
6. To move to the next page of the wizard, click **Next**.



What is a Transporter?

A Transporter is a service that runs actual backup, replication, and recovery tasks.
Transporters are also responsible for backup repository management.

One transporter called the "Onboard transporter" is already included into your installation.
If you run a large environment or have multiple sites, you may need additional transporters.

How To Add More Transporters?

Generic Transporter

- Download the transporter installer or virtual appliance from www.nakivo.com.
- Deploy the virtual appliance or install the transporter onto an existing machine.
- Add the installed transporter at Configuration > Transporters.

VMware Transporter

- Add your VMware vCenter or standalone host at Configuration > Inventory.
- Deploy a new VMware transporter at Configuration > Transporters.

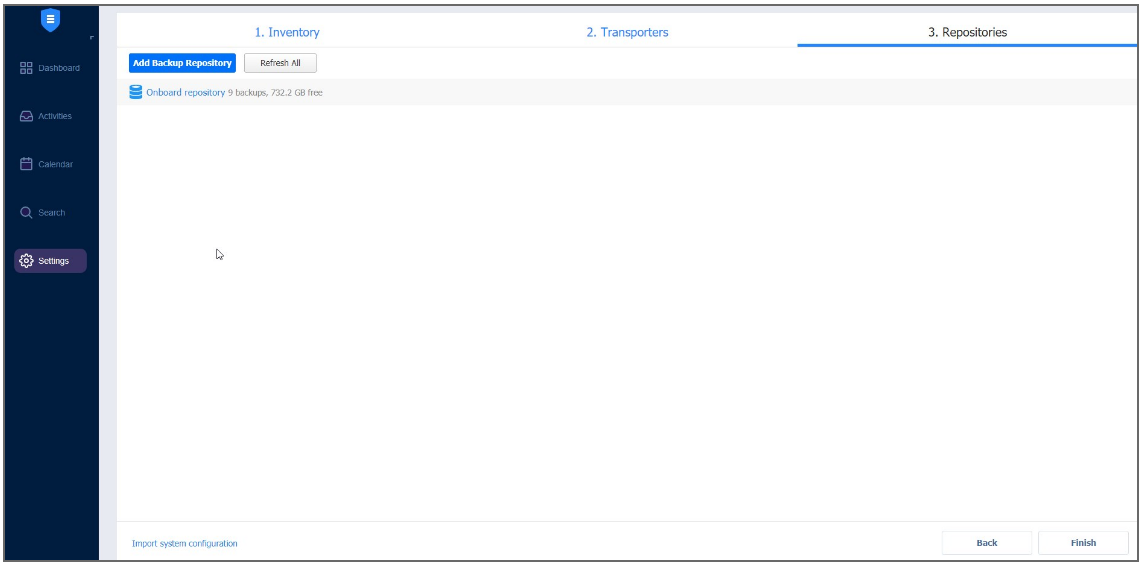
AWS Transporter

- Add your AWS account at Configuration > Inventory.
- Deploy a new AWS EC2 transporter at Configuration > Transporters.

Hyper-V Transporter

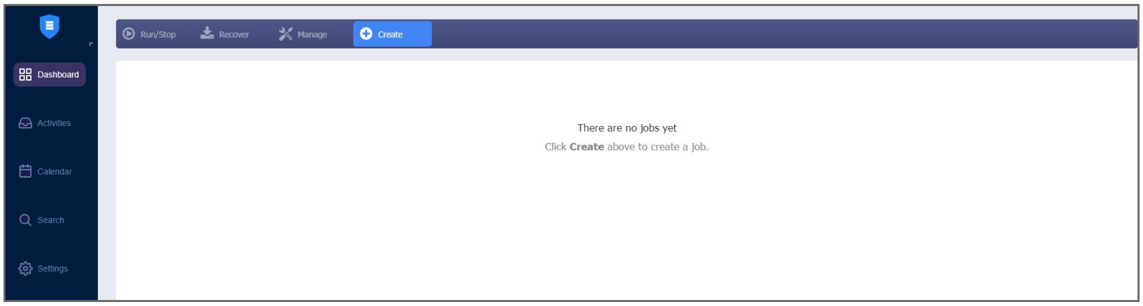
- Every time you add a Hyper-V host to Inventory, a transporter is auto installed on the host.
- You do not need to install an additional Hyper-V transporter manually.

7. On the **Repositories** page of the wizard, you can add a local or a remote Backup Repository to your application by clicking **Add Backup Repository**.



Onboard repository 9 backups, 732.2 GB free

8. Click **Finish**.
9. The **Dashboard** of the application opens. Proceed with creating your backup jobs.



There are no jobs yet
Click **Create** above to create a job.

If your current license type is **Free** and the **Trial** license has not yet been applied to the current deployment of NAKIVO Backup & Replication, a dialog box appears. Using this dialog box, you can contact the sales team to change your license type or try the full functionality of the solution for 15 days. If you do not want to upgrade your license type right away, you can do it at any time in the Help menu.

Note

If you switch the license type to **Trial**, the product will automatically go back to using your **Free** license after expiration.

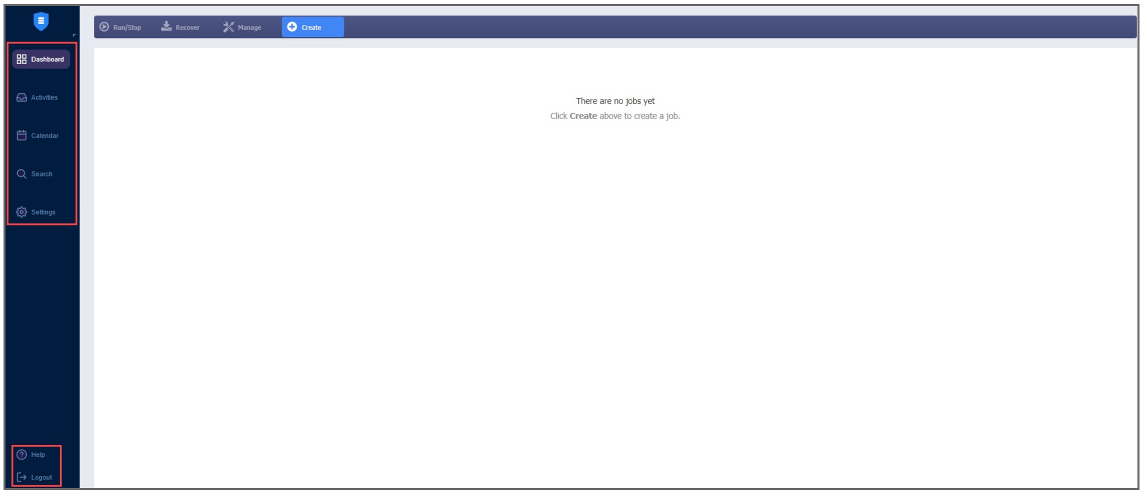
Web Interface Components

The interface of NAKIVO Backup & Replication consists of the following components:

- Main Menu
- Dashboard
- Activities
- Calendar
- Search
- Settings
- Help Menu
- Online Chat Dialog
- Special Offers Toolbar
- Tenants Dashboard

Main Menu

The main menu of NAKIVO Backup & Replication is located on the left side of the product interface. It provides access to the jobs dashboard, activities, calendar, global search, and product settings. It also contains the **Help** menu and **Log Out** button.



There are no jobs yet

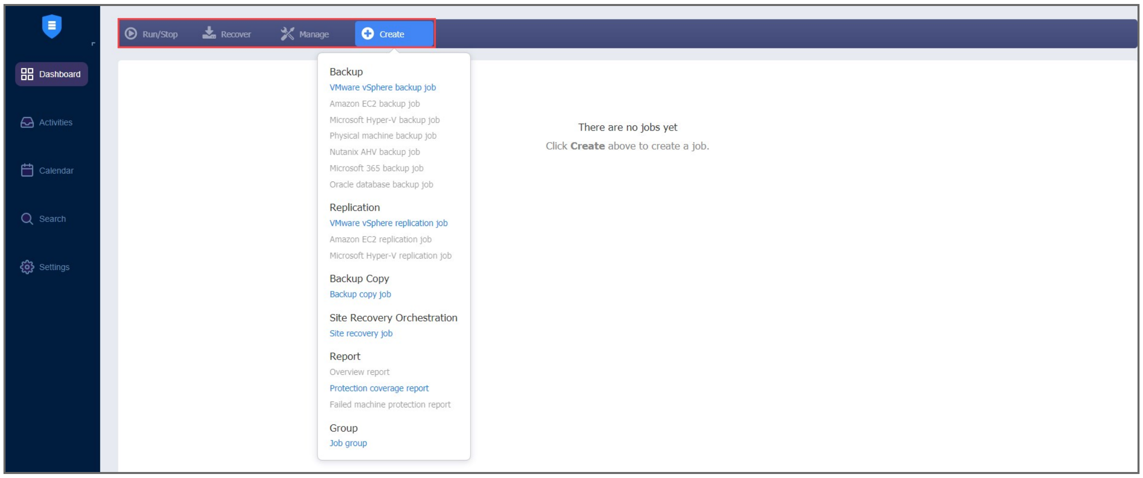
Click **Create** above to create a job.

Dashboard

Using the **Dashboard**, you can:

- View, run, and stop jobs on demand
- Recover files, objects and entire sites
- Manage jobs
- Create backup jobs

- Create and manage job groups


Dashboard
Activities
Calendar
Search
Settings
Run/Stop
Recover
Manage
Create
Backup
VMware vSphere backup job
Amazon EC2 backup job
Microsoft Hyper-V backup job
Physical machine backup job
Nutanix AHV backup job
Microsoft 365 backup job
Oracle database backup job
Replication
VMware vSphere replication job
Amazon EC2 replication job
Microsoft Hyper-V replication job
Backup Copy
Backup copy job
Site Recovery Orchestration
Site recovery job
Report
Overview report
Protection coverage report
Failed machine protection report
Group
Job group

There are no jobs yet

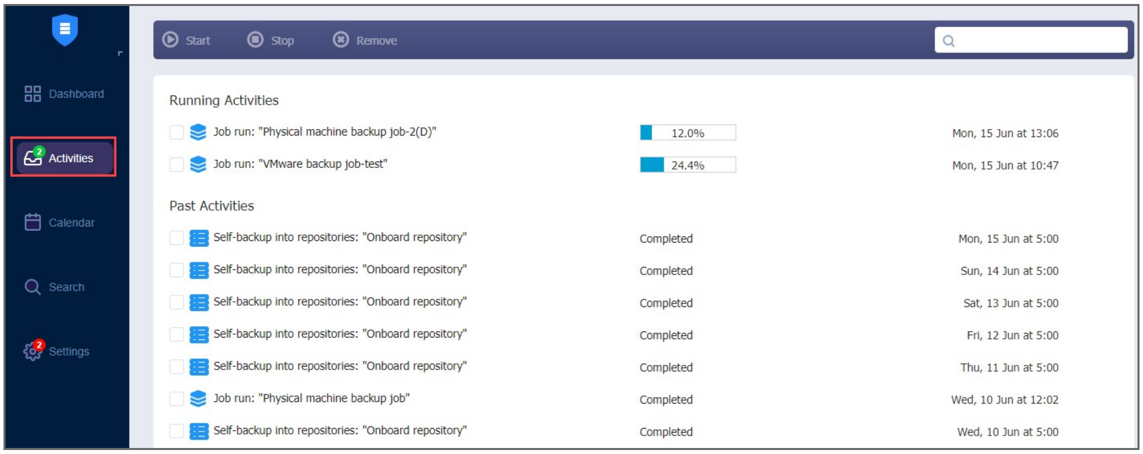
Click **Create** above to create a job.

Activities

The **Activities** page displays a list of all running and past activities, such as:

- Job run
- Repository Self-Backup
- Other

For further details and information, refer to “Managing Activities” on page 48 .



Running Activities

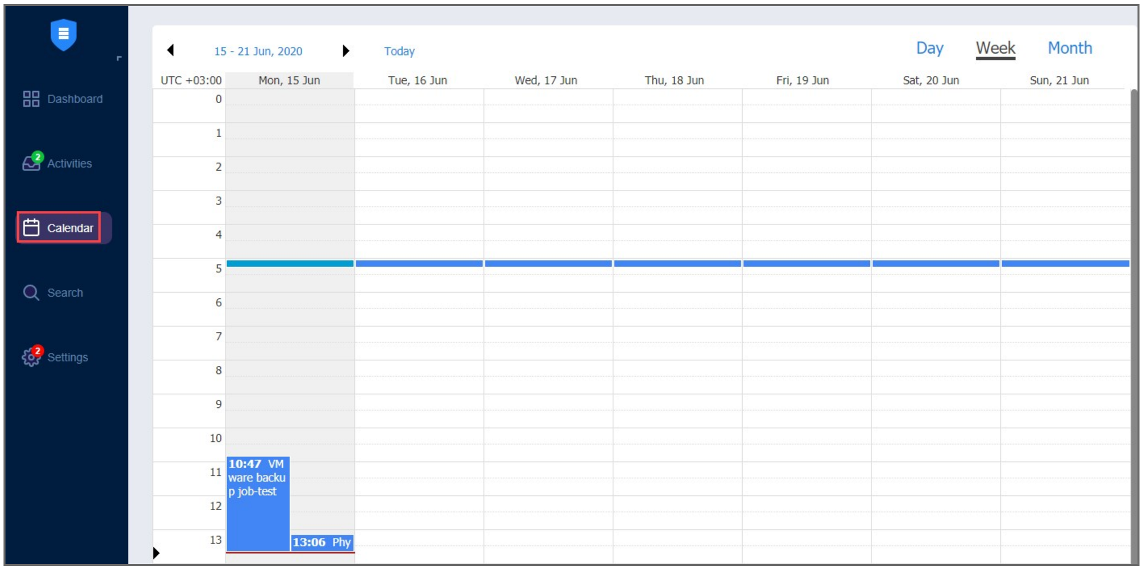
Job run: "Physical machine backup job-2(D)"	12.0%	Mon, 15 Jun at 13:06
Job run: "VMware backup job-test"	24.4%	Mon, 15 Jun at 10:47

Past Activities

Self-backup into repositories: "Onboard repository"	Completed	Mon, 15 Jun at 5:00
Self-backup into repositories: "Onboard repository"	Completed	Sun, 14 Jun at 5:00
Self-backup into repositories: "Onboard repository"	Completed	Sat, 13 Jun at 5:00
Self-backup into repositories: "Onboard repository"	Completed	Fri, 12 Jun at 5:00
Self-backup into repositories: "Onboard repository"	Completed	Thu, 11 Jun at 5:00
Job run: "Physical machine backup job"	Completed	Wed, 10 Jun at 12:02
Self-backup into repositories: "Onboard repository"	Completed	Wed, 10 Jun at 5:00

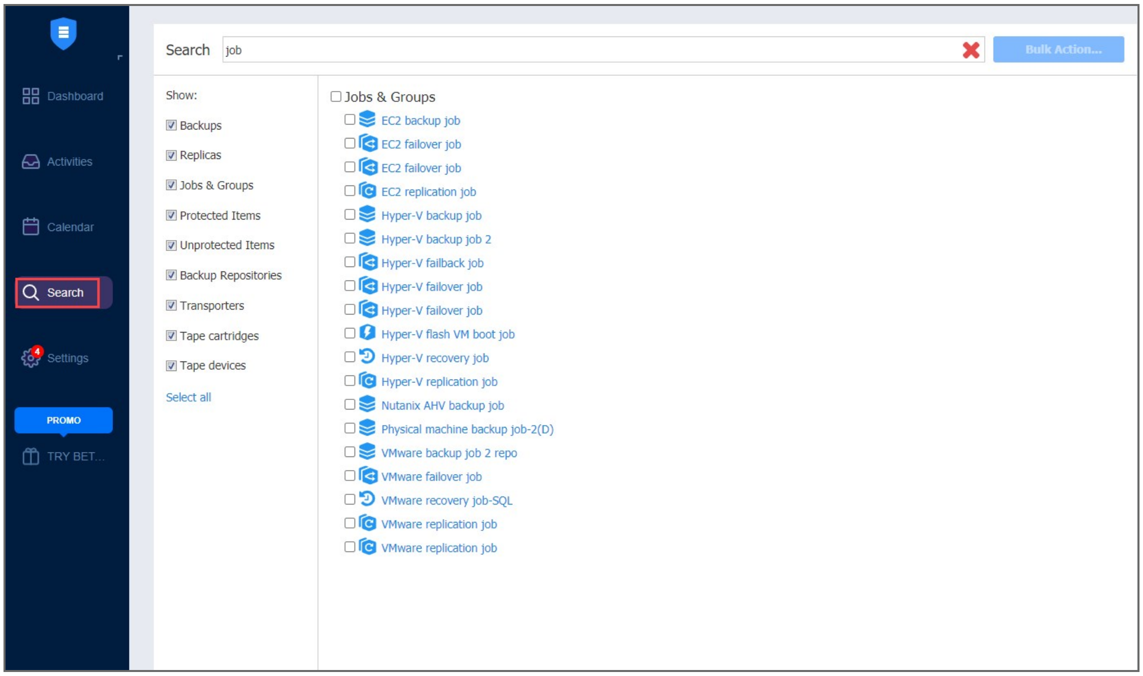
Calendar

The **Calendar** allows you to schedule jobs and to view the history of all job runs right from the calendar. For more information, refer to “Using Calendar” on page 52.



Search

The **Search** page allows you to search for items within the entire N AKIVO Backup & Replication – in the inventory, Transporters, Backup Repositories, tape devices, jobs, backups, replicas, and other. For more details, refer to “Using Global Search” on page 53.



Search job

Show:

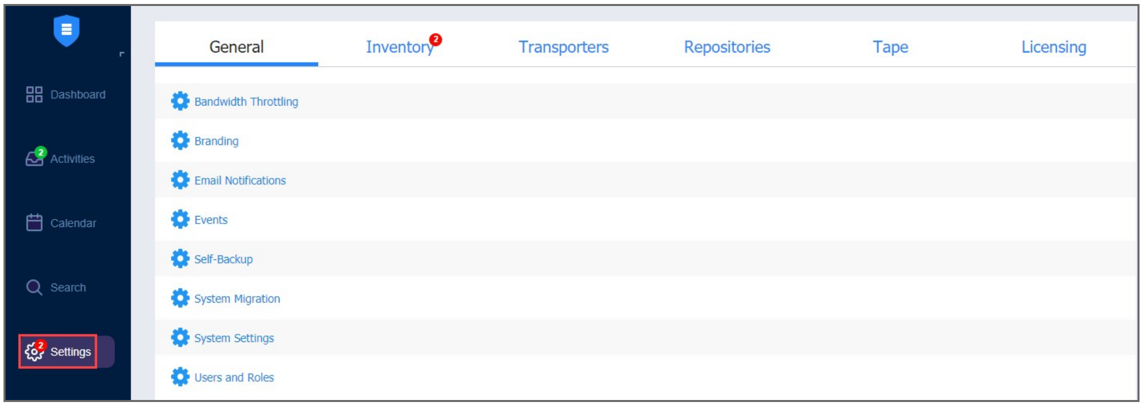
☑ Backups
☑ Replicas
☑ Jobs & Groups
☑ Protected Items
☑ Unprotected Items
☑ Backup Repositories
☑ Transporters
☑ Tape cartridges
☑ Tape devices

□ Jobs & Groups

- □ EC2 backup job
- □ EC2 failover job
- □ EC2 failover job
- □ EC2 replication job
- □ Hyper-V backup job
- □ Hyper-V backup job 2
- □ Hyper-V failback job
- □ Hyper-V failover job
- □ Hyper-V failover job
- □ Hyper-V flash VM boot job
- □ Hyper-V recovery job
- □ Hyper-V replication job
- □ Nutanix AHV backup job
- □ Physical machine backup job-2(D)
- □ VMware backup job 2 repo
- □ VMware failover job
- □ VMware recovery job-SQL
- □ VMware replication job
- □ VMware replication job

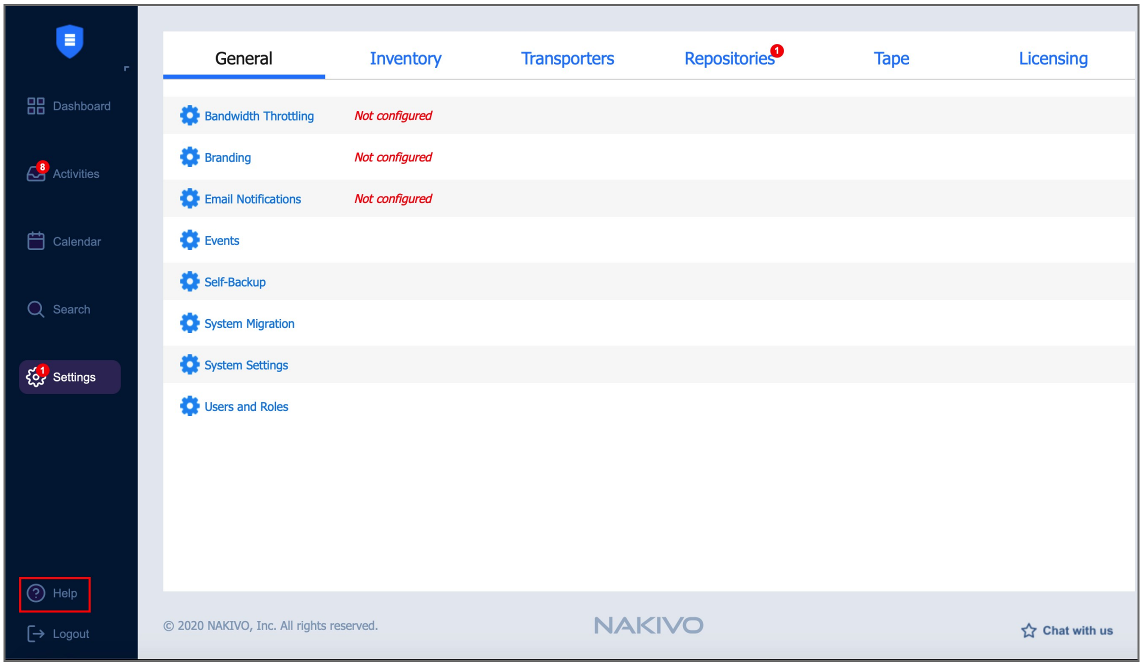
Settings

On the **Settings** page, you can configure NAKIVO Backup & Replication general settings, inventory, Transporters, Backup Repositories, and licensing. Refer to “Settings” on page 190 for more details.



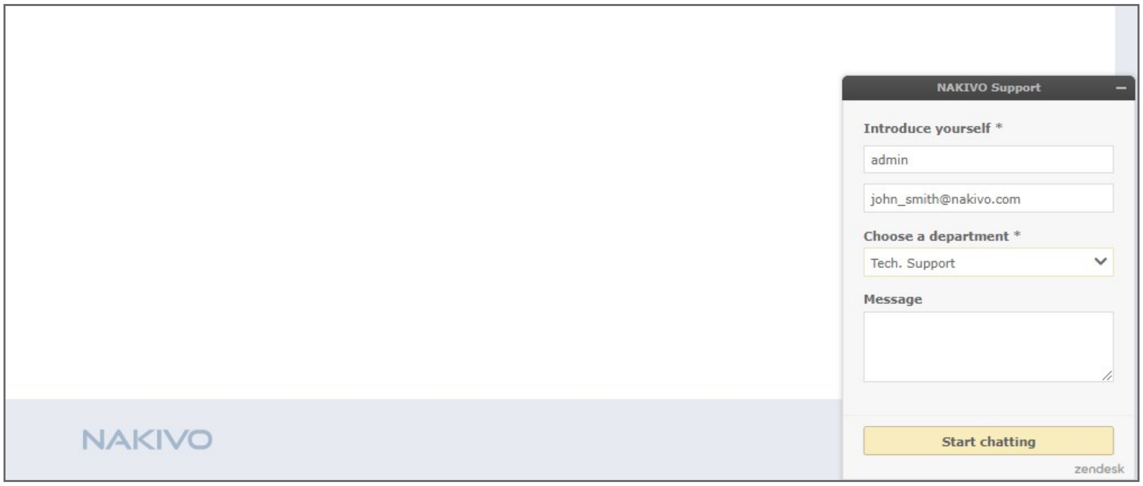
Help Menu

Use the **Help** menu to request technical support and access the NAKIVO online help center. If you are evaluating NAKIVO Backup & Replication, you can use the **How to Buy** section of the **Help** menu to view pricing, upgrade your Free license to Trial for 15 days with the **Try full functionality** option, and request a live demo or a quote.



Online Chat Dialog

The **NAKIVO Support** online chat is located in the right bottom corner of the application. It enables you to quickly request help from a sales or technical support representative.



Introduce yourself *

admin

john_smith@nakivo.com

Choose a department *

Tech. Support

Message

Special Offers Toolbar

This element of the interface is located to the left of the NAKIVO Backup & Replication dashboard. The toolbar contains special offers. If you click the button, a dialog opens displaying information about a specific offer. If needed, the **Special Offers** toolbar can be disabled. Refer to “System Settings” on page 205 for details.

Tenants Dashboard

If you use NAKIVO Backup & Replication in a multi-tenant mode, the **Tenants** dashboard allows you to create, manage, and configure tenants.

Managing Jobs and Activities

Using NAKIVO Backup & Replication interface, you can manage jobs and tasks. This section covers the following topics:

- "Running Jobs on Demand" on page 37
- "Managing Jobs" on page 39
- "Jobs Alarms and Notifications" on page 46
- "Managing Activities" on page 48
- "Using Calendar" on page 52
- "Using Global Search" on page 53

Running Jobs on Demand

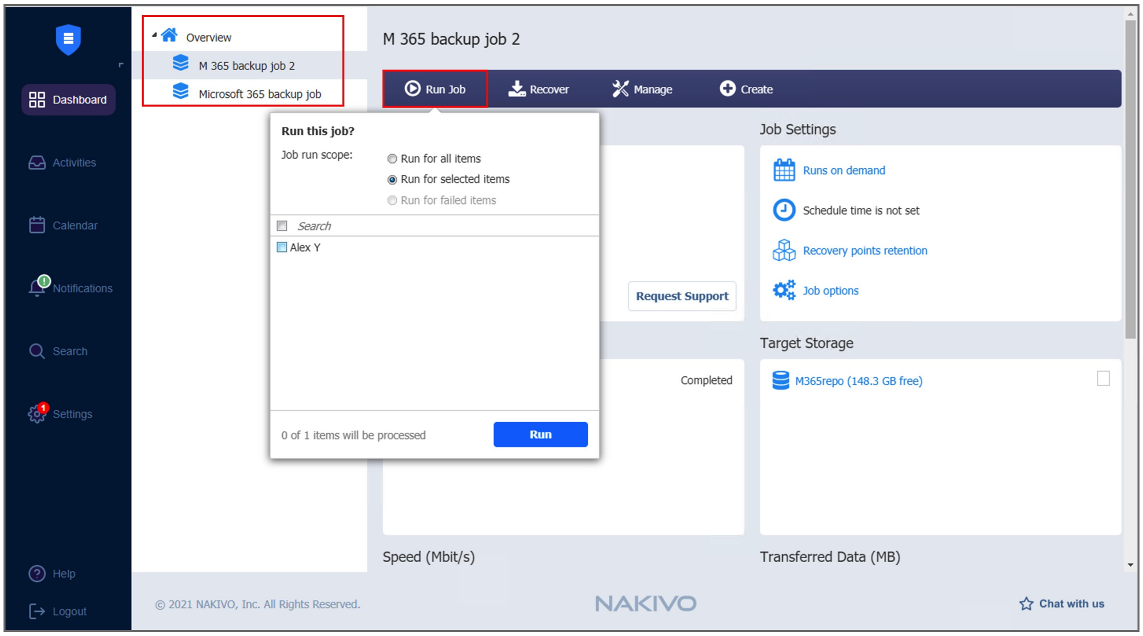
Use the **Dashboard** to start and stop jobs on demand.

- Starting Jobs
- Stopping Jobs

Starting Jobs

To start a job, follow the steps below:

1. Go to the **Dashboard**, select the job from the list of jobs, and click **Run Job.**
2. Choose one of the following options:
   - **Run for all items**: The job will run for all items.
   - **Run for selected items**: The job will run for the items you select.
   - **Run for failed items**: The job will run for previously failed items only.
3. In the dialog that opens, define the scope of your job:
4. Click the **Run** button to confirm your operation.



Run this job?

Job run scope:
○ Run for all items
● Run for selected items
○ Run for failed items

□ Search
□ Alex Y

0 of 1 items will be processed

Run

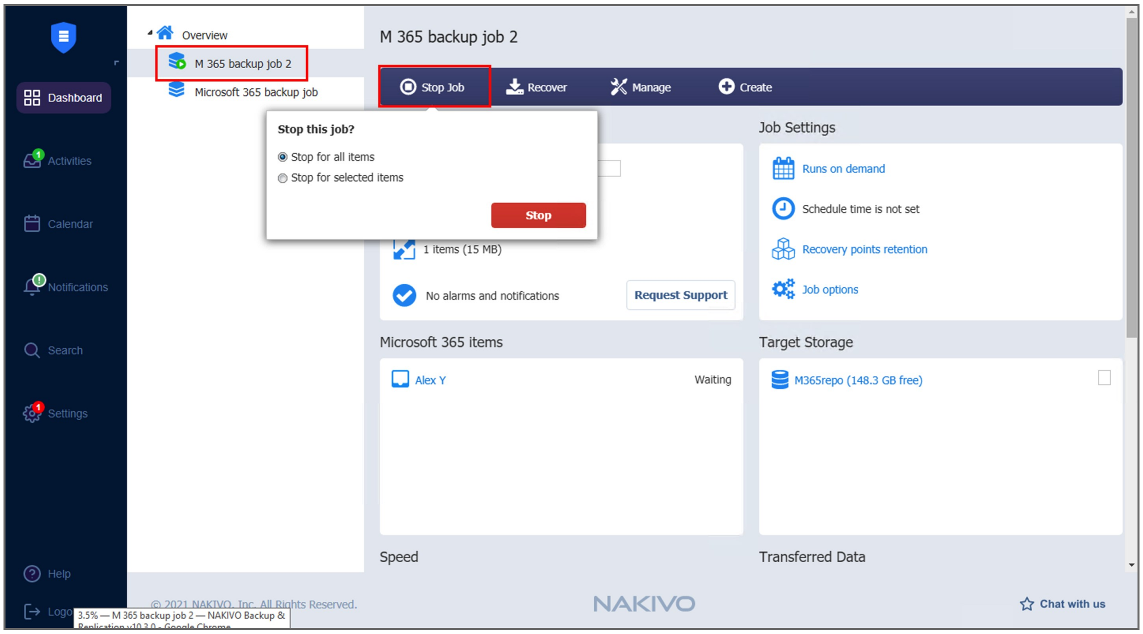
The product will close the dialog box and start running your job.

Stopping Jobs

To stop a job that is currently running, follow the steps below:

1. Go to the **Dashboard**, select the job from the list of jobs, and click **Stop Job**.
2. In the dialog that opens, choose either of the following:
   - **Stop for all items**: Your job will stop for all items.
   - **Stop for selected items**: Your job will stop for the items you select.

3. Click the **Stop** button in the dialog to confirm your operation.



The product will close the dialog box and stop your job.

Managing Jobs

Using the **Dashboard**, you can easily manage your jobs. Go to the **Manage** menu to rename, edit, delete and enable/disable jobs.

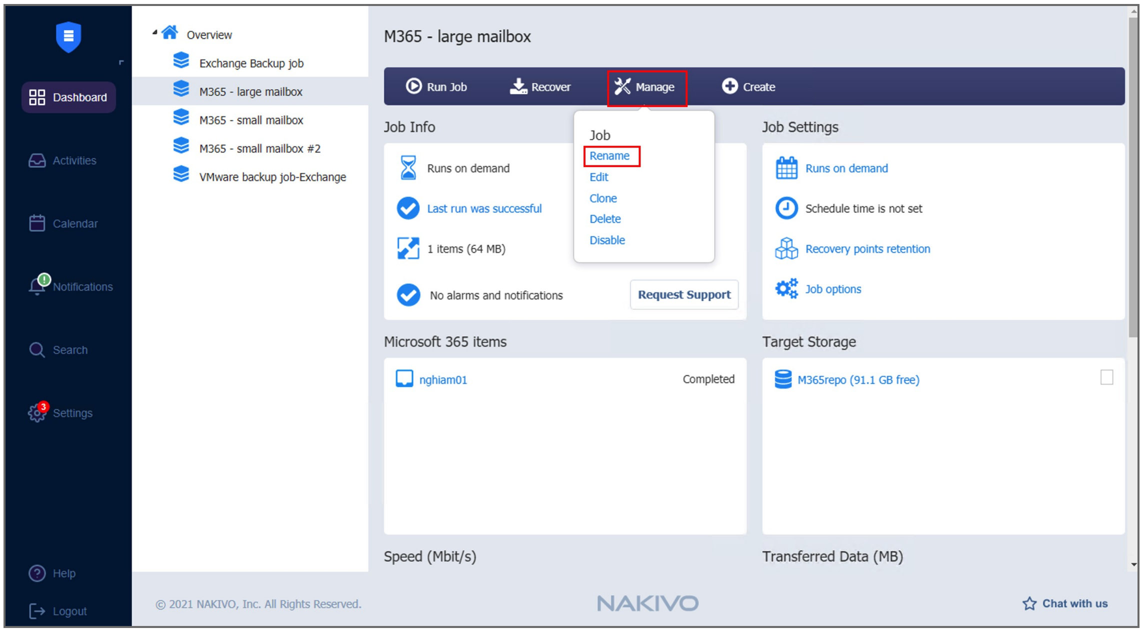
- Renaming Jobs
- Editing Jobs
- Cloning Jobs
- Deleting Jobs
- Disabling and Enabling Jobs
- Grouping Jobs
    - Creating Groups
- Creating Job Reports

Renaming Jobs

1. From the list of jobs, select the job you wish to rename.
2. On the **Dashboard**, click **Manage**.
3. Click **Rename**.
4. In the dialog box that opens, specify the new name for the job.
5. Click **Rename**.

   Note

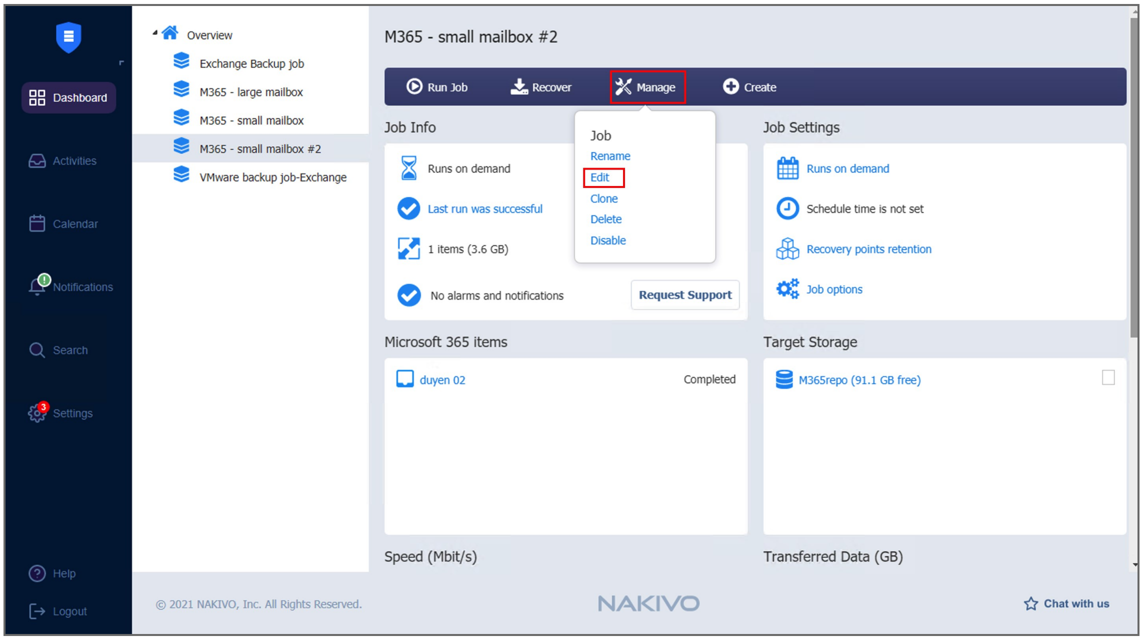
   You can also rename jobs by right-clicking on a job and selecting **Rename** from the **Manage Job** menu.



Editing Jobs

To edit a job, follow the steps below:

1. Select the job you wish to edit from the list of jobs.
2. On the **Dashboard**, click **Manage**.
3. Click **Edit**.



4. In the **Edit** wizard, click the necessary page to open it for editing.
5. Make the required changes and then click **Save** or **Save & Run**.

Notes

- You can edit the job while it is running, but the changes will be applied only when the job run has completed.
- You can also edit jobs by right-clicking on a job and selecting **Edit** from the **Manage Job** menu.

Cloning Jobs

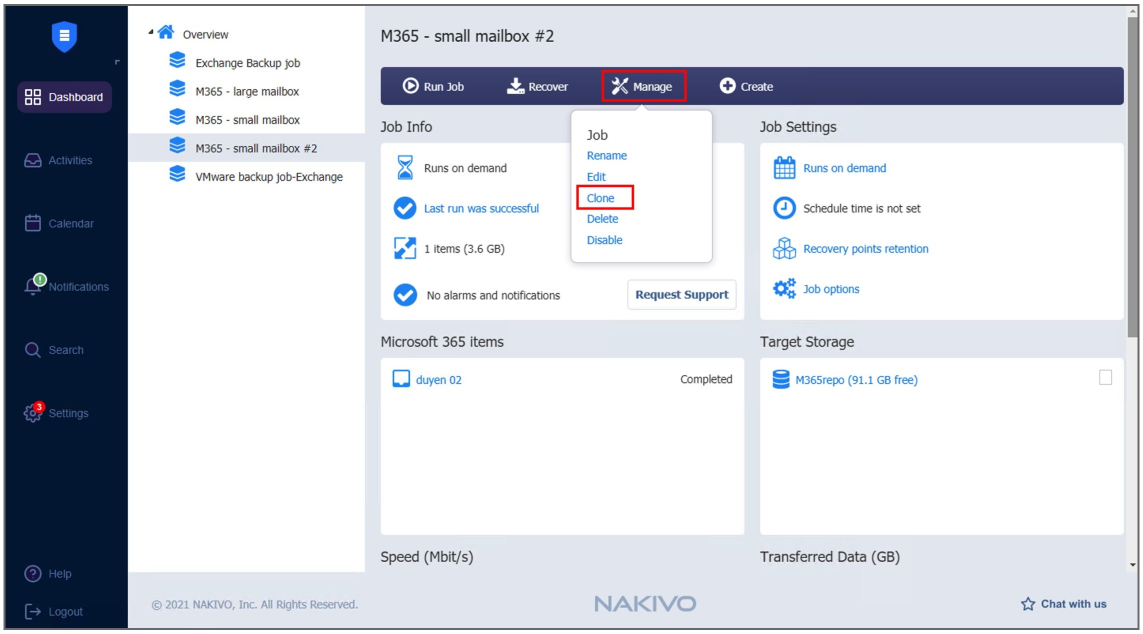
To clone a job, follow the steps below:

1. Select the job you would like to clone from the list of jobs.
2. On the **Dashboard**, click **Manage**.
3. Click **Clone**.

   Notes

   - You can also clone jobs by right-clicking on a job and selecting **Clone** from the **Manage Job** menu.
   - If the original job is using an existing backup or replica as a target, it will be reset for the cloned

job.



Deleting Jobs

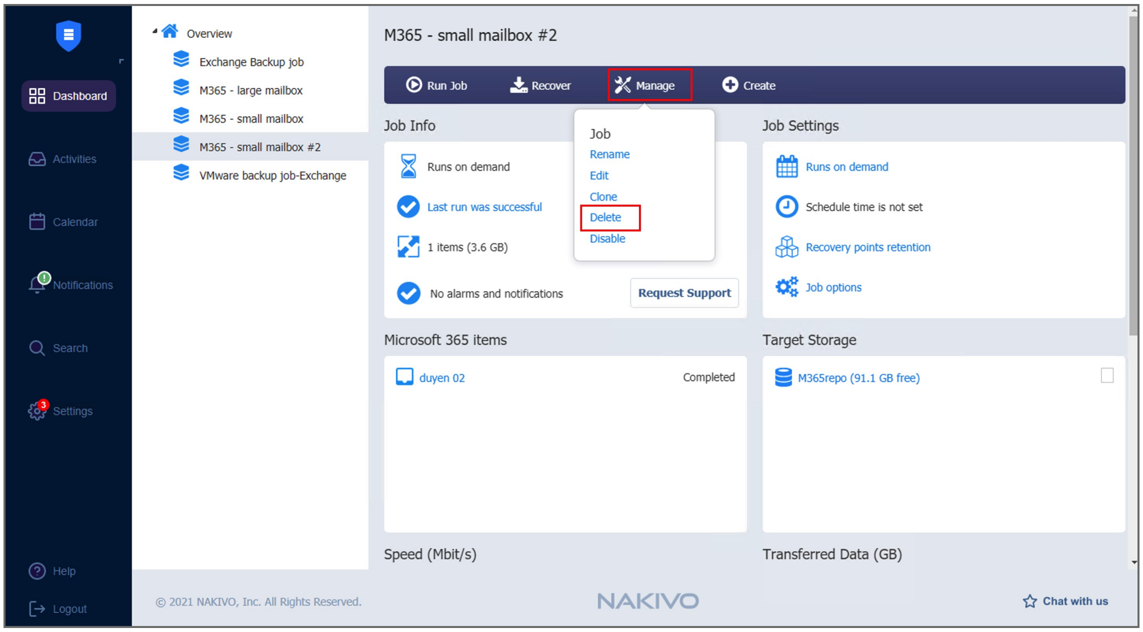
To delete a job follow the steps below:

1. Select the job you want to delete from the list of jobs.
2. On the **Dashboard**, click **Manage**.
3. Click **Delete**.
4. From the dialog box that opens, select one of the following:
   - **Delete job and keep backups**
   - **Delete job and keep backups**
5. Click **Delete**

   Notes

   - You can also delete jobs by right-clicking on a job and selecting **Delete** from the **Manage Job** menu.

- Backups can also be deleted from Backup Repositories.

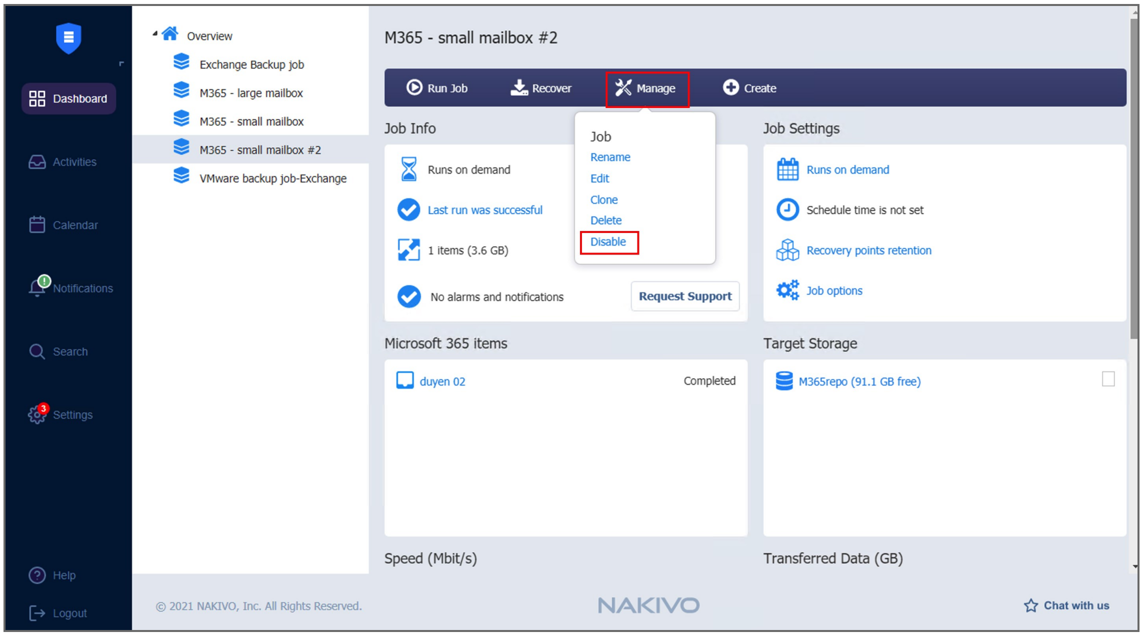


Disabling and Enabling Jobs

NAKIVO Backup & Replication provides you with the ability to disable jobs. A disabled job does not run on a schedule, nor can it be run on demand.

To disable a job, follow the steps below

1. From the list of jobs, select the job you want to disable.
2. On the **Dashboard**, click **Manage**.
3. Click **Disable**.



To enable a job, select **Enable** from the **Manage** menu.

Note

You can also disable/enable jobs by right-clicking on a job and selecting **Disable/Enable** from the **Manage Job** menu.

Grouping Jobs

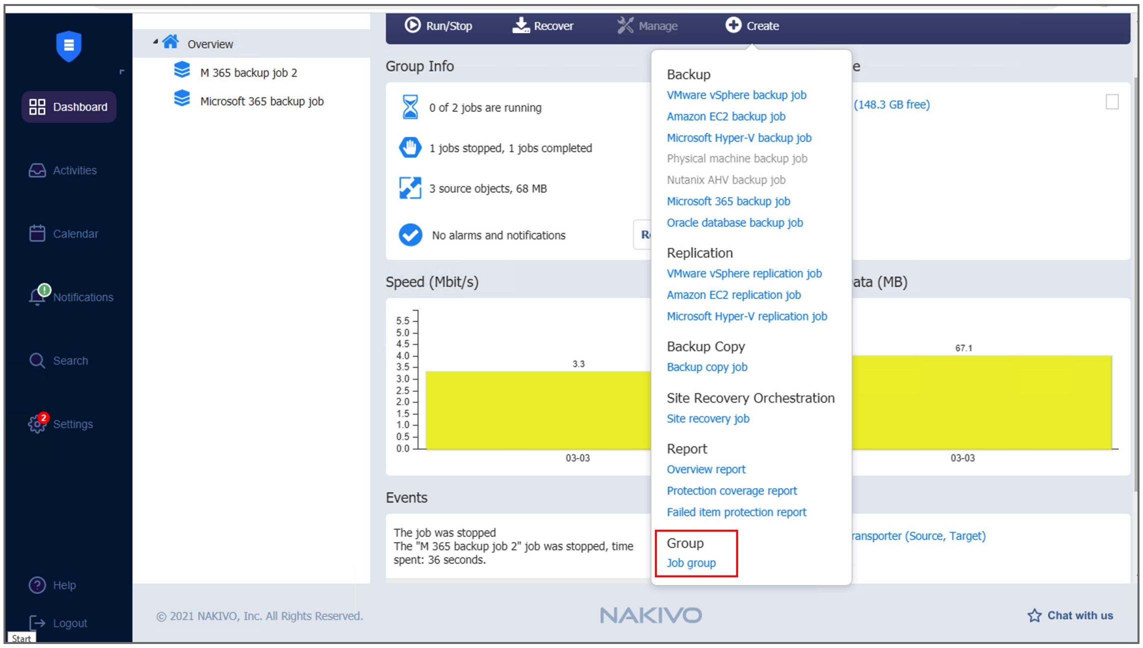
Groups are folders which allow you to:

- Logically arrange jobs (to represent organizations, locations, services, etc.).
- Perform bulk actions with all or selected jobs in a group.

Creating Groups

To create a group, follow the steps below:

1. On the **Dashboard**, click **Create** and then click **Job group**.
2. Type in the group name in the dialog box that appears and click **OK**.



0 of 2 jobs are running

1 jobs stopped, 1 jobs completed

3 source objects, 68 MB

No alarms and notifications

The job was stopped
The "M 365 backup job 2" job was stopped, time spent: 36 seconds.

© 2021 NAKIVO, Inc. All Rights Reserved.

The following actions are available to manage groups:

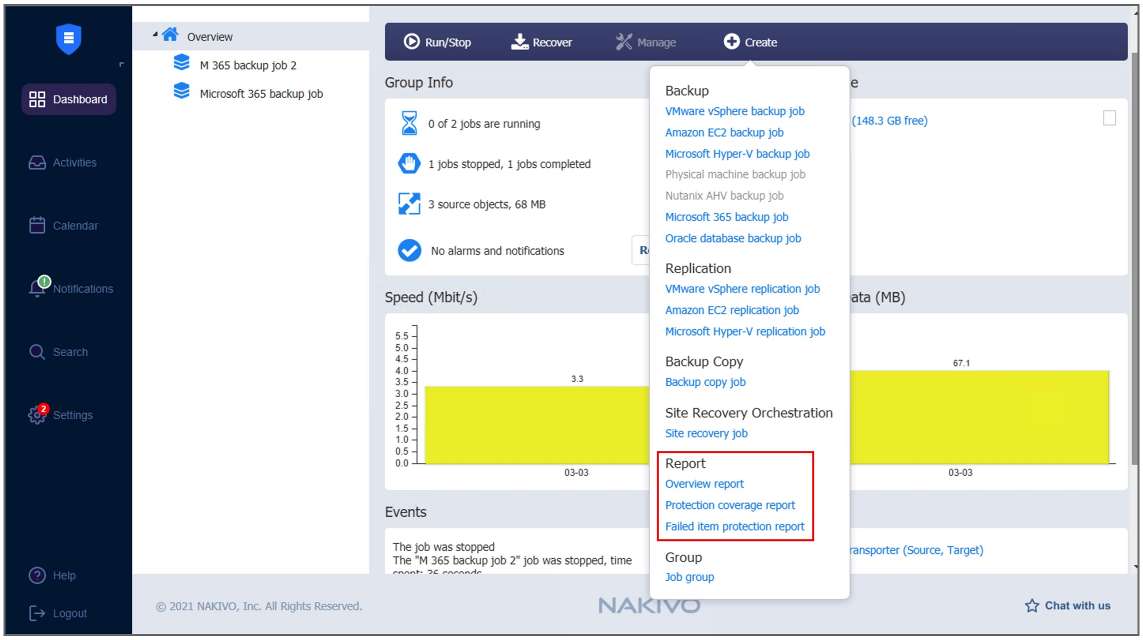
- To add a job to a group, simply drag the job into the group.
- To remove a job from the group, drag the job outside the group.
- To delete a group, right-click the group and choose **Delete** from the shortcut menu that appears. Confirm the group deletion when prompted to do so. Note that when deleting a group, its jobs are not deleted and are moved to the parent group (or Overview).
- To rename a group, double-click the group and enter a new name.
- To enable or disable all jobs inside a group, click the **Enable/Disable** switch.
- To run jobs available in a group, click **Run/Stop** and then click **Run** Jobs. In the dialog box that appears, select the jobs you wish to run and click **Run Jobs**.

- To stop running the jobs available in a group, click **Run/Stop** and then click **Stop Jobs**. In the dialog box that appears, select the jobs you would like to stop and click **Stop Jobs**.

Creating Job Reports

To create a general report for all your jobs:

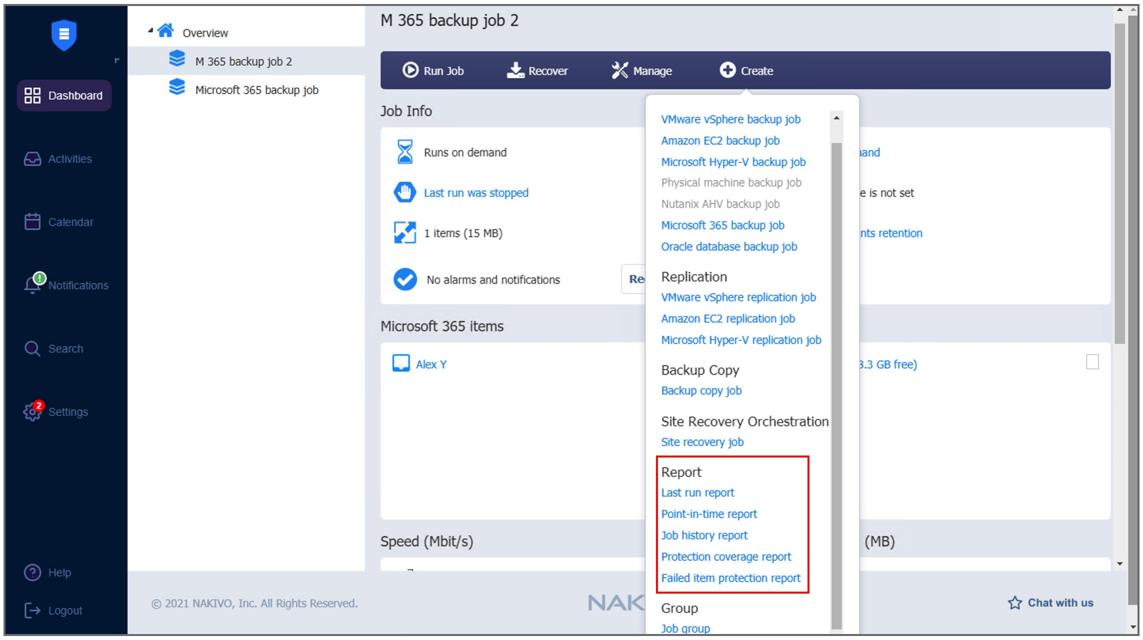
1. Select **Overview** on the **Dashboard**.
2. Click **Create**.
3. Choose one of the following reports in the **Report** section:
   - **Overview report**: Contains information about the status and errors of all your jobs.
   - **Protection coverage report**: Contains information about all VMs and instances protected by backup and/or replication jobs, as well as about all unprotected VMs and instances. Choose either PDF or CSV formats for your **Protection coverage report** and click **Create**.
   - **Failed machine protection report**: Contains information about all VMs and instances which had failed to be protected by backup and/or replication jobs, and the error message. Select the date range for your **Failed machine protection report** and click **Create**.
4. Choose a location to save the report and click **Save**.



To generate reports from for an individual job, do the following:

1. Go to the list of jobs.
2. Select the job that you need to generate a report for and right-click on it or click **Create**.
3. Select one of the following reports from the **Create report** menu:
   - **Last-run report**: Provides data on the last run of the job.
   - **Point-in-time Report**: Provides data on a particular job run. To generate a report, pick a date in the popup that appears and click **Create.**

- **Job history report**: Provides data on job runs that occurred during a specified time period. To generate a report, pick a start date on the left and finish date on the right in the popup that appears and click **Create**.
- **Protection coverage report**:Contains information about all VMs and instances protected by backup and/or replication jobs, as well as about all unprotected VMs and instances.
- **Failed machine protection report**: Contains information about job objects processing of which were failed during the last job run. Only backup and replication jobs included.
- **Site Recovery Job report**: Contains a summary of the Site Recovery Job, including the result of passing the Recovery time objective value, information about all actions performed, and all registered alarms and notifications.



Jobs Alarms and Notifications

NAKIVO Backup & Replication displays:

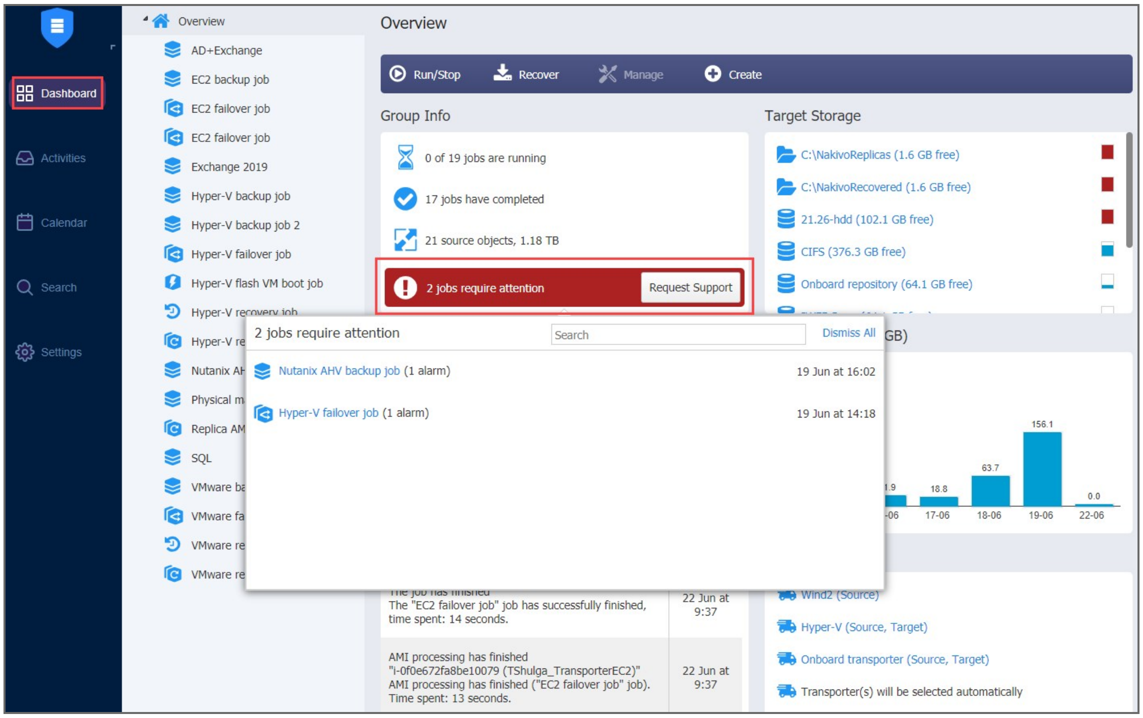
- **Alarms:** Job failures
- **Notifications**: Infrastructure changes and minor errors that do not lead to processing failure

For details, refer to the following sections:

- Viewing Alarms and Notifications
- Dismissing Alarms and Notifications

Viewing Alarms and Notifications

To view alarms and notifications, click the red box in the Job info widget.



0 of 19 jobs are running

17 jobs have completed

21 source objects, 1.18 TB

2 jobs require attention

C:\NakivoReplicas (1.6 GB free)

C:\NakivoRecovered (1.6 GB free)

21.26-hdd (102.1 GB free)

CIFS (376.3 GB free)

Onboard repository (64.1 GB free)

2 jobs require attention

Nutanix AHV backup job (1 alarm)	19 Jun at 16:02
Hyper-V failover job (1 alarm)	19 Jun at 14:18

The job has finished The "EC2 failover job" job has successfully finished, time spent: 14 seconds.	22 Jun at 9:37
AMI processing has finished "i-0f0e672fa8be10079 (TShulga_TransporterEC2)" AMI processing has finished ("EC2 failover job" job). Time spent: 13 seconds.	22 Jun at 9:37

Wind2 (Source)

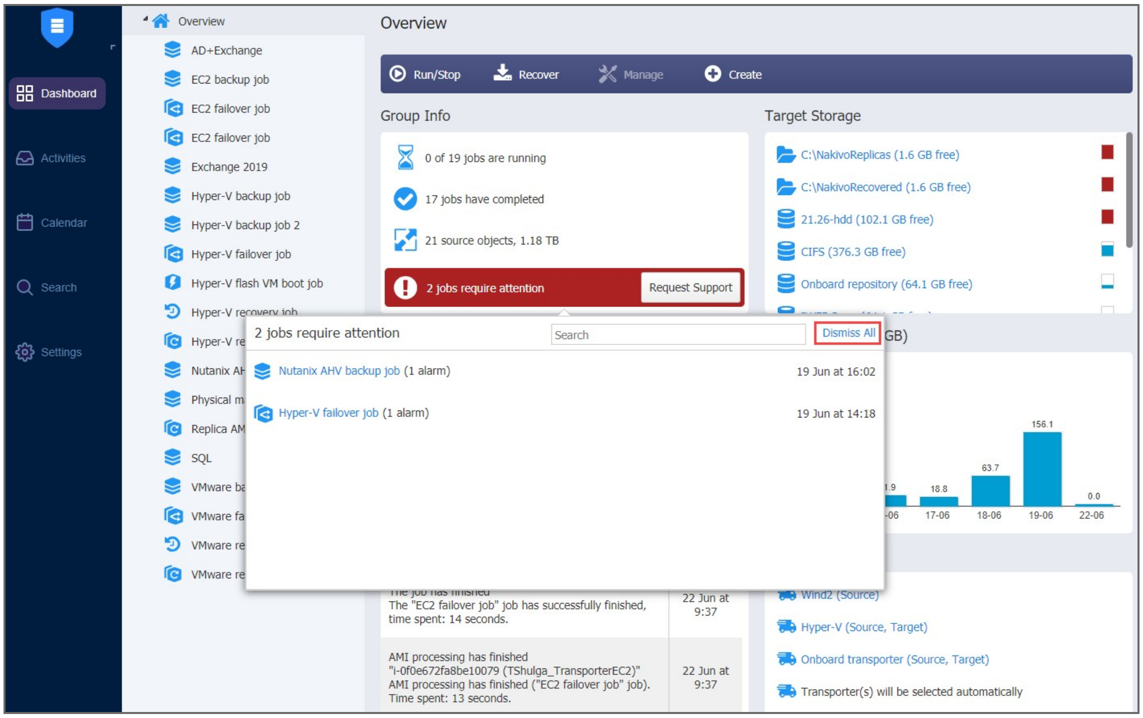
Hyper-V (Source, Target)

Onboard transporter (Source, Target)

Transporter(s) will be selected automatically

Dismissing Alarms and Notifications

To dismiss all alarms and notifications in a job, click **Dismiss All**. To dismiss an individual alarm or notification, hover the mouse pointer over the alarm or notification and click **Dismiss**.



Nutanix AHV backup job (1 alarm) 19 Jun at 16:02

Hyper-V failover job (1 alarm) 19 Jun at 14:18

The job has finished The "EC2 failover job" job has successfully finished, time spent: 14 seconds.	22 Jun at 9:37
AMI processing has finished "i-0f0e672fa8be10079 (TShulga_TransporterEC2)" AMI processing has finished ("EC2 failover job" job). Time spent: 13 seconds.	22 Jun at 9:37

Managing Activities

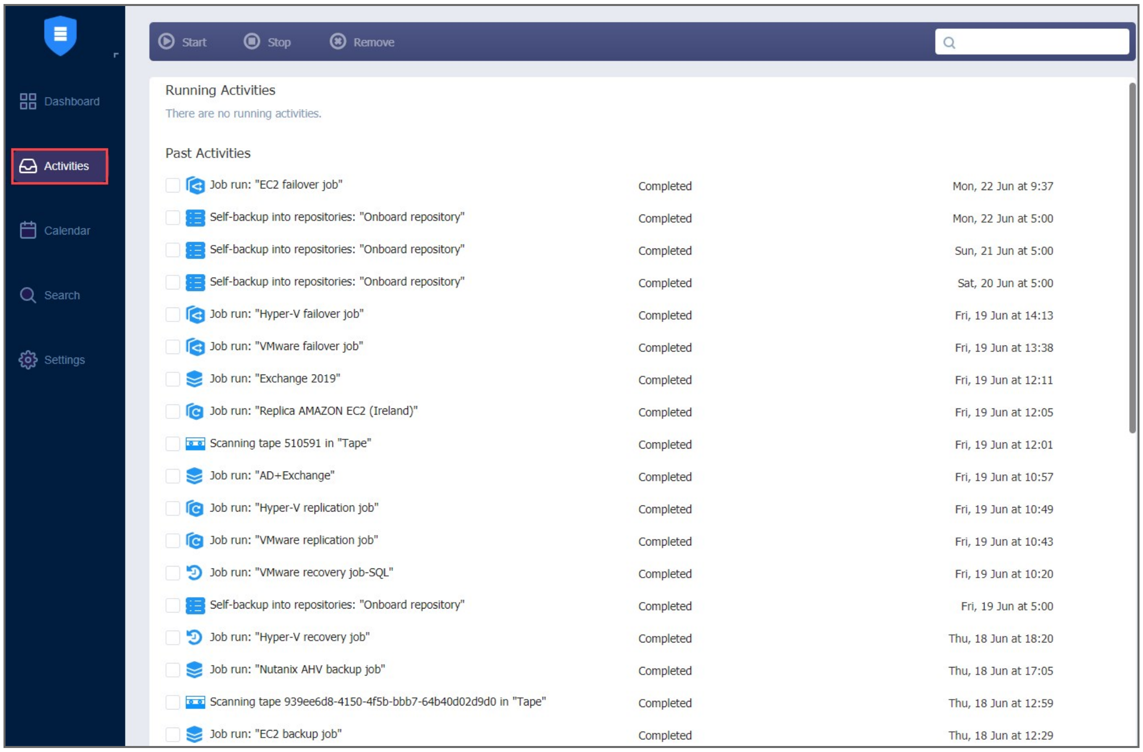
The **Activities** page displays current and past tasks performed by NAKIVO Backup & Replication. From this dashboard, the following actions can be done:

- Viewing Activities
- Searching for Activities
- Viewing Activity Details
- Stopping Running Activities
- Running Activities Again
- Removing Activities

Past activities are stored for the number of days specified in the **Store job history for the last X days** setting in the General tab.

Viewing Activities

The **Activities** dashboard allows viewing all your current and past activities in the application.



Running Activities

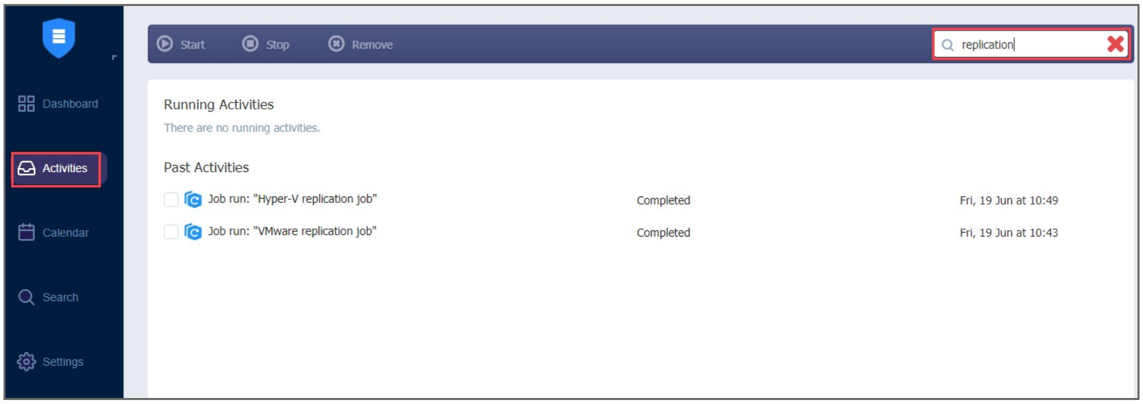
There are no running activities.

Past Activities

□ Job run: "EC2 failover job"	Completed	Mon, 22 Jun at 9:37
□ Self-backup into repositories: "Onboard repository"	Completed	Mon, 22 Jun at 5:00
□ Self-backup into repositories: "Onboard repository"	Completed	Sun, 21 Jun at 5:00
□ Self-backup into repositories: "Onboard repository"	Completed	Sat, 20 Jun at 5:00
□ Job run: "Hyper-V failover job"	Completed	Fri, 19 Jun at 14:13
□ Job run: "VMware failover job"	Completed	Fri, 19 Jun at 13:38
□ Job run: "Exchange 2019"	Completed	Fri, 19 Jun at 12:11
□ Job run: "Replica AMAZON EC2 (Ireland)"	Completed	Fri, 19 Jun at 12:05
□ Scanning tape 510591 in "Tape"	Completed	Fri, 19 Jun at 12:01
□ Job run: "AD+Exchange"	Completed	Fri, 19 Jun at 10:57
□ Job run: "Hyper-V replication job"	Completed	Fri, 19 Jun at 10:49
□ Job run: "VMware replication job"	Completed	Fri, 19 Jun at 10:43
□ Job run: "VMware recovery job-SQL"	Completed	Fri, 19 Jun at 10:20
□ Self-backup into repositories: "Onboard repository"	Completed	Fri, 19 Jun at 5:00
□ Job run: "Hyper-V recovery job"	Completed	Thu, 18 Jun at 18:20
□ Job run: "Nutanix AHV backup job"	Completed	Thu, 18 Jun at 17:05
□ Scanning tape 939ee6d8-4150-4f5b-bbb7-64b40d02d9d0 in "Tape"	Completed	Thu, 18 Jun at 12:59
□ Job run: "EC2 backup job"	Completed	Thu, 18 Jun at 12:29

Searching for Activities

Find activity by typing in part of its name in the **Search** field.



Running Activities

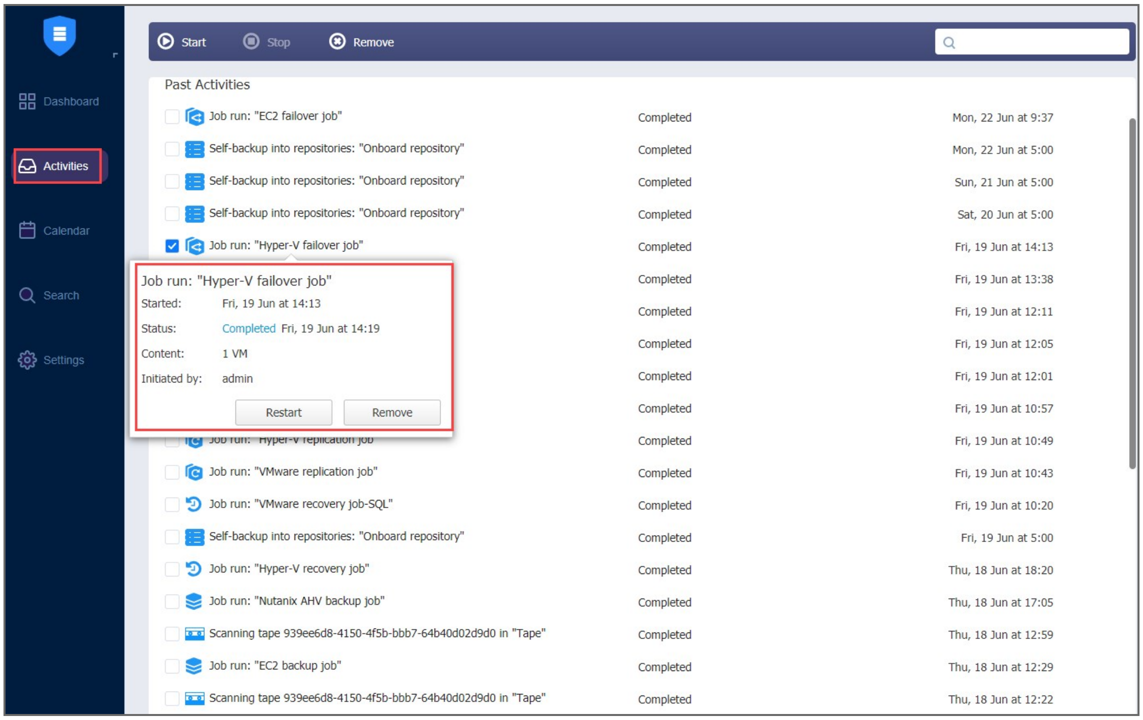
There are no running activities.

Past Activities

□ Job run: "Hyper-V replication job"	Completed	Fri, 19 Jun at 10:49
□ Job run: "VMware replication job"	Completed	Fri, 19 Jun at 10:43

Viewing Activity Details

View the details of an activity by selecting an activity name.



Past Activities

□ Job run: "EC2 failover job"	Completed	Mon, 22 Jun at 9:37
□ Self-backup into repositories: "Onboard repository"	Completed	Mon, 22 Jun at 5:00
□ Self-backup into repositories: "Onboard repository"	Completed	Sun, 21 Jun at 5:00
□ Self-backup into repositories: "Onboard repository"	Completed	Sat, 20 Jun at 5:00
☑ Job run: "Hyper-V failover job"	Completed	Fri, 19 Jun at 14:13
	Completed	Fri, 19 Jun at 13:38
	Completed	Fri, 19 Jun at 12:11
	Completed	Fri, 19 Jun at 12:05
	Completed	Fri, 19 Jun at 12:01
	Completed	Fri, 19 Jun at 10:57
□ Job run: "Hyper-V replication job"	Completed	Fri, 19 Jun at 10:49
□ Job run: "VMware replication job"	Completed	Fri, 19 Jun at 10:43
□ Job run: "VMware recovery job-SQL"	Completed	Fri, 19 Jun at 10:20
□ Self-backup into repositories: "Onboard repository"	Completed	Fri, 19 Jun at 5:00
□ Job run: "Hyper-V recovery job"	Completed	Thu, 18 Jun at 18:20
□ Job run: "Nutanix AHV backup job"	Completed	Thu, 18 Jun at 17:05
□ Scanning tape 939ee6d8-4150-4f5b-bbb7-64b40d02d9d0 in "Tape"	Completed	Thu, 18 Jun at 12:59
□ Job run: "EC2 backup job"	Completed	Thu, 18 Jun at 12:29
□ Scanning tape 939ee6d8-4150-4f5b-bbb7-64b40d02d9d0 in "Tape"	Completed	Thu, 18 Jun at 12:22

Job run: "Hyper-V failover job"

Started: Fri, 19 Jun at 14:13

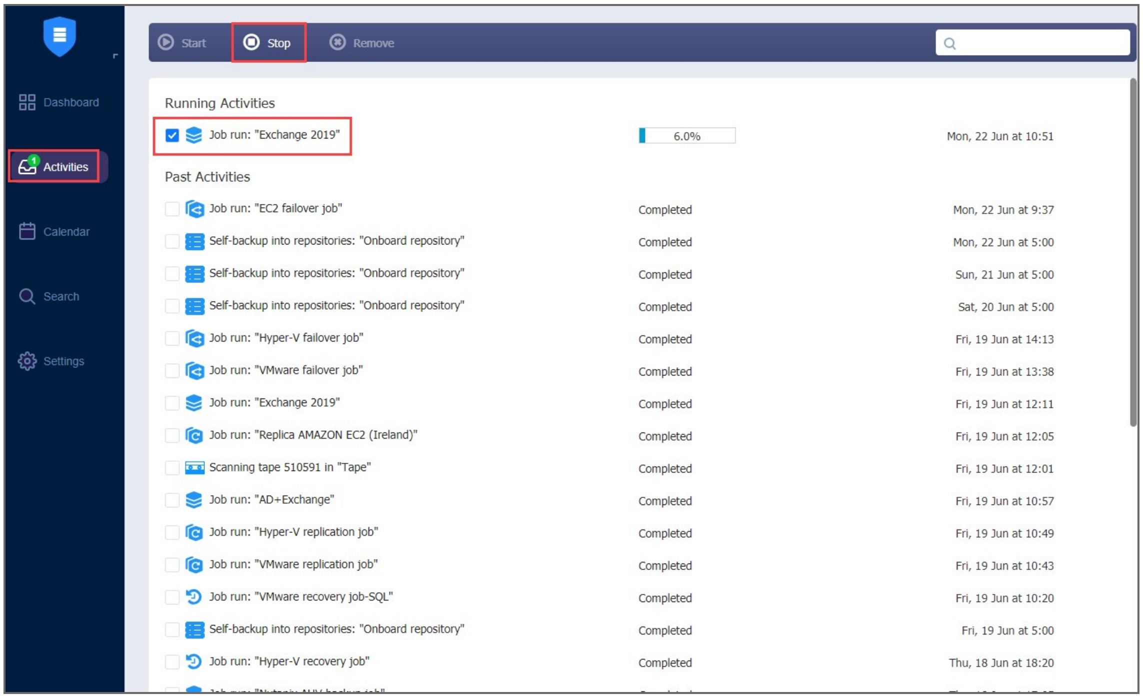
Status: Completed Fri, 19 Jun at 14:19

Content: 1 VM

Initiated by: admin

Stopping Running Activities

To stop a running activity, select the checkbox next to the activity and click **Stop** in the toolbar at the top. Optionally, you can stop multiple activities by selecting the checkboxes next to them or stop all running activities by clicking **Select/Deselect all**.



Running Activities

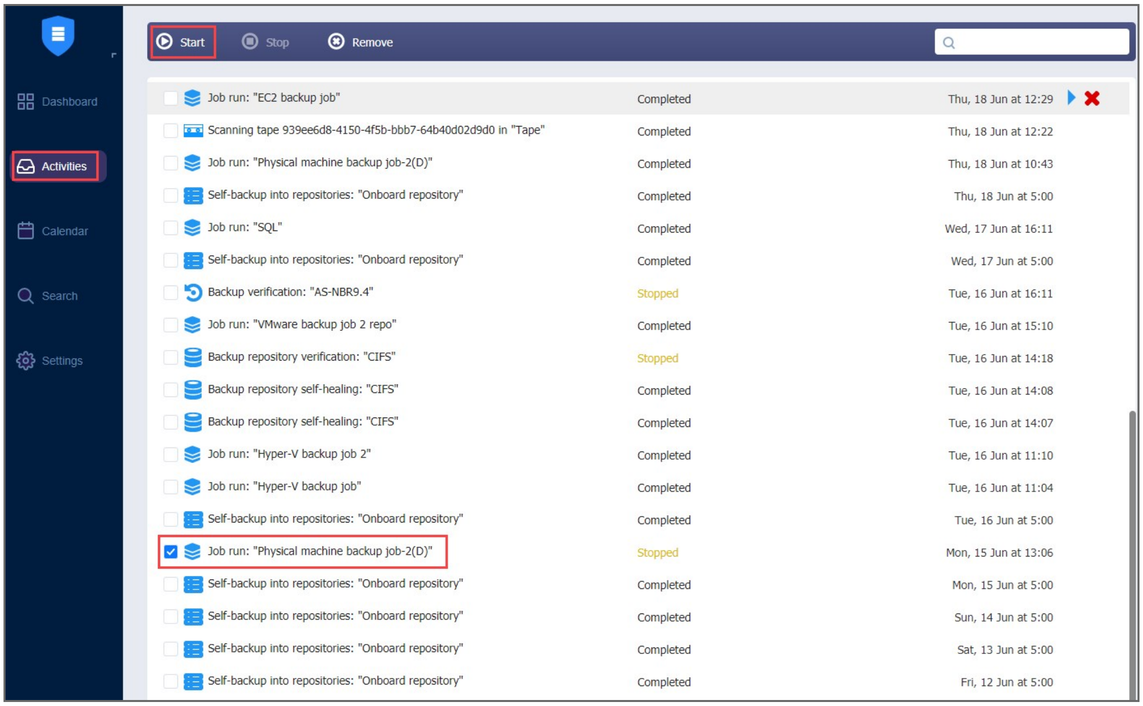
☑ Job run: "Exchange 2019"	6.0%	Mon, 22 Jun at 10:51

Past Activities

□ Job run: "EC2 failover job"	Completed	Mon, 22 Jun at 9:37
□ Self-backup into repositories: "Onboard repository"	Completed	Mon, 22 Jun at 5:00
□ Self-backup into repositories: "Onboard repository"	Completed	Sun, 21 Jun at 5:00
□ Self-backup into repositories: "Onboard repository"	Completed	Sat, 20 Jun at 5:00
□ Job run: "Hyper-V failover job"	Completed	Fri, 19 Jun at 14:13
□ Job run: "VMware failover job"	Completed	Fri, 19 Jun at 13:38
□ Job run: "Exchange 2019"	Completed	Fri, 19 Jun at 12:11
□ Job run: "Replica AMAZON EC2 (Ireland)"	Completed	Fri, 19 Jun at 12:05
□ Scanning tape 510591 in "Tape"	Completed	Fri, 19 Jun at 12:01
□ Job run: "AD+Exchange"	Completed	Fri, 19 Jun at 10:57
□ Job run: "Hyper-V replication job"	Completed	Fri, 19 Jun at 10:49
□ Job run: "VMware replication job"	Completed	Fri, 19 Jun at 10:43
□ Job run: "VMware recovery job-SQL"	Completed	Fri, 19 Jun at 10:20
□ Self-backup into repositories: "Onboard repository"	Completed	Fri, 19 Jun at 5:00
□ Job run: "Hyper-V recovery job"	Completed	Thu, 18 Jun at 18:20

Running Activities Again

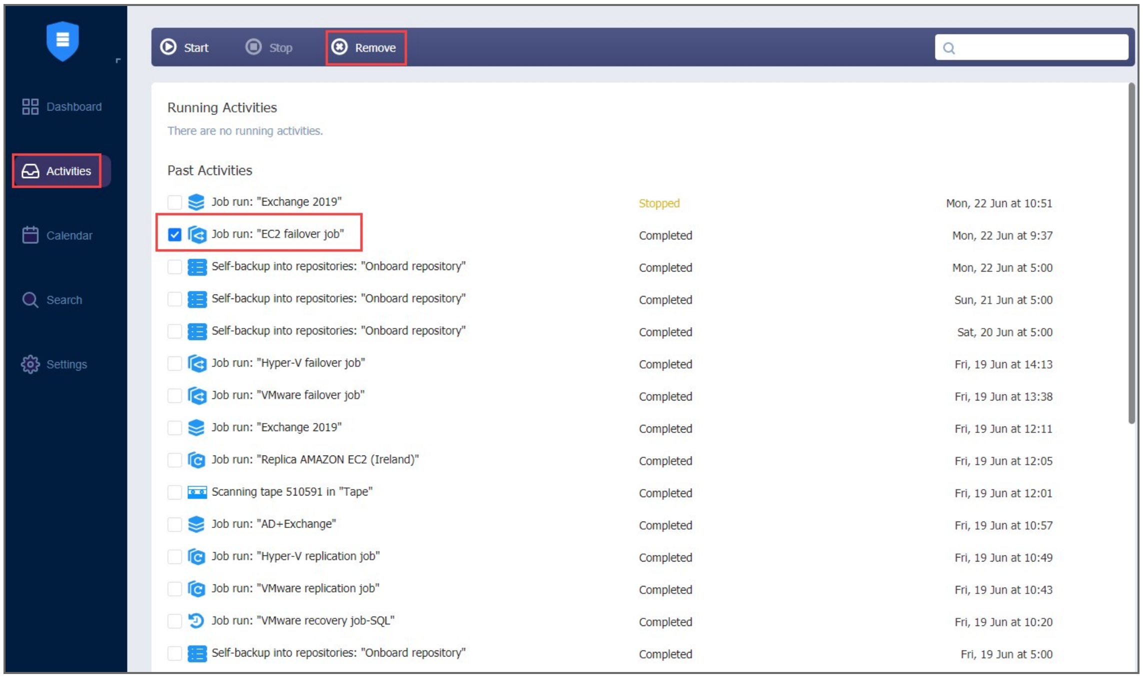
To run an activity again (if possible), select the checkbox next to the activity and click **Start** in the toolbar at the top. Optionally, you can run multiple activities by selecting the checkboxes next to them or run all stopped activities by clicking **Select/Deselect all**.



□ Job run: "EC2 backup job"	Completed	Thu, 18 Jun at 12:29
□ Scanning tape 939ee6d8-4150-4f5b-bbb7-64b40d02d9d0 in "Tape"	Completed	Thu, 18 Jun at 12:22
□ Job run: "Physical machine backup job-2(D)"	Completed	Thu, 18 Jun at 10:43
□ Self-backup into repositories: "Onboard repository"	Completed	Thu, 18 Jun at 5:00
□ Job run: "SQL"	Completed	Wed, 17 Jun at 16:11
□ Self-backup into repositories: "Onboard repository"	Completed	Wed, 17 Jun at 5:00
□ Backup verification: "AS-NBR9.4"	Stopped	Tue, 16 Jun at 16:11
□ Job run: "VMware backup job 2 repo"	Completed	Tue, 16 Jun at 15:10
□ Backup repository verification: "CIFS"	Stopped	Tue, 16 Jun at 14:18
□ Backup repository self-healing: "CIFS"	Completed	Tue, 16 Jun at 14:08
□ Backup repository self-healing: "CIFS"	Completed	Tue, 16 Jun at 14:07
□ Job run: "Hyper-V backup job 2"	Completed	Tue, 16 Jun at 11:10
□ Job run: "Hyper-V backup job"	Completed	Tue, 16 Jun at 11:04
□ Self-backup into repositories: "Onboard repository"	Completed	Tue, 16 Jun at 5:00
☑ Job run: "Physical machine backup job-2(D)"	Stopped	Mon, 15 Jun at 13:06
□ Self-backup into repositories: "Onboard repository"	Completed	Mon, 15 Jun at 5:00
□ Self-backup into repositories: "Onboard repository"	Completed	Sun, 14 Jun at 5:00
□ Self-backup into repositories: "Onboard repository"	Completed	Sat, 13 Jun at 5:00
□ Self-backup into repositories: "Onboard repository"	Completed	Fri, 12 Jun at 5:00

Removing Activities

Remove an activity from the list by selecting the checkbox next to the activity and clicking **Remove** in the toolbar.



Running Activities

There are no running activities.

Past Activities

□	Job run: "Exchange 2019"	Stopped	Mon, 22 Jun at 10:51
☑	Job run: "EC2 failover job"	Completed	Mon, 22 Jun at 9:37
□	Self-backup into repositories: "Onboard repository"	Completed	Mon, 22 Jun at 5:00
□	Self-backup into repositories: "Onboard repository"	Completed	Sun, 21 Jun at 5:00
□	Self-backup into repositories: "Onboard repository"	Completed	Sat, 20 Jun at 5:00
□	Job run: "Hyper-V failover job"	Completed	Fri, 19 Jun at 14:13
□	Job run: "VMware failover job"	Completed	Fri, 19 Jun at 13:38
□	Job run: "Exchange 2019"	Completed	Fri, 19 Jun at 12:11
□	Job run: "Replica AMAZON EC2 (Ireland)"	Completed	Fri, 19 Jun at 12:05
□	Scanning tape 510591 in "Tape"	Completed	Fri, 19 Jun at 12:01
□	Job run: "AD+Exchange"	Completed	Fri, 19 Jun at 10:57
□	Job run: "Hyper-V replication job"	Completed	Fri, 19 Jun at 10:49
□	Job run: "VMware replication job"	Completed	Fri, 19 Jun at 10:43
□	Job run: "VMware recovery job-SQL"	Completed	Fri, 19 Jun at 10:20
□	Self-backup into repositories: "Onboard repository"	Completed	Fri, 19 Jun at 5:00

Using Calendar

The **Calendar** allows you to schedule and view the history of past job runs.

- Creating Jobs with Calendar
- Editing Jobs with Calendar

Creating Jobs with Calendar

To create a job:

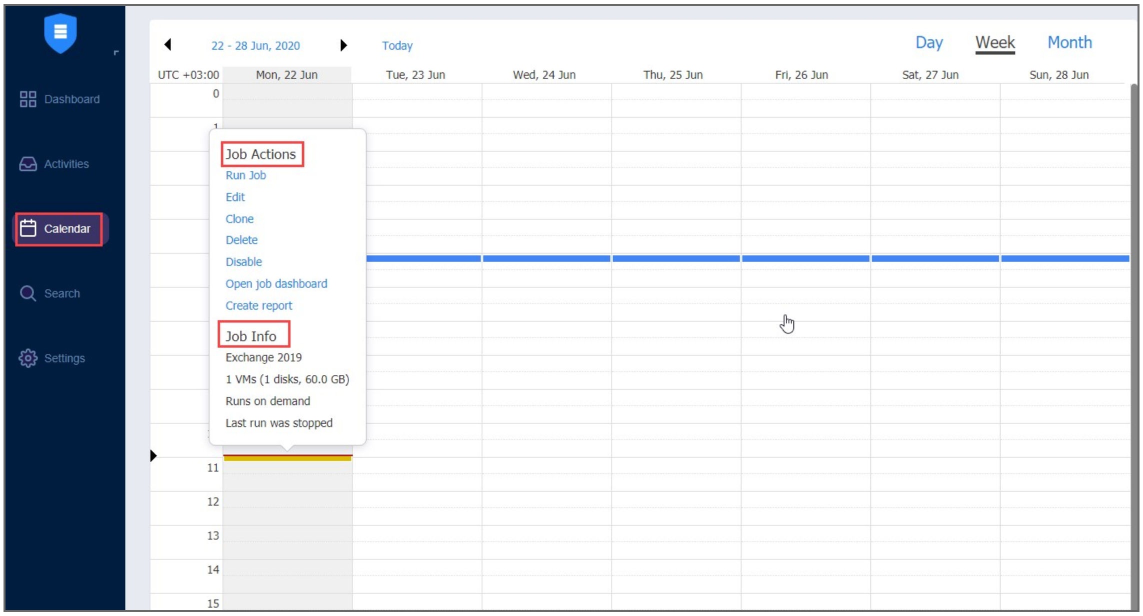
1. Click on the date and time when you'd like to run the job
2. Select the type of job you need.
3. On the **Schedule** page of the wizard, the time you've selected in the **Calendar** will be selected.

Editing Jobs with Calendar

If you click on the job title on the Calendar dashboard, the **Job Actions** menu will appear.

Using this menu, you can:

- Run a job overriding the schedule.
- Edit a job.
- Clone a job
- Delete the job. If the job is repeated, this action will affect all job runs.
- Disable/Enable a job. If the job is repeated, this action will affect all job runs.
- Open the Dashboard.
- Create a report.



Using Global Search

Using the **Global Search** dashboard, search for items within the entire inventory of NAKIVO Backup & Replication, Transporters, Backup Repositories, jobs, backups, and other.

- Opening Global Search
- Running Global Search
- Filtering Search Results
- Applying Bulk Action
- Viewing Object Info

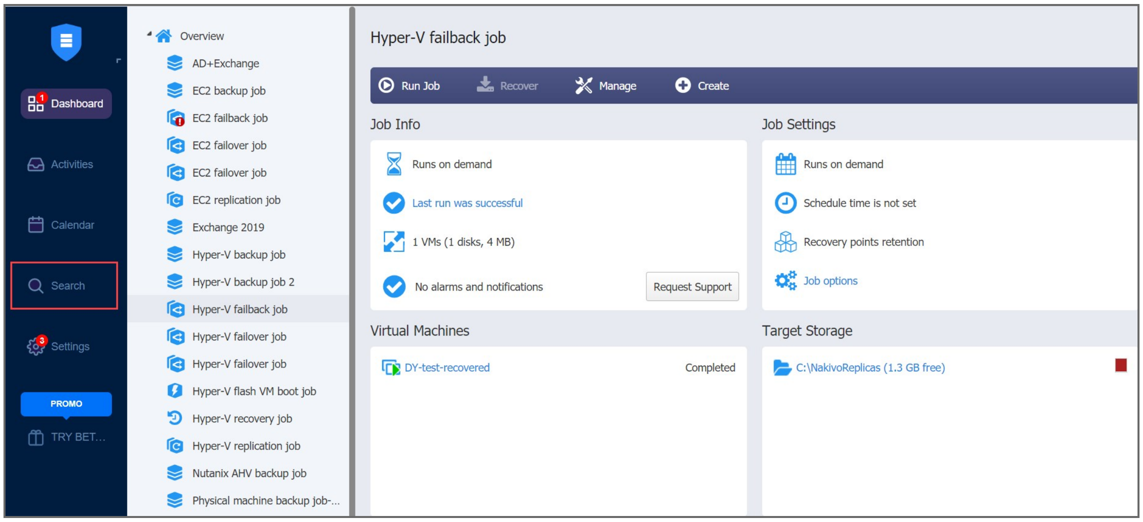
Note

When the multi-tenant mode is enabled, Global Search will operate within a specific tenant. For more information about multi-tenancy in NAKIVO Backup & Replication, please consult with the following resources:

- “Multi-Tenancy” on page 16
- “Multi-Tenant Mode” on page 343

Opening Global Search

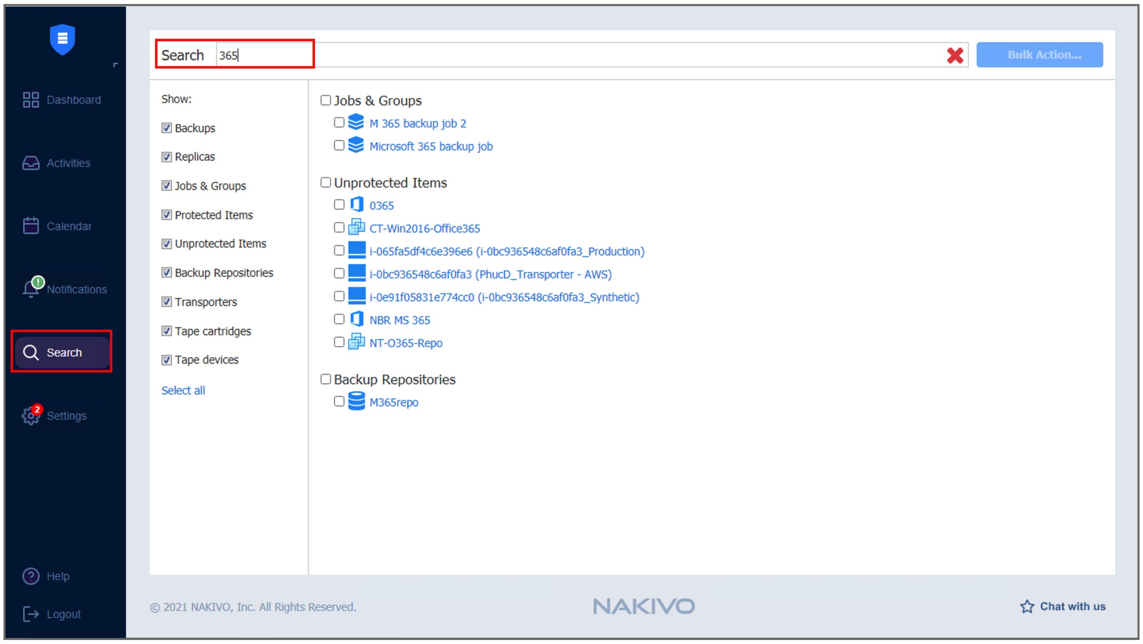
To open **Global Search**, click the **Search** icon in the main toolbar of the application.



Running Global Search

When the **Global Search** dashboard opens, you can enter your search string into the search box.
The string you have entered will be immediately followed by a display of the search results in the form of a list.
To help you fine-tune your search, the following wildcards are applicable:

- "**?**" representing a single character.
- "*****" representing zero or more characters.



Search 365

Show:

☑ Backups
☑ Replicas
☑ Jobs & Groups
☑ Protected Items
☑ Unprotected Items
☑ Backup Repositories
☑ Transporters
☑ Tape cartridges
☑ Tape devices

Select all

□ Jobs & Groups
- □ M 365 backup job 2
- □ Microsoft 365 backup job

□ Unprotected Items
- □ 0365
- □ CT-Win2016-Office365
- □ i-065fa5df4c6e396e6 (i-0bc936548c6af0fa3_Production)
- □ i-0bc936548c6af0fa3 (PhucD_Transporter - AWS)
- □ i-0e91f05831e774cc0 (i-0bc936548c6af0fa3_Synthetic)
- □ NBR MS 365
- □ NT-O365-Repo

□ Backup Repositories
- □ M365repo

© 2021 NAKIVO, Inc. All Rights Reserved.

Please note the following:

- Search is case insensitive.
- Search results are grouped by categories.

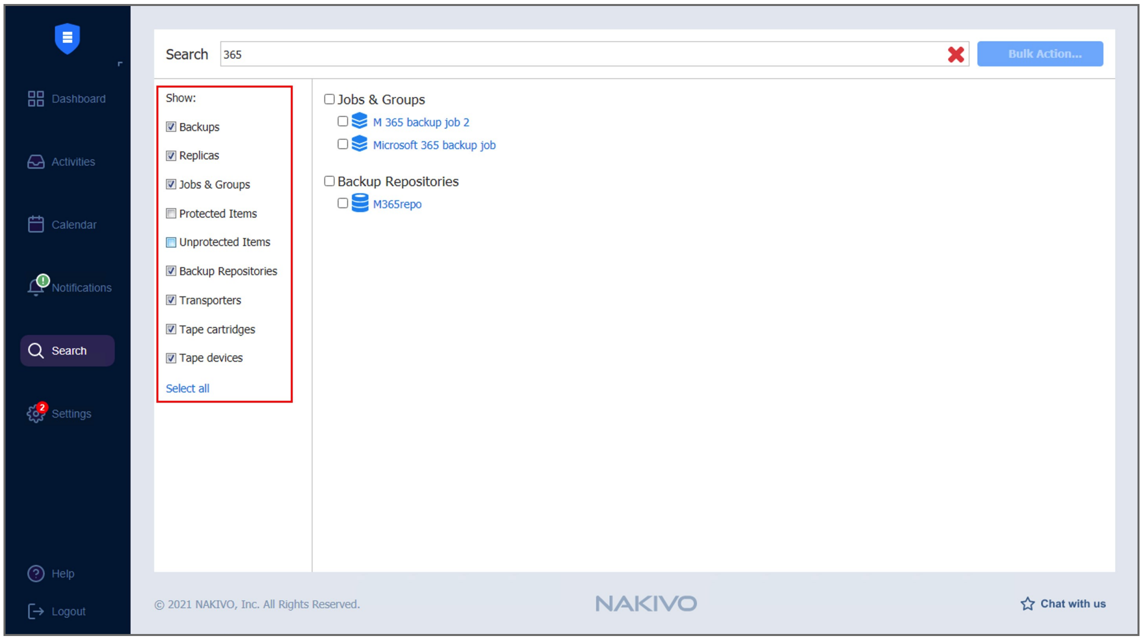
Filtering Search Results

By default, your search results are unfiltered. This means that the search is applied to all categories of NAKIVO Backup & Replication objects.

To narrow your search results, deselect some categories in the categories list:

- Backups
- Replicas
- Jobs & Groups
- Protected Items
- Unprotected Items
- Backup Repositories
- Transporters

The filtered search results will be displayed immediately in the search results list.



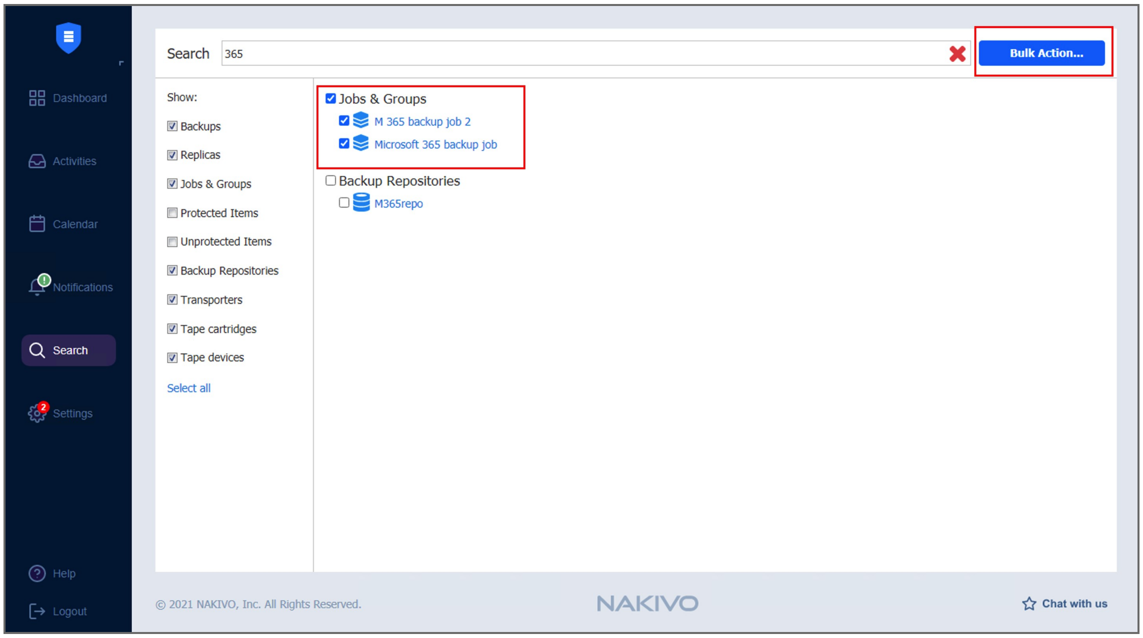
To get back to the default filtering settings, click **Select all** below the categories list.

Applying Bulk Action

With NAKIVO Backup & Replication Global Search, you can apply a bulk action to objects belonging to the same category and of the same type.

Proceed as follows to apply a bulk action:

1. In the search result list, select similar objects.
2. The **Bulk Action** button becomes active in the upper right corner of the dialog. Click **Bulk Action**.



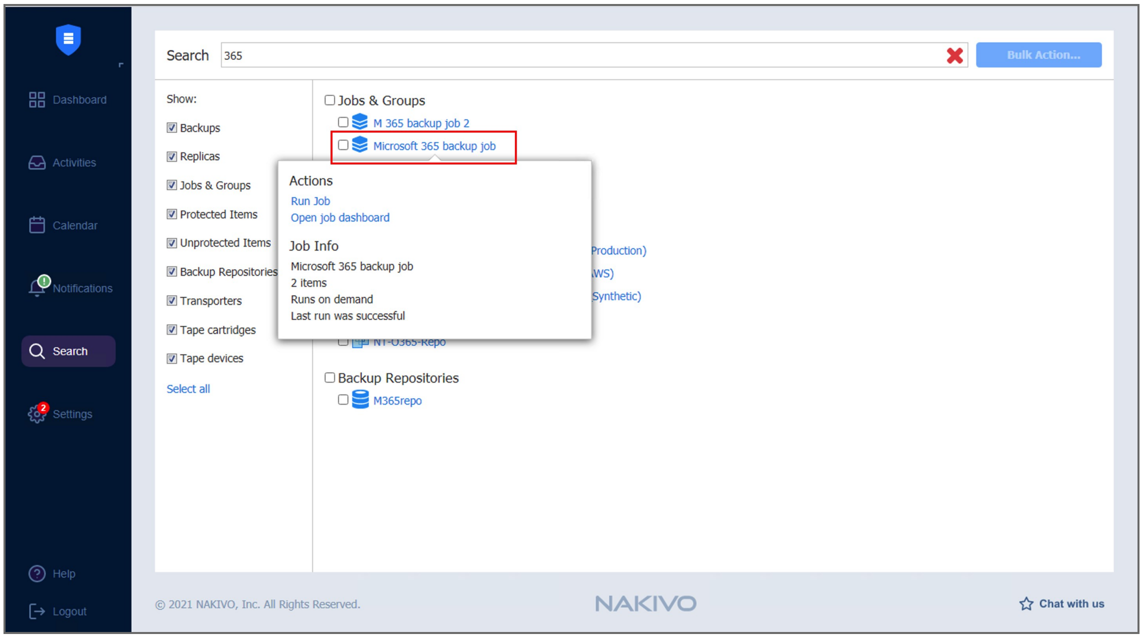
A dialog opens with the list of actions applicable to the selected items. To proceed with the necessary action, click the corresponding item in the list of actions.

Note

Bulk actions are not applicable to NAKIVO Backup & Replication dissimilar objects.

Viewing Object Info

To view info on a specific object available in the search result, click the object.



Actions
Run Job
Open job dashboard

Job Info
Microsoft 365 backup job
2 items
Runs on demand
Last run was successful

A dialog opens displaying object info, along with the list of typical actions applicable to the object.

Deployment

This section contains the following topics :

Architecture

- What is NAKIVO Backup & Replication?
- Solution Components

What is NAKIVO Backup & Replication?

NAKIVO Backup & Replication is an all-in-one solution designed to back up, replicate, and recover virtual machines and cloud instances. The product can also back up and recover physical machines.

Solution Components

NAKIVO Backup & Replication is a server application that can be installed on a virtual or physical machine. The application is designed to achieve top speeds for CPU and RAM to achieve the top speed of VM backup, replication, and recovery. Thus, NAKIVO Backup & Replication components should be installed on a machine designated for backup and replication so it does not interfere with the performance of other applications.

NAKIVO Backup and Replication consists of the following components:

- "Director" on page 59
- "Transporter" on page 61
- "Backup Repository" on page 65

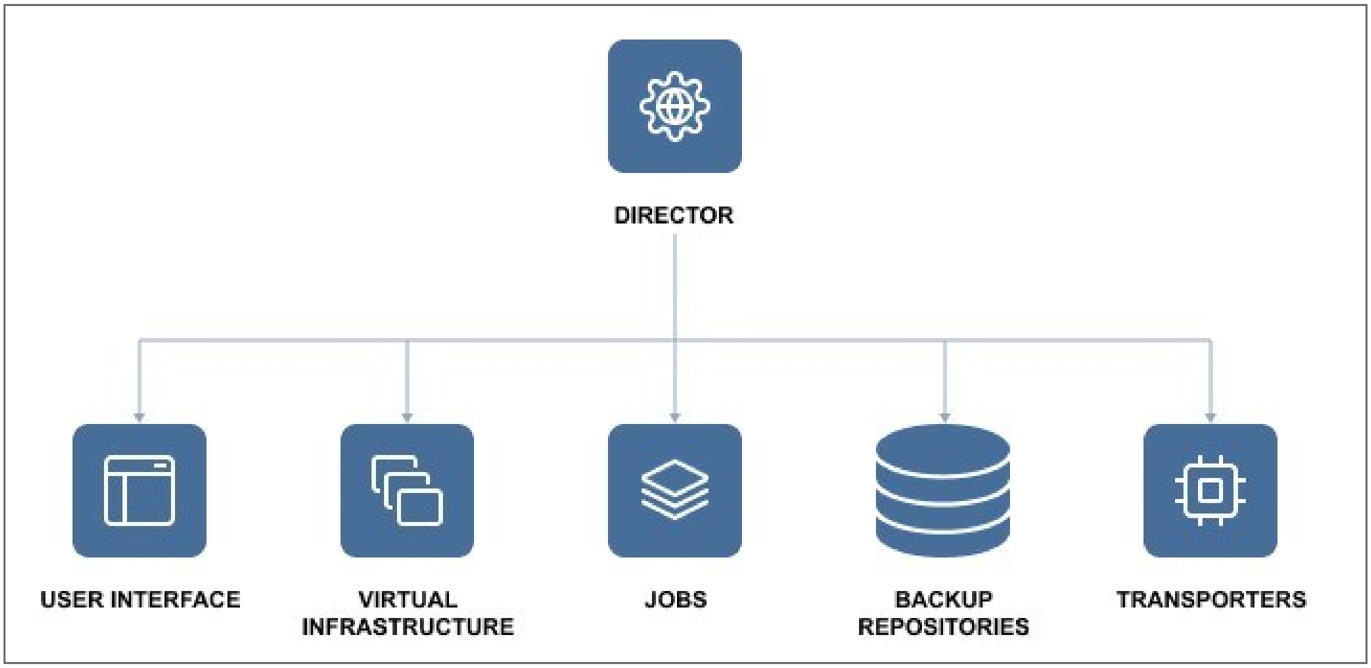
All components can be installed on a single machine or can be distributed across multiple machines and geographical locations.

Director

- [What is Director?]
- [How Many Directors Should be Deployed?]

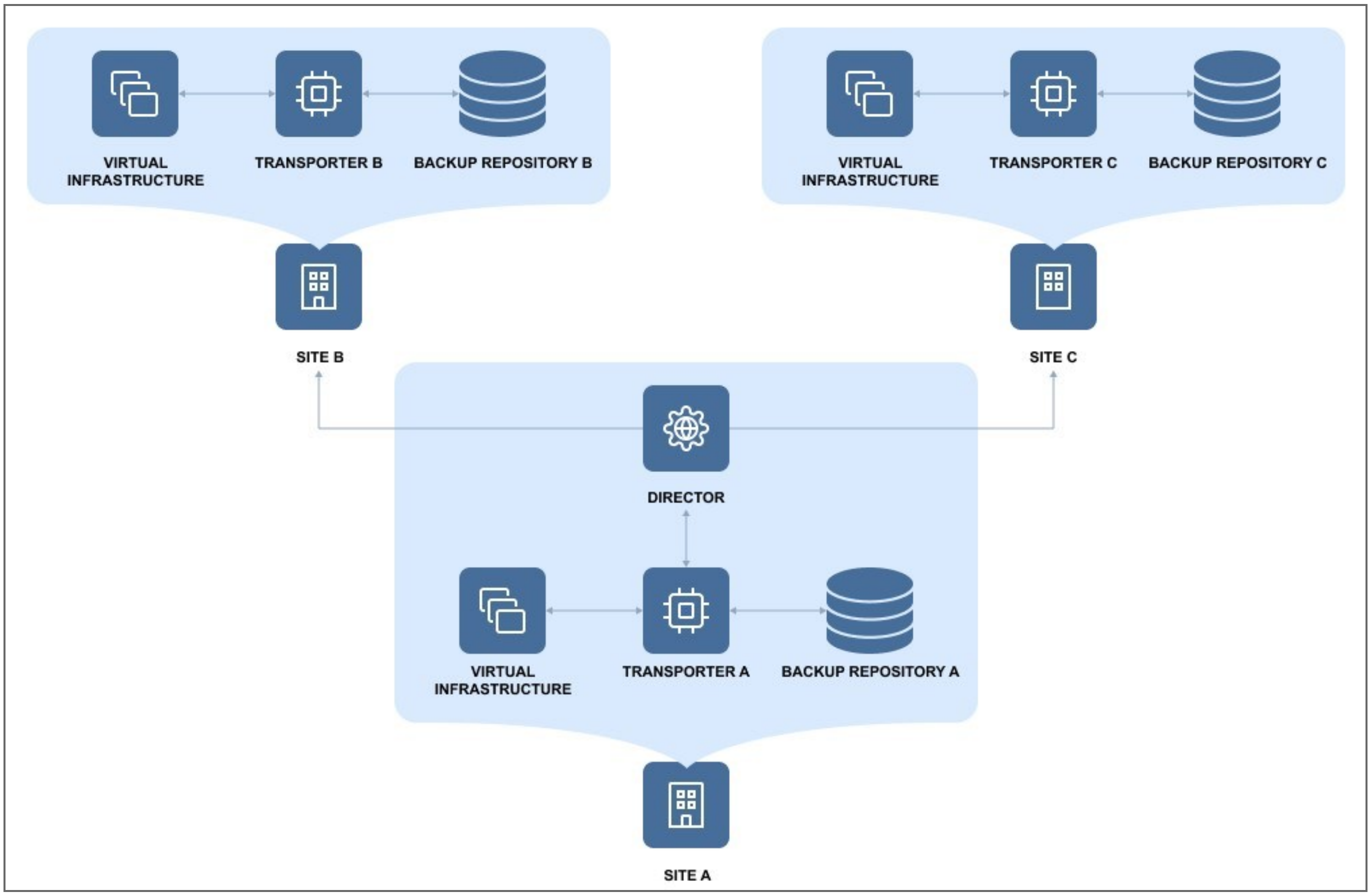
What is Director?

Director is the central management instance of the product. It provides Web interface, locates and maintains the inventory, provides users with the ability to create and run jobs, manages Backup Repositories, Transporters, and other product elements.



How Many Directors Should be Deployed

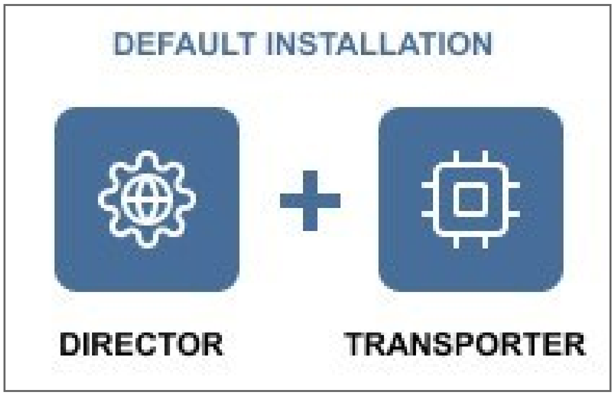
Only one instance of the Director should be installed per customer. As a central management point for data protection, one instance of the Director can manage multiple geographically distributed virtual and cloud environments, Backup Repositories, and Transporters. See the example below.


VIRTUAL INFRASTRUCTURE
TRANSPORTER B
BACKUP REPOSITORY B
VIRTUAL INFRASTRUCTURE
TRANSPORTER C
BACKUP REPOSITORY C
SITE B
SITE C
DIRECTOR
VIRTUAL INFRASTRUCTURE
TRANSPORTER A
BACKUP REPOSITORY A
SITE A

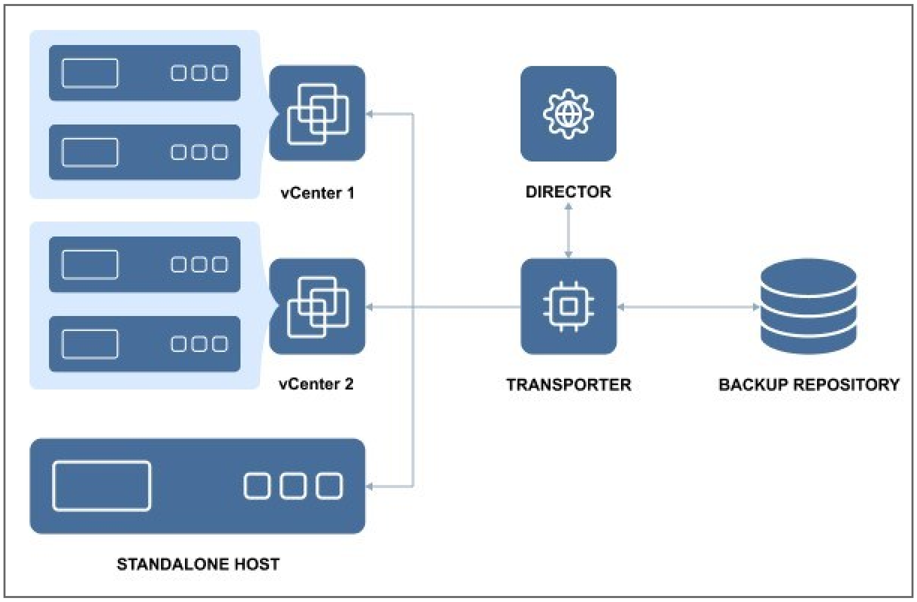
Transporter

What is Transporter?

Transporter is the component of the product that does all of the heavy lifting. It performs backup, replication, and recovery, as well as data compression, deduplication, and encryption. An instance of the Transporter is automatically installed along with the Director to enable backup, replication, and recovery out of the box. The default Transporter is called "Onboard Transporter", and it must not be removed or added to the product by another Director.



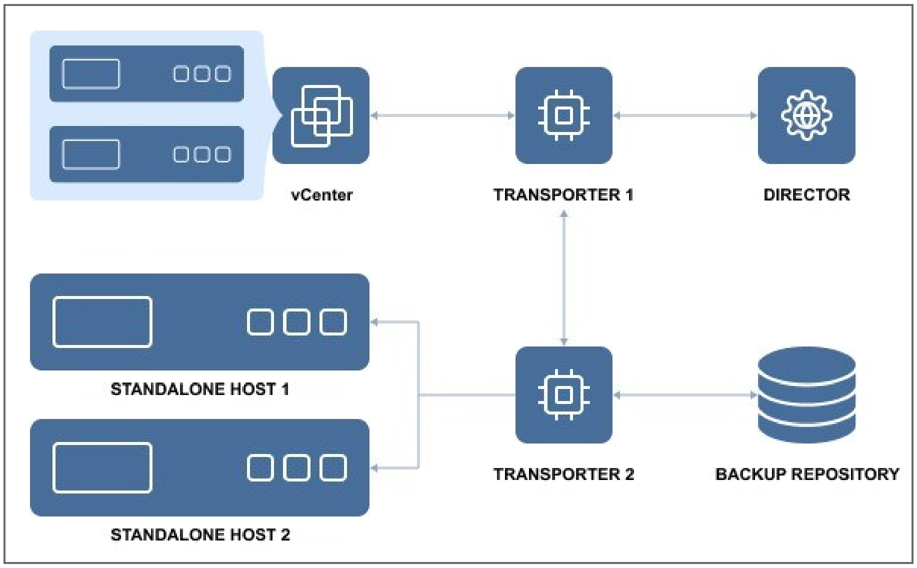
A single Transporter can back up, replicate, and recover multiple VMs and cloud instances.



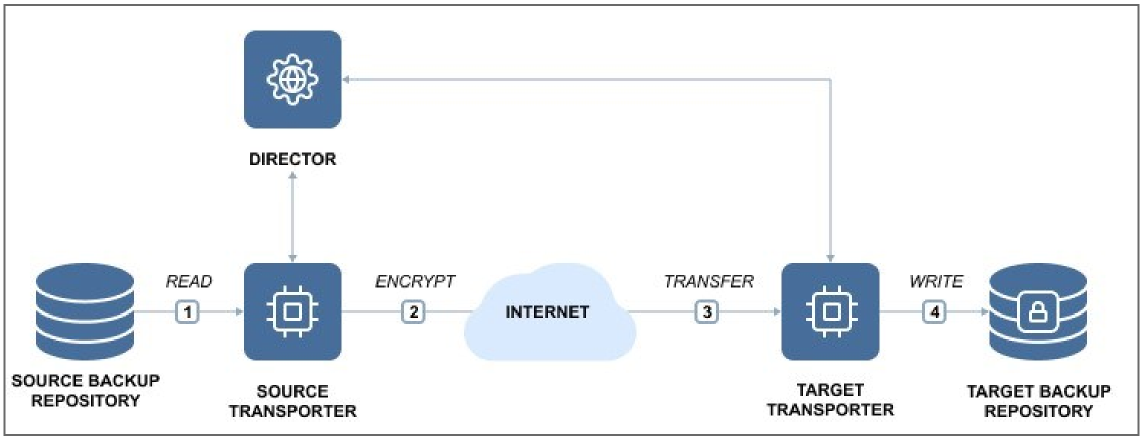
One Transporter can simultaneously process multiple source disks (6 by default) during backup, replication, and recovery. If jobs contain more disks than the Transporter is set to process simultaneously, the disks will be put in a queue and will be processed once the Transporter frees up.

How Many Transporters Should be Deployed?

In most cases, it is sufficient to deploy only one Transporter per site. In large environments, where multiple source items need to be processed simultaneously, multiple Transporters can be deployed to distribute the workload.



Deploying multiple Transporters also enables network acceleration and AES 256 encryption of traffic between a pair of Transporters. For example, if VMs are replicated over WAN between two sites, the Transporter installed in the source site can compress and encrypt data before transferring it over WAN, and the Transporter installed in the Target site can unencrypt and decompress the data prior to writing it to the target server.

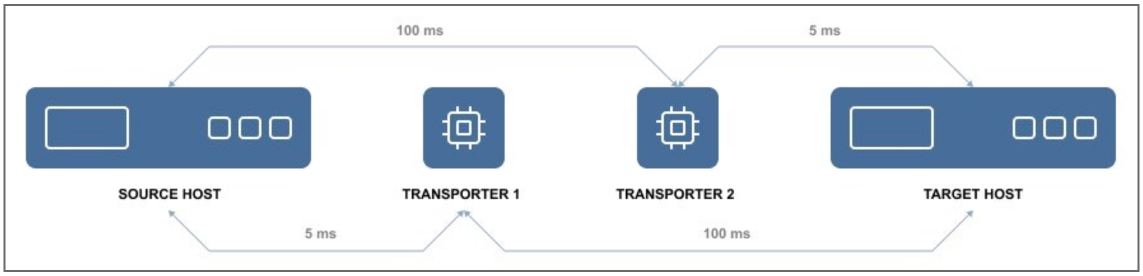


If you plan to transfer data over WAN without a VPN connection from your source site to the target site, make sure the source and target Transporters are added to the product using external IP addresses or DNS names that can be properly resolved in WAN, so that the two Transporters can connect to each other.

How Transporters are Selected for Jobs

In large and geographically distributed environments multiple Transporters can be deployed to distribute the data protection workload, optimize network traffic, and improve data transfer speeds. Thus, if more than one Transporter is deployed for NAKIVO Backup & Replication, it is important to determine which one should be used to read data from a particular source and which one should be used to write data to a target.

By default, the product automatically determines which Transporter should be used based on the proximity of a Transporter to the source or target server. The proximity is measured by using the ping round trip time.



In the example above, Transporter 1 will be selected to read data from the Source ESXi, and Transporter 2 will be selected to write data to the Target ESXi.

The Transporter selection can also be configured manually during job creation.

Transporter Security

It is possible to set a Master Password for the Transporter and use a CA certificate to make NAKIVO Backup & Replication more secure. The certificate can be set for the Onboard Transporter during the full installation of the product or for individual Transporters during Transporter-only installation, or by using the Windows Updater on Windows operating systems. The master password can be set only during the Transporter-only installation.

This option is available for the following supported target platforms:

- VMware vSphere
- Microsoft Hyper-V
- Amazon EC2
- Nutanix AHV
- Supported NAS models
- Virtual Appliances
- Physical machines

To use CA certificates, make sure that they adhere to the necessary requirements. Refer to Custom CA-Signed Certificate Compatibility.

Backup Repository

- What is a Backup Repository?
- How Much Data Can Be Stored in a Backup Repository?
- How is a Backup Repository Managed?

What is a Backup Repository?

A Backup Repository is a folder used by NAKIVO Backup & Replication to store backups. When you add a Backup Repository to the product, NAKIVO Backup & Replication creates a folder named "NakivoBackup" in the specified location and keeps all backed up data and Backup Repository metadata in that folder.

Important

- Do not modify or delete any files inside the "NakivoBackup" folder. Modifying or deleting any file inside the "NakivoBackup" folder may irreversibly damage an entire Backup Repository.
- To avoid disrupting NAKIVO Backup & Replication processes and data corruption, add the application to the whitelist/exclusions list of the antivirus software running on the machine on which the NAKIVO Backup Repository is set up.

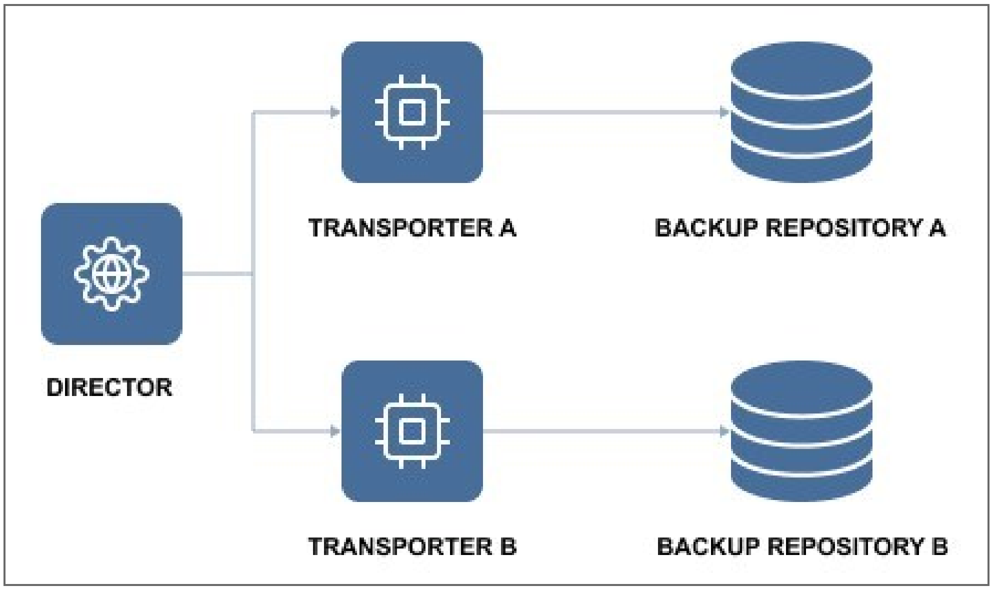
By default, a Backup Repository is created when the full solution (both Director and Transporter) is installed. The default Backup Repository is named "Onboard repository".

How Much Data Can Be Stored in a Backup Repository?

NAKIVO Backup & Replication can store up to 128 TB of data in a single Backup Repository. The number of Backup Repositories per installation is unlimited. By default, backups are compressed and deduplicated at the block level across the entire Backup Repository to save storage space.

How is a Backup Repository Managed?

Each Backup Repository is managed by a single Transporter called an Assigned Transporter. In other words, only one Transporter can read data from and write data to a particular Backup Repository.



The Assigned Transporter is responsible for all interaction with its Backup Repository. A single Transporter can be assigned to and manage multiple Backup Repositories.

System Requirements

Before you start using NAKIVO Backup & Replication, make sure that the servers or machines that you plan to use as backup infrastructure components meet the requirements listed in the following topics:

- “Supported Platforms” on page 68
- “Deployment Requirements” on page 70

Supported Platforms

NAKIVO Backup & Replication provides data protection for the following platforms:

- Microsoft 365 (Exchange Online, OneDrive for Business, SharePoint Online)

Notes

- To learn about limitations of NAKIVO Backup & Replication related to supported platforms, refer to the Platform Limitations section of the latest Release Notes.
- To add a supported platform to the NAKIVO Backup & Replication, make sure that your system has been updated with the latest patch and all the necessary requirements are met.

Find the necessary requirements below:

- Microsoft 365 Requirements

Microsoft 365 Requirements

To provide data protection for your Microsoft 365, the following requirements must be met:

- Exchange Online must be purchased as a part of the Microsoft 365 plan or a standalone service.
- The required API permissions must be provided to NAKIVO Backup & Replication. Refer to Required API Permissions for Microsoft 365.
- For automatic enabling of the "Site Collection Administrator" role, a Microsoft 365 account user must have the "SharePoint admin" or "Global admin" role. This is required for backing up and recovery of SharePoint Online sites.
- Two-factor/multi-factor authentication must be disabled in SharePoint Online administrator account.
- Microsoft 365 account must be accessible over the network.
- To backup and restore Microsoft 365 services, a Transporter should be installed on one of the following operating systems:

Windows

- Windows Server 2019 Standard (x64)
- Windows Server 2016 Standard (x64)
- Windows Server 2012 R2 Standard (x64)
    - Update for Windows Server 2012 R2 (KB3179574)
- Windows Server 2012 Standard (x64)
- Windows Server 2008 R2 Standard (x64)
- Windows 10 Pro (x64)
- Windows 8 Professional (x64)
- Windows 7 Professional (x64)

Linux

- Ubuntu 18.04 Server (x64)
- Ubuntu 16.04 Server (x64)
- SUSE Linux Enterprise Server 12 SP3 (x64)

- Red Hat Enterprise Linux 7.6 (x64)
- Red Hat Enterprise Linux 7.5 (x64)
- Red Hat Enterprise Linux 7.4 (x64)

NAS

Refer to “Deployment Requirements” on page 70 to see the list of supported NAS devices.

Note

ARM-based NAS devices and FreeNAS devices are not supported for backup and recovery of Microsoft 365 accounts.

Deployment Requirements

NAKIVO Backup & Replication can be deployed as a virtual appliance (VA) or installed directly onto a supported machine or network-attached storage (NAS). Below is the list of deployment requirements.

Hardware

VM or Physical Machine

NAKIVO Backup & Replication can be installed on a machine with the following minimum hardware characteristics:

Director and Onboard Transporter:

- **CPU**: x86-64, 2 cores
- **RAM**: 4 GB + 250 MB for each concurrent task
  - For SaaS Backup Repository-related activities:
    - additional 2 GB
    - additional 100 MB for each concurrent Java Transporter task
- **Free space**: 10 GB

Transporter only:

- **CPU**: x86-64, 2 cores
- **RAM**: 2 GB + 250 MB for each concurrent task
  - For SaaS Backup Repository-related activities:
    - additional 2 GB
    - additional 100 MB for each concurrent Java Transporter task
- **Free space**: 5 GB

Network Attached Storage

NAKIVO Backup & Replication can be installed on supported NAS with the following minimum hardware characteristics:

Director and Onboard Transporter:

- **CPU**: x86-64, 2 cores
- **RAM**: 1 GB
    - For SaaS Backup Repository-related activities:
        - minimum total RAM: 4 GB
        - additional 100 MB for each concurrent Java Transporter task
- **Free space**: 10 GB

Transporter only:

- **CPU**: x86-64, 2 cores
- **RAM**: 512 MB
    - For SaaS Backup Repository-related activities:
        - minimum total RAM: 4 GB
        - additional 100 MB for each concurrent Java Transporter task
- **Free space**: 5 GB

Note

Onboard Transporters installed on NAS devices with ARM CPU do not support VMware infrastructures. Refer to Transporter Does Not Support VMware vSphere for a solution.

Supported NAS Devices

- **Synology**: For a full list of supported models, refer to "Supported Synology NAS Devices" on page 86
- **QNAP**: For a full list of supported models, refer to "Supported QNAP NAS Devices" on page 80
- **ASUSTOR**: For a full list of supported models, refer to "Supported ASUSTOR NAS Devices" on page 75
- **NETGEAR**: For a full list of supported. For a full list of supporter models, refer to "Supported NETGEAR NAS Devices" on page 77.
- **Western Digital**: For a full list of supported models, refer to "Supported Western Digital NAS Devices" on page 90.

Operating Systems

NAKIVO Backup & Replication can be installed on the following operating systems:

Windows

- Windows Server 2019 Standard (x64)
- Windows Server 2016 Standard (x64)
- Windows Server 2012 R2 Standard (x64)
- Windows Server 2012 Standard (x64)
- Windows Server 2008 R2 Standard (x64)
- Windows 10 Professional (x64)
- Windows 8 Professional (x64)
- Windows 7 Professional (x64)

Linux

- Ubuntu 20.04 Server (x64)
- Ubuntu 18.04 Server (x64)

- Ubuntu 16.04 Server (x64)
- SUSE Linux Enterprise Server 15 SP2 (x64)
- SUSE Linux Enterprise Server 15 SP1 (x64)
- SUSE Linux Enterprise Server 12 SP5 (x64)
- SUSE Linux Enterprise Server 12 SP4 (x64)
- SUSE Linux Enterprise Server 12 SP3 (x64)
- Red Hat Enterprise Linux 8.3 (x64)
- Red Hat Enterprise Linux 8.2 (x64)
- Red Hat Enterprise Linux 8.1 (x64)
- Red Hat Enterprise Linux 8.0 (x64)
- Red Hat Enterprise Linux 7.9 (x64)
- Red Hat Enterprise Linux 7.8 (x64)
- Red Hat Enterprise Linux 7.7 (x64)
- Red Hat Enterprise Linux 7.6 (x64)
- Red Hat Enterprise Linux 7.5 (x64)
- Red Hat Enterprise Linux 7.4 (x64)
- CentOS Linux 8.0 (x64)
- CentOS Linux 7.9 (x64)
- CentOS Linux 7.8 (x64)
- CentOS Linux 7.7 (x64)
- CentOS Linux 7.6 (x64)
- CentOS Linux 7.5 (x64)
- CentOS Linux 7.4 (x64)
- CentOS Linux 7.3 (x64)
- CentOS Linux 7.2 (x64)
- CentOS Linux 7.1 (x64)
- CentOS Linux 7.0 (x64)

NAS

- ASUSTOR ADM v3.5
- Netgear ReadyNAS OS v6.10.3
- Netgear ReadyNAS OS v6.9
- Synology DSM 6.2.3
- Synology DSM v6.2
- Synology DSM v6.1
- Synology DSM v6.0
- QNAP QTS v4.5.1
- QNAP QTS v4.4
- QNAP QTS v4.3
- WD MyCloud v3
- TrueNAS CORE 12

Supported Operating System Localizations

NAKIVO Backup & Replication can be installed on a supported OS with the following OS localization:

- English
- Italian
- German
- French
- Spanish

Networking Requirements

Required TCP Ports

NAKIVO Backup & Replication requires the following TCP ports to be open for a successful operation:

TC Port (Default)	Where	Description
NAKIVO Backup & Replication		
4443	Director	Used to access the Director web UI. Must be opened on the Director machine.
9446	Transporter	Used by Director and Transporters to communicate with the Transporter. Must be opened on the Transporter machine.
9448 - 10000	Transporter	Used by Transporters for cross-Transporter data transfer. Must be opened on the Transporter machine.
VMware		
443	vCenter Server, ESXi host	Used by Director and Transporters to access VMware infrastructure. Must be opened on vCenter Servers and ESXi hosts.
902	ESXi hosts	Used by Transporters to access VMware infrastructure. Must be opened on ESXi hosts.
Hyper-V		
137 - 139	Hyper-V hosts	Used by Director to upload files and install configuration service. Must be opened on Hyper-V servers.
445	Hyper-V hosts	Used by Director to upload files and install configuration service.
5986 (opens automatically)	Hyper-V hosts	Used by Transporter to add a host to inventory and establish a connection with it.

9445 (opens automatically)	Hyper-V hosts	Used by Director to upload files and install configuration service. Must be opened on Hyper-V host if NAKIVO Backup & Replication is installed on a host and this host is added to inventory simultaneously.
9446 (opens automatically)	Hyper-V hosts	Used by Director and Transporters to communicate with the Transporter. Must be opened on Used by Transporters for cross-Transporter data transfer. Must be opened on the Transporter machine. the Transporter machine.
9448 -10000 (opens automatically)	Hyper-V hosts	Used by Transporters for cross-Transporter data transfer. Must be opened on the Transporter machine.
Physical machine (Windows)		
445	Windows machine	Used by Director to upload files and install configuration service via SMB.
9446 (opens automatically)	Windows machine	Used to create the Transporter installed by default.
Physical machine (Linux)		
22	Linux machine	Used by Director to access a Linux physical machine via SSH.
9446 (opens automatically)	Linux machine	Used to create the Transporter installed by default.

Network Conditions

NAKIVO Backup & Replication has been tested to work in the following minimal network conditions:

- **Latency (RTT)**: Up to 250 ms
- **Packet loss**: Up to 1 %
- **Bandwidth**: 1 Mb/s or higher
- **ICMP ping traffic:** It should be allowed on all hosts on which NAKIVO Backup & Replication components are installed as well as on all source and target hosts.

Web Browsers

NAKIVO Backup & Replication user interface can be accessed through the following web browsers:

- Google Chrome: Version 80
- Mozilla Firefox: Version 74

Supported ASUSTOR NAS Devices

NAKIVO Backup & Replication supports the following ASUSTOR NAS devices :

Director and Onboard Transporter

- AS3102T
- AS3102T v2
- AS3104T
- AS3202T
- AS3204T
- AS3204T v2
- AS4002T
- AS4004T
- AS5202T
- AS5304T
- AS5002T
- AS5004T
- AS5008T
- AS5010T
- AS6102T
- AS6104T
- AS6302T
- AS5102T
- AS5104T
- AS5108T
- AS5110T
- AS6202T
- AS6204T
- AS6208T
- AS6210T
- AS6404T
- AS6204RS / AS6204RD
- AS-609RS / AS-609RD
- AS7004T
- AS7008T
- AS7010T
- AS6212RD
- AS7009RD / AS7009RDX
- AS7012RD / AS7012RDX
- AS-602T
- AS-604RS / AS-604RD

- AS-604T
- AS-606T
- AS-608T
- AS6508T
- AS6510T
- AS7110T
- AS6602T
- AS6604T
- AS7116RDX
- AS7112RDX

Transporter Only

- AS1002T
- AS1002T v2
- AS1004T
- AS1004T v2

For minimum hardware requirements, refer to “Network Attached Storage” on page 70.

Supported NETGEAR NAS Devices

NAKIVO Backup & Replication supports the following NETGEAR NAS devices:

Director and Onboard Transporter

- RN51600
- RN51661D
- RN51661E
- RN51662D
- RN51662E
- RN51663D
- RN51663E
- RN51664E
- ReadyNAS 524X
- ReadyNAS 526X
- ReadyNAS 528X
- ReadyNAS 626X
- ReadyNAS 628X
- RN716X
- RN628X
- RN626X
- RN528X
- RN526X
- RN524X
- RN31600
- RN31661D
- RN31661E
- RN31662D
- RN31662E
- RN31663D
- RN31663E
- RN31664E
- ReadyNAS 422
- ReadyNAS 424
- ReadyNAS 426
- ReadyNAS 428
- RN516
- RN426
- RN424
- RN422
- RN31400

- RN31421D
- RN31441D
- RN31441E
- RN31442D
- RN31442E
- RN31443D
- RN31443E
- RN316
- RN31200
- RN31211D
- RN31212D
- RN31221D
- RN31221E
- RN31222D
- RN31222E
- RN31223D
- RN314
- RN312
- RN322121E
- RN322122E
- RN322123E
- RN322124E
- RN32261E
- RN32262E
- RN32263E
- RN4220S
- RN4220X
- RN422X122
- RN422X123
- RN422X124
- RN422X62E
- RN422X63E
- RN422X64E
- RR2304
- RN21241D
- RN21241E
- RN21243D
- RN21243E
- RN3130
- RN31342E
- RN3138
- RN3220
- RR2312

- RR3312
- RN4220
- RR4312X
- RR4312S
- RR4360X
- RR4360S

Transporter Only

- RN102
- RN10200
- RN10211D
- RN10221D
- RN10222D
- RN10223D
- RN104
- RN10400
- RN10421D
- RN10441D
- RN10442D
- RN10443D

For minimum hardware requirements, refer to “Network Attached Storage” on page 70

Supported QNAP NAS Devices

NAKIVO Backup & Replication supports the following QNAP NAS Devices:

Director and Onboard Transporter

- HS-251+
- HS-453DX
- TS-251
- TS-251+
- TS-251A
- TS-251B
- TS-253Be
- TS-328
- TS-332X
- TS-351
- TS-431P
- TS-431P2
- TS-431X
- TS-431X2
- TS-431XeU
- TS-432XU
- TS-432XU-RP
- TS-451
- TS-451+
- TS-451A
- IS-400 Pro
- IS-453S
- TBS-453A
- TBS-453DX
- TS-128A
- TS-131P
- TS-231P
- TS-231P2
- TS-253 Pro
- TS-253A
- TS-253B
- TS-228A
- TS-451U
- TS-453 mini
- TS-453 Pro
- TS-453A

- TS-453B
- TS-453Be
- TS-453Bmini
- TS-453BT3
- TS-453BU
- TS-453BU-RP
- TS-453U
- TS-453U-RP
- TS-463U
- TS-463U-RP
- TS-463XU
- TS-463XU-RP
- TS-473
- TS-563
- TS-653 Pro
- TS-653A
- TS-653B
- TS-653B
- TS-673
- TS-677
- TS-832X
- TS-832XU
- TS-832XU-RP
- TS-853 Pro
- TS-853A
- TS-853BU
- TS-853BU-RP
- TS-853U
- TS-853U-RP
- TS-863U
- TS-863U-RP
- TS-863XU
- TS-863XU-RP
- TS-873
- TS-873U
- TS-873U-RP
- TS-877
- TS-877XU
- TS-877XU-RP
- TS-883XU
- TS-883XU-RP
- TS-932X
- TS-963X

- TS-977XU
- TS-977XU-RP
- TS-983XU
- TS-983XU-RP
- TS-1232XU
- TS-1232XU-RP
- TS-1253BU
- TS-1253BU-RP
- TS-1253U
- TS-1253U-RP
- TS-1263U-RP
- TS-1263U
- TS-1263XU
- TS-1263XU-RP
- TS-1273U
- TS-1273U-RP
- TS-1277
- TS-1277XU-RP
- TS-1283XU-RP
- TS-1635AX
- TS-1673U
- TS-1673U-RP
- TS-1677X
- TS-1677XU-RP
- TS-1683XU-RP
- TS-1685
- TS-2477XU-RP
- TS-2483XU-RP
- TVS-463
- TVS-471
- TVS-472XT
- TVS-473e
- TVS-473
- TVS-663
- TVS-671
- TVS-672XT
- TVS-673
- TVS-673e
- TVS-682
- TVS-682T
- TVS-863
- TVS-863+
- TVS-871

- TVS-871T
- TVS-871U-RP
- TVS-872XT
- TVS-872XU
- TVS-872XU-RP
- TVS-873e
- TVS-873
- TVS-882
- TVS-882T
- TVS-882ST2
- TVS-882BR
- TVS-882BRT3
- TVS-882ST3
- TVS-951X
- TVS-972XU
- TVS-972XU-RP
- TVS-1271U-RP
- TVS-1272XU-RP
- TVS-1282
- TVS-1282T
- TVS-1282T3
- TVS-1582TU
- TVS-1672XU-RP
- TVS-2472XU-RP
- SS-EC1279U-SAS-RP
- SS-EC1879U-SAS-RP
- SS-EC2479U-SAS-RP
- TDS-16489U
- TES-3085U
- TES-1885U
- TS-EC880U
- TS-EC880U R2
- TS-EC1280U
- TS-EC1280U R2
- TS-EC1680U
- TS-EC1680U R2
- TS-EC2480U
- TS-EC2480U R2
- TVS-EC880
- TVS-EC1080
- TVS-EC1080+
- TVS-EC1280U-SAS-RP
- TVS-EC1580MU-SAS-RP

- TVS-EC1680U-SAS-RP
- TVS-EC1680U-SAS-RP R2
- TVS-EC2480U-SAS-RP
- TVS-EC2480U-SAS-RP R2
- TVS-EC2480U-SAS-RP R2
- TVS-EC1580MU-SAS-RP R2
- TVS-EC1280U-SAS-RP R2
- TDS-16489U-SE1-R2
- TDS-16489U-SE2-R2
- TDS-16489U-SF2-R2
- TDS-16489U-SF3-R2
- TS-2888X-W2195-512G
- TS-2888X-W2195-256G
- TS-2888X-W2195-128G
- TS-2888X-W2175-512G
- TS-2888X-W2175-256G
- TS-2888X-W2175-128G
- TS-2888X-W2145-512G
- TS-2888X-W2145-256G
- TS-2888X-W2145-128G
- TS-2888X-W2133-64G
- TS-2888X-W2123-32G
- ES2486dc
- TS-1886XU-RP
- TS-230
- TS-251C
- TS-251D
- TS-253D
- TS-451DeU
- TS-453D
- TS-653B
- TS-653D
- TS-h1277XU-RP
- TS-h1283XU-RP
- TS-h977XU-RP
- TVS-472XT-PT
- TVS-672N
- TVS-872N
- TVS-EC2480U-SAS-RP-R2
- TS-431P3
- TS-231P3
- TS-431X3
- TS-h686-D1602

- TS-h886-D1622
- TS-873AU
- TS-873AU-RP
- TS-1273AU-RP
- TS-1673AU-RP
- TS-932PX
- GM-1001
- TS-432PXU
- TS-432PXU-RP
- TS-832PXU
- TS-832PXU-RP
- TS-1232PXU-RP
- TS-451D2
- TS-h2490FU-7232P-64G
- TS-h2490FU-7302P-128G
- TS-h1886XU-RP
- TS-h1683XU-RP
- TS-h2483XU-RP
- TVS-h1288X
- TVS-h1688X
- TS-h973AX-8G
- TS-h973AX-32G
- TS-832PX
- TS-h3088XU-RP-W1270-64G
- TS-h3088XU-RP-W1250-32G
- TS-453DU-4G

Transporter Only

- TS-131P
- TS-231P
- TS-431P
- TS-431X

For minimum hardware requirements, refer to “Network Attached Storage” on page 70.

Supported Synology NAS Devices

NAKIVO Backup & Replication supports the following Synology NAS devices:

Director and Onboard Transporter

- FS3017
- FS2017
- FS1018
- RS18017xs+
- RS18016xs+
- RS10613xs+
- RS4017xs+
- RS3618xs
- RS3617xs+
- RS3617RPxs
- RS3617xs
- RS3614xs+
- RS3614RPxs
- RS3614xs
- RS3413xs+
- RS3412RPxs
- RS3412xs
- RS3411RPxs
- RS3411xs
- RS2818RP+
- RS2418RP+
- RS2418+
- RS2416RP+
- RS2416+
- RS2414RP+
- RS2414+
- RS2212RP+
- RS2212+
- RS2211RP+
- RS2211+
- RS1619xs+
- RS1219+
- RS818RP+
- RS818+
- RS816
- RS815RP+

- RS815+
- RS815
- RS814RP+
- RS814+
- RS814
- RS812RP+
- RS812+
- RS812
- RS810RP+
- RS810+
- RC18015xs+
- DS3617xs
- DS3615xs
- DS3612xs
- DS3611xs
- DS3018xs
- DS2415+
- DS2413+
- DS2411+
- DS2015xs
- DS1819+
- DS1817+
- DS1817
- DS1815+
- DS1813+
- DS1812+
- DS1618+
- DS1517+
- DS1517
- DS1515+
- DS1515
- DS1513+
- DS1512+
- DS1511+
- DS918+
- DS916+
- DS718+
- DS716+II
- DS716+
- DS715
- DS713+
- DS712+
- DS710+

- DS418
- DS418play
- DS418j
- DS416
- DS416play
- DS415+
- DS414
- DS412+
- DS411+II
- DS411+
- DS218+
- DS218
- DS218play
- DS216+II
- DS216+
- DS216play
- DS215+
- DS214+
- DS118
- DS116
- DS1019+
- DS2419+
- DS420+
- DS420j
- DS620slim
- DS720+
- DS920+
- FS3400
- FS3600
- FS6400
- RS819
- RS820+
- RS820RP+
- SA3200D
- SA3400
- SA3600
- DS1520+
- DS1621+
- DS1621xs+
- DS1821+
- DS220
- RS1221+
- RS1221RP+

- RS2421+
- RS2421RP+

Transporter Only

- RS217
- RS214
- DS416slim
- DS416j
- DS414slim
- DS414j
- DS218j
- DS216
- DS216j
- DS215j
- DS214
- DS213j
- DS115
- DS114
- DS220j
- DS419slim

Important

Backup and recovery of Microsoft 365 accounts is not supported on Synology NAS devices with ARMv8 CPU architecture.

For minimum hardware requirements, refer to “Network Attached Storage” on page 70.

Supported Western Digital NAS Devices

NAKIVO Backup & Replication supports the following Western Digital NAS devices for Director and Onboard installation:

- MyCloud DL2100
- MyCloud DL4100
- MyCloud PR2100
- MyCloud PR4100

For minimum hardware requirements, refer to “Network Attached Storage” on page 70.

Installing NAKIVO Backup & Replication

Refer to the sections below to learn how to install NAKIVO Backup & Replication:

- "Deploying VMware Virtual Appliance" on page 92
- "Deploying Nutanix AHV Virtual Appliance" on page 107
- "Installing on Windows" on page 116
- "Installing on Linux" on page 127
- "Installing on Synology NAS" on page 136
- "Installing on QNAP NAS" on page 143
- "Installing on Western Digital NAS" on page 153
- "Installing on ASUSTOR NAS" on page 148
- "Installing on NETGEAR ReadyNAS" on page 155
- "Deploying Amazon Machine Image in Amazon EC2" on page 115

Deploying VMware Virtual Appliance

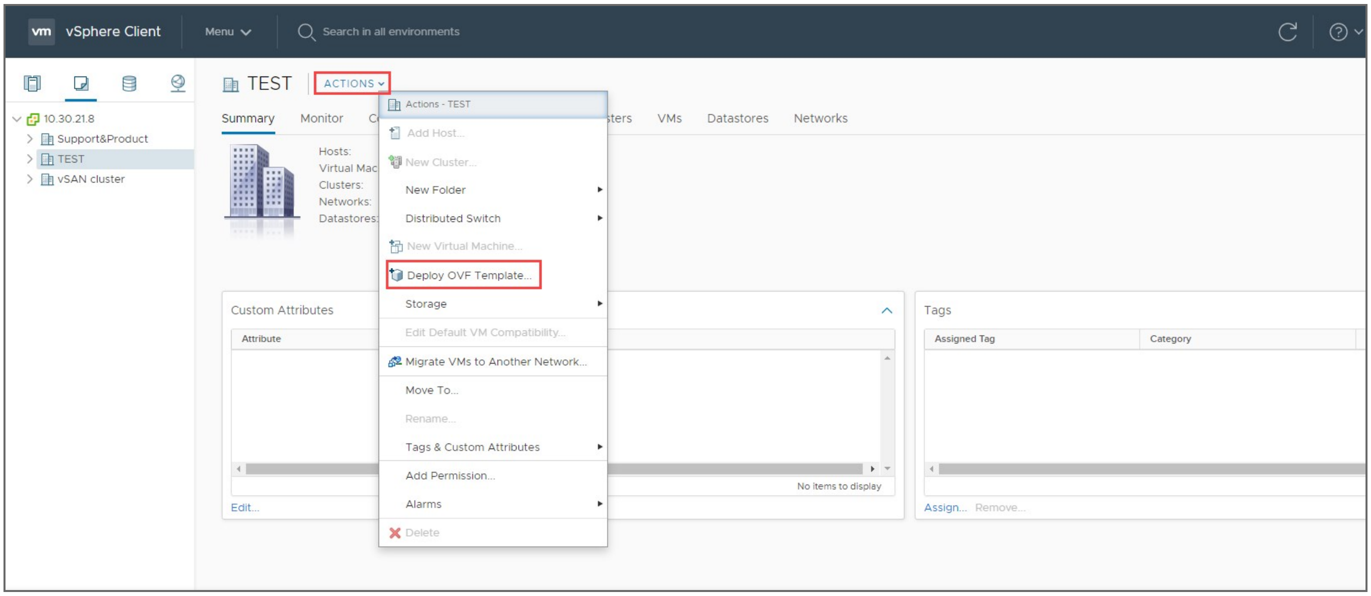
NAKIVO Backup & Replication offers the following VA deployment options:

- Full Solution
- Full Solution without Backup Repository
- Transporter-only
- Transporter with Backup Repository
- Multi-tenant Director

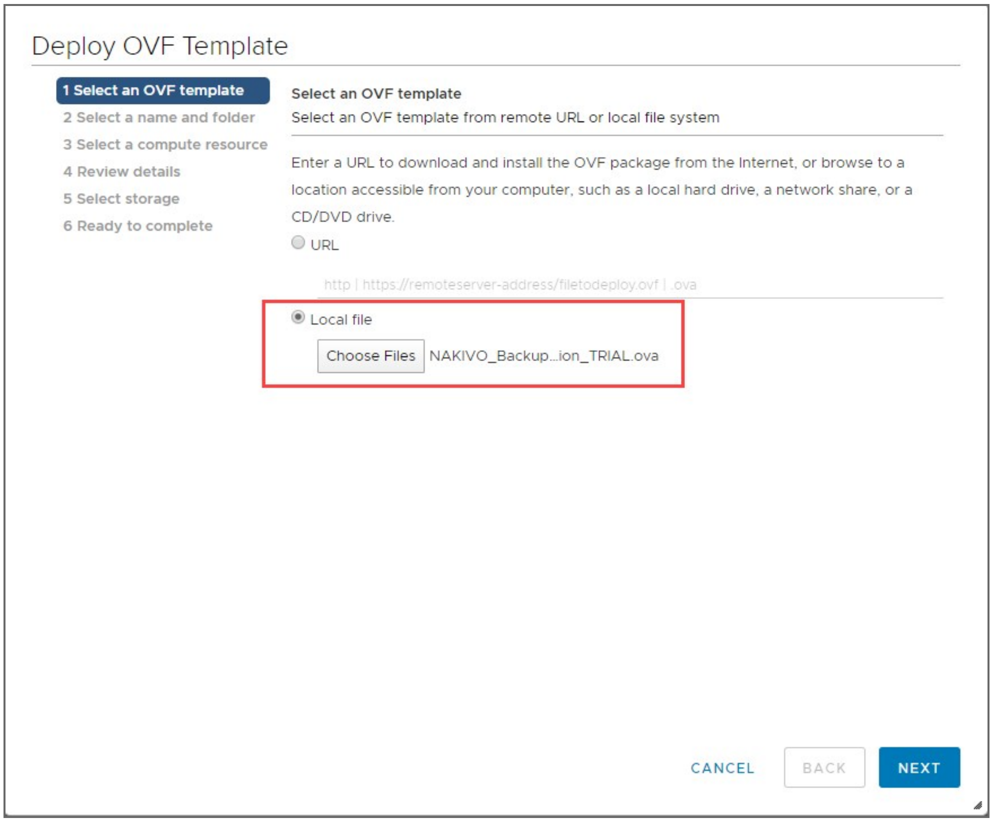
The Virtual Appliance (VA) has two disks: the first (30 GB) contains a Linux OS with NAKIVO Backup & Replication, and the second (500 GB) is used as a Backup Repository. If you deploy the Virtual Appliance disks using the **Thin Provision** option, then the disks will not reserve space on your datastore and will only consume space when actual data (such as your backups) is written to disks.

Deploying Virtual Appliance with vSphere Web Client

1. Download NAKIVO Backup & Replication VA.
2. Log in to your vSphere vCenter with the vSphere Web Client.
3. Select **Deploy OVF Template** from the **Actions** menu. Note that the Client Integration Plug-in must be installed to enable OVF functionality.



4. On the **Select an OVF template** page of the **Deploy OVF Template** wizard, select **Local file** and upload the VA file (.ova) you've downloaded. Click **Next**.



Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage
6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

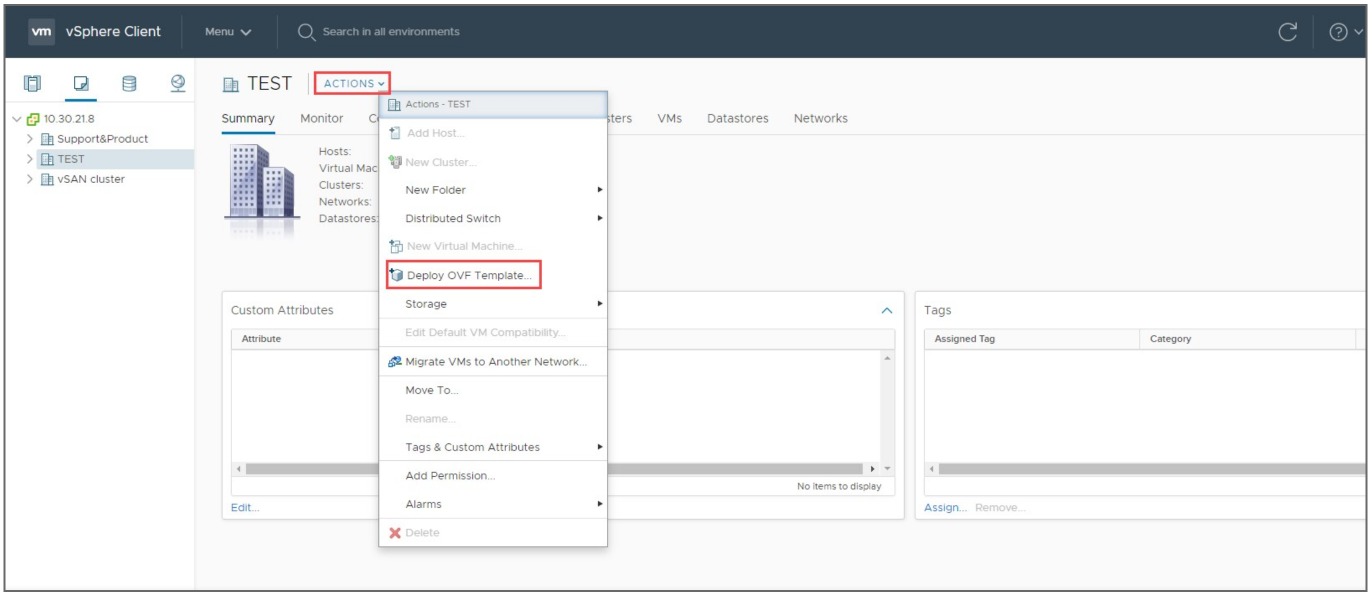
○ URL

http | https://remoteserver-address/filetodeploy.ovf | .ova

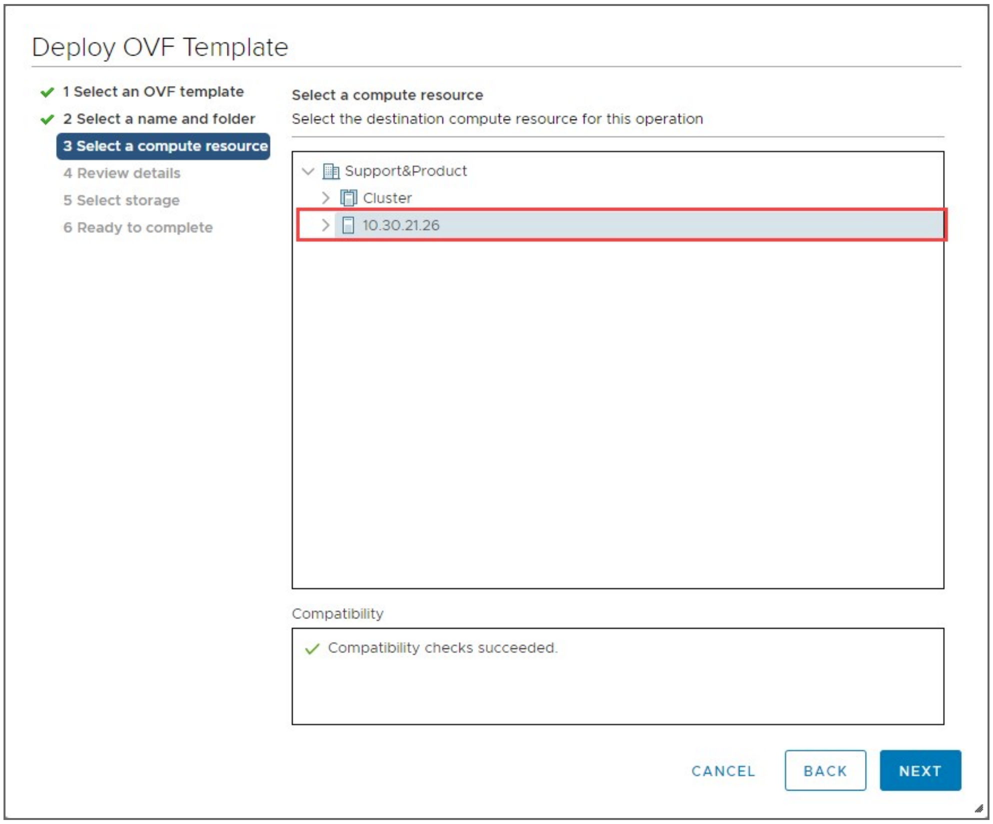
● Local file

Choose Files NAKIVO_Backup...ion_TRIAL.ova

5. On the **Select a name and folder** page, specify a unique name and target location for the Virtual Appliance. Click **Next**.



6. On the **Select a computer resource** page, select the resource pool within which you would like to deploy the Virtual Appliance and click **Next**.



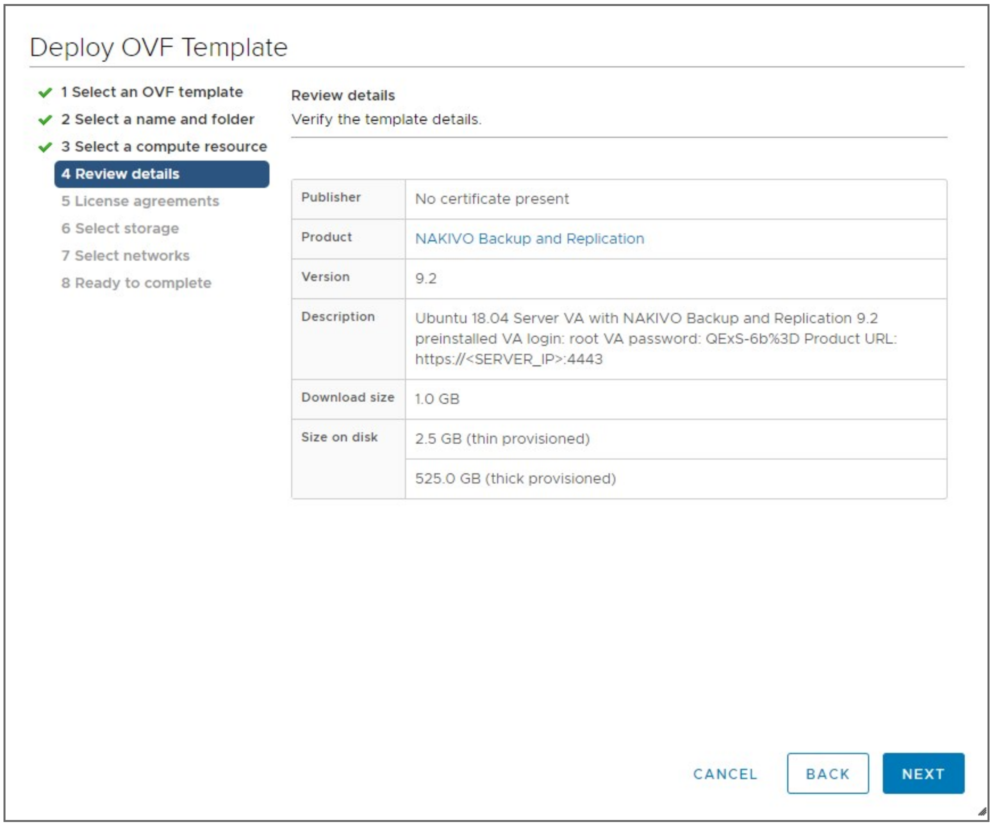
Select a compute resource

Select the destination compute resource for this operation

Compatibility

✓ Compatibility checks succeeded.

7. On the **Review details** page, review the template details and click **Next**.

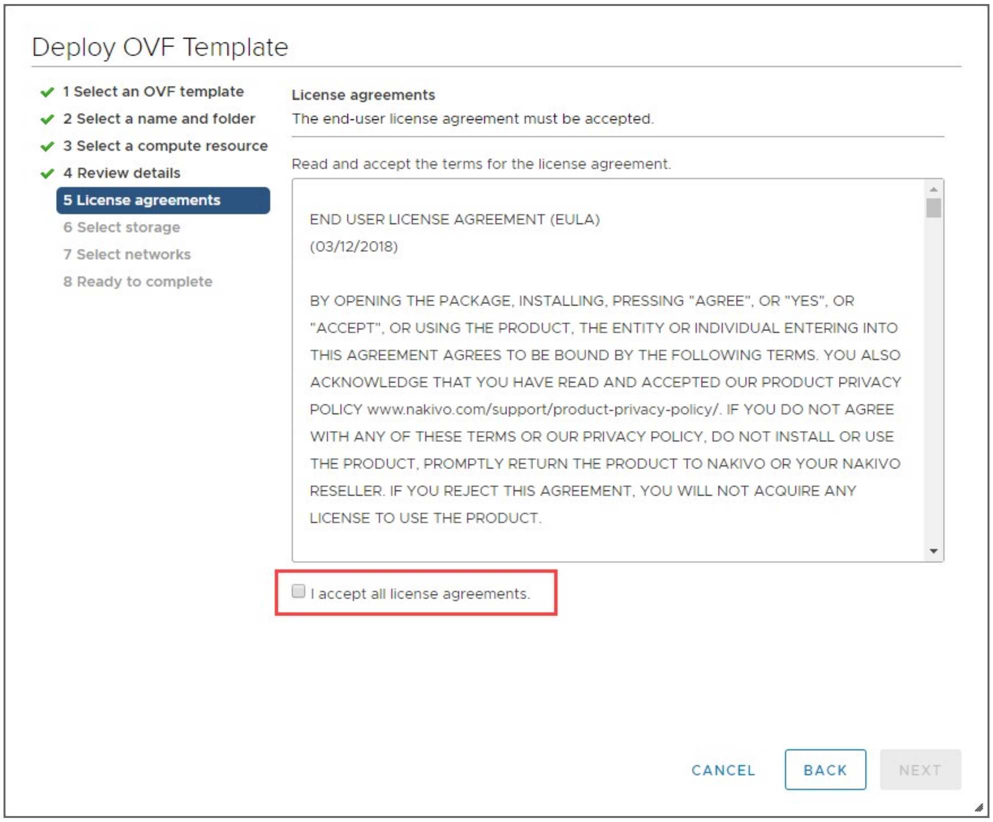


Review details

Verify the template details.

Publisher	No certificate present
Product	NAKIVO Backup and Replication
Version	9.2
Description	Ubuntu 18.04 Server VA with NAKIVO Backup and Replication 9.2 preinstalled VA login: root VA password: QExS-6b%3D Product URL: https://<SERVER_IP>:4443
Download size	1.0 GB
Size on disk	2.5 GB (thin provisioned)
	525.0 GB (thick provisioned)

8. On the **License agreements** page, read the end-user license agreement (EULA). If you agree to its terms, select **I accept all license agreements** and then click **Next**.



Deploy OVF Template

License agreements

The end-user license agreement must be accepted.

Read and accept the terms for the license agreement.

END USER LICENSE AGREEMENT (EULA)

(03/12/2018)

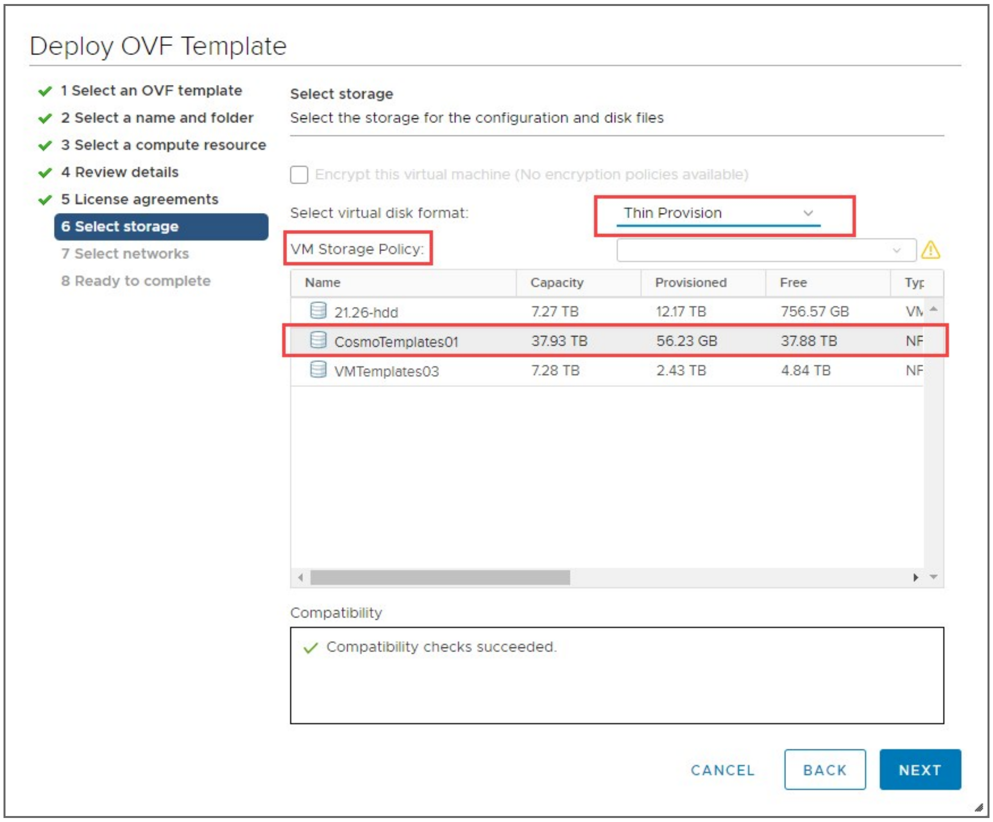
BY OPENING THE PACKAGE, INSTALLING, PRESSING "AGREE", OR "YES", OR "ACCEPT", OR USING THE PRODUCT, THE ENTITY OR INDIVIDUAL ENTERING INTO THIS AGREEMENT AGREES TO BE BOUND BY THE FOLLOWING TERMS. YOU ALSO ACKNOWLEDGE THAT YOU HAVE READ AND ACCEPTED OUR PRODUCT PRIVACY POLICY www.nakivo.com/support/product-privacy-policy/. IF YOU DO NOT AGREE WITH ANY OF THESE TERMS OR OUR PRIVACY POLICY, DO NOT INSTALL OR USE THE PRODUCT, PROMPTLY RETURN THE PRODUCT TO NAKIVO OR YOUR NAKIVO RESELLER. IF YOU REJECT THIS AGREEMENT, YOU WILL NOT ACQUIRE ANY LICENSE TO USE THE PRODUCT.

□ I accept all license agreements.

9. On the **Select storage** page, select a datastore in which you would like to keep the Virtual Appliance disk, virtual disk format (*Thin Provisioning* is recommended), VM storage policy and click **Next**.

   Important

   If you use thick provisioning instead of thin provisioning, keep in mind that NAKIVO Backup & Replication can take up to 0,5 TB of data. Check to see if it is 0,5 TB by default for all cases.



Deploy OVF Template

Select storage

Select the storage for the configuration and disk files

□ Encrypt this virtual machine (No encryption policies available)

Select virtual disk format: Thin Provision

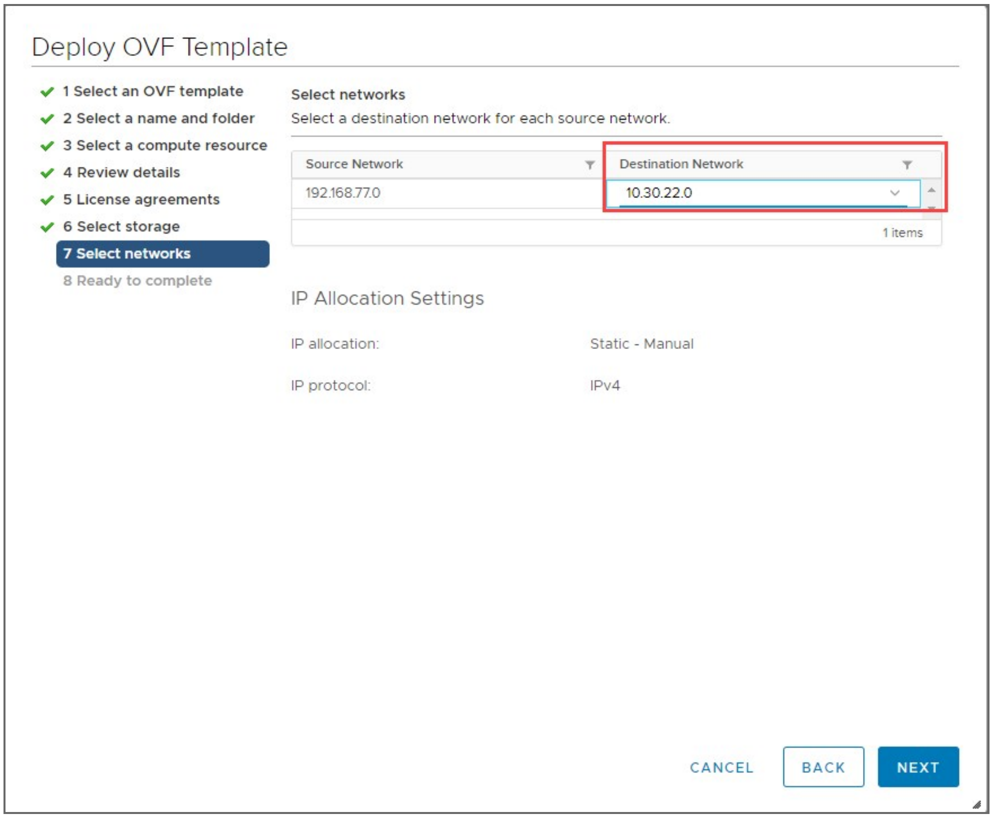
VM Storage Policy:

Name	Capacity	Provisioned	Free	Typ
21.26-hdd	7.27 TB	12.17 TB	756.57 GB	VM
CosmoTemplates01	37.93 TB	56.23 GB	37.88 TB	NF
VMTemplates03	7.28 TB	2.43 TB	4.84 TB	NF

Compatibility

✓ Compatibility checks succeeded.

10. On the **Select networks** page, select a network to which the Virtual Appliance will be connected. Opting for a network with DHCP and Internet access is recommended. Click **Next**.



Deploy OVF Template

Select networks

Select a destination network for each source network.

Source Network	Destination Network
192.168.77.0	10.30.22.0

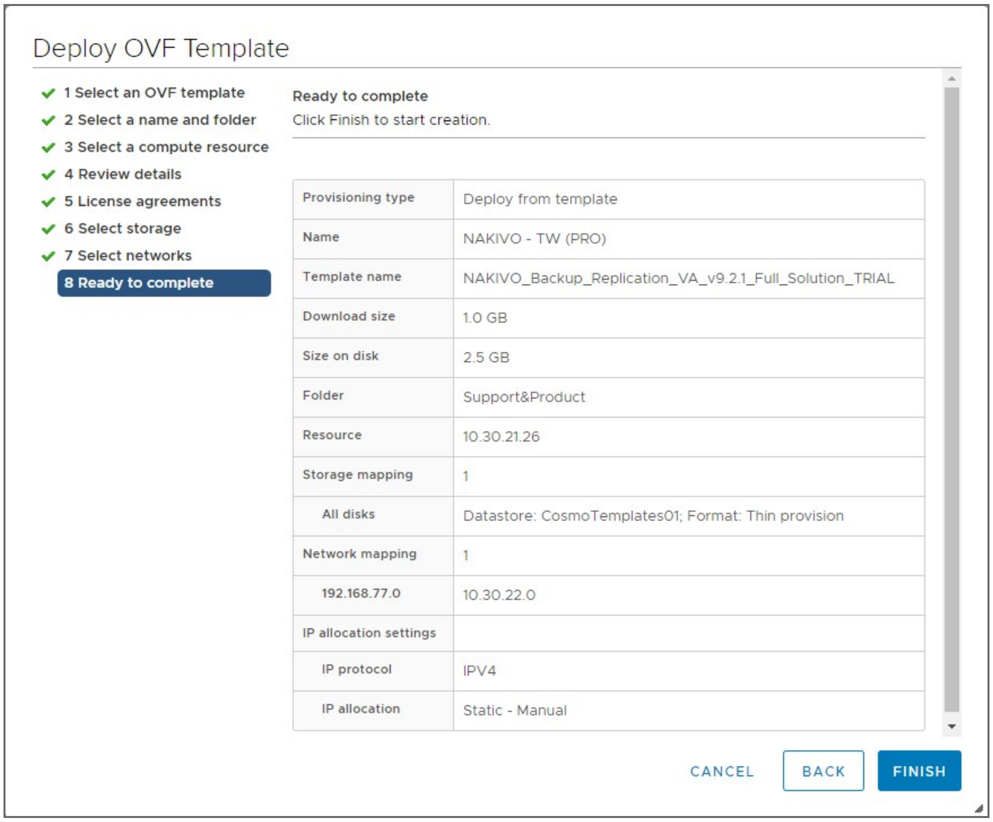
1 items

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

11. On the **Ready to complete** page, review the summary of the setups you have configured and click **Finish** to complete deployment.



Ready to complete

Click Finish to start creation.

Provisioning type	Deploy from template
Name	NAKIVO - TW (PRO)
Template name	NAKIVO_Backup_Replication_VA_v9.2.1_Full_Solution_TRIAL
Download size	1.0 GB
Size on disk	2.5 GB
Folder	Support&Product
Resource	10.30.21.26
Storage mapping	1
All disks	Datastore: CosmoTemplates01; Format: Thin provision
Network mapping	1
192.168.77.0	10.30.22.0
IP allocation settings	
IP protocol	IPV4
IP allocation	Static - Manual

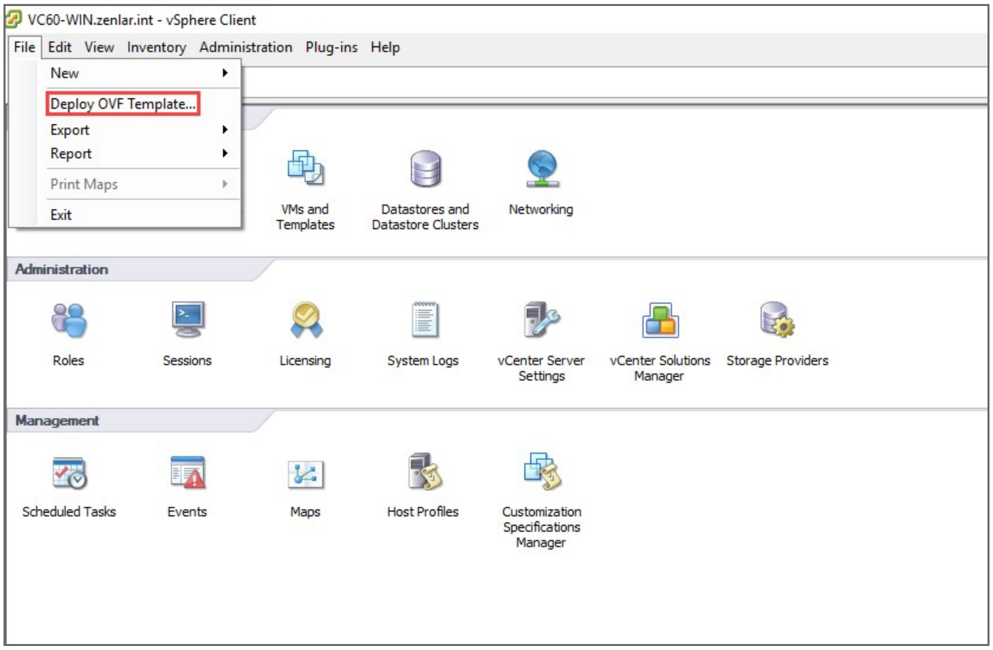
After the Virtual Appliance is deployed, you may need to configure it.

Important

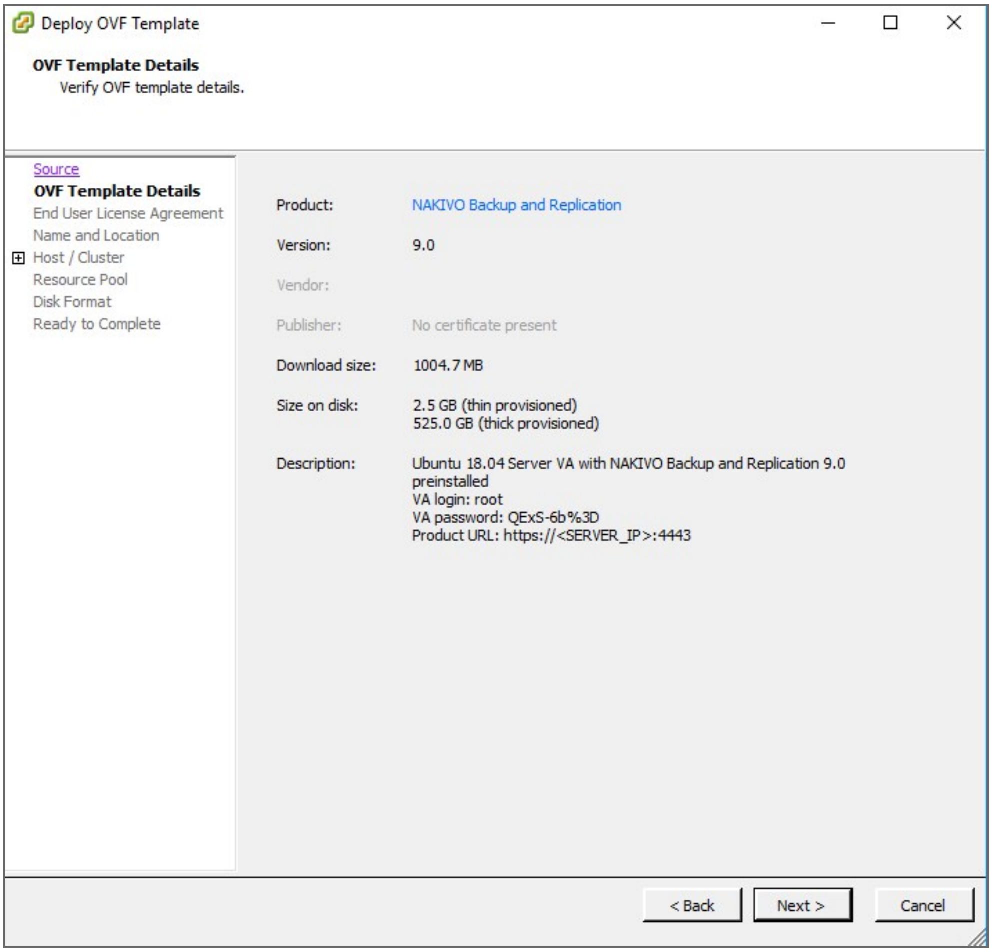
If you plan to expose the Virtual Appliance to the Internet, change the default credentials and set up a login and password for the Web interface

Deploying Virtual Appliance with vSphere Client

1. Download NAKIVO Backup & Replication VA.
2. Log in to your vSphere vCenter with the vSphere Client, go to **File** in the top menu and select **Deploy OV Template.**



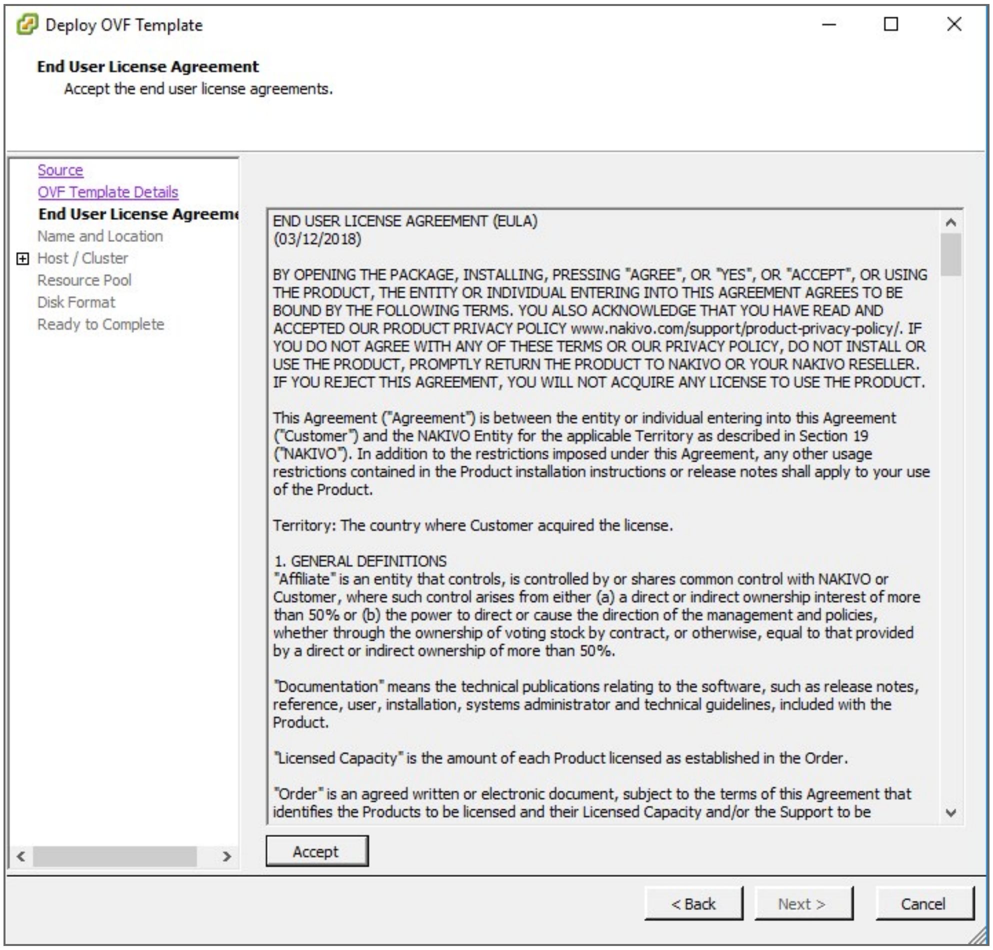
3. On the **Source** page of the **Deploy OVF Template** wizard, select and locate the file with the template. Click **Next**.
4. On the **OVF Template Details** page, review the template details and click **Next**.



OVF Template Details
Verify OVF template details.

Product:	NAKIVO Backup and Replication
Version:	9.0
Vendor:	
Publisher:	No certificate present
Download size:	1004.7 MB
Size on disk:	2.5 GB (thin provisioned) 525.0 GB (thick provisioned)
Description:	Ubuntu 18.04 Server VA with NAKIVO Backup and Replication 9.0 preinstalled VA login: root VA password: QExS-6b%3D Product URL: https://<SERVER_IP>:4443

5. On the **End User License Agreement** page, read the license agreement. If you agree to its terms, click **Accept** and then click **Next.**



END USER LICENSE AGREEMENT (EULA)
(03/12/2018)

BY OPENING THE PACKAGE, INSTALLING, PRESSING "AGREE", OR "YES", OR "ACCEPT", OR USING THE PRODUCT, THE ENTITY OR INDIVIDUAL ENTERING INTO THIS AGREEMENT AGREES TO BE BOUND BY THE FOLLOWING TERMS. YOU ALSO ACKNOWLEDGE THAT YOU HAVE READ AND ACCEPTED OUR PRODUCT PRIVACY POLICY www.nakivo.com/support/product-privacy-policy/. IF YOU DO NOT AGREE WITH ANY OF THESE TERMS OR OUR PRIVACY POLICY, DO NOT INSTALL OR USE THE PRODUCT, PROMPTLY RETURN THE PRODUCT TO NAKIVO OR YOUR NAKIVO RESELLER. IF YOU REJECT THIS AGREEMENT, YOU WILL NOT ACQUIRE ANY LICENSE TO USE THE PRODUCT.

This Agreement ("Agreement") is between the entity or individual entering into this Agreement ("Customer") and the NAKIVO Entity for the applicable Territory as described in Section 19 ("NAKIVO"). In addition to the restrictions imposed under this Agreement, any other usage restrictions contained in the Product installation instructions or release notes shall apply to your use of the Product.

Territory: The country where Customer acquired the license.

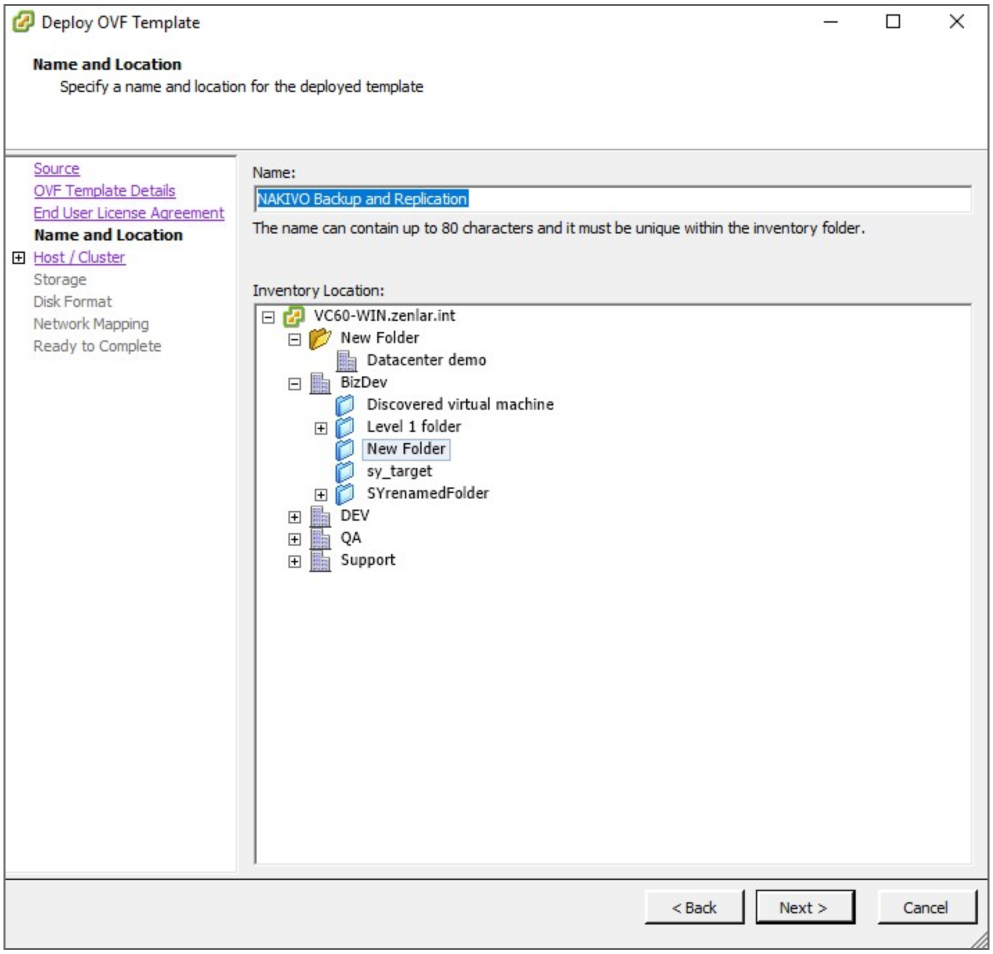
1. GENERAL DEFINITIONS
"Affiliate" is an entity that controls, is controlled by or shares common control with NAKIVO or Customer, where such control arises from either (a) a direct or indirect ownership interest of more than 50% or (b) the power to direct or cause the direction of the management and policies, whether through the ownership of voting stock by contract, or otherwise, equal to that provided by a direct or indirect ownership of more than 50%.

"Documentation" means the technical publications relating to the software, such as release notes, reference, user, installation, systems administrator and technical guidelines, included with the Product.

"Licensed Capacity" is the amount of each Product licensed as established in the Order.

"Order" is an agreed written or electronic document, subject to the terms of this Agreement that identifies the Products to be licensed and their Licensed Capacity and/or the Support to be

6. On the **Name and Location** page, specify a name and location for the deployed VA and click **Next**.



Deploy OVF Template

Name and Location

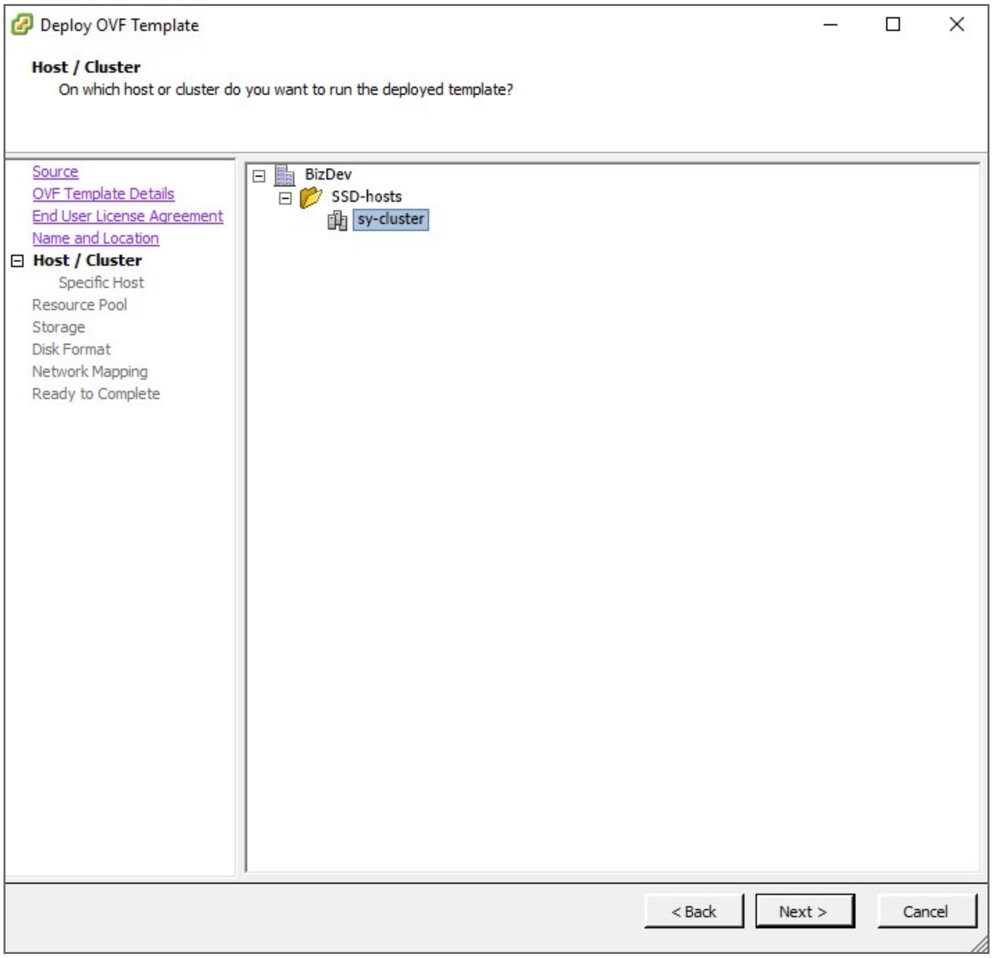
Specify a name and location for the deployed template

Name: NAKIVO Backup and Replication

The name can contain up to 80 characters and it must be unique within the inventory folder.

Inventory Location:

7. On the **Host/Cluster** page, select the host or cluster on which you wish to run the deployed template and click **Next**.

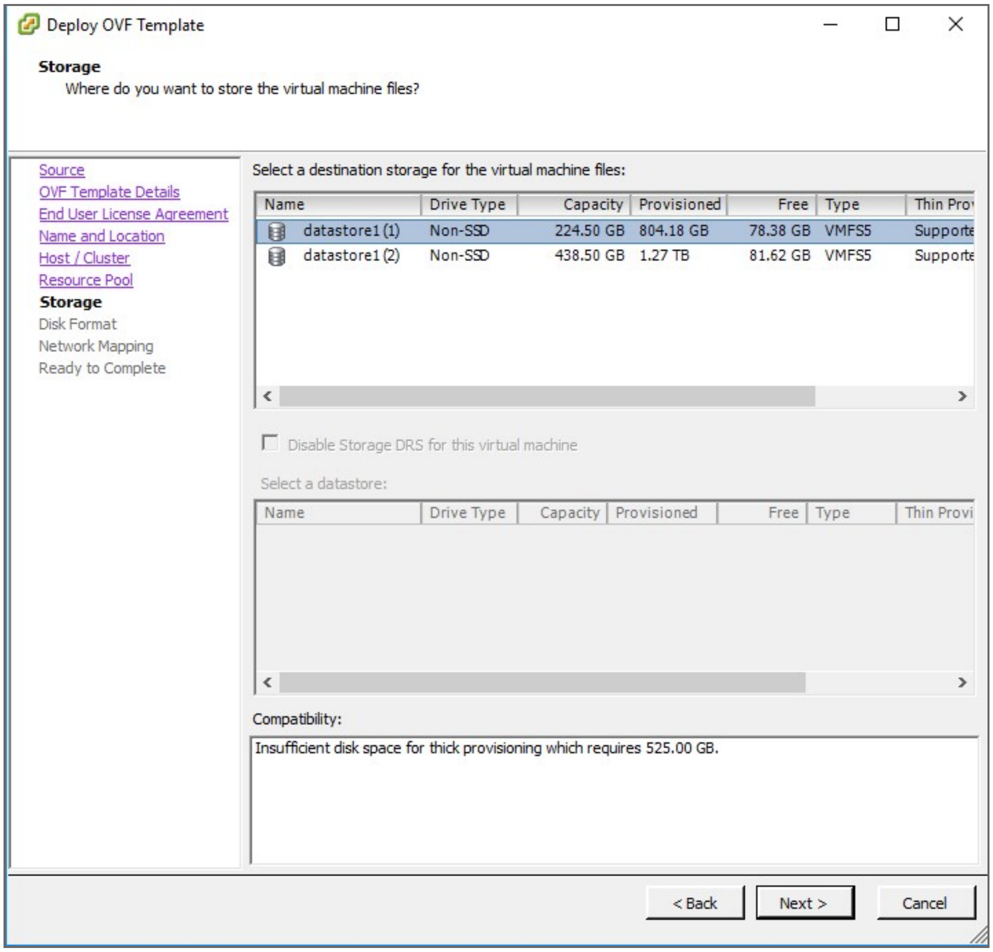


Deploy OVF Template

Host / Cluster

On which host or cluster do you want to run the deployed template?

8. On the **Storage** page, select a datastore where you would like to keep the VA disk and click **Next**.



Select a destination storage for the virtual machine files:

Name	Drive Type	Capacity	Provisioned	Free	Type	Thin Pro
datastore1 (1)	Non-SSD	224.50 GB	804.18 GB	78.38 GB	VMFS5	Supporte
datastore1 (2)	Non-SSD	438.50 GB	1.27 TB	81.62 GB	VMFS5	Supporte

☐ Disable Storage DRS for this virtual machine

Select a datastore:

Name	Drive Type	Capacity	Provisioned	Free	Type	Thin Provi

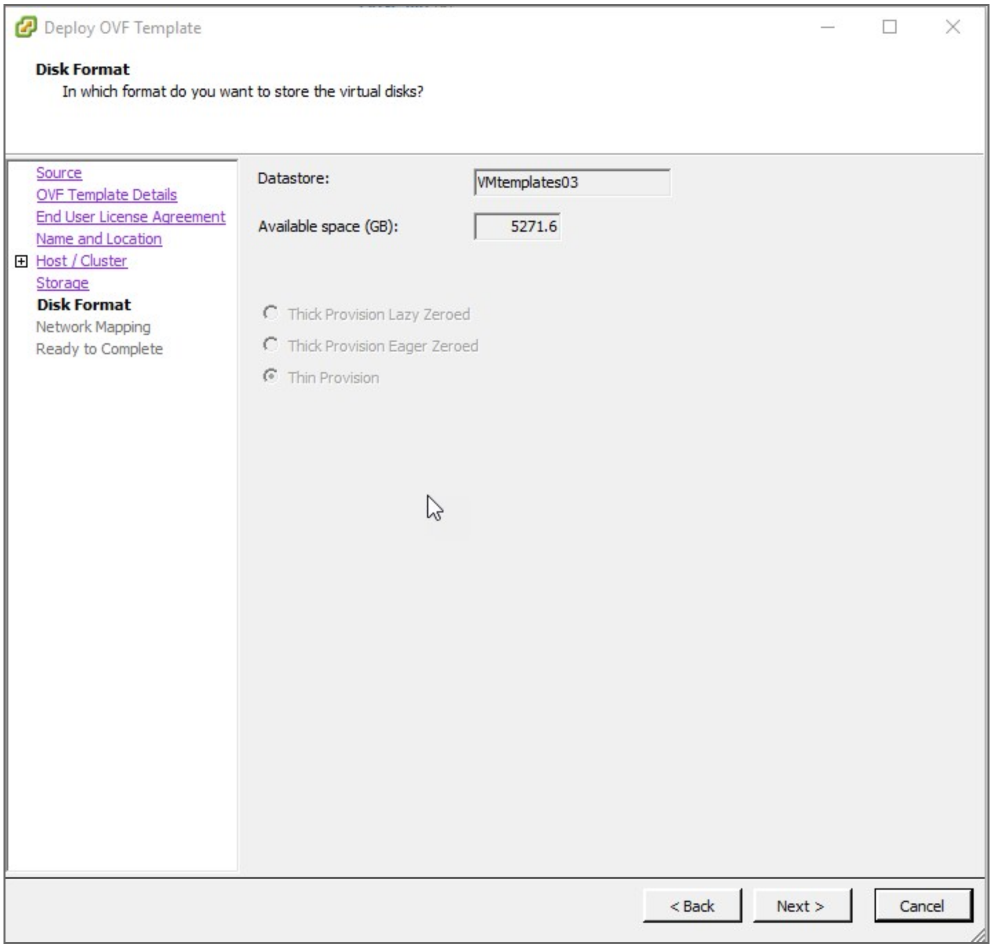
Compatibility:

Insufficient disk space for thick provisioning which requires 525.00 GB.

9. On the **Disk Format** page, select a virtual disk format (**Thin Provision** is recommended) and click **Next**.

Important

If you wish to select one of the **Thick Provision** options instead of **Thin Provision**, keep in mind that NAKIVO Backup & Replication can take 0,5 TB of data. Check to see if it is 0,5 TB by default for all cases.



Deploy OVF Template

Disk Format

In which format do you want to store the virtual disks?

Datastore: VMtemplates03

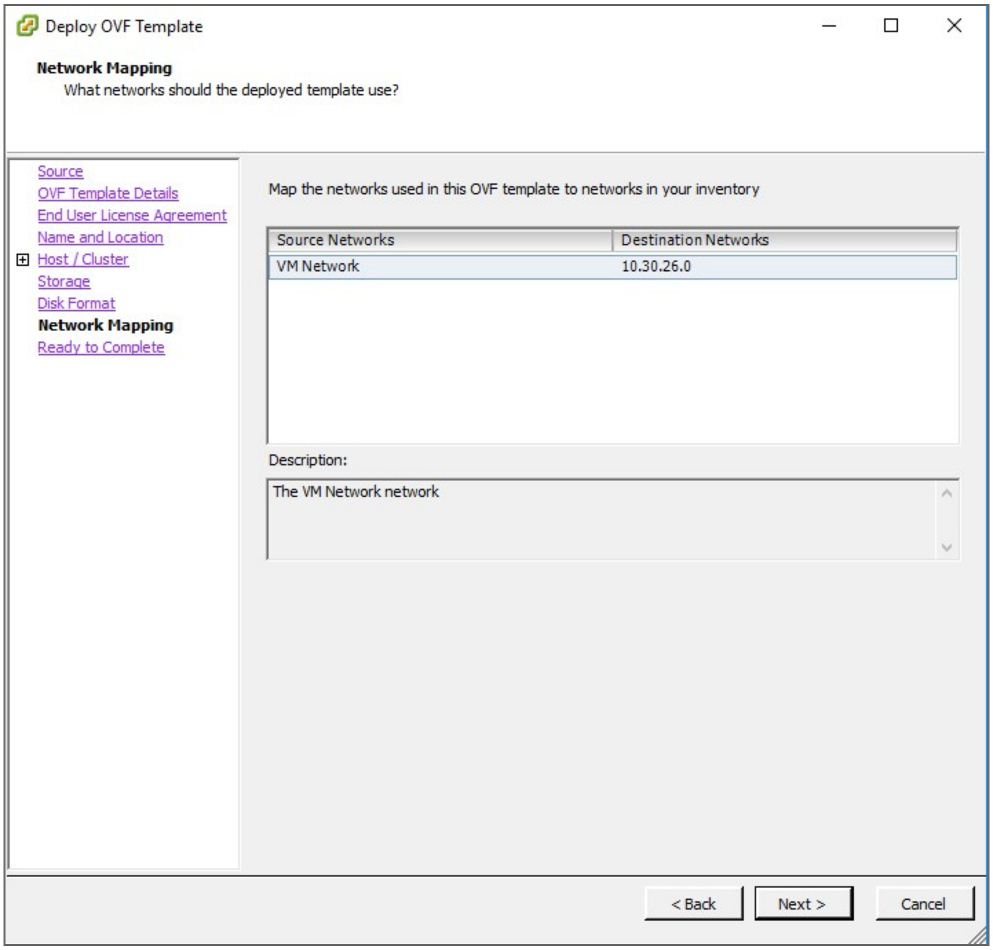
Available space (GB): 5271.6

○ Thick Provision Lazy Zeroed

○ Thick Provision Eager Zeroed

● Thin Provision

10. On the **Network Mapping** page, select a network to which the VA will be connected. It is recommended that you choose a network with DHCP and Internet access. Click **Next**.



Network Mapping

What networks should the deployed template use?

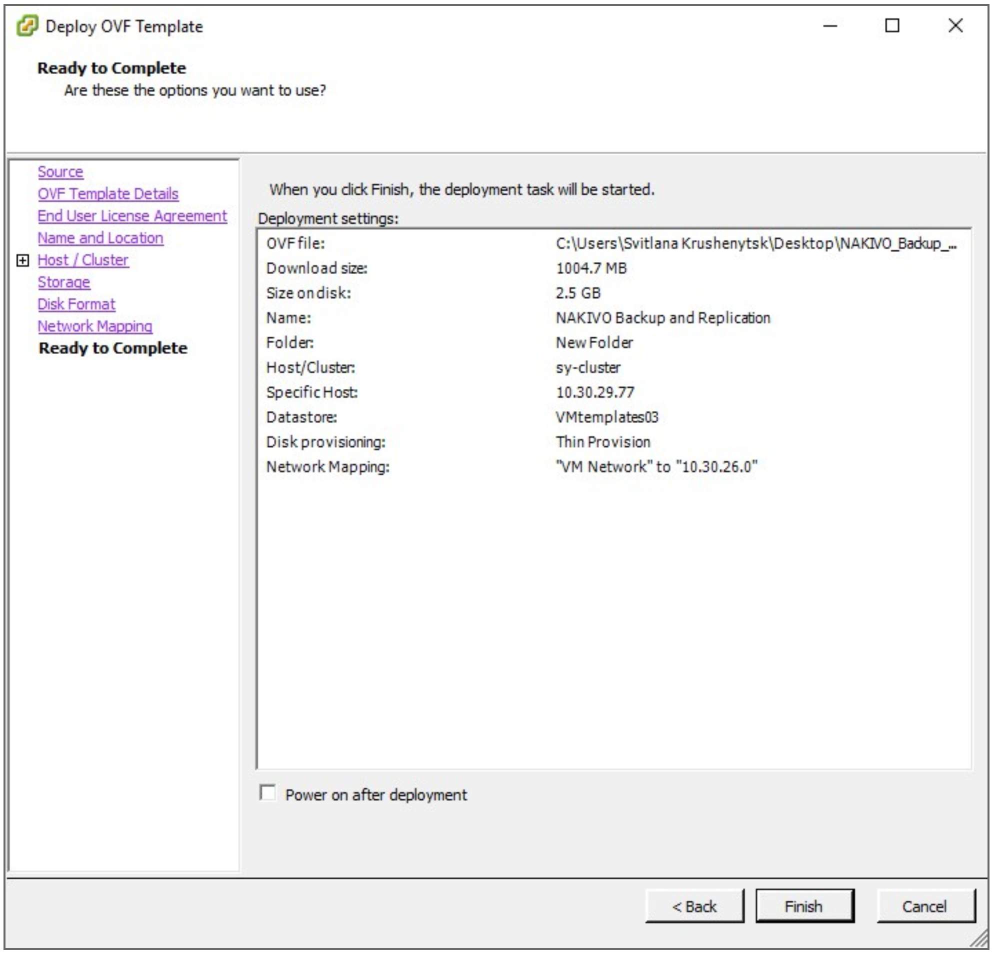
Map the networks used in this OVF template to networks in your inventory

Source Networks	Destination Networks
VM Network	10.30.26.0

Description:

The VM Network network

11. On the **Ready to Complete** page, review the summary of the options you have configured and select the **Power on after deployment** option.



Ready to Complete

Are these the options you want to use?

When you click Finish, the deployment task will be started.

Deployment settings:

OVF file:	C:\Users\Svitlana Krushenytsk\Desktop\NAKIVO_Backup_...
Download size:	1004.7 MB
Size on disk:	2.5 GB
Name:	NAKIVO Backup and Replication
Folder:	New Folder
Host/Cluster:	sy-cluster
Specific Host:	10.30.29.77
Datastore:	VMtemplates03
Disk provisioning:	Thin Provision
Network Mapping:	"VM Network" to "10.30.26.0"

□ Power on after deployment

12. Click **Finish** to complete the deployment.
13. After the Virtual Appliance is deployed, configure it if necessary.

After the installation is complete, you can log in to NAKIVO Backup & Replication by opening the following URL in your web browser: `https://machine_IP_or_DNS:director_https_port`

Virtual Appliance OS, Credentials, and Security

The appliance runs Ubuntu 20.04, 64-bit. Use the following credentials to log in to the appliance:

- **Username**: nkvuser
- **Password**: QExS-6b%3D

For the versions of NAKIVO Backup & Replication older than 7.2, the password is `root`.

Important

If you plan to expose the Virtual Appliance to the Internet, change the default VA credentials and set up a login and password for the Web interface.

To enable Backup Immutability for **Amazon S3** or **Local Folder** type of Backup Repository deployed as part of virtual appliance, NAKIVO Backup & Replication does the following:

- Creates a new user for all administrative needs and adds it to the *sudo* group.
- Disables root user.
- Changes default SSH port to 2221.
- Configure the following kernel parameters via **sysctl.conf**:
    - Limits network-transmitted configuration for IPv4/IPv6
    - Turns on execshield protection
    - Prevents the common 'syn flood attack'
    - Turns on source IP address verification
    - Prevents a cracker from using a spoofing attack against the IP address of the server.
    - Logs several types of suspicious packets, such as spoofed packets, source-routed packets, and redirects.
    - Configures swap. Sets **vm.swappiness** to 15
    - Sets **kernel.unprivileged_bpf_disabled** to 1
    - Sets **kernel.core_pattern** to **/tmp/%e.%p.core**
    - Sets **kernel.core_uses_pid** to 1
    - Sets **kernel.dmesg_restrict** to 1
    - Sets **kernel.kptr_restrict** to 2
    - Sets **kernel.sysrq** to 0
- Secures */tmp* and */var/tmp*
- Secures Shared Memory
- Prevents IP Spoofing
- Installs and configures fail2ban

Web Interface Login

Open the following URL to access the product's web interface: `https://Appliance_VM_IP:4443`. Refer to the Getting Started section to better understand how to continue working with NAKIVO Backup & Replication.

Deploying Nutanix AHV Virtual Appliance

- Deploying Nutanix AHV Virtual Appliance
- Virtual Appliance OS, Credentials, and Security
- Web Interface Login

Deploying Nutanix AHV Virtual Appliance

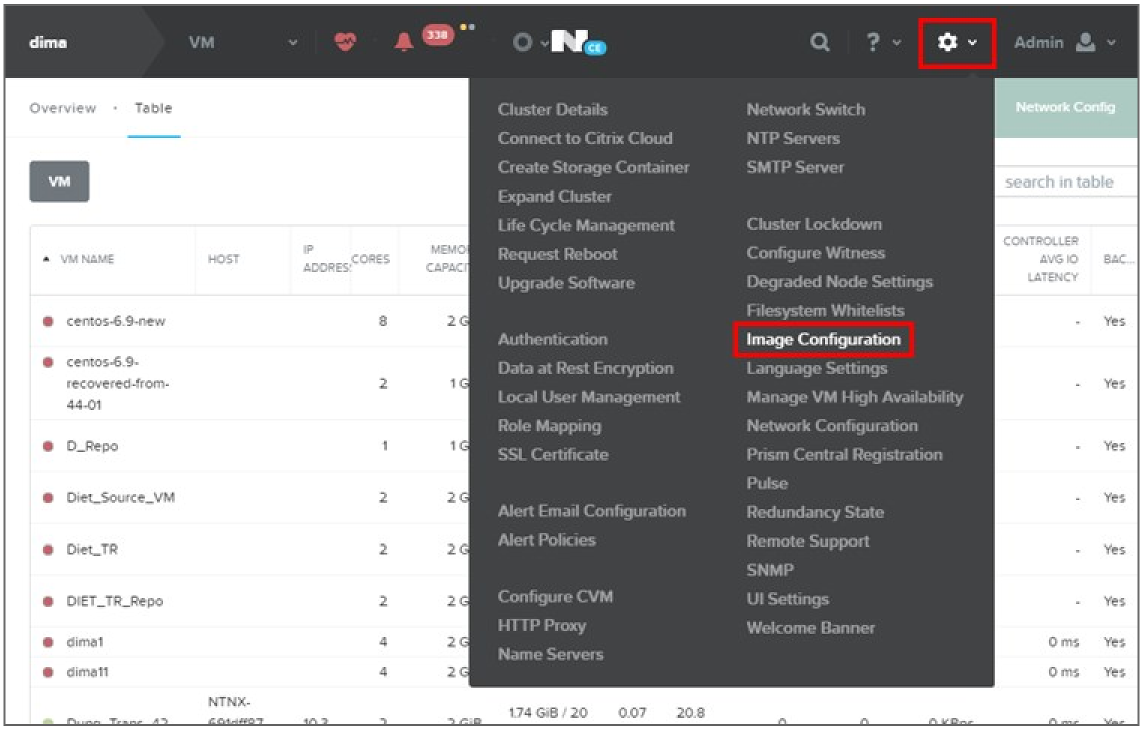
The NAKIVO Backup & Replication instance must be deployed in a Nutanix AHV cluster in order to enable backup and recovery functions.

NAKIVO Backup & Replication offers the following solutions:

- Full Solution (Single Tenant) - requires a 100 GB thin provisioned disk
- Transporter-only - requires a 20 GB thin provisioned disk

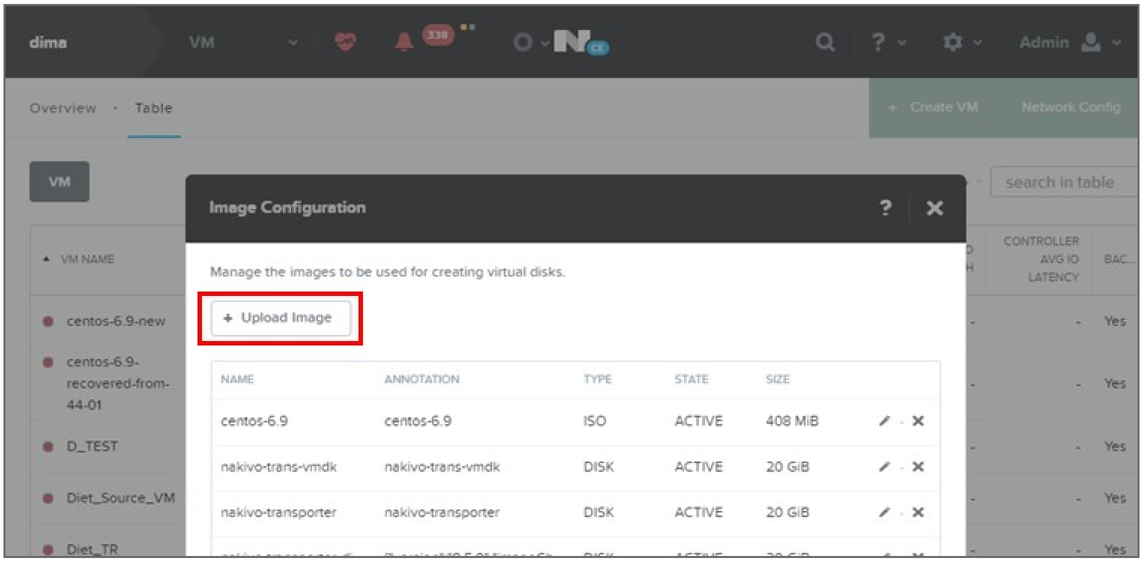
To deploy a virtual appliance via the Nutanix Prism application, follow the steps below:

1. Download the .VMDK file with a full or transporter-only image from the Nakivo website and store it locally.
2. Log in to the Prism console.
3. From the **Configurations** menu, select **Image Configuration**.



VM NAME	HOST	IP ADDRES	CORES	MEMO CAPACI	CONTROLLER AVG IO LATENCY	BAC...
centos-6.9-new			8	2 G	-	Yes
centos-6.9-recovered-from-44-01			2	1 G	-	Yes
D_Repo			1	1 G	-	Yes
Diet_Source_VM			2	2 G	-	Yes
Diet_TR			2	2 G	-	Yes
DIET_TR_Repo			2	2 G	-	Yes
dima1			4	2 G	0 ms	Yes
dima11			4	2 G	0 ms	Yes

4. In the **Image Configuration** dialog, click **Upload Image**.

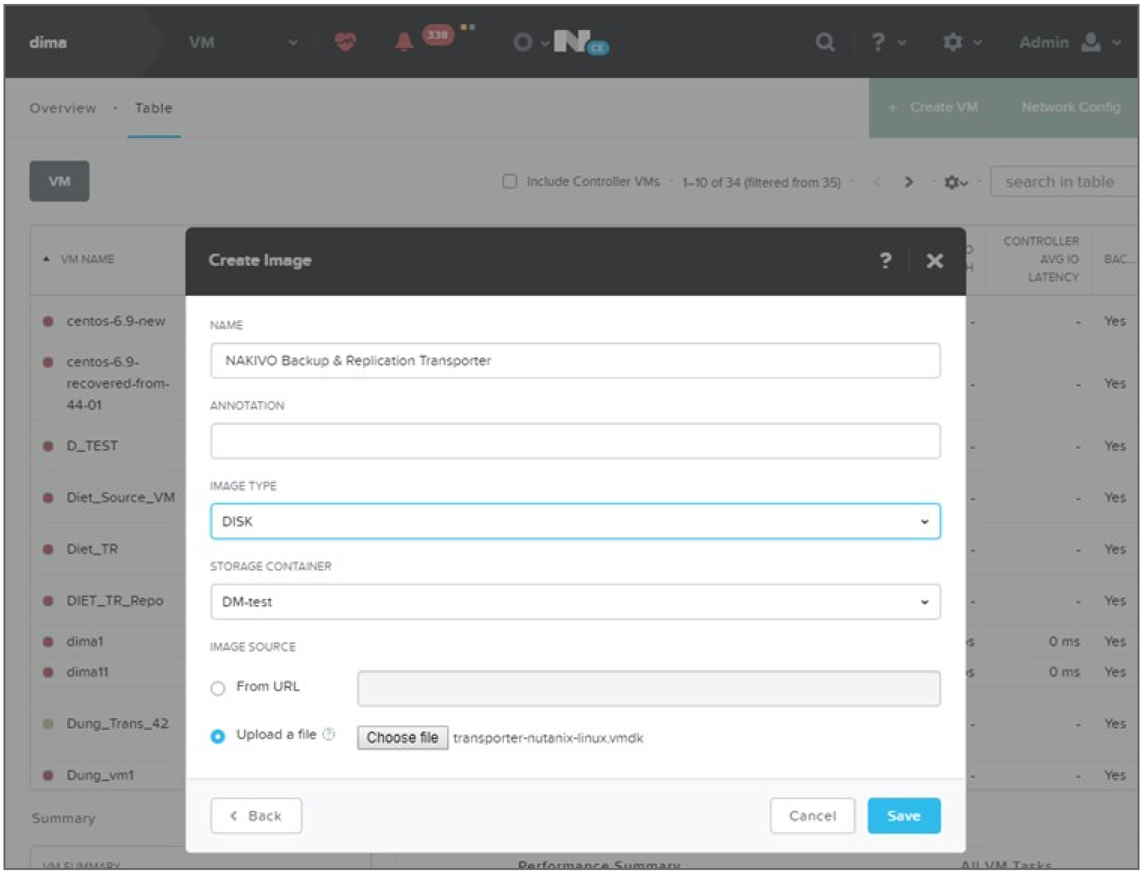


Manage the images to be used for creating virtual disks.

NAME	ANNOTATION	TYPE	STATE	SIZE
centos-6.9	centos-6.9	ISO	ACTIVE	408 MiB
nakivo-trans-vmdk	nakivo-trans-vmdk	DISK	ACTIVE	20 GiB
nakivo-transporter	nakivo-transporter	DISK	ACTIVE	20 GiB

5. In the **Create Image** dialog, fill in the following options:
    - **Name**: Enter a name for the new image.
    - **Image Type**: From the drop-down list, select **DISK**.
    - **Storage Container**: Select the storage container you wish to use from the drop-down list. The list includes all storage containers created for this cluster. If there are no storage containers currently available, a **Create Storage Container** link is displayed.
    - **Image Source**: Click the **Upload a file** radio button to upload a file from your workstation. Click the **Choose**

File button and then select the file to upload from the file search window.



Create Image

NAME: NAKIVO Backup & Replication Transporter

ANNOTATION:

IMAGE TYPE: DISK

STORAGE CONTAINER: DM-test

IMAGE SOURCE

○ From URL

● Upload a file Choose file transporter-nutanix-linux.vmdk

6. When all fields are correct, click the **Save** button.
   After the file uploading completes, the **Create Image** window closes and the **Image Configuration** window reappears with the new image present in the list.

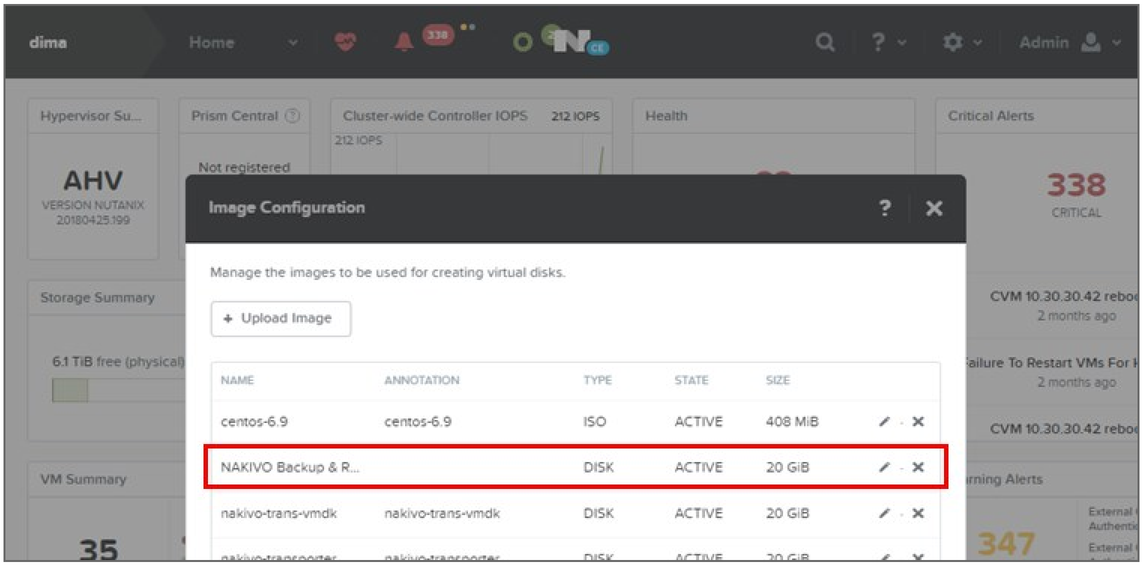


Image Configuration

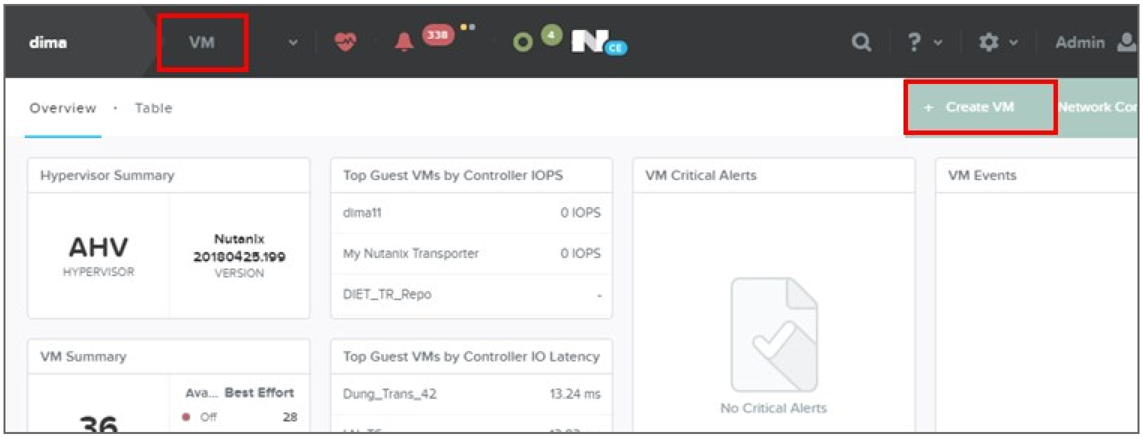
Manage the images to be used for creating virtual disks.

NAME	ANNOTATION	TYPE	STATE	SIZE
centos-6.9	centos-6.9	ISO	ACTIVE	408 MiB
NAKIVO Backup & R...		DISK	ACTIVE	20 GiB
nakivo-trans-vmdk	nakivo-trans-vmdk	DISK	ACTIVE	20 GiB
nakivo-transporter	nakivo-transporter	DISK	ACTIVE	20 GiB

Note

Make sure the status of the disk is **Active** before proceeding to the next step.

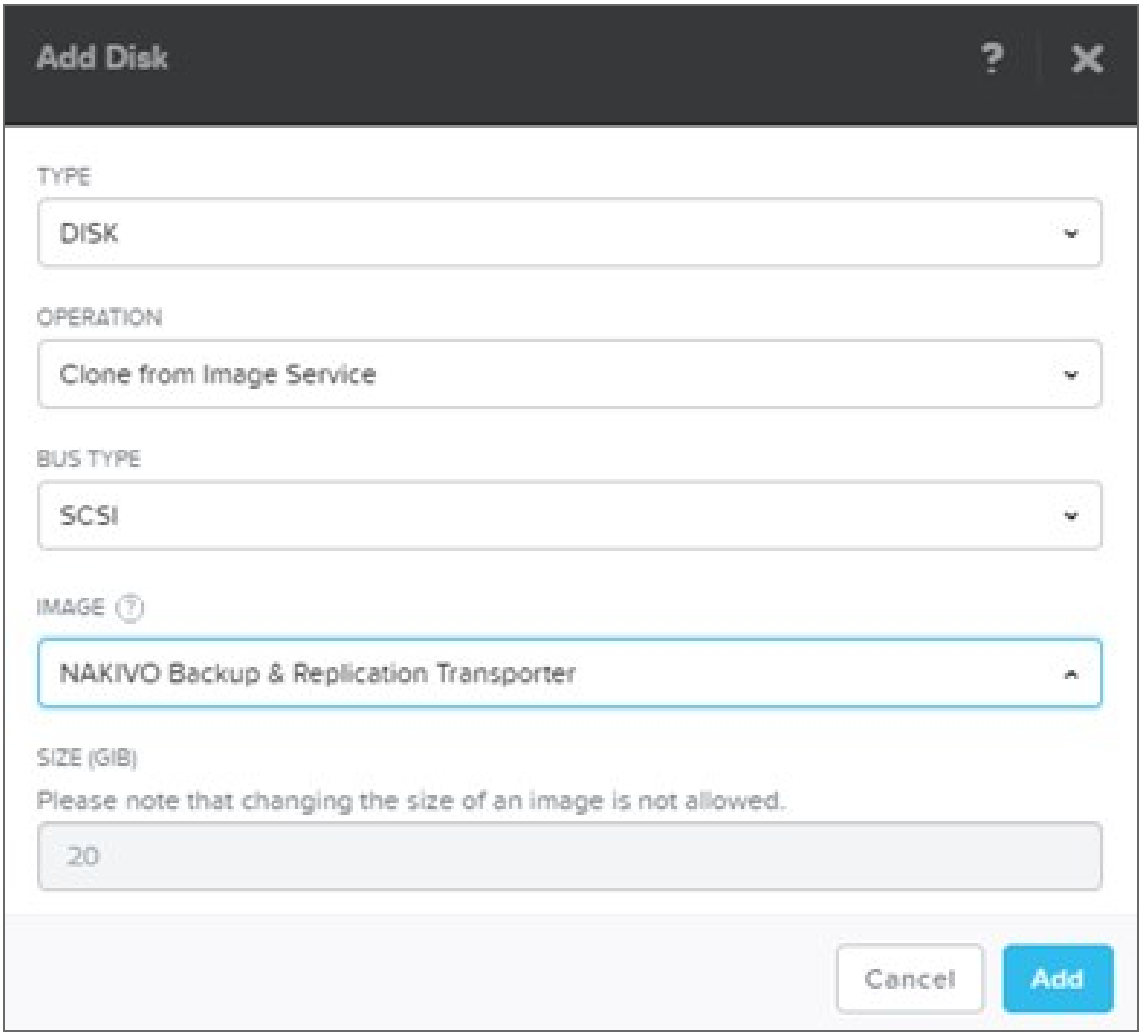
7. Close the **Image Configuration** window, go to the **VM** view and click **Create VM**.



8. In the **Create VM** dialog, fill in the following options:

- **Name**: Enter a name for the VM.
- **vCPU(s)**: Enter the number of virtual CPUs to allocate to this VM (minimum 1).
- **Number of Cores per vCPU**: Enter the number of cores assigned to each virtual CPU (minimum 2).
- **Memory**: Enter the amount of memory (in GBs) to allocate to this VM (minimum 4 GB + 250 MB for each concurrent job for full solution/minimum 2 GB + 250 MB for each concurrent job Transporter-only solution).
- In the **Disk** section, click **Add New Disk**, and specify the following settings in the **Add Disk** dialog:
    a. **Type**: Select **Disk**.
    b. **Operation**: Select **Clone from Image Service**.
    c. **Bus Type**: Select **SCSI**.

d. **Image**: Select your uploaded image from the list.



TYPE: DISK

OPERATION: Clone from Image Service

BUS TYPE: SCSI

IMAGE: NAKIVO Backup & Replication Transporter

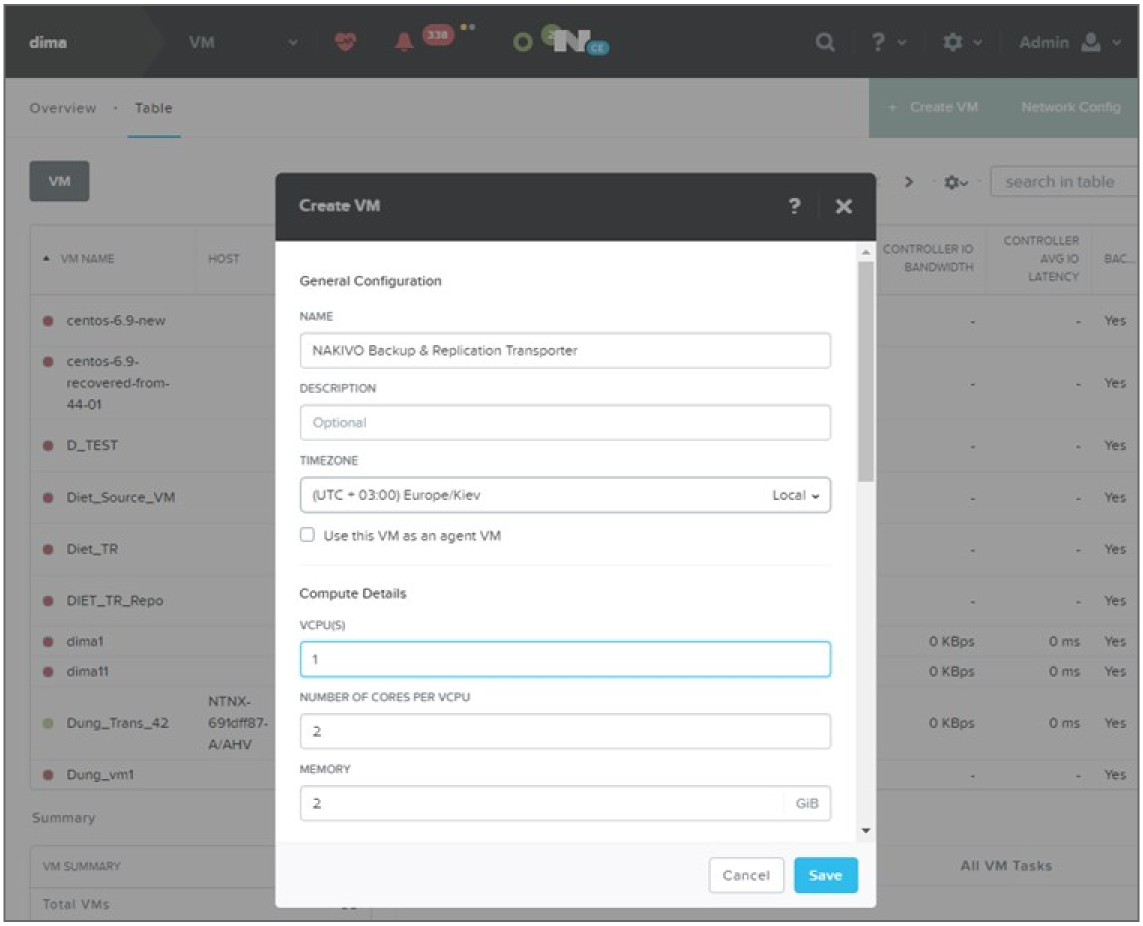
SIZE (GIB)

Please note that changing the size of an image is not allowed.

20

- In the **Network Adapters (NIC)** section, click **Add New NIC** and select an available VLAN from the list.

9. Click **Save**.



Create VM

General Configuration

NAME: NAKIVO Backup & Replication Transporter

DESCRIPTION: Optional

TIMEZONE: (UTC + 03:00) Europe/Kiev — Local

☐ Use this VM as an agent VM

Compute Details

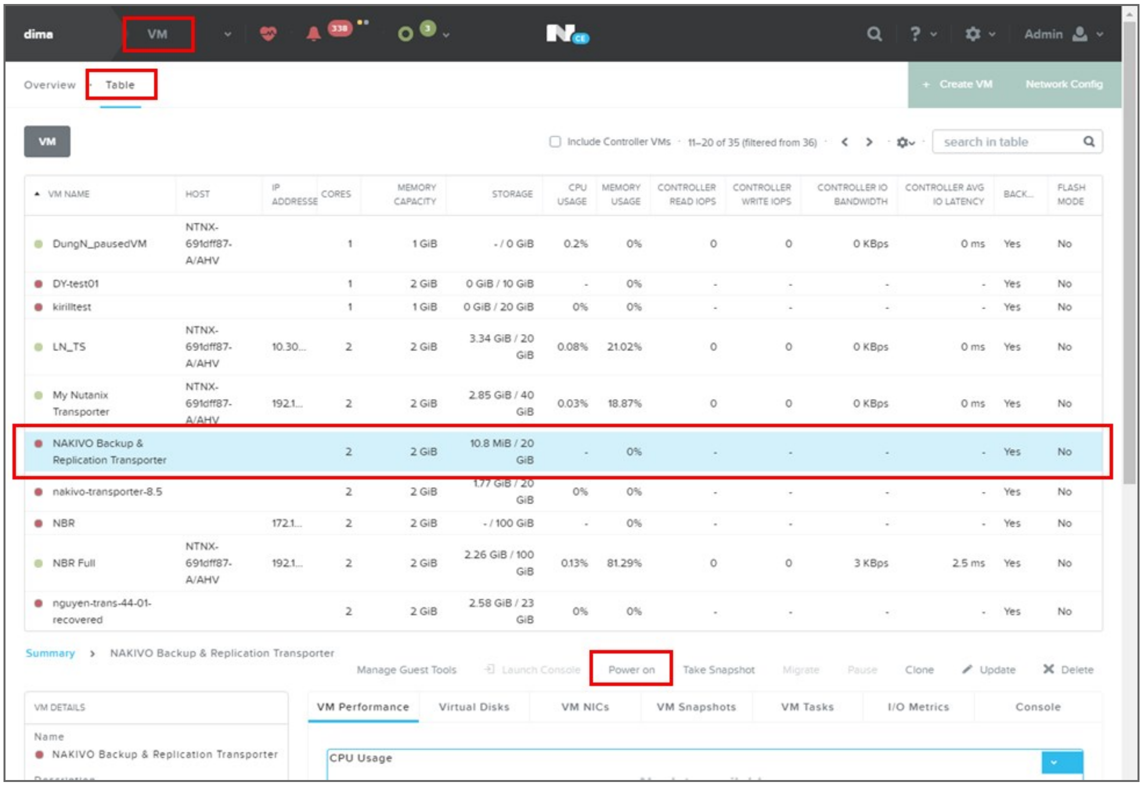
VCPU(S): 1

NUMBER OF CORES PER VCPU: 2

MEMORY: 2 GiB

10. Wait until the process of VM creation is complete and locate your newly-created VM on the list.

11. Select your VM and click **Power On**.



VM NAME	HOST	IP ADDRESSE	CORES	MEMORY CAPACITY	STORAGE	CPU USAGE	MEMORY USAGE	CONTROLLER READ IOPS	CONTROLLER WRITE IOPS	CONTROLLER IO BANDWIDTH	CONTROLLER AVG IO LATENCY	BACK...	FLASH MODE
● DungN_pausedVM	NTNX-691dff87-A/AHV		1	1 GiB	- / 0 GiB	0.2%	0%	0	0	0 KBps	0 ms	Yes	No
● DY-test01			1	2 GiB	0 GiB / 10 GiB	-	0%	-	-	-	-	Yes	No
● kirilltest			1	1 GiB	0 GiB / 20 GiB	0%	0%	-	-	-	-	Yes	No
● LN_TS	NTNX-691dff87-A/AHV	10.30...	2	2 GiB	3.34 GiB / 20 GiB	0.08%	21.02%	0	0	0 KBps	0 ms	Yes	No
● My Nutanix Transporter	NTNX-691dff87-A/AHV	192.1...	2	2 GiB	2.85 GiB / 40 GiB	0.03%	18.87%	0	0	0 KBps	0 ms	Yes	No
● NAKIVO Backup & Replication Transporter			2	2 GiB	10.8 MiB / 20 GiB	-	0%	-	-	-	-	Yes	No
● nakivo-transporter-8.5			2	2 GiB	1.77 GiB / 20 GiB	0%	0%	-	-	-	-	Yes	No
● NBR		172.1...	2	2 GiB	- / 100 GiB	-	0%	-	-	-	-	Yes	No
● NBR Full	NTNX-691dff87-A/AHV	192.1...	2	2 GiB	2.26 GiB / 100 GiB	0.13%	81.29%	0	0	3 KBps	2.5 ms	Yes	No
● nguyen-trans-44-01-recovered			2	2 GiB	2.58 GiB / 23 GiB	0%	0%	-	-	-	-	Yes	No

Name
● NAKIVO Backup & Replication Transporter

12. After the Virtual Appliance is deployed and powered on, you may need to configure it.

After the installation is complete, you can log in to NAKIVO Backup & Replication by opening the following URL in your web browser: https://machine_IP_or_DNS:director_https_port.

Virtual Appliance OS, Credentials, and Security

The appliance runs Ubuntu 18.04, 64-bit. Use the following credentials to log in to the appliance:

- **Username**: root
- **Password**: QExS-6b%3D

For the versions of NAKIVO Backup & Replication older than 7.2, the password is `root`.

Important

If you plan to expose the Virtual Appliance to the Internet, change the default VA credentials and set up a login and password for the Web interface.

To enable Backup Immutability for **Amazon S3** or **Local Folder** type of Backup Repository deployed as part of virtual appliance, NAKIVO Backup & Replication does the following:

- Creates a new user for all administrative needs and adds it to the *sudo* group.
- Disables root user.
- Changes default SSH port to 2221.
- Configure the following kernel parameters via **sysctl.conf**:

  - Limits network-transmitted configuration for IPv4/IPv6
  - Turns on execshield protection
  - Prevents the common 'syn flood attack'
  - Turns on source IP address verification
  - Prevents a cracker from using a spoofing attack against the IP address of the server.
  - Logs several types of suspicious packets, such as spoofed packets, source-routed packets, and redirects.
  - Configures swap. Sets **vm.swappiness** to 15
  - Sets **kernel.unprivileged_bpf_disabled** to 1
  - Sets **kernel.core_pattern** to **/tmp/%e.%p.core**
  - Sets **kernel.core_uses_pid** to 1
  - Sets **kernel.dmesg_restrict** to 1
  - Sets **kernel.kptr_restrict** to 2
  - Sets **kernel.sysrq** to 0
- Secures */tmp* and */var/tmp*
- Secures Shared Memory
- Prevents IP Spoofing
- Installs and configures fail2ban

Web Interface Login

Open the following URL to access the product's web interface: https://Appliance_VM_IP:4443.
Refer to “Getting Started” on page 21 to better understand how to continue working with NAKIVO Backup & Replication.

Deploying Amazon Machine Image in Amazon EC2

You can deploy NAKIVO Backup & Replication as a pre-configured Amazon Machine Image (AMI) in Amazon EC2. After you fill out our download form, you will get a link to the AWS marketplace page where you can download the AMI.

Configure the following AMI parameters:

1. **Instance Type**: More powerful instances can process tasks faster and run more tasks simultaneously. The minimum requirement for NAKIVO Backup & Replication is the t2.micro instance type; the t2 medium instance type is recommended.
2. **Instance Details**: Assign a public IP to the instance if you wish to access the instance from the Internet.
3. **Security Group**: Either use the "All Traffic" rule or create a set of rules listed below:

Type	Port Range	Source	Description
SSH	22	0.0.0.0/0	Enables remote SSH access to the Instance
Custom TCP	80	0.0.0.0/0	Enables access to the Web interface
Custom TCP	443	0.0.0.0/0	Required for local Transporter import
Custom TCP	902	0.0.0.0/0	Required for local Transporter import
Custom TCP	4443	0.0.0.0/0	Enables access to the Web interface
Custom TCP	9446	0.0.0.0/0	Enables access to a remote Transporters
Custom TCP	9448-10000	0.0.0.0/0	Enables access to a remote Transporters
All ICMP	0-65535	0.0.0.0/0	Enables access to a remote Transporter

4. **Key pair**: Select an existing key pair or create a new key pair for your instance. If you select an existing key pair, make sure you have the access to the private key file.

   Refer to "Getting Started" on page 21 to understand better how to continue working with NAKIVO Backup & Replication.

Installing on Windows

NAKIVO Backup & Replication offers the following installation options for Windows machines:

- Full Solution
- Transporter-Only Solution
- Multi-Tenant Solution

After successful product installation, refer to the Getting Started section to learn how to continue working with NAKIVO Backup & Replication.

- Installing Full Solution on Windows
- Installing Transporter-Only on Windows
- Installing Full Solution in Multi-Tenant Mode on Windows
- Silent Installation

Installing Full Solution on Windows

To install NAKIVO Backup & Replication with default options, simply run the NAKIVO Backup & Replication installer for Windows and click **Install**. This will install all product components (Director, Transporter, and Backup Repository) and you will be able to use all product features after installation.

You can also change the installation options as follows:

1. Set the installation options as follows:
    - **Installation type**: Leave the **Full solution** option selected to install the key product components (Director and Transporter)
    - **Create repository**: Leave the checkbox selected to create a Backup Repository on the machine on which NAKIVO Backup & Replication is installed.
    - Optionally, click **Browse** and select a folder to change the default location of the Backup Repository.
    - Optionally, you can select the **Transporter certificate** checkbox. This allows you to use a CA Certificate. Enter the path to the folder containing the certificate file in the field.

      Notes

        - When the checkbox is not selected, NAKIVO Backup & Replication automatically installs a self-signed certificate.
        - It is possible to install a CA-signed certificate for the Transporter by conducting silent installation using the command-line arguments passed to the installer:

- Use the following command for Windows OS:

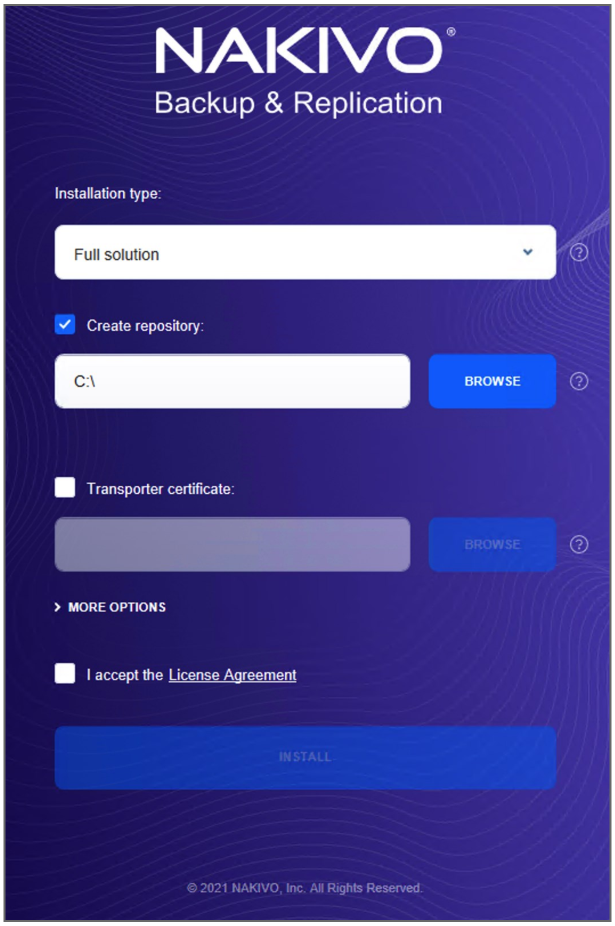
  ```
  installer.exe --cert C:\certificate.pem --eula-accept
  ```

  The short option for the Windows OS command is the following:

  ```
  installer.exe -ct C:\certificate.pem -ea
  ```

- Use the following command for Linux OS:

  ```
  installer.sh --cert /tmp/certificate.pem --eula-accept
  ```


Installation type: Full solution

☑ Create repository: C:\

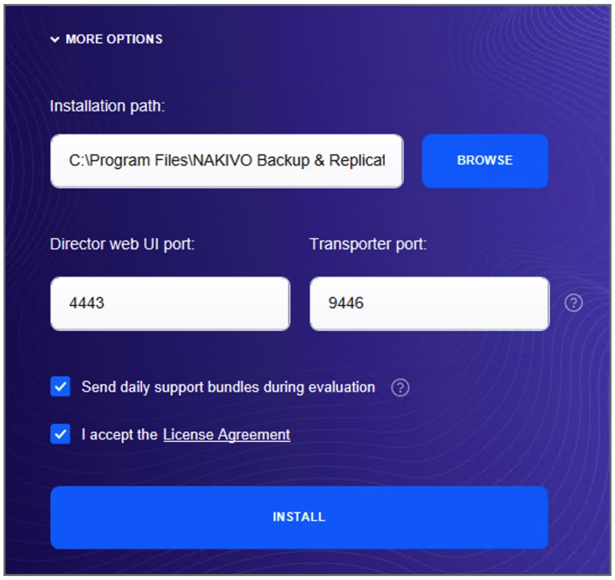
□ Transporter certificate:

□ I accept the License Agreement

2. Click **MORE OPTIONS** to set up more installation options:
   - **Installation path**: The location where NAKIVO Backup & Replication will be installed. If you want to change the default path to NAKIVO Backup & Replication, click **Browse** and select a new location.
   - **Director Web UI port**: The default port that will be used to connect to the Web UI of NAKIVO Backup & Replication. Make sure that the port you specify is open in your firewall.
   - **Transporter port**: The default port that will be used by the Director to communicate with the Onboard Transporter. Make sure that the port you specify is open in your firewall.

   - **Send daily support bundles during evaluation**: When this option is selected, NAKIVO Backup & Replication automatically creates, encrypts, and uploads support bundles once a day to a NAKIVO support server during the evaluation period. The NAKIVO support team may use this information to improve the product experience and may be able to identify and resolve product issues faster.

3. **I accept the License Agreement**: Select this option to confirm that you have read and agreed to the License Agreement.
4. Click **Install**.



Installation path:

C:\Program Files\NAKIVO Backup & Replicat

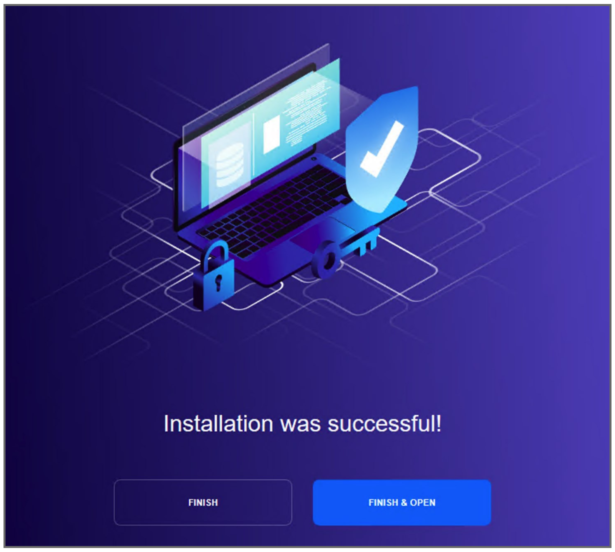
Director web UI port: 4443

Transporter port: 9446

☑ Send daily support bundles during evaluation

☑ I accept the License Agreement

5. Click **Finish** to complete the installation process or **Finish & Open** to complete installation and start using NAKIVO Backup & Replication.



Installation was successful!

6. To prevent unauthorized access to the product, create your user account. Fore more details, refer to "Logging in to NAKIVO Backup & Replication" on page 22 .

Installing Transporter-Only on Windows

If you have already installed the full solution (both Director and Transporter) and wish to deploy an additional Transporter, run the NAKIVO Backup & Replication installer for Windows and follow the steps below:

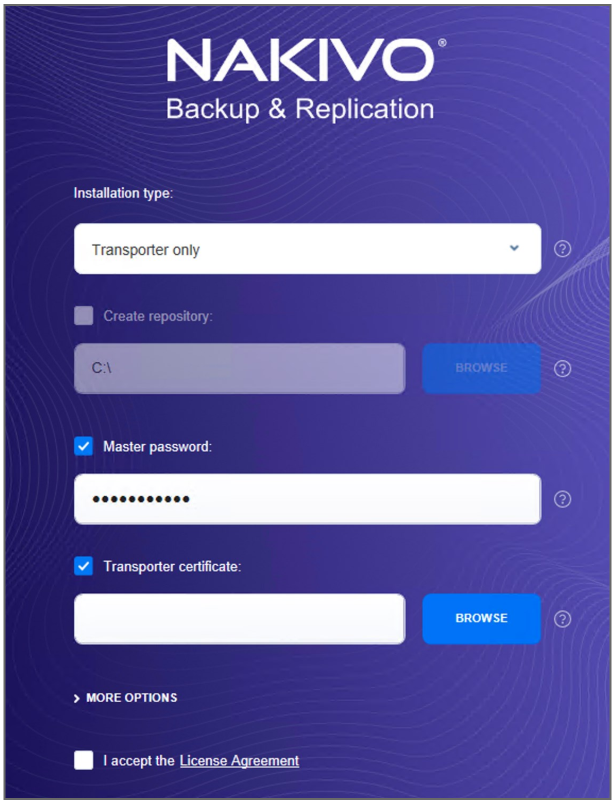
Transporter Installation Prerequisites

Prior to installing the Transporter, make sure the following prerequisites are met:

- Make sure the machine on which you plan to install the Transporter has a connection to the relevant items below:
    - The machine on which the Director is installed.
    - VMware/Hyper-V/Nutanix AHV servers on which you plan to back up or replicate VMs (provided that you plan to retrieve VM data using the Transporter you are about to install)
    - Machines on which you have installed other Transporters (provided that you plan to set up data transfer between an existing Transporter and the one you are about to install)
    - Backup Repository (provided that you plan to assign the Transporter you are about to install to a Backup Repository)
    - VMware/Hyper-V/Nutanix AHV servers which you plan to use as a destination for replicated VMs (provided that you plan to write data to the target servers and datastores using the Transporter you are about to install)
- For VMware/Hyper-V/Nutanix AHV servers discovered with DNS names, make sure those DNS names can be resolved on the machine on which to install the Transporter.

Transporter Installation Process

1. Run the NAKIVO Backup & Replication installer.
2. Choose **Transporter only** from the **Installation type** drop-down list.



Installation type: Transporter only

□ Create repository: C:\

☑ Master password: •••••••••••

☑ Transporter certificate:

□ I accept the License Agreement

3. Optionally, you can select the **Master password** checkbox and enter the password that will be used to generate a pre-shared key and secure the Transporter.

   Notes

   - The master password must adhere to the following requirements:
     - Minimal length - 5 characters.
     - Maximum length - 50 characters.
   - The master password can be set and re-set manually by running the command on the machine housing the Transporter. Follow these steps:
     - Enter the following command `bhsvc -b P@ssword123`
     - Restart the Transporter service.

4. Optionally, you can select the **Transporter certificate** checkbox. This allows you to use a CA Certificate. Enter the path to the folder containing the certificate file in the field.

   Notes

   - When the checkbox is not selected, NAKIVO Backup & Replication automatically installs a self-signed certificate.
   - It is possible to set up a master password and CA-signed certificate for the Transporter by conducting silent installation using the command-line arguments passed to the installer:

- Use the following command for Windows OS:

  ```
  installer.exe --cert C:\certificate.pem --master-pass P@ssword123 --eula-accept
  ```

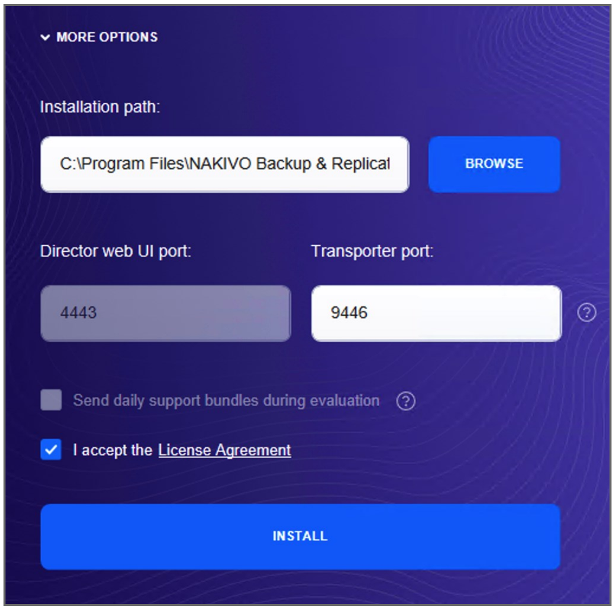
  The short option for the Windows OS command is the following:

  ```
  installer.exe -ct C:\certificate.pem -b P@ssword123 -ea
  ```

- Use the following command for Linux OS:

  ```
  installer.sh --cert /tmp/certificate.pem -b P@ssword123 --eula-accept
  ```

5. Click **MORE OPTIONS** and set up the following:
   - **Installation path**: The location where the Transporter will be installed. If you want to change the default path to the Transporter installation folder, click **Browse** and select a new location.
   - **Transporter port**: The default port that will be used by the Director to communicate with the Onboard Transporter. Make sure that the port you specify is open in your firewall.
   - **Send daily support bundles during evaluation**: If this option is selected, NAKIVO Backup & Replication will automatically create, encrypt, and upload support bundles once a day to a NAKIVO support server during the evaluation period. NAKIVO Support team may use this information to improve the product experience and may be able to identify and resolve product issues faster.
6. **I accept the License Agreement**: Select this option to confirm that you have read and agreed to the License Agreement.
7. Click **Install**.



Installation path: C:\Program Files\NAKIVO Backup & Replicat

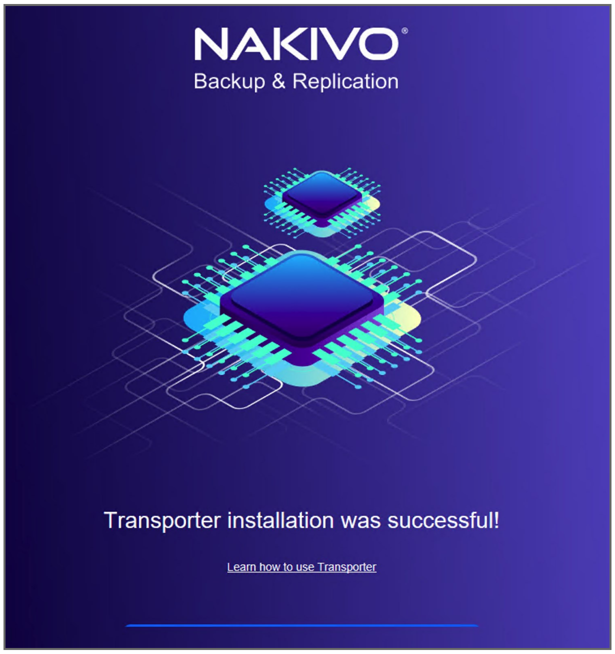
Director web UI port: 4443

Transporter port: 9446

□ Send daily support bundles during evaluation

☑ I accept the License Agreement

8. When the installation is complete the **Transporter installation was successful** notification appears.



Transporter installation was successful!

9. Add the Transporter to NAKIVO Backup & Replication.

Installing Full Solution in Multi-Tenant Mode on Windows

To install the full solution in multi-tenant mode on a Windows OS, run the NAKIVO Backup & Replication installer for Windows and follow the steps below:

1. Choose **Multi tenant solution** from the **Installation type** drop-down list.
2. Optionally, you can select the **Transporter certificate** checkbox. This allows you to use a CA Certificate. Enter the path to the folder containing the certificate file in the field.

   Notes

   - When the checkbox is not selected, NAKIVO Backup & Replication automatically installs a self-signed certificate.
   - It is possible to install a CA-signed certificate for the Transporter by conducting silent installation using the command-line arguments passed to the installer:
     - Use the following command for Windows OS:

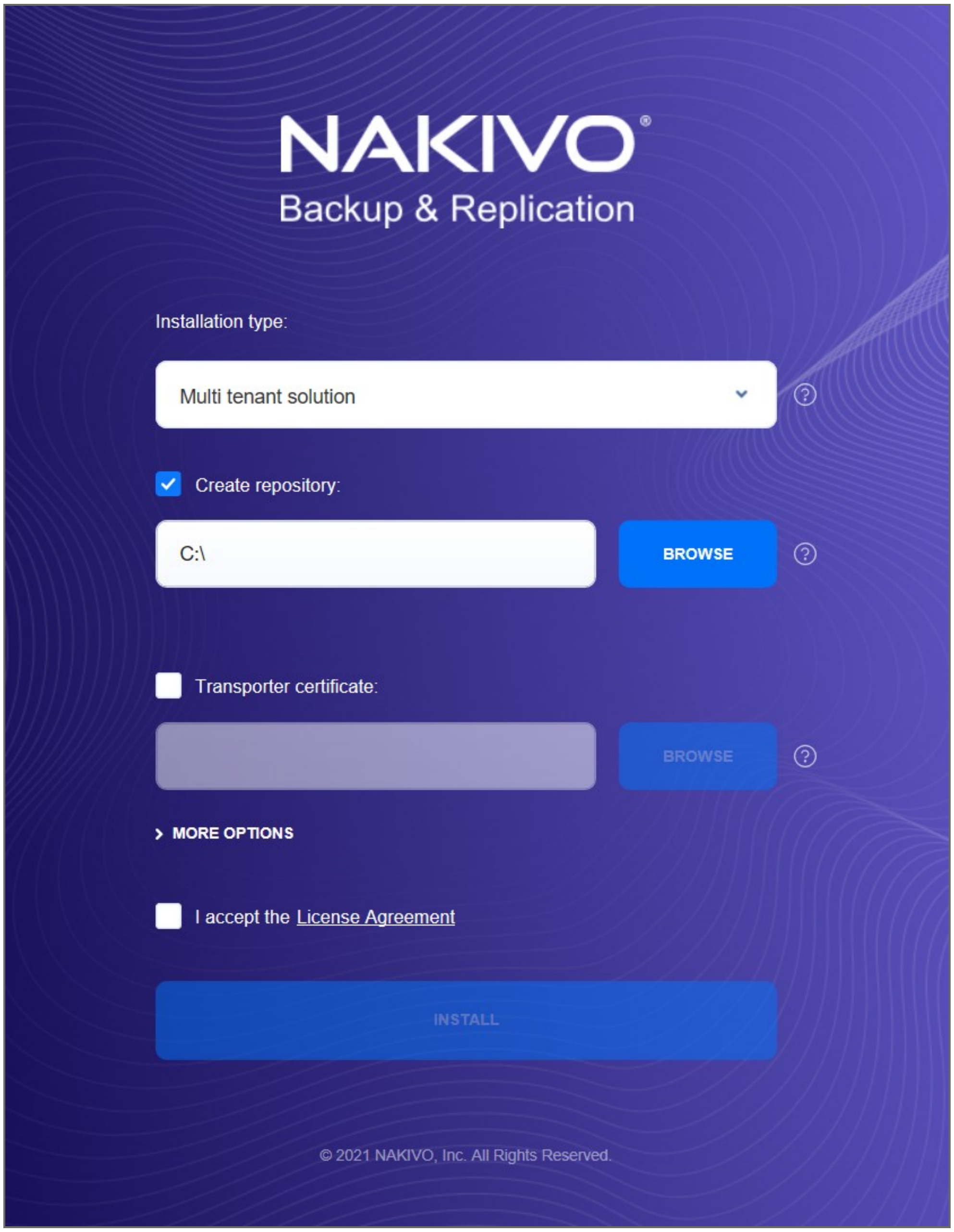
       ```
       installer.exe --cert C:\certificate.pem --eula-accept
       ```

       The short option for the Windows OS command is the following:

       ```
       installer.exe -ct C:\certificate.pem -ea
       ```

- Use the following command for Linux OS:

```
installer.sh --cert /tmp/certificate.pem --eula-accept
```



Installation type: Multi tenant solution

☑ Create repository: C:\

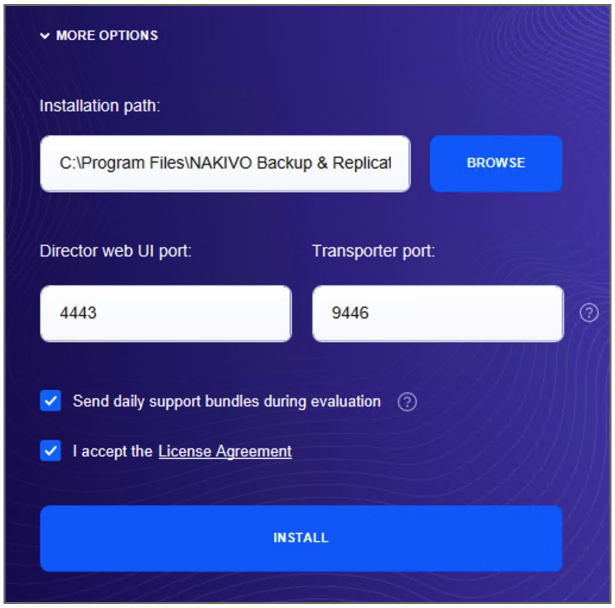
□ Transporter certificate:

□ I accept the License Agreement

3. Click **MORE OPTIONS** to set up more installation options:
   - **Installation path**: The location where NAKIVO Backup & Replication will be installed. If you want to change the default path to the product, click **Browse** and select a new location.
   - **Director Web UI port**: The default port that will be used to connect to the Web UI of NAKIVO Backup & Replication. Make sure that the port you specify is open in your firewall.
   - **Transporter port**: The default port that will be used by the Director to communicate with the Onboard Transporter. Make sure that the port you specify is open in your firewall.

- **Send daily support bundles during evaluation**: When this option is selected, NAKIVO Backup & Replication automatically creates, encrypts, and uploads support bundles once a day to a NAKIVO support server during the evaluation period. The NAKIVO support team may use this information to improve the product experience and may be able to identify and resolve product issues faster.

4. **I accept the License Agreement**: Select this option to confirm that you have read and agreed to the License Agreement.
5. Click **Install**.



Installation path: C:\Program Files\NAKIVO Backup & Replicat

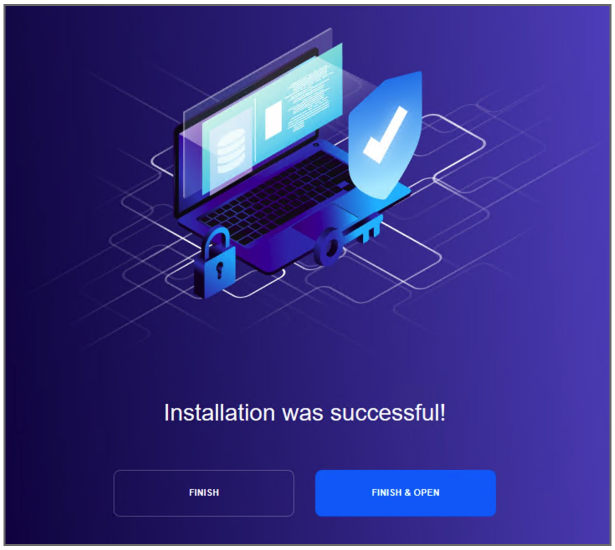
Director web UI port: 4443

Transporter port: 9446

☑ Send daily support bundles during evaluation

☑ I accept the License Agreement

6. Click **Finish** to complete the installation process or **Finish & Open** to complete installation and start using NAKIVO Backup & Replication.



Installation was successful!

Note

The onboard backup repository for the Master Tenant is automatically created after the installation.

7. Create an account by completing the form. Fore details, refer to "Logging in to NAKIVO Backup & Replication" on page 22 .

Credentials are not required to log in as Master Admin after installation. However, the default credentials are required to log into the product after the first tenant is created. To log in as Master Admin, specify "admin" as the username and leave the password field empty. You can change credentials in the product configuration.

Silent Installation on Windows

You can install NAKIVO Backup & Replication in silent mode via a command line by running the following command: **installer.exe -f --eula-accept** This installs all product components (Director, Transporter, and Backup Repository), and you will be able to use all product features after installation.

The following arguments are available:

Argument	Description
-h	Display the list of available arguments without starting the installation.
--eula-accept, -ea	Indicates that you have read and agree to the End User License Agreement.
-f	Performs the silent installation of the full solution (Director and Transporter).
-t	Performs the silent installation of Transporter only.
-m	Performs the silent installation of the full solution in multi-tenant mode.
-u	Performs the silent update of the installed product components.
--release-notes, -n	Indicates the user has read the release notes for the new release during an update.
-sii	Performs the silent install or update ignoring the single installer instance check.
--ignore-pre-install-action-failures, -ipiaf	All pre-install action failures are ignored.

--cert	Allows to set up a custom Transporter certificate.
--master-pass (short version: **-b**)	Allows to set up a custom master password for the Transporter.

Installing on Linux

Linux Installation Prerequisites

In order to install and use NAKIVO Backup & Replication on a Linux OS, make sure the following requirements are met:

- On Ubuntu and SLES, NAKIVO Backup & Replication relies on the following packages:
  - cifs-utils
  - open-iscsi
  - ntfs-3g
- On RedHat Enterprise Linux, NAKIVO Backup & Replication relies on the following packages:
  - cifs-utils
  - iscsi-initiator-utils
  - ntfs-3g

Silent Installation on Linux

You can install NAKIVO Backup & Replication in silent mode via a command line. To install the full solution, simply run the following command: `installer.sh -f --eula-accept` This will install all product components (Director, Transporter, Backup Repository) and you will be able to use all product features after installation.

The following arguments are available:

Argument	Description
-h, -help, help	Display the list of available arguments without starting the installation.
--eula-accept, -ea	Indicates that you have read and agree to the End User License Agreement.
-f	Shall perform the silent installation of the full solution (Director and Transporter).

Argument	**Description**
-t	Shall perform the silent installation of Transporter only.
-m	Shall perform the silent installation of the full solution in multi-tenant mode.
-u	Shall perform the silent update of the installed product components.
-e	Shall install Transporter on Amazon EC2, or update Transporter installed on Amazon EC2. Refer to Updating on Amazon EC2 for details.
-a	Shall enable uploading support bundles to support team server (Call Home). Refer to System Settings for details.
-y	Shall accept limitations silently.
-i <install_path>	Shall install to the specified installation path.
-d <director_port>	Shall provide a custom Director port.
-p <transporter_port>	Shall provide a custom Transporter port.
-r <port1>-<port2>	Shall provide a custom transporter data ports range.
-C	Shall suppress creating the repository.
-c <repo_path>	Shall create the repository. The **<repo_path>** parameter is optional.
--rt <repo_type>	Shall create a repository of the specified type. The **<repo_type>** parameter may accept the following values: **1** – "Forever incremental with deduplication"; **2** – "Forever incremental without deduplication"; **3** – "Incremental with full backups (deduplication devices)".
--rc <compress_level>	Shall specify the repository compression level. The parameter may accept the following values: Disabled; Fast; Medium; Best.
--pnp-cleanup	Shall clean up the database of the device manager for the Linux kernel.
--cert	Allows to set up a custom Transporter certificate.
--master-pass (short version: **-b**)	Allows to set up a custom master password for the Transporter.

Installing Full Solution on Linux

Follow the steps below to install all components of NAKIVO Backup & Replication (both Director and Transporter) on a Linux OS:

1. Upload the installer file to the machine on which you want to install NAKIVO Backup & Replication in the *binary transfer mode*. For example:
   - Upload the installer from a Windows-based machine.
   - Upload the product from a Linux-based machine: run the following command: `wget 'server_ip/shared/NAKIVO_Backup_&_Replication_TRIAL.sh'`
2. Log in to the Linux machine and allow the execution of the installer file.
   For example: `chmod +x NAKIVO_Backup_&_Replication_TRIAL.sh`
3. Execute the installer file with root privileges.
   For example: `sudo ./NAKIVO_Backup_&_Replication_TRIAL.sh`
4. Review the license agreement (press **Space** to go to the next page of the agreement). If you agree to the terms of the license agreement, press "Y" and then press **Enter**.
5. Type "S" to install the full solution and press **Enter**.
6. Optionally, you can install CA Transporter certificate. Enter the path to the folder containing the certificate file and press **Enter**.

   Notes
   - If no path to the CA certificate was provided, NAKIVO Backup & Replication automatically installs a self-signed certificate.
   - It is possible to set up CA-signed certificate for the Transporter by conducting silent installation using the command-line arguments passed to the installer. Use the following command:
     `installer.sh --cert /tmp/certificate.pem --eula-accept`
7. Specify the installation path for the product: Press **Enter** to accept the default installation path "/opt/nakivo" or enter a custom path and press **Enter**.
8. Specify the Director HTTPS port (which will be used to access the Web UI of NAKIVO Backup & Replication): Press **Enter** to accept the default port "4443" or enter a custom port number and press **Enter**. Make sure the port you specify is open in your firewall.
9. Specify whether to allow the product to automatically send support bundles to a NAKIVO server during the evaluation period (Call Home). If this option is enabled, NAKIVO Backup & Replication will automatically create, encrypt, and upload support bundles once a day to a NAKIVO support server during the evaluation period. NAKIVO Support team may use this information to improve the product experience and will be able to identify and resolve product issues faster.
10. Specify the Transporter port (which will be used to connect to the Transporter that is installed by default with the Director): Press **Enter** to accept the default port "9446" or enter a custom port number (1 to 65535) and press **Enter**. Make sure the port you specify is open in your firewall.

11. Specify a range of port numbers (from 1 to 65535) that will be used to transfer data by the Onboard Transporter (default are 9448-10000). The range you specify should contain at least 100 ports. Make sure that the ports you specify are open in your firewall.
12. Specify a path to the default Backup Repository: Press **Enter** to accept the default path "/opt/nakivo/repository" or enter a custom path and press **Enter** to begin the installation process.

After the installation is complete, you can log in to NAKIVO Backup & Replication by opening the following URL in your web browser: `https://machine_IP_or_DNS:director_https_port`

By default, login name and password are not required to access NAKIVO Backup & Replication. To prevent unauthorized access to the product, you can set up credentials in Configuration.

Installing Transporter on Linux

If you have already installed the full solution (both Director and Transporter) and want to deploy an additional Transporter, run the NAKIVO Backup & Replication installer for Windows and follow the steps below:

Transporter Installation Prerequisites

Prior to installing a Transporter, make sure the following prerequisites are met:

1. Make sure the machine on which you plan to install the Transporter has a connection to the relevant items below:
   - The machine on which the Director is installed
   - VMware/Hyper-V servers on which you plan to back up or replicate VMs (if you plan to retrieve VM data using the Transporter you are about to install)
   - Machines on which you have installed other Transporters (if you plan to set up data transfer between an existing Transporter and the one you are about to install)
   - Backup repository (if you plan to assign the Transporter you are about to install to a Backup Repository)
   - VMware/Hyper-V servers which you plan to use as a destination for replicated VMs (if you plan to write data to the target servers and datastores using the Transporter you are about to install)
2. If you have discovered VMware/Hyper-V servers using DNS names, make sure those DNS names can be resolved on the machine on which you plan to install the Transporter.

Transporter Installation

1. Upload the installer file to the machine on which you wish to install NAKIVO Backup & Replication in the *binary transfer mode*. For example:
   - Upload the installer from a Windows-based machine.
   - Upload the product from a Linux-based machine: run the following command: `wget 'server_ip/shared/NAKIVO_Backup_&_Replication_TRIAL.sh'`

2. Allow the execution of the installer file. For example: `chmod +x NAKIVO_Backup_&_Replication_TRIAL.sh`
3. Execute the installer file with root privileges. For example:`sudo ./NAKIVO_Backup_&_Replication_TRIAL.sh`
4. Review the license agreement (press **Space** to go to the next page of the agreement). If you agree to the terms of the license agreement, press "Y" and then press **Enter**.
5. Type "T" to install only the Transporter and press **Enter**.

   Note

   Alternatively, you can use the **-t** argument to install the Transporter silently:

   ```
   sudo ./NAKIVO_Backup_&_Replication_TRIAL.sh -t
   ```
6. Optionally, enter the master password that will be used to generate a pre-shared key and secure the Transporter and then press **Enter**.

   Notes

   - The master password must adhere to the following requirements:
     - Minimal length - 5 characters.
     - Maximum length - 50 characters.
   - The master password can be set and re-set manually by running the command on the machine housing the Transporter. Follow these steps:
     - Enter the following command: `bhsvc -b P@ssword123`
     - Restart the Transporter service.
7. Specify the installation path for the product: Press **Enter** to accept the default installation path "/opt/nakivo" or enter a custom path and press **Enter**.
8. Optionally, you can install CA Transporter certificate. Enter the path to the folder containing the certificate file and press **Enter**.

   Notes

   - If no path to the CA certificate was provided, NAKIVO Backup & Replication automatically installs a self-signed certificate.
   - It is possible to set up a master password and a CA-signed certificate for the Transporter by conducting silent installation using the command-line arguments passed to the installer. Use the following command:

     ```
     installer.sh --cert /tmp/certificate.pem -b P@ssword123 --eula-accept
     ```
9. Specify the Transporter port (used to connect to the Transporter): Press **Enter** to accept the default port "9446" or enter a custom port number and press **Enter** to begin the installation process. Make sure the port you specify is open in your firewall.

After the installation is complete, add the Transporter to NAKIVO Backup & Replication.

Installing Full Solution in Multi-Tenant Mode on Linux

Follow the steps below to install the full solution in multi-tenant mode on a Linux OS:

1. Upload the installer file to the machine on which you want to install NAKIVO Backup & Replication in the *binary transfer mode*. For example:
   - Upload the installer from a Windows-based machine.
   - Upload the product from a Linux-based machine: run the following command: `wget 'server_ip/shared/NAKIVO_Backup_&_Replication_TRIAL.sh'`
2. Log in to the Linux machine and allow the execution of the installer file.
   For example: `chmod +x NAKIVO_Backup_&_Replication_TRIAL.sh`
3. Execute the installer file with root privileges.
   For example: `sudo ./NAKIVO_Backup_&_Replication_TRIAL.sh`
4. Review the license agreement (press **Space** to go to the next page of the agreement). If you agree to the terms of the license agreement, press "Y" and then press **Enter**.
5. Type “M” to install the Director in Multi-tenant mode and press **Enter**.

   Note

   Alternatively, you can use the **-m** argument to install the solution in multi-tenant mode silently:
   ```
   sudo ./NAKIVO_Backup_&_Replication_TRIAL.sh -m
   ```
6. Optionally, you can install CA Transporter certificate. Enter the path to the folder containing the certificate file and press **Enter**.

   Notes

   - If no path to the CA certificate was provided, NAKIVO Backup & Replication automatically installs a self-signed certificate.
   - It is possible to set up CA-signed certificate for the Transporter by conducting silent installation using the command-line arguments passed to the installer. Use the following command:
     ```
     installer.sh --cert /tmp/certificate.pem --eula-accept
     ```
7. Specify the installation path for the product: Press **Enter** to accept the default installation path “/opt/nakivo” or enter a custom path and press **Enter**.
8. Specify the Director HTTPS port (which will be used to access the Web UI of NAKIVO Backup & Replication): Press **Enter** to accept the default port “4443” or enter a custom port number and press **Enter**. Make sure the port you specify is open in your firewall.
9. Specify whether to allow the product to automatically send support bundles to a NAKIVO server during the evaluation period. If this option is enabled, NAKIVO Backup & Replication will automatically create, encrypt, and upload support bundles once a day to a NAKIVO support server during the evaluation period. NAKIVO Support team may use this information to improve the product experience and will be able to identify and resolve product issues faster.

10. Specify the Transporter port (which will be used to connect to the Transporter that is installed by default with the Director): Press **Enter** to accept the default port “9446” or enter a custom port number (1 to 65535) and press **Enter**. Make sure the port you specify is open in your firewall.
11. Specify a range of port numbers (from 1 to 65535) that will be used to transfer data by the Onboard Transporter (default are 9448-10000). The range you specify should contain at least 100 ports. Make sure that the ports you specify are open in your firewall.
12. The onboard backup repository for the Master Tenant is automatically created after the installation.
13. Specify a path to the default backup repository: Press **Enter** to accept the default path `/opt/nakivo/repository` or enter a custom path and press **Enter** to begin the installation process.

Note

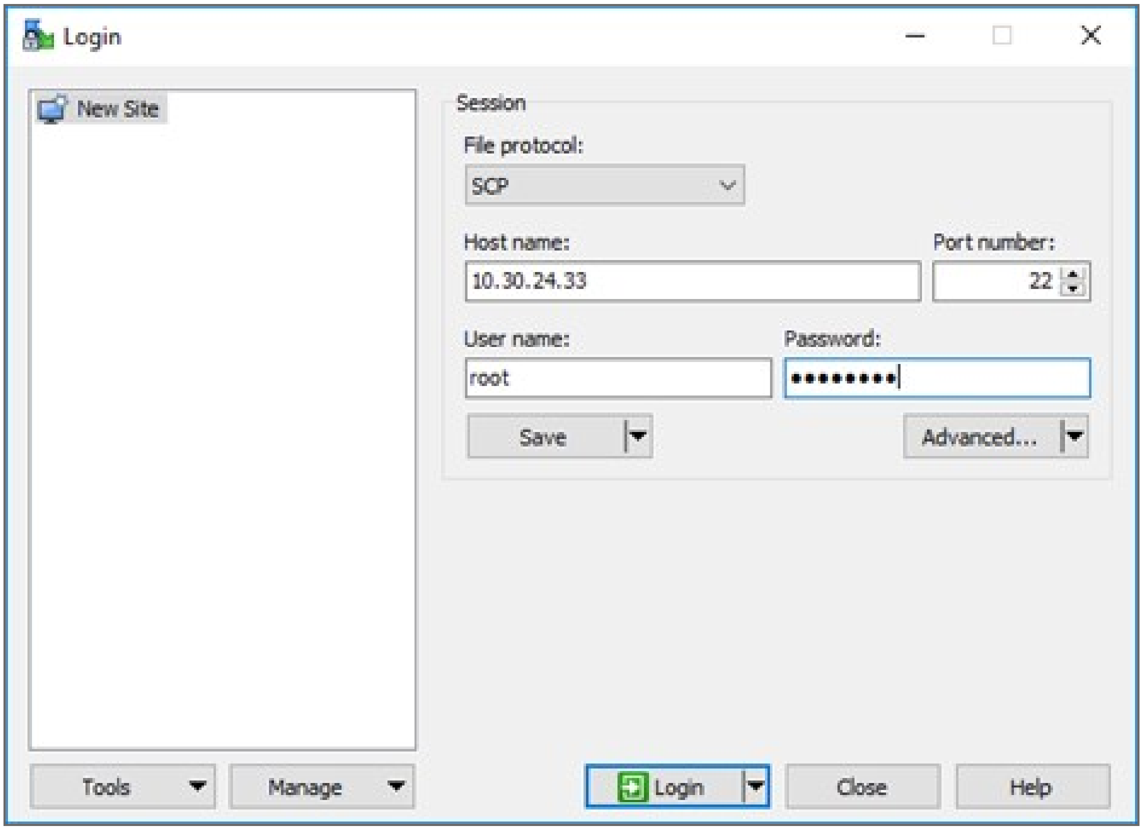
The onboard backup repository for the Master Tenant is automatically created after the installation.

After the installation is complete, you can log in to NAKIVO Backup & Replication by going to the following URL in your web browser: `https://machine_IP_or_DNS:director_https_port`.
Refer to “Getting Started” on page 21 to know how to continue working with NAKIVO Backup & Replication.

Uploading Installer from Windows Machine to Linux Machine

To upload the installer from a Windows-based machine, follow the steps below:

1. Download the free WinSCP client from http://winscp.net, install, and run it.
2. Choose **SCP** from the **File protocol** list.
3. Specify the IP address or the hostname of the Linux machine on which you would like to install the product in the **Host name** field.
4. Specify the username and password to the Linux machine in the appropriate boxes.
5. Leave other options as is and click **Login**.



File protocol: SCP

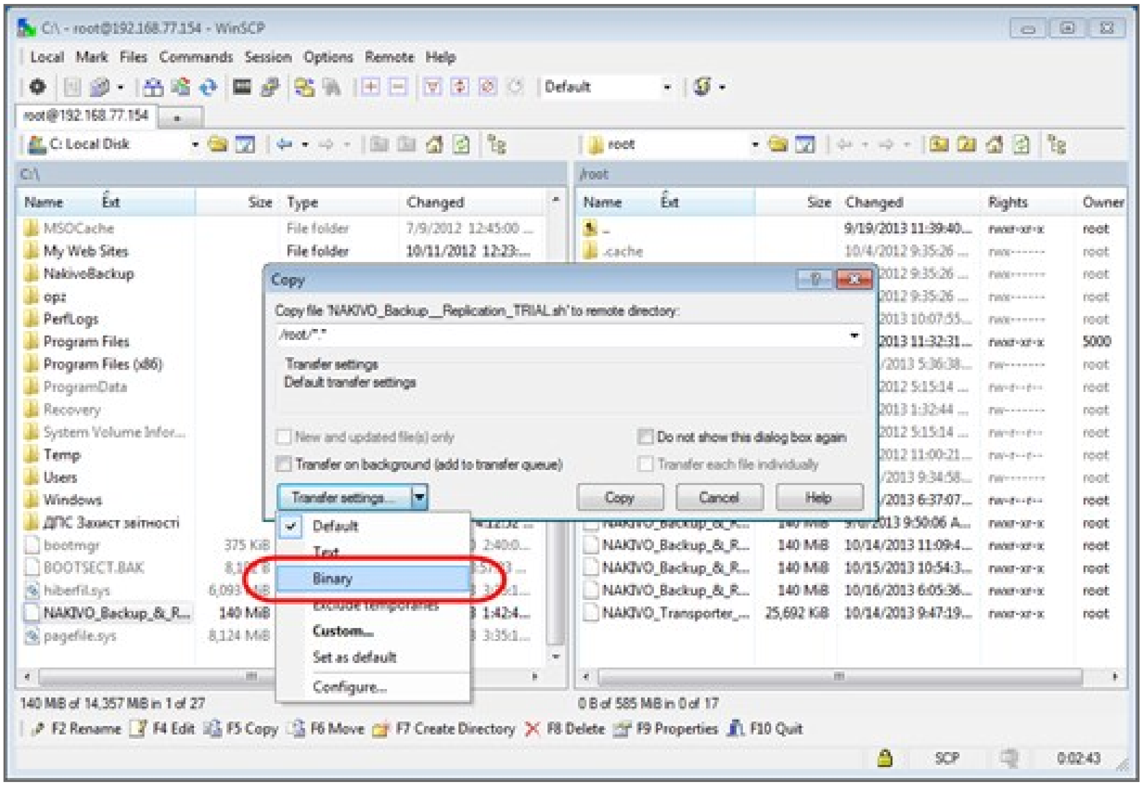
Host name: 10.30.24.33

Port number: 22

User name: root

Password: •••••••••

6. Click **Yes** in the dialog box that opens.
7. In the left pane, find the folder that contains the Linux installer, in the right pane, go up to the root folder.
8. Drag and drop the installer from left to the right pane.
9. Choose **Binary** from the **Transfer settings** drop-down list in the Copy dialog box that opens.



Name	Size	Type	Changed
MSOCache		File folder	7/9/2012 12:45:00 ...
My Web Sites		File folder	10/11/2012 12:23:...
NakivoBackup			
opz			
PerfLogs			
Program Files			
Program Files (x86)			
ProgramData			
Recovery			
System Volume Infor...			
Temp			
Users			
Windows			
ДПС Захист звітності			
bootmgr	375 KiB		2:40:0...
BOOTSECT.BAK	8,1		
hiberfil.sys	6,093		
NAKIVO_Backup_&_R...	140 MiB		1:42:4...
pagefile.sys	8,124 MiB		3:35:1...

Name	Size	Changed	Rights	Owner
..		9/19/2013 11:39:40...	rwxr-xr-x	root
.cache		10/4/2012 9:35:26 ...	rwx------	root
NAKIVO_Backup_&_R...	140 MiB	10/14/2013 11:09:4...	rwxr-xr-x	root
NAKIVO_Backup_&_R...	140 MiB	10/15/2013 10:54:3...	rwxr-xr-x	root
NAKIVO_Backup_&_R...	140 MiB	10/16/2013 6:05:36...	rwxr-xr-x	root
NAKIVO_Transporter_...	25,692 KiB	10/14/2013 9:47:19...	rwxr-xr-x	root

Copy file 'NAKIVO_Backup__Replication_TRIAL.sh' to remote directory:

/root/*.*

Transfer settings
Default transfer settings

□ New and updated file(s) only
□ Do not show this dialog box again
□ Transfer on background (add to transfer queue)
□ Transfer each file individually

140 MiB of 14,357 MiB in 1 of 27

0 B of 585 MiB in 0 of 17

10. Click **Copy**.

Installing on Synology NAS

NAKIVO Backup & Replication can be installed directly on a supported Synology NAS to create your own, high-performance backup appliance. With the appliance, all VM data protection components are unified in a single system that is fast to deploy and easy to manage, while also not consuming your environment's valuable resources. Moreover, you are getting an all-in-one backup hardware, backup software, backup storage, and data deduplication in a single box. This results in a zero VMware footprint, less power and cooling, less required maintenance, time, money, and – most of all – higher VM backup performance.

You can install a Synology package with either all NAKIVO Backup & Replication components (Director, Transporter, Backup Repository) or a Transporter only. The product can be installed via Package Center or manually. For more details, refer to the corresponding topics below:

- "Installing on Synology NAS via Package Center" on page 137
- "Installing on Synology NAS Manually" on page 139

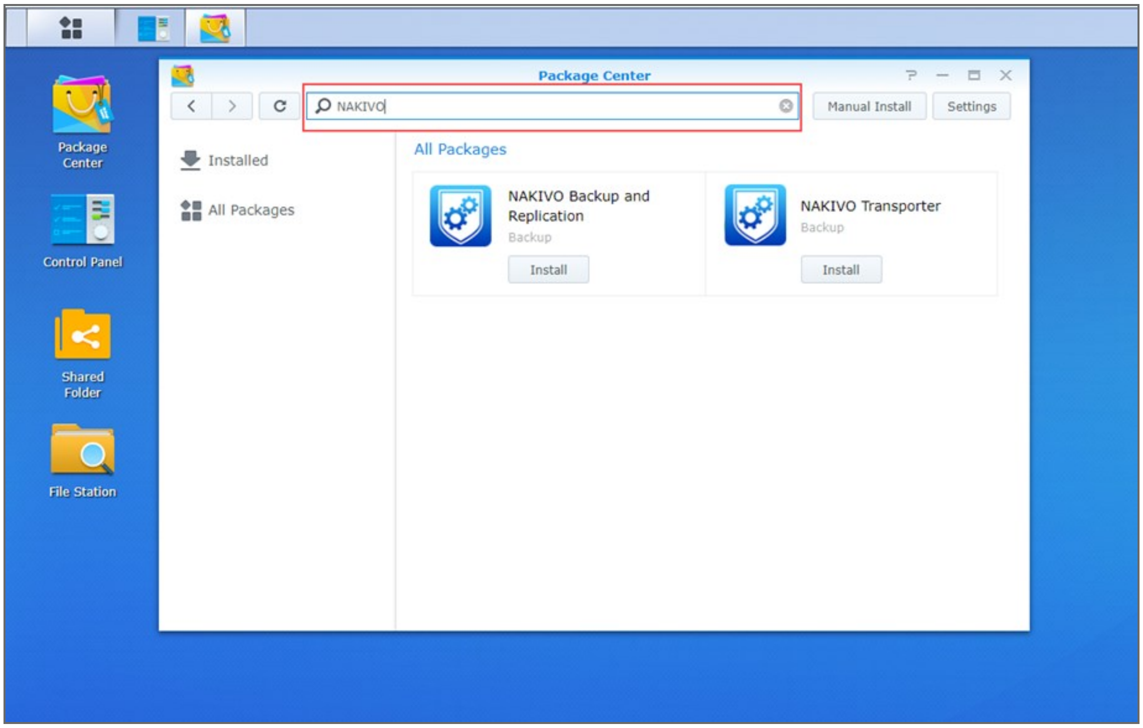
Note

A pre-shared key is not created during Transporter-only installation. When adding this Transporter to NAKIVO Backup & Replication, filling out the master password field is not required. The master password can be manually set and reset later. For details. refer to "Adding Installed Transporters" on page 251.

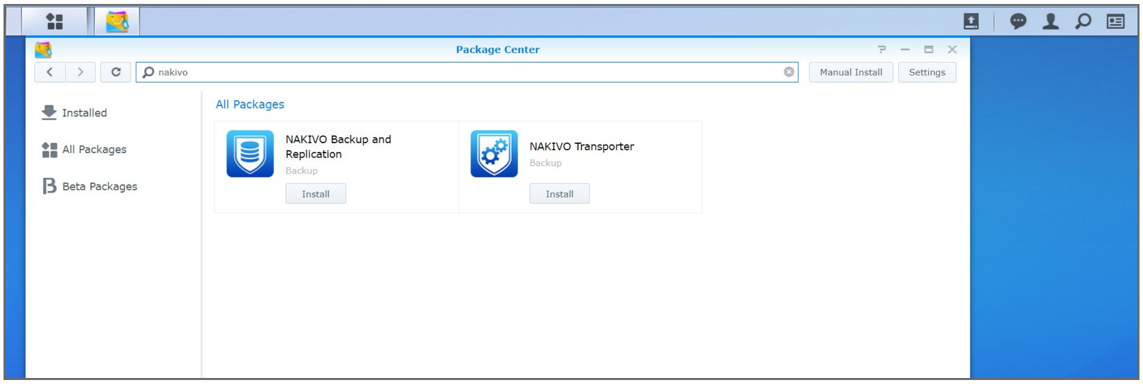
Installing on Synology NAS via Package Center

To automatically install a NAKIVO Backup & Replication application on a Synology NAS, do the following:

1. Log in to your Synology account and open **Package Center** in the management interface.
2. Use the search box to find NAKIVO Backup & Replication packages.

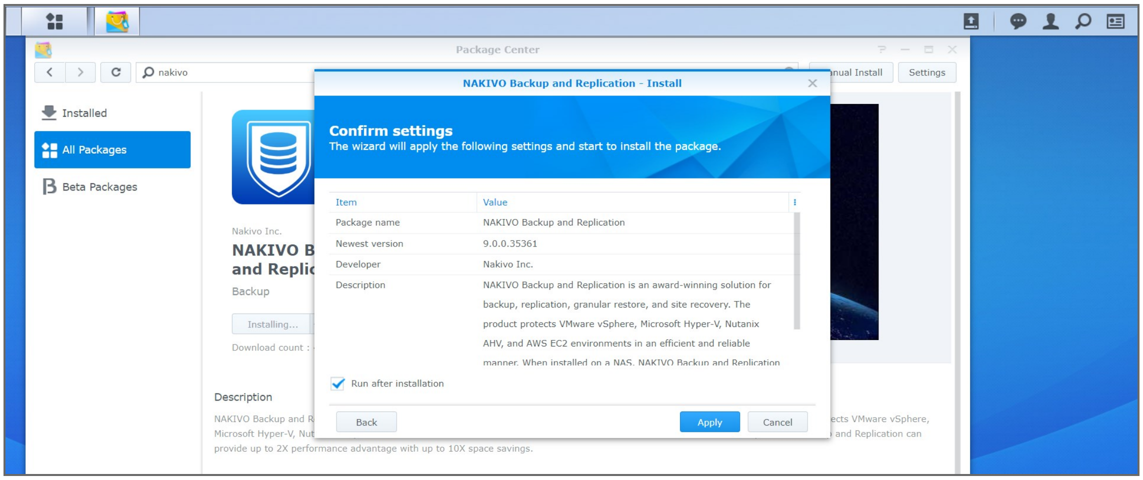


3. Click **Install** on one of the following:
   - **NAKIVO Backup and Replication** to install all product components.
   - **NAKIVO Transporter**to install a Transporter only.



4. Select the **I accept the terms of the license agreement** checkbox and click **Next**.

5. In the **Confirm settings** dialog box, click **Apply**.



NAKIVO Backup and Replication - Install

Confirm settings

The wizard will apply the following settings and start to install the package.

Item	Value
Package name	NAKIVO Backup and Replication
Newest version	9.0.0.35361
Developer	Nakivo Inc.
Description	NAKIVO Backup and Replication is an award-winning solution for backup, replication, granular restore, and site recovery. The product protects VMware vSphere, Microsoft Hyper-V, Nutanix AHV, and AWS EC2 environments in an efficient and reliable manner. When installed on a NAS, NAKIVO Backup and Replication

☑ Run after installation

Back | Apply | Cancel

Refer to “Getting Started” on page 21 to better understand how to continue working with NAKIVO Backup & Replication.

Installing on Synology NAS Manually

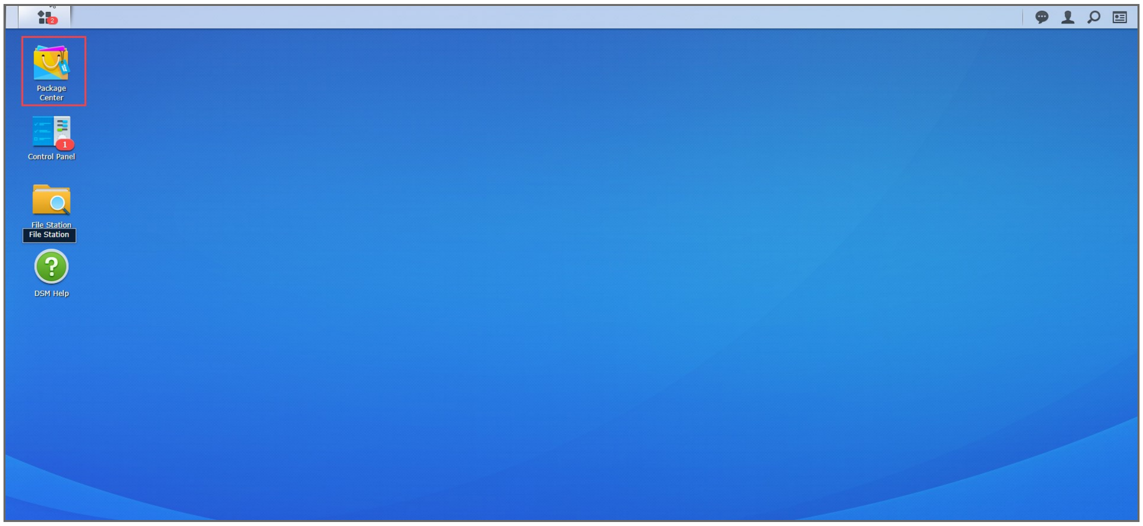
If for any reason installation of NAKIVO Backup & Replication via Package Center is not available for your Synology NAS, you can install it manually.

The following packages are available for manual installation:

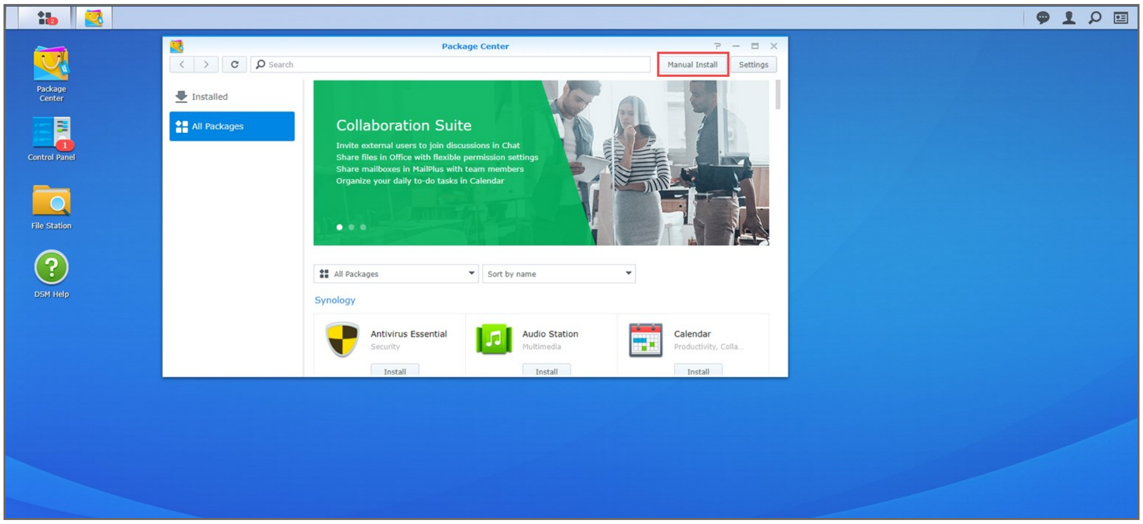
- Synology package
- Synology Transporter package
- Synology ARM package
- Synology ARM Transporter package

To manually install NAKIVO Backup & Replication on a Synology NAS, do the following:

1. Download a Synology NAS package.
2. Log in to your Synology account and open the **Package Center** in the management interface.



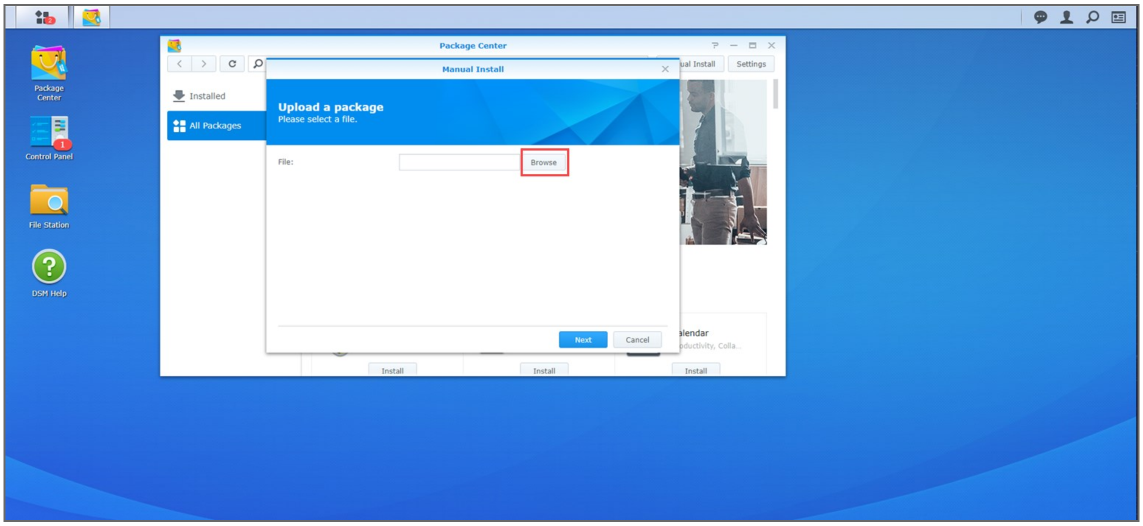
3. Click **Manual Install.**



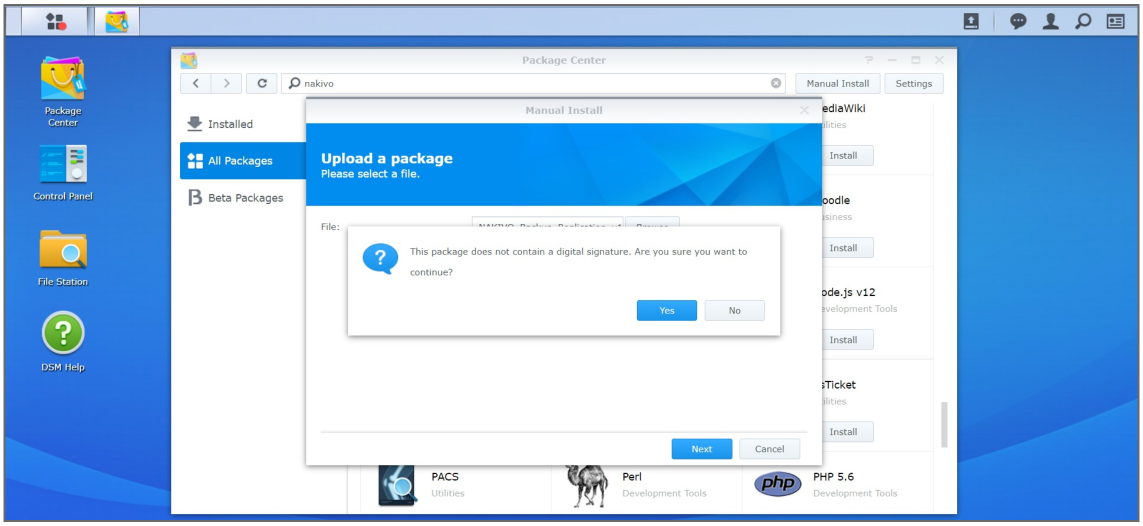
Collaboration Suite

Invite external users to join discussions in Chat
Share files in Office with flexible permission settings
Share mailboxes in MailPlus with team members
Organize your daily to-do tasks in Calendar

4. Click **Browse**, navigate to the Synology NAS package that you have downloaded, select it, and click **Open**.

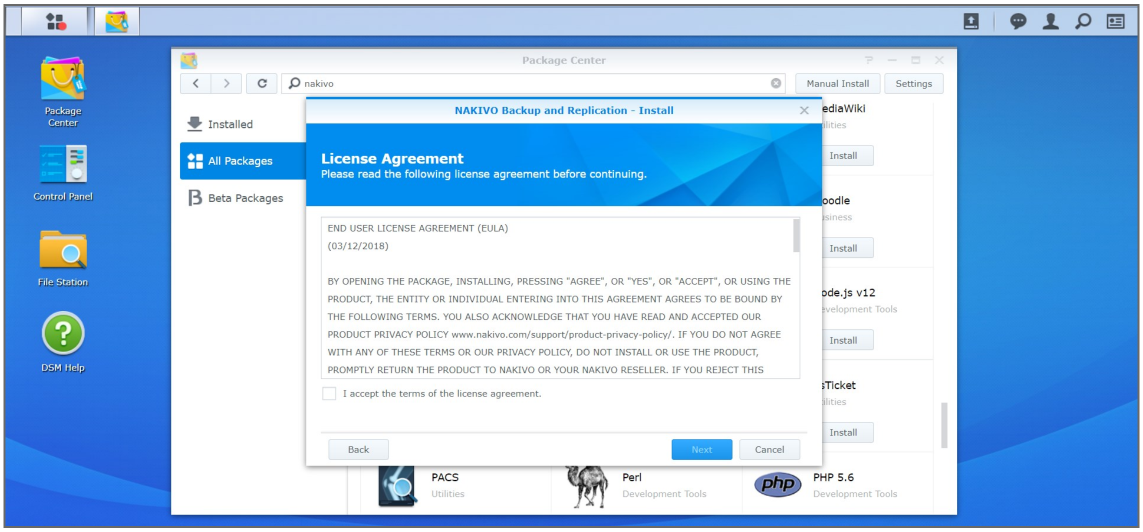


5. Click **Yes** to proceed.



This package does not contain a digital signature. Are you sure you want to continue?

6. After reading through the License Agreement, check **I accept the terms of the license agreement** and click **Next**.



NAKIVO Backup and Replication - Install

License Agreement

Please read the following license agreement before continuing.

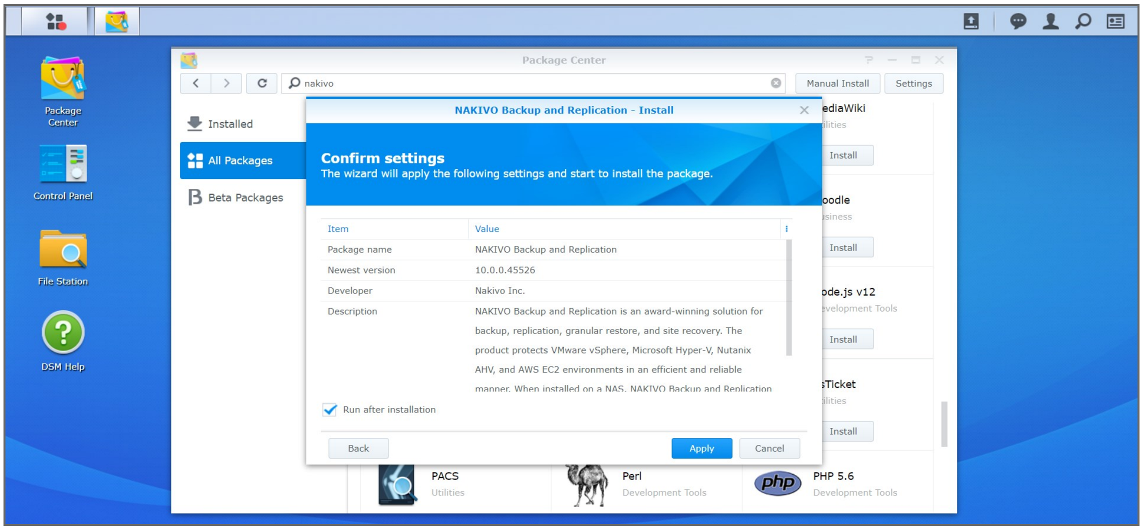
END USER LICENSE AGREEMENT (EULA)

(03/12/2018)

BY OPENING THE PACKAGE, INSTALLING, PRESSING "AGREE", OR "YES", OR "ACCEPT", OR USING THE PRODUCT, THE ENTITY OR INDIVIDUAL ENTERING INTO THIS AGREEMENT AGREES TO BE BOUND BY THE FOLLOWING TERMS. YOU ALSO ACKNOWLEDGE THAT YOU HAVE READ AND ACCEPTED OUR PRODUCT PRIVACY POLICY www.nakivo.com/support/product-privacy-policy/. IF YOU DO NOT AGREE WITH ANY OF THESE TERMS OR OUR PRIVACY POLICY, DO NOT INSTALL OR USE THE PRODUCT, PROMPTLY RETURN THE PRODUCT TO NAKIVO OR YOUR NAKIVO RESELLER. IF YOU REJECT THIS

☐ I accept the terms of the license agreement.

7. Optionally check **Run after installation** to start NAKIVO Backup & Replication immediately after the install process is finished. Click **Apply.**



NAKIVO Backup and Replication - Install

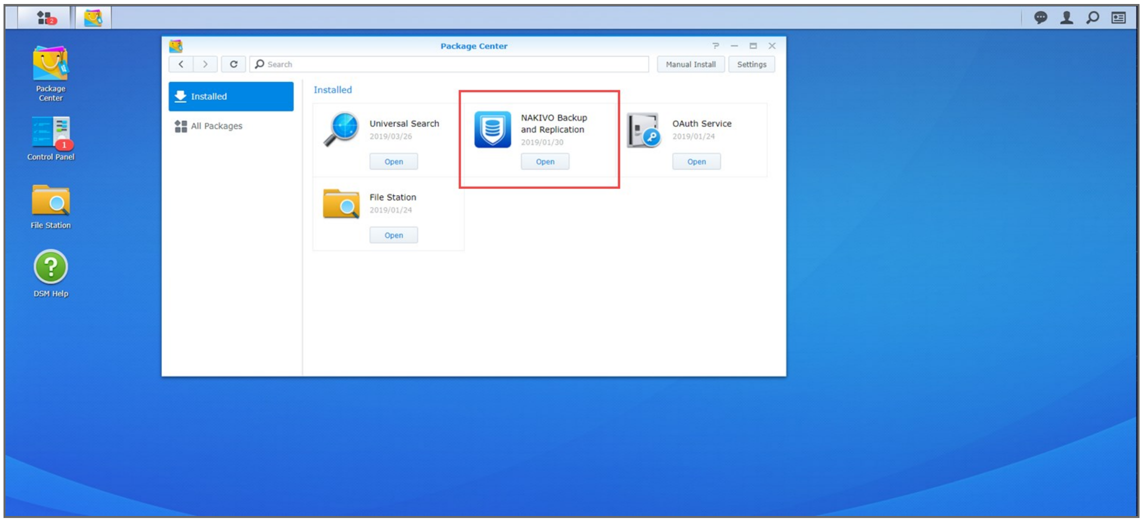
Confirm settings

The wizard will apply the following settings and start to install the package.

Item	Value
Package name	NAKIVO Backup and Replication
Newest version	10.0.0.45526
Developer	Nakivo Inc.
Description	NAKIVO Backup and Replication is an award-winning solution for backup, replication, granular restore, and site recovery. The product protects VMware vSphere, Microsoft Hyper-V, Nutanix AHV, and AWS EC2 environments in an efficient and reliable manner. When installed on a NAS, NAKIVO Backup and Replication

☑ Run after installation

8. Now NAKIVO Backup & Replication is installed on your NAS. To open the NAKIVO Backup & Replication Web interface, go to the following address in your web browser: `https://NAS_IP_address:4443`, or click the NAKIVO Backup & Replication icon in the main menu of the NAS.



Refer to "Getting Started" on page 21 to better understand how to continue working with NAKIVO Backup & Replication.

Installing on QNAP NAS

You can install a QNAP package with either all NAKIVO Backup & Replication components (Director, Transporter, Backup Repository) or a Transporter only.

NAKIVO Backup & Replication can be installed directly on a supported QNAP NAS to create your own, high-performance backup appliance. With this appliance, all VM data protection components are unified in a single system that is quick to deploy and easy to manage, while also not consuming your environment's valuable resources. Moreover, you are getting an all-in-one backup hardware, backup software, backup storage, and data deduplication in a single box. This results in a zero VMware footprint, less power and cooling, less required maintenance, time, money, and – most of all – higher VM backup performance.

You can install NAKIVO Backup & Replication either via QNAP store or manually.

- “Installing on QNAP NAS via QNAP Store” on page 144
- “Installing on QNAP NAS Manually” on page 146

Note

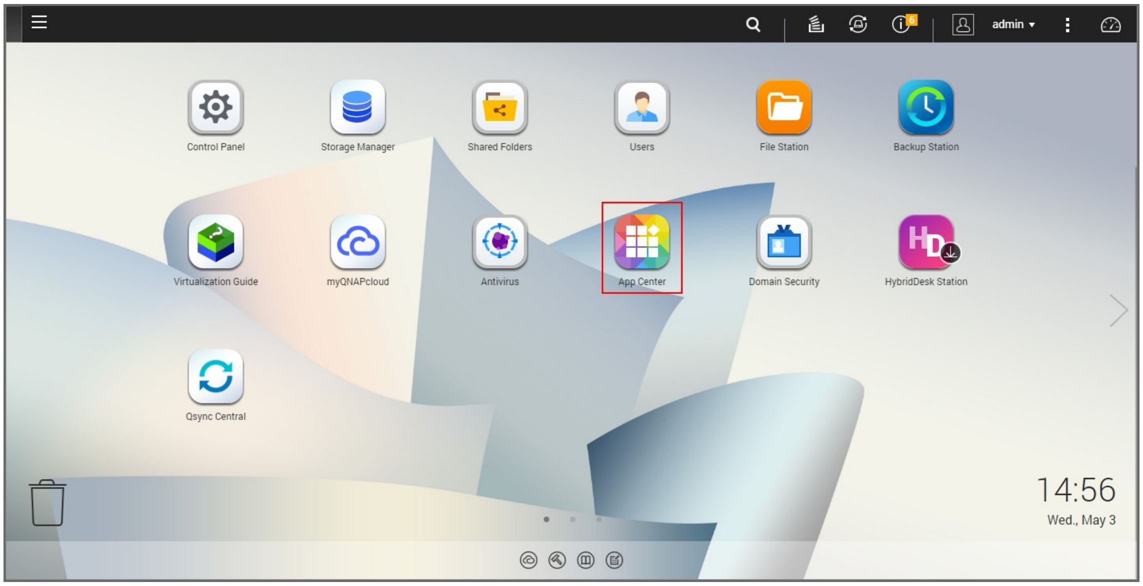
A pre-shared key is not created during Transporter-only installation. When adding this Transporter to NAKIVO Backup & Replication, filling out the master password field is not required. The master password can be manually set and reset later. For details. refer to “Adding Installed Transporters” on page 251.

Installing on QNAP NAS via QNAP Store

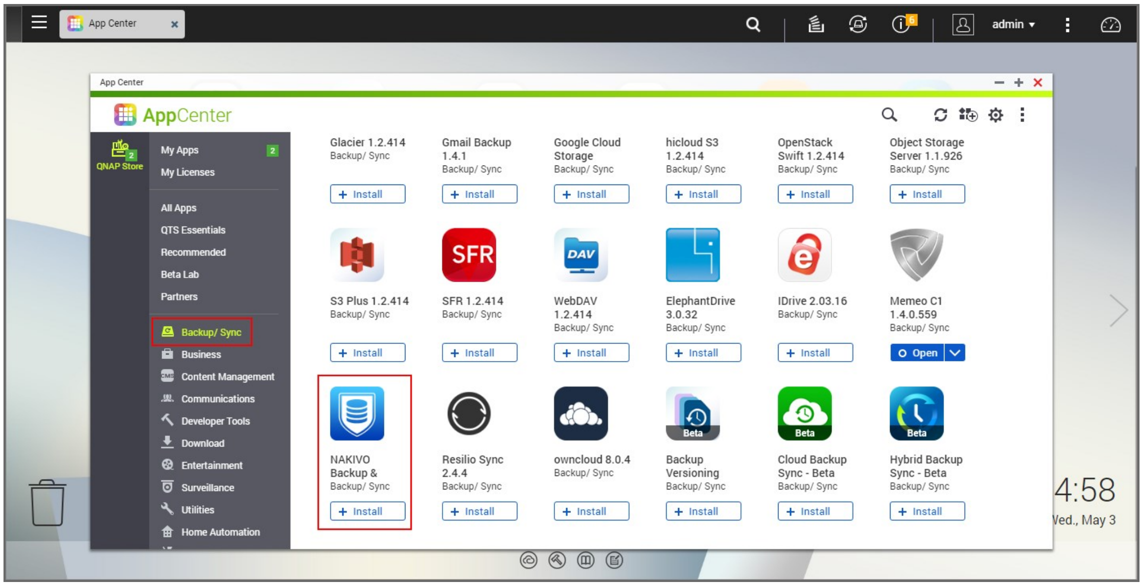
Check to see if your NAS model is supported before you begin installing NAKIVO Backup & Replication on a QNAP NAS.

To install NAKIVO Backup & Replication take the following steps:

1. Open the QNAP Desktop in your browser by entering the IP address of your QNAP NAS.



2. Go to **App Center**.
3. Select the **Backup/Sync** category and locate NAKIVO Backup & Replication. Alternatively, you can use the search bar at the top of the App Center window. Click on the magnifying glass icon and enter 'Nakivo'.


App Center
admin
AppCenter
QNAP Store
My Apps
My Licenses
All Apps
QTS Essentials
Recommended
Beta Lab
Partners
Backup/ Sync
Business
Content Management
Communications
Developer Tools
Download
Entertainment
Surveillance
Utilities
Home Automation
Glacier 1.2.414 Backup/ Sync
Gmail Backup 1.4.1 Backup/ Sync
Google Cloud Storage Backup/ Sync
hicloud S3 1.2.414 Backup/ Sync
OpenStack Swift 1.2.414 Backup/ Sync
Object Storage Server 1.1.926 Backup/ Sync
S3 Plus 1.2.414 Backup/ Sync
SFR 1.2.414 Backup/ Sync
WebDAV 1.2.414 Backup/ Sync
ElephantDrive 3.0.32 Backup/ Sync
IDrive 2.03.16 Backup/ Sync
Memeo C1 1.4.0.559 Backup/ Sync
NAKIVO Backup & Backup/ Sync
Resilio Sync 2.4.4 Backup/ Sync
owncloud 8.0.4 Backup/ Sync
Backup Versioning Backup/ Sync
Cloud Backup Sync - Beta Backup/ Sync
Hybrid Backup Sync - Beta Backup/ Sync
+ Install
Open
4:58
Ved., May 3

4. Click **Install**.
5. Wait till the installation is completed.

By default, NAKIVO Backup & Replication interface is available by the IP address of your QNAP NAS on the port 4443: `https://<IP_address_of_QNAP_NAS>:4443`.

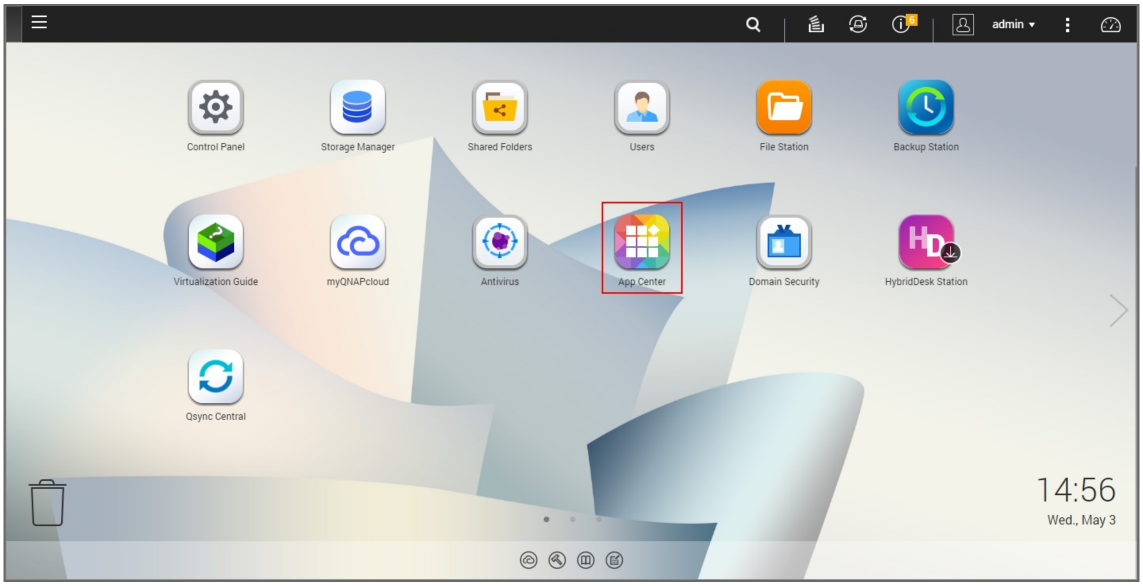
Refer to "Getting Started" on page 21 to know how to continue working with NAKIVO Backup & Replication.

Installing on QNAP NAS Manually

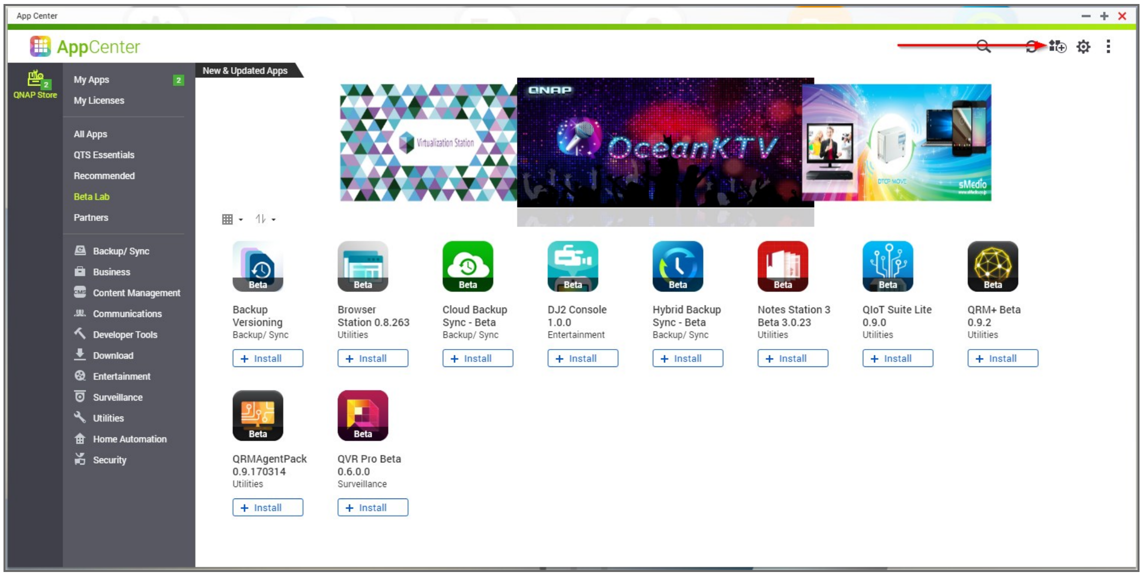
Before you begin installing NAKIVO Backup & Replication on a NAS, make sure your NAS model is supported and you have downloaded the installer (.qpkg file) for QNAP NAS.

To install NAKIVO Backup & Replication on a NAS:

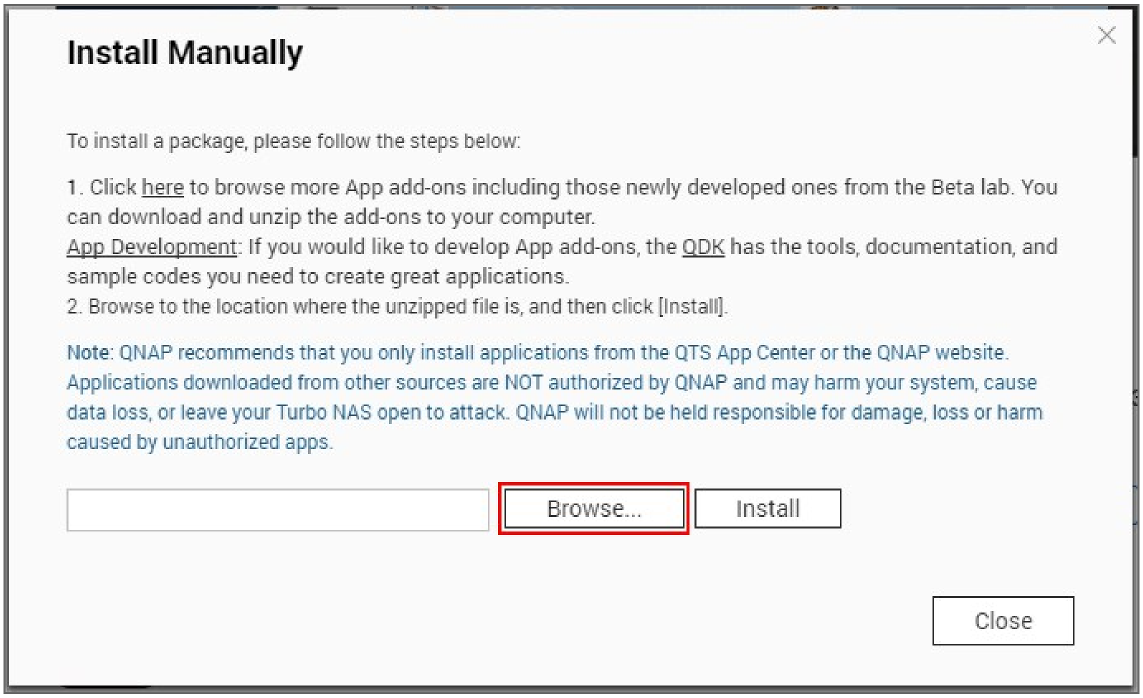
1. Open the QNAP Desktop in your browser by entering the IP address of your QNAP NAS.



2. Go to **App Center**.
3. Click the **Install Manually** icon.



4. Click **Browse** in the window that appears and locate the installer (.qpkg file) on your computer.



Install Manually

To install a package, please follow the steps below:

1. Click here to browse more App add-ons including those newly developed ones from the Beta lab. You can download and unzip the add-ons to your computer.
App Development: If you would like to develop App add-ons, the QDK has the tools, documentation, and sample codes you need to create great applications.
2. Browse to the location where the unzipped file is, and then click [Install].

Note: QNAP recommends that you only install applications from the QTS App Center or the QNAP website. Applications downloaded from other sources are NOT authorized by QNAP and may harm your system, cause data loss, or leave your Turbo NAS open to attack. QNAP will not be held responsible for damage, loss or harm caused by unauthorized apps.

5. Click **Install**.
6. Wait until the installation is complete.

By default, NAKIVO Backup & Replication interface is available at the IP address of your QNAP NAS on the port 4443: `https://<IP_address_of_QNAP_NAS>:4443`.

Refer to “Getting Started” on page 21 to better understand how to continue working with NAKIVO Backup & Replication.

Installing on ASUSTOR NAS

You can install an ASUSTOR package with either all NAKIVO Backup & Replication components (Director, Transporter, Backup Repository) or a Transporter only.

NAKIVO Backup & Replication can be installed directly on a supported ASUSTOR NAS to create your own, high-performance backup appliance. With the appliance, all VM data protection components are unified in a single system that is fast to deploy and easy to manage, while also not consuming your environment's valuable resources. Moreover, you are getting an all-in-one backup hardware, backup software, backup storage, and data deduplication in a single box.

- "Installing on ASUSTOR NAS via App Central" on page 149
- "Installing on ASUSTOR NAS Manually" on page 151

Note

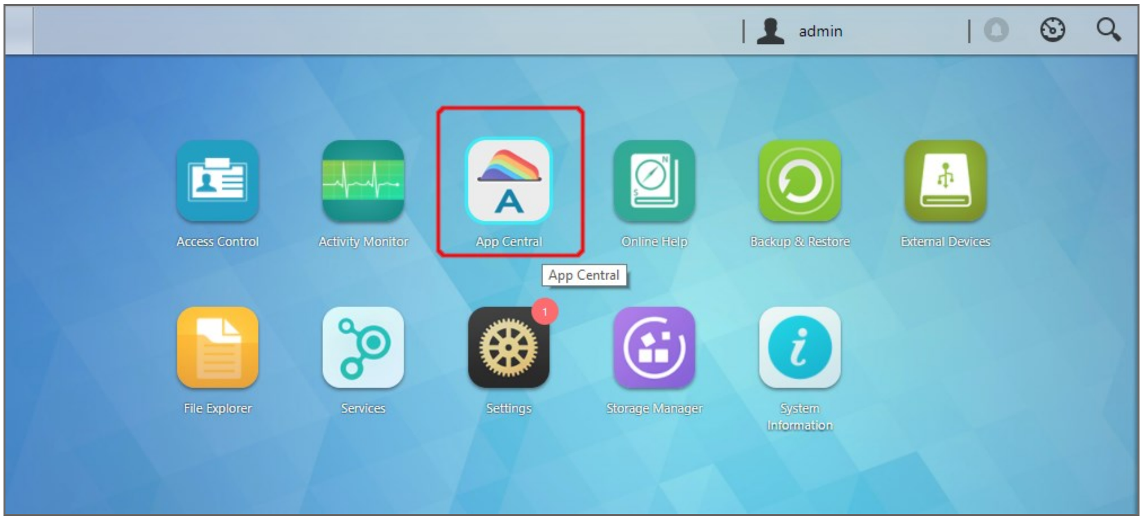
A pre-shared key is not created during Transporter-only installation. When adding this Transporter to NAKIVO Backup & Replication, filling out the master password field is not required. The master password can be manually set and reset later. For details. refer to "Adding Installed Transporters" on page 251.

Installing on ASUSTOR NAS via App Central

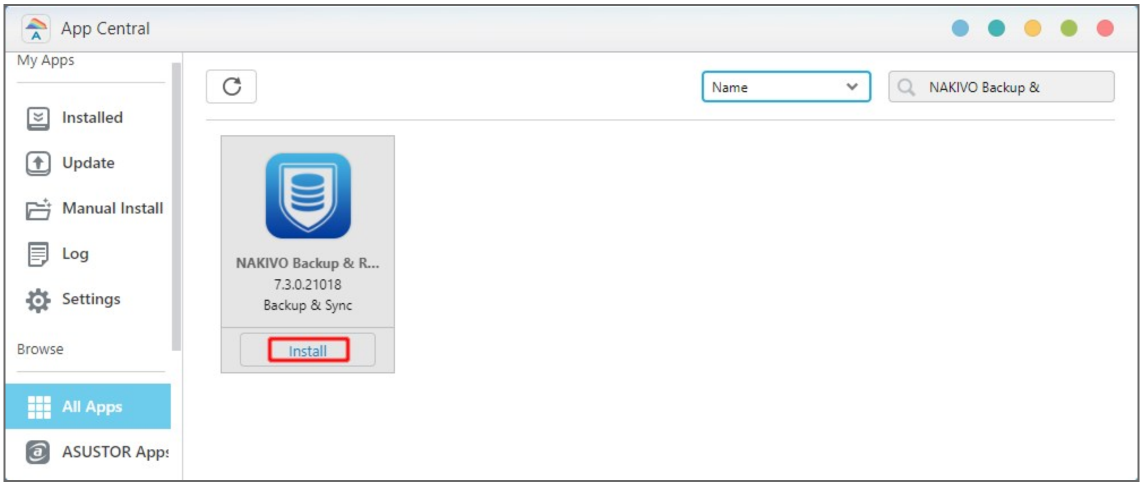
Before you begin installing NAKIVO Backup & Replication on a NAS make sure your NAS model is supported.

To install NAKIVO Backup & Replication on ASUSTOR NAS via App Central:

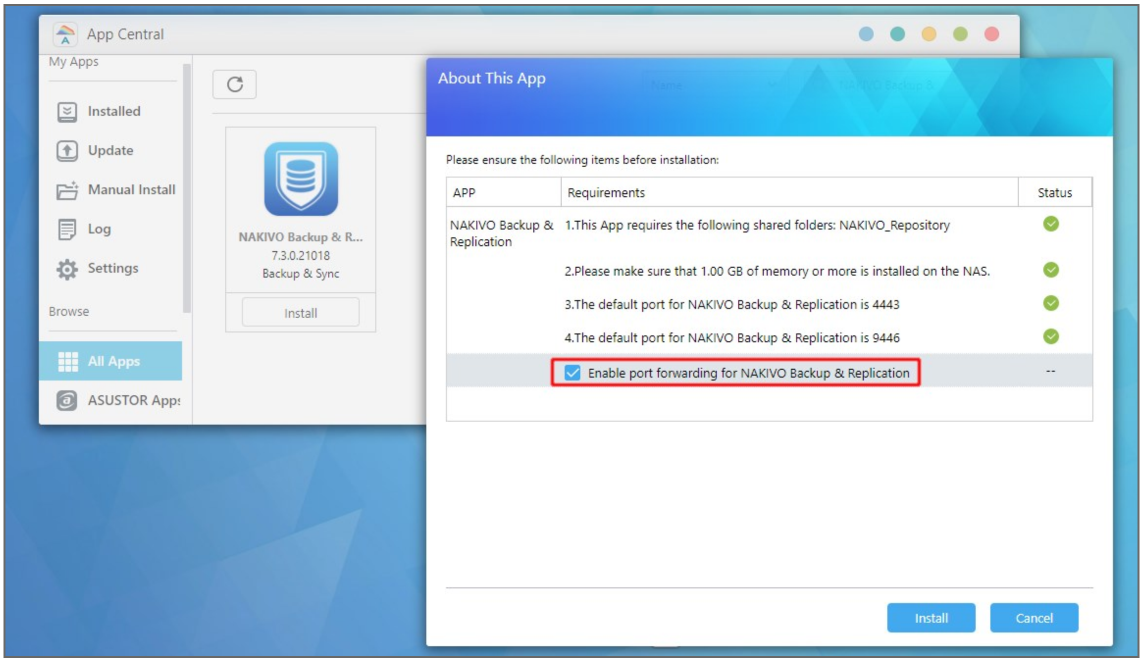
1. Open the ASUSTOR Desktop in your browser by entering the IP address of your ASUSTOR NAS.



2. Go to **App Central**.
3. Go to **Browse** > **All Apps**.
4. Find **NAKIVO Backup & Replication** in the store. Alternatively, enter **Nakivo** in the search box.
5. Click **Install**.



6. In the **About This App** dialog box that opens, select **Enable port forwarding for NAKIVO Backup & Replication** and then click **Install**.



About This App

Please ensure the following items before installation:

APP	Requirements	Status
NAKIVO Backup & Replication	1.This App requires the following shared folders: NAKIVO_Repository	✓
	2.Please make sure that 1.00 GB of memory or more is installed on the NAS.	✓
	3.The default port for NAKIVO Backup & Replication is 4443	✓
	4.The default port for NAKIVO Backup & Replication is 9446	✓
	☑ Enable port forwarding for NAKIVO Backup & Replication	--

7. Wait until the installation is complete.

By default, the NAKIVO Backup & Replication interface is available at the IP address of your ASUSTOR NAS on the port 4443: `https://<IP_address_of_ASUSTOR_NAS>:4443`.

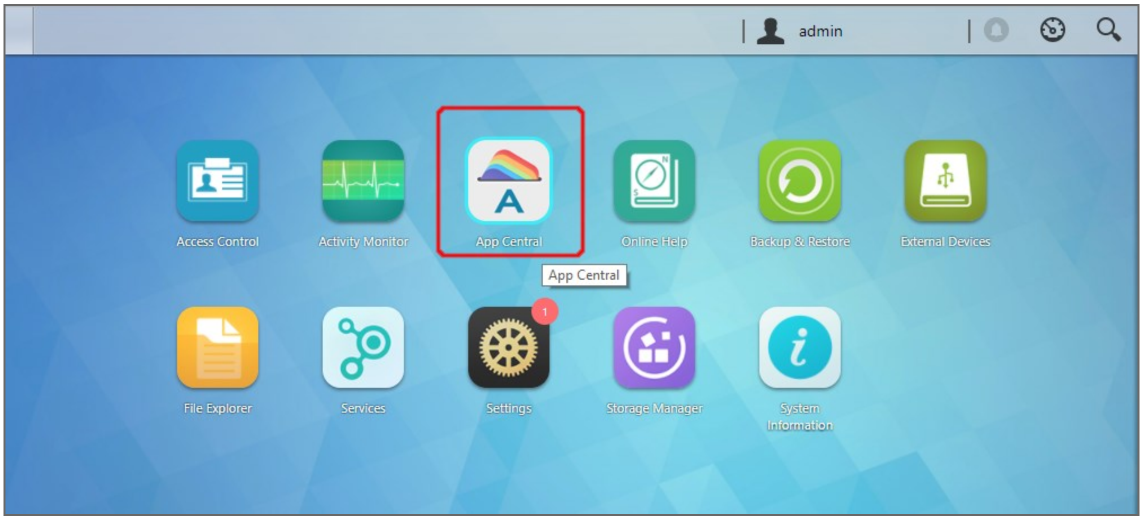
Refer to “Getting Started” on page 21 to understand better how to continue working with NAKIVO Backup & Replication.

Installing on ASUSTOR NAS Manually

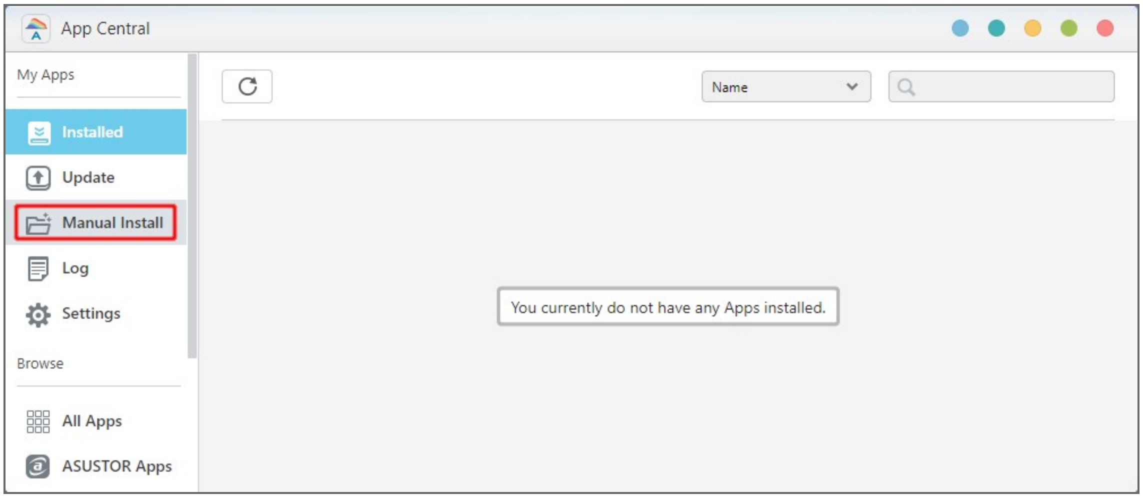
Before you begin installing NAKIVO Backup & Replication on a NAS, make sure your NAS model is supported and you have downloaded an installer (.apk file) for ASUSTOR NAS.

To manually install NAKIVO Backup & Replication on ASUSTOR NAS:

1. Open the ASUSTOR Desktop in your browser by entering the IP address of your ASUSTOR NAS.
2. Go toApp Central.

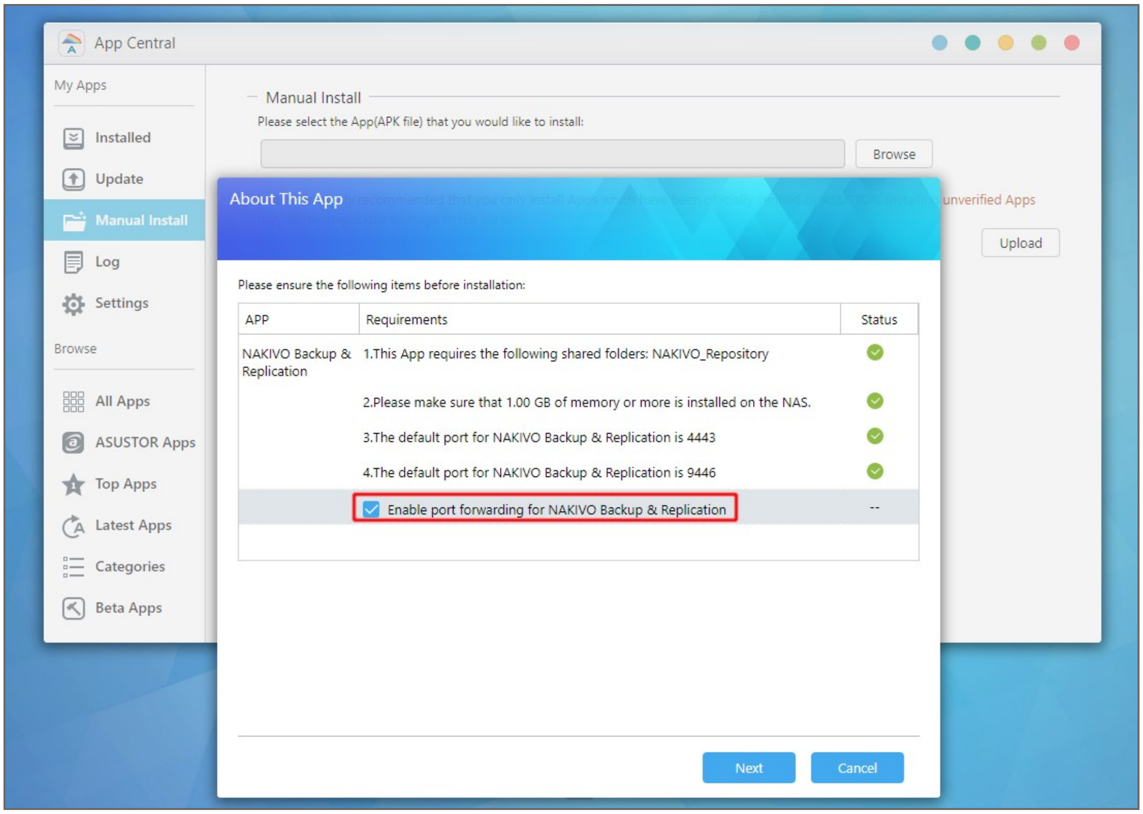


3. Click **Manual Install**.



You currently do not have any Apps installed.

4. Click **Browse**. In the dialog box that opens, locate the installer (.apk file) on your computer.
5. Click **Upload**.
6. In the **About This App** dialog box that opens, check **Enable port forwarding for NAKIVO Backup & Replication**.



Please select the App(APK file) that you would like to install:

Please ensure the following items before installation:

APP	Requirements	Status
NAKIVO Backup & Replication	1.This App requires the following shared folders: NAKIVO_Repository	✓
	2.Please make sure that 1.00 GB of memory or more is installed on the NAS.	✓
	3.The default port for NAKIVO Backup & Replication is 4443	✓
	4.The default port for NAKIVO Backup & Replication is 9446	✓
	☑ Enable port forwarding for NAKIVO Backup & Replication	--

7. Click **Next**.
8. In the warning dialog box that opens, select **I understand the risks associated with installing unverified apps**.
9. Click **Install**.
10. Wait until the installation is complete.

By default, the NAKIVO Backup & Replication interface is available at the IP address of your ASUSTOR NAS on the port 4443: `https://<IP_address_of_ASUSTOR_NAS>:4443`.

Refer to “Getting Started” on page 21 to understand better how to continue working with NAKIVO Backup & Replication.

Installing on Western Digital NAS

You can install a Western Digital MyCloud package with either all NAKIVO Backup & Replication components (Director, Transporter, Backup Repository) or a Transporter only. The following packages are available:

- Western Digital MyCloud DL2100 package
- Western Digital MyCloud DL2100 Transporter package
- Western Digital MyCloud DL4100 package
- Western Digital MyCloud DL4100 Transporter package
- Western Digital MyCloud PR2100 package
- Western Digital MyCloud PR 2100 Transporter package
- Western Digital MyCloud PR 4100 package
- Western Digital MyCloud PR 4100 Transporter package

NAKIVO Backup & Replication can be installed directly on a Western Digital MyCloud NAS to create your own, high-performance backup appliance. With this appliance, all VM data protection components are unified in a single system that is quick to deploy and easy to manage, while also not consuming your environment's valuable resources. Moreover, you are getting an all-in-one backup hardware, backup software, backup storage, and data deduplication in a single box. This results in a zero VMware footprint, less power and cooling, less required maintenance, time, money, and – most of all – higher VM backup performance.

NAKIVO Backup & Replication is installed on a NAS hard drive (not on the NAS Flash memory), so if you remove the hard drive from the NAS you will also remove the product from it.

Note

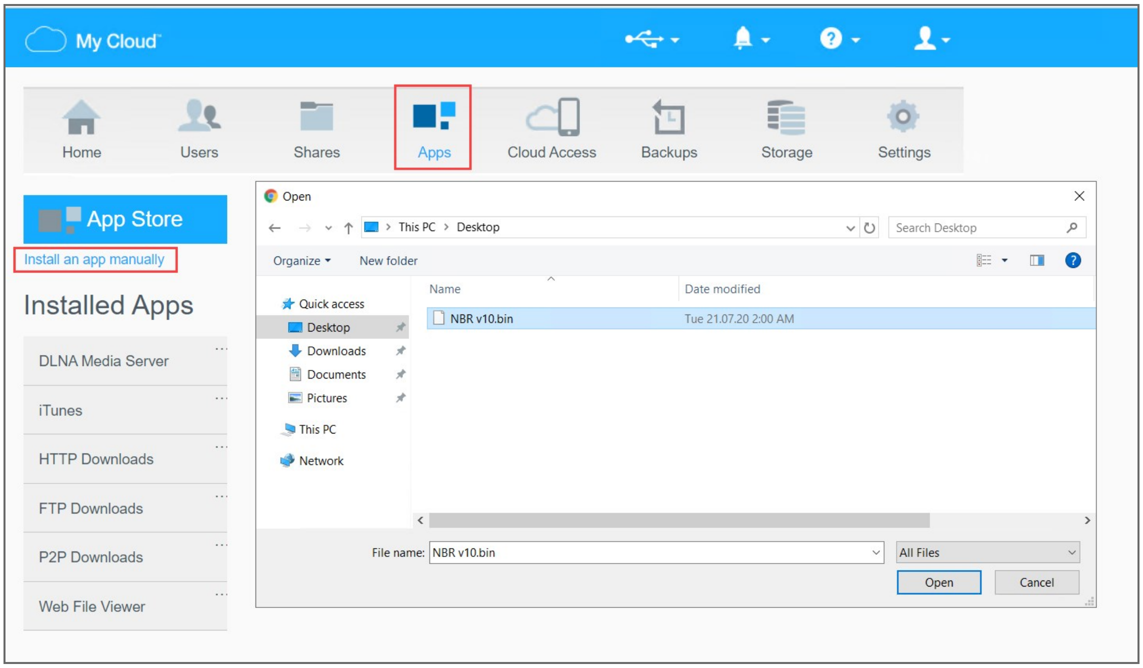
A pre-shared key is not created during Transporter-only installation. When adding this Transporter to NAKIVO Backup & Replication, filling out the master password field is not required. The master password can be manually set and reset later. For details. refer to “Adding Installed Transporters” on page 251.

Prior to installing NAKIVO Backup & Replication onto a Western Digital MyCloud NAS device, make sure the following requirements have been met:

1. Your Western Digital MyCloud NAS model is supported by NAKIVO Backup & Replication.
2. You have access to the NAS **My Cloud** Dashboard.
3. You have NAKIVO Backup & Replication installer for Western Digital NAS available on your computer.

Follow the steps below to install NAKIVO Backup & Replication on a Western Digital MyCloud NAS device:

1. On the **My Cloud** dashboard, click **Apps**. The list of installed NAS applications opens on the left side of the page.
2. Above the list of NAS installed applications, click **Install an app manually**. The **File Upload** dialog opens.



NBR v10.bin Tue 21.07.20 2:00 AM

File name: NBR v10.bin

3. In the **File Upload** dialog, navigate to your copy of NAKIVO Backup & Replication installer and click **Open**. The installation progress bar opens.
4. When the installation finishes successfully, a dialog box opens with a message informing you about it. Click **OK** to close the dialog box.

After the installation is complete, NAKIVO Backup & Replication will appear in the list of installed NAS applications. To access the product, do either of the following:

- Open the `https://<NAS_IP>:4443` address in your browser.
- In the list of installed NAS applications, click **NAKIVO Backup & Replication** and then click **Configure**.

Refer to "Getting Started" on page 21 to better understand how to continue working with NAKIVO Backup & Replication.

Installing on NETGEAR ReadyNAS

You can install the NETGEAR package that includes all NAKIVO Backup & Replication components (Director, Transporter, Backup Repository) or the NETGEAR Transporter package.

NAKIVO Backup & Replication can be installed directly on a supported NETGEAR ReadyNAS to create your own high-performance backup appliance. With the appliance, all VM data protection components are unified in a single system that is fast to deploy and easy to manage, while also not consuming your environment's valuable resources. Moreover, you are getting an all-in-one backup hardware, backup software, backup storage, and data deduplication in a single box. For installation instructions, refer to the following topics:

- "Installing on NETGEAR ReadyNAS via Available Apps" on page 156
- "Installing on NETGEAR ReadyNAS Manually" on page 157

Note

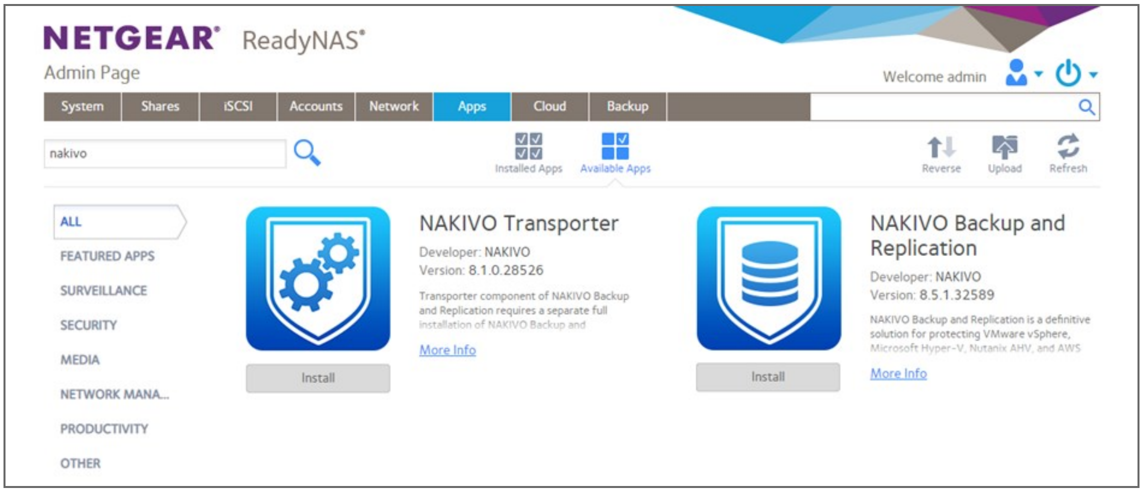
A pre-shared key is not created during Transporter-only installation. When adding this Transporter to NAKIVO Backup & Replication, filling out the master password field is not required. The master password can be manually set and reset later. For details. refer to "Adding Installed Transporters" on page 251.

Installing on NETGEAR ReadyNAS via Available Apps

Before you begin installing NAKIVO Backup & Replication or NAKIVO Transporter on a NETGEAR ReadyNAS device, please check if your NETGEAR ReadyNAS model is supported.

To install NAKIVO Backup & Replication or NAKIVO Transporter, take the following steps:

1. Open the NETGEAR ReadyNAS **Admin Page** in your browser by entering the IP address of your NAS.
2. Go to **Apps** -> **Available Apps**.
3. Find **NAKIVO Backup & Replication** or **NAKIVO Transporter** in the list of available applications. Alternatively, you can enter `NAKIVO` to the filtering box in the upper left corner of the **Admin Page**.
4. Click the **Install** button below the corresponding item.



NAKIVO Transporter

Developer: NAKIVO

Version: 8.1.0.28526

Transporter component of NAKIVO Backup and Replication requires a separate full installation of NAKIVO Backup and

NAKIVO Backup and Replication

Developer: NAKIVO

Version: 8.5.1.32589

NAKIVO Backup and Replication is a definitive solution for protecting VMware vSphere, Microsoft Hyper-V, Nutanix AHV, and AWS

Note

Make sure that only one instance of the NAKIVO solution - either Full Product or Transporter-only - is installed on the device concurrently. Having both products installed at once may lead to incorrect operation.

5. Wait until the installation is completed.

By default, the **NAKIVO Backup & Replication** interface is available at the IP address of your NETGEAR ReadyNAS on the port 4443: `https://<IP_address_of_ NETGEAR_ReadyNAS>:4443`.

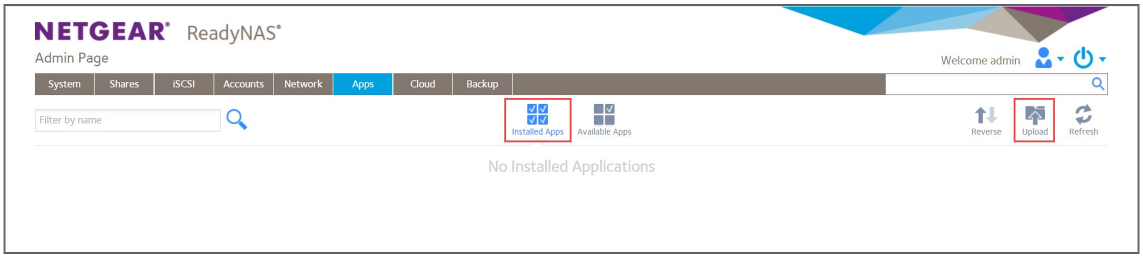
Refer to “Getting Started” on page 21 to know how to continue working with NAKIVO Backup & Replication.

Installing on NETGEAR ReadyNAS Manually

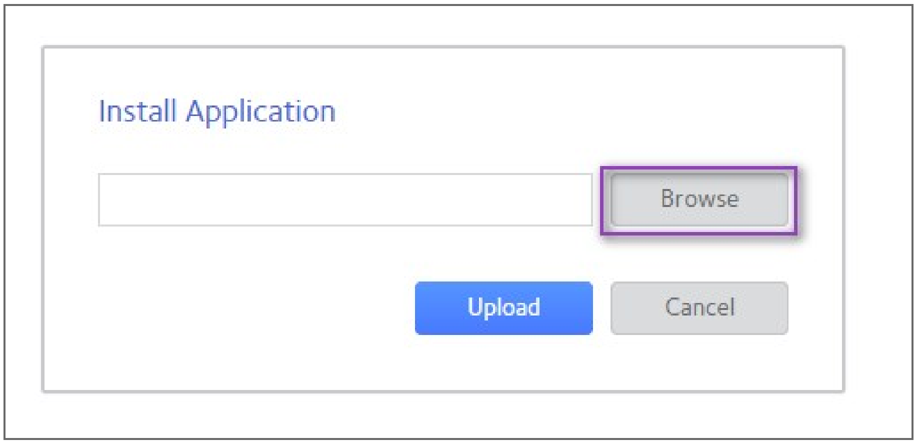
Before you begin installing NAKIVO Backup & Replication or NAKIVO Transporter on a NETGEAR ReadyNAS device, make sure your NAS model is supported and you have downloaded a relevant installer (`.deb` file) for NETGEAR ReadyNAS.

To install NAKIVO Backup & Replication or NAKIVO Transporter, take the following actions:

1. Open the NETGEAR ReadyNAS **Admin Page** in your browser by entering the IP address of your NAS.
2. Go to **Apps** and click **Upload**.



3. The **Install Application** dialog box opens. Click **Browse**.



4. In the dialog box that opens, locate the downloaded installer (`.deb` file) and then click **Upload**.
5. Wait until the installation has been completed.

   Note

   Make sure that only one instance of the NAKIVO solution - either Full Product or Transporter-only - is installed on the device concurrently. Having both products installed may lead to incorrect operations.

By default, NAKIVO Backup & Replication interface is available at the IP address of your NETGEAR ReadyNAS on the port 4443: `https://<IP_address_of_ NETGEAR_ReadyNAS>:4443.`

Refer to "Getting Started" on page 21 to understand better how to continue working with NAKIVO Backup & Replication.

Updating NAKIVO Backup & Replication

NAKIVO Backup & Replication automatically checks for updates once each day. If an update is available, a notification is displayed in the product web interface. Click the notification link to view information about the update.

Starting from v8.5, a full solution of the NAKIVO Backup & Replication installed on Windows or Linux can be updated automatically. Should you find that product auto updating is not supported or there are some network issues, you can update the product manually. For more details, refer to the corresponding articles below.

To manually update any copy of NAKIVO Backup & Replication, go to the download page with updaters.

To update your copy of the product to a newer version, you need to download an appropriate updater and run it on:

- Each machine on which you have additionally installed the Transporter.
- The machine on which the Director is installed.

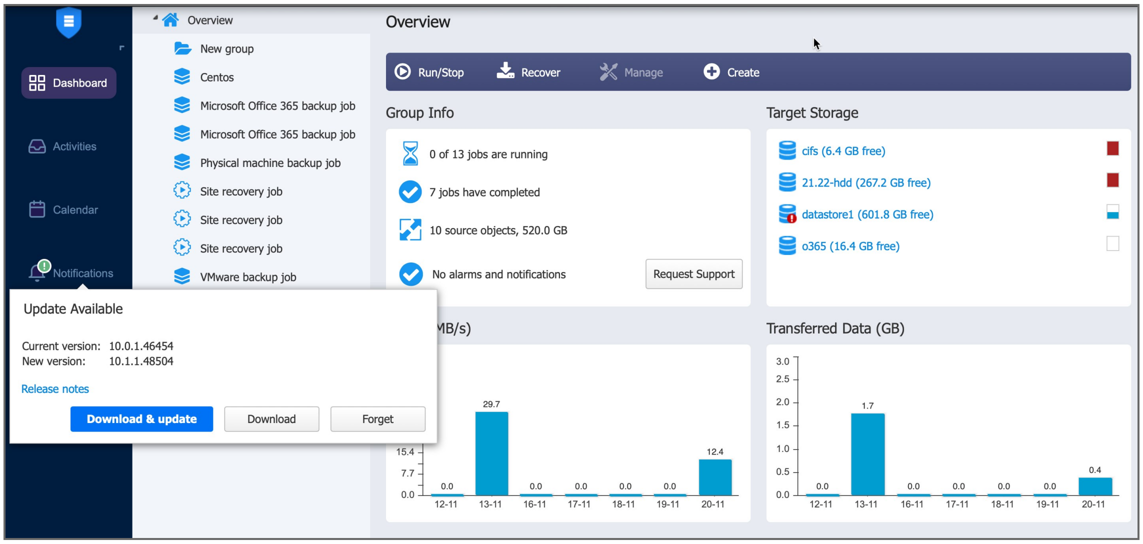
Refer to the following topics for more information:

- "Auto Updating NAKIVO Backup and Replication" on page 159
- "Updating Virtual Appliance" on page 163
- "Updating on Windows" on page 168
- "Updating on Linux" on page 170
- "Updating on Synology NAS" on page 171
- "Updating on Western Digital NAS" on page 173
- "Updating on Amazon EC2" on page 174
- "Updating on QNAP NAS" on page 180
- "Updating on ASUSTOR NAS" on page 183
- "Updating on NETGEAR ReadyNAS" on page 185

Auto Updating NAKIVO Backup and Replication

- Download & Update Option
- Download Option
- Forgetting Update

If the full solution of NAKIVO Backup & Replication is installed on a Windows or Linux machine, you can download product updates and install them using NAKIVO Backup & Replication interface. Once the update becomes available, the **Update available** notification appears in the main menu of the product. You can choose to either download and update the product immediately or download the update and run it at a later time.



Current version: 10.0.1.46454
New version: 10.1.1.48504

Note

If you are using a multi-tenant solution, only master-tenant users who have appropriate permissions will be able to see and manage this button.

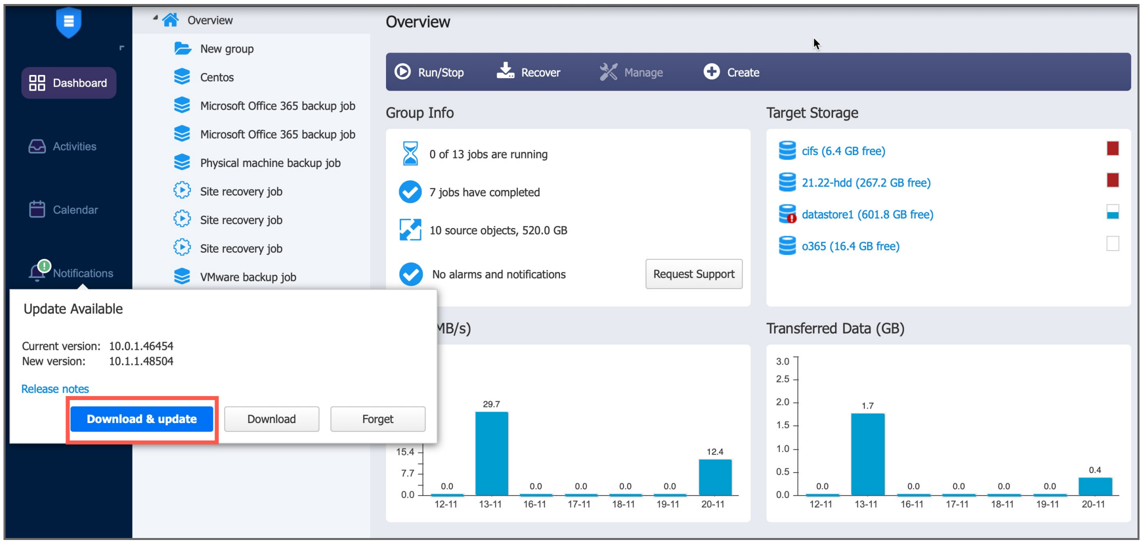
Product Auto-Updating Prerequisites

- At least 1GB of free space must be available on the machine on which the full solution is installed.
- Make sure your Maintenance & Support period is active. You can verify this on the product Licensing page.

Download & Update Option

To download and install the update in a single click, do the following:

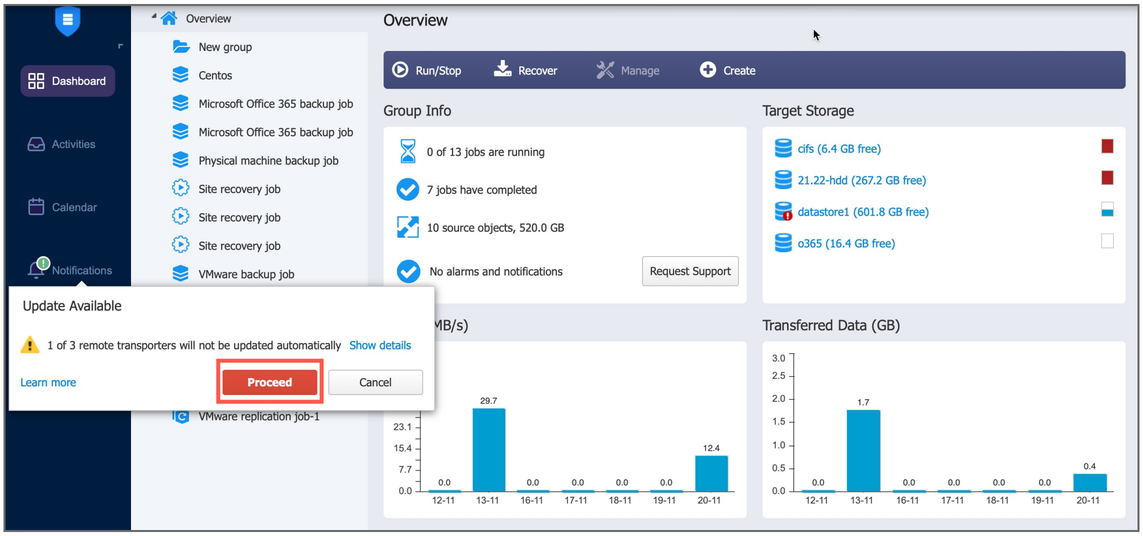
1. Click the **Update Available** button.
2. Optionally, click **Release Notes** to see features and improvements implemented in the new product version.
3. In the **Update Available** dialog box, click **Download & update**.



Update Available

Current version: 10.0.1.46454
New version: 10.1.1.48504

4. In the **Update Available** dialog box, click **Proceed** to confirm stopping all current activities and start downloading the update. When the download is complete, the product updating process will begin.



Update Available

⚠ 1 of 3 remote transporters will not be updated automatically

The product will download the update to the Director first. When the Director is updated, the update will be downloaded to the Transporters that in turn will be updated simultaneously. If some Transporters are not updated, you can update them outside the product. Refer to the corresponding articles for details.

Updating the product will conduct self-backup and stop all current activities including running jobs, recovery jobs, repository maintenance, etc.

Notes

- Only the following NAKIVO Backup & Replication Transporters can be auto-updated:
  - Windows including Hyper-V Transporters
  - Linux including Hyper-V Transporters

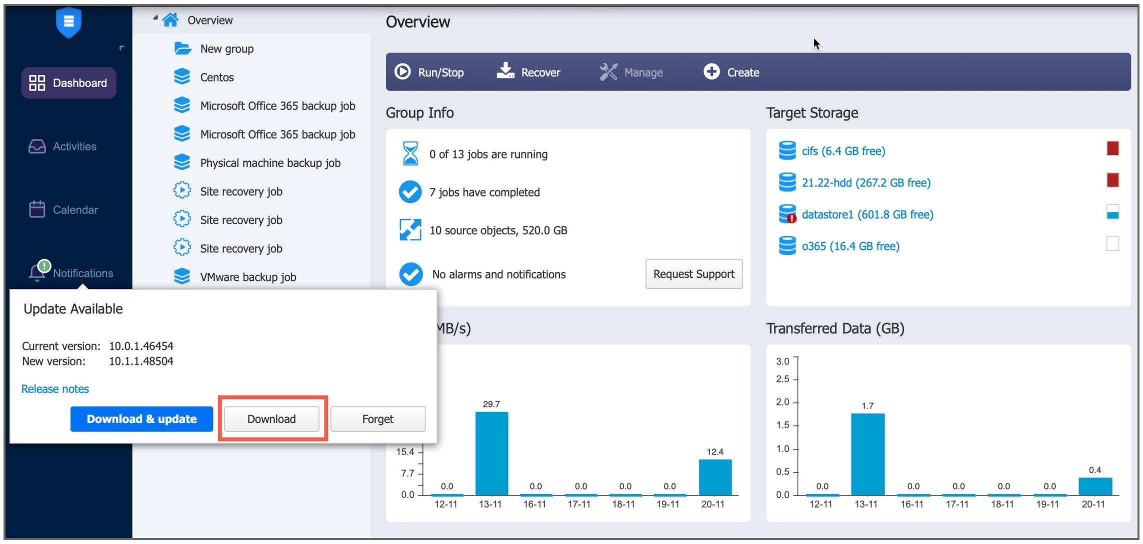
    - Amazon EC2 Transporters
    - VMware Transportes
  - Only 20 Transporters can be updated simultaneously. All other Transporters will be sent to a queue and updated when their turn comes.

5. If the full solution is updated successfully, the **Update Complete** dialog box opens. Click **Close** to dismiss the dialog box.

Download Option

If you wish to postpone updating or schedule it for a certain period of time, take the following steps to download the update only:

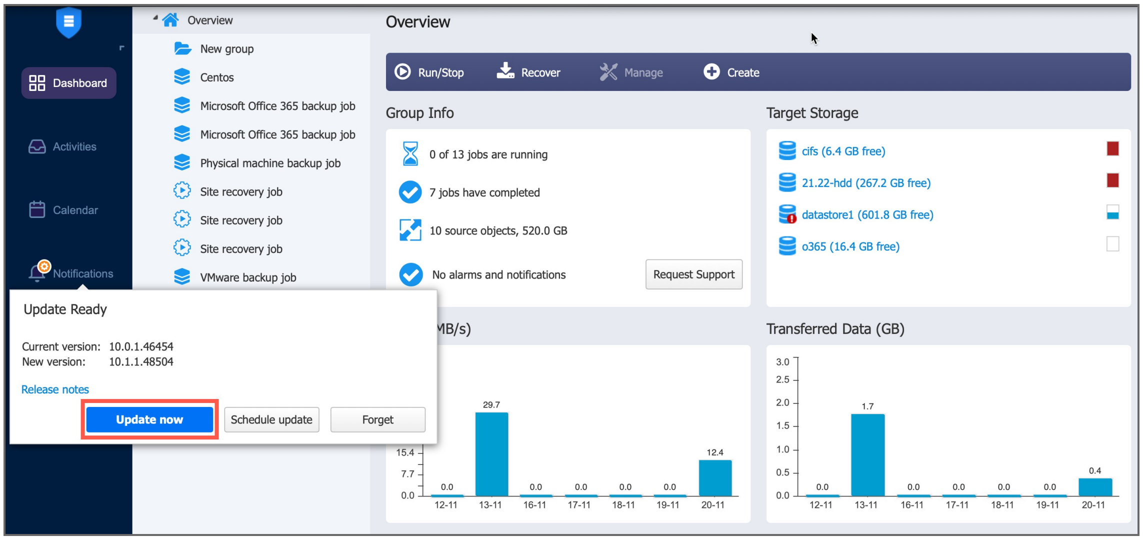
1. Click the **Update Available** button in the product interface.
2. In the **Update Available** dialog box, click **Download** to start downloading the update.



Update Available

Current version: 10.0.1.46454
New version: 10.1.1.48504

3. When downloading is complete, the **Update Ready** dialog box appears in **Notifications**.
4. Do either of the following:
   - Click **Update Now** if you want to start the updating process. In the confirmation dialog box that opens, click **Proceed**. Updating the product will stop all current activities, including running jobs, recovery jobs, repository maintenance, etc.

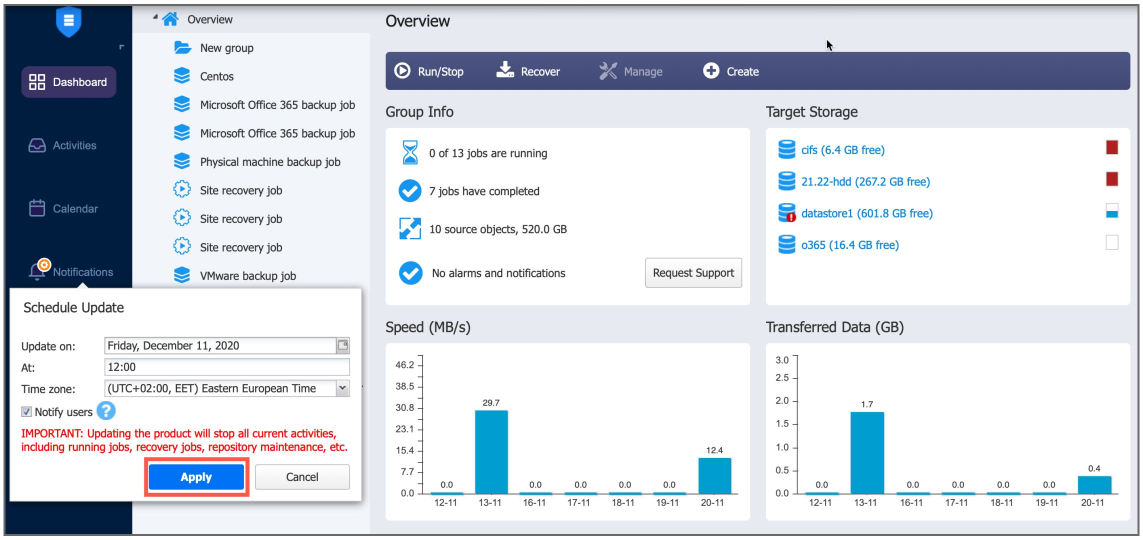


Update Ready

Current version: 10.0.1.46454
New version: 10.1.1.48504

- Click **Schedule Update** to update the solution on a schedule:

1. In the dialog box that opens, pick a day and time for updating. Click **Apply**.



Schedule Update

Update on: Friday, December 11, 2020
At: 12:00
Time zone: (UTC+02:00, EET) Eastern European Time
☑ Notify users

IMPORTANT: Updating the product will stop all current activities, including running jobs, recovery jobs, repository maintenance, etc.

2. On a working day before the scheduled update, you will see the notification in the product menu with the **Update Reminder** dialog box. Do any of the following:

   a. Click **Reschedule** if you want to reschedule the update and pick a different time.

   b. Click **Cancel update** to cancel updating of the full solution.

      Note

      A notification about the update will also be sent to your email if email settings are configured.

Forgetting Update

In the **Update Available** dialog box, you can click **Forget** to dismiss all notifications. If you select this option, you will not receive a notification regarding a product update until the next update is available.

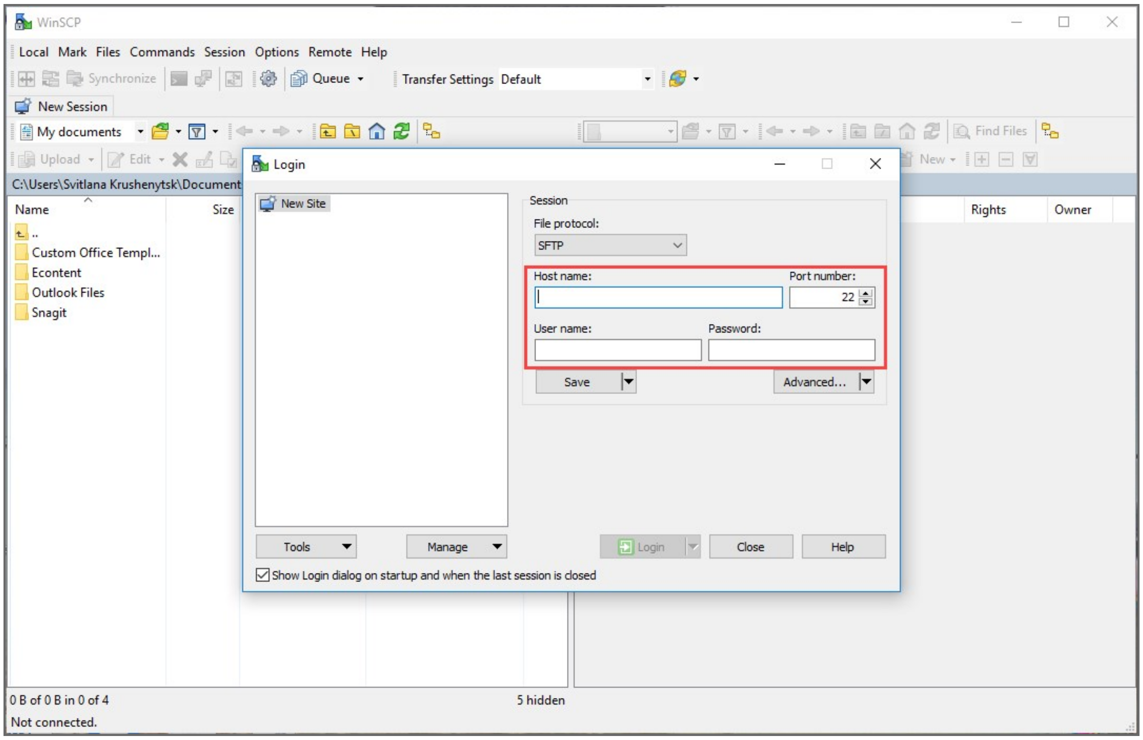
Updating Virtual Appliance

Prior to updating your virtual appliance (VA):

1. Make sure that no jobs or repository maintenance tasks are running in the product.
2. Create a snapshot of the VA to revert to the previous version in case any failure occurs.

Follow the steps below to update your VA:

1. Using SSH client, log in to the VA that needs to be updated.



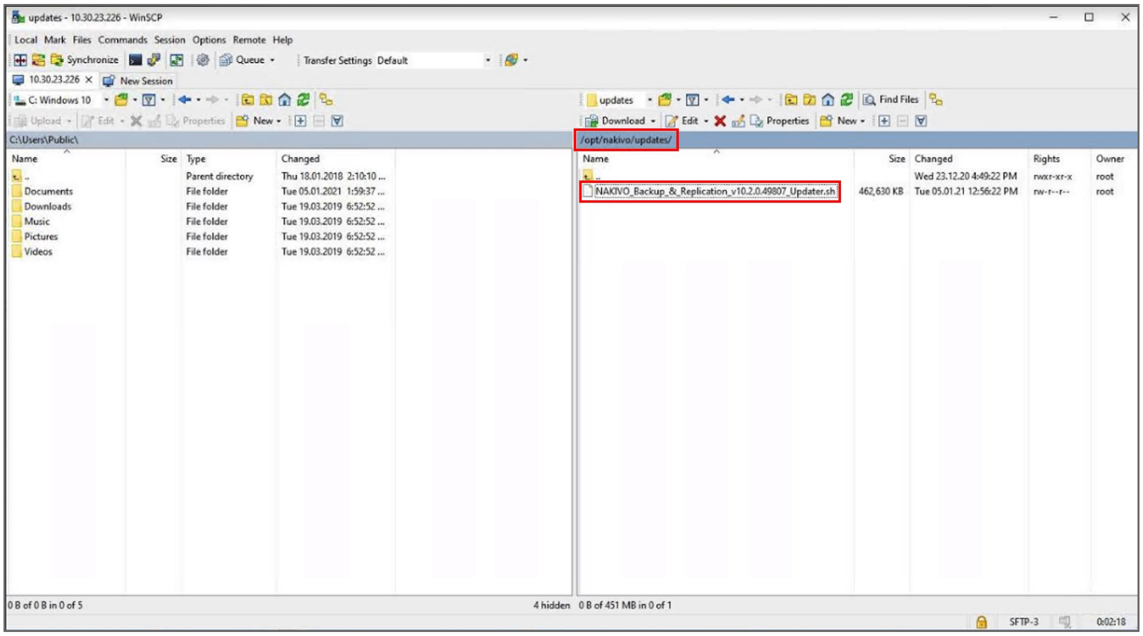
File protocol: SFTP

Port number: 22

☑ Show Login dialog on startup and when the last session is closed

2. Download the latest *VA and Linux updater* from www.nakivo.com/resources/download/update/.

3. Change the directory to `/opt/nakivo/updates` and locate the updater.



C:\Users\Public\

Name	Size	Type	Changed
..		Parent directory	Thu 18.01.2018 2:10:10 ...
Documents		File folder	Tue 05.01.2021 1:59:37 ...
Downloads		File folder	Tue 19.03.2019 6:52:52 ...
Music		File folder	Tue 19.03.2019 6:52:52 ...
Pictures		File folder	Tue 19.03.2019 6:52:52 ...
Videos		File folder	Tue 19.03.2019 6:52:52 ...

0 B of 0 B in 0 of 5 4 hidden

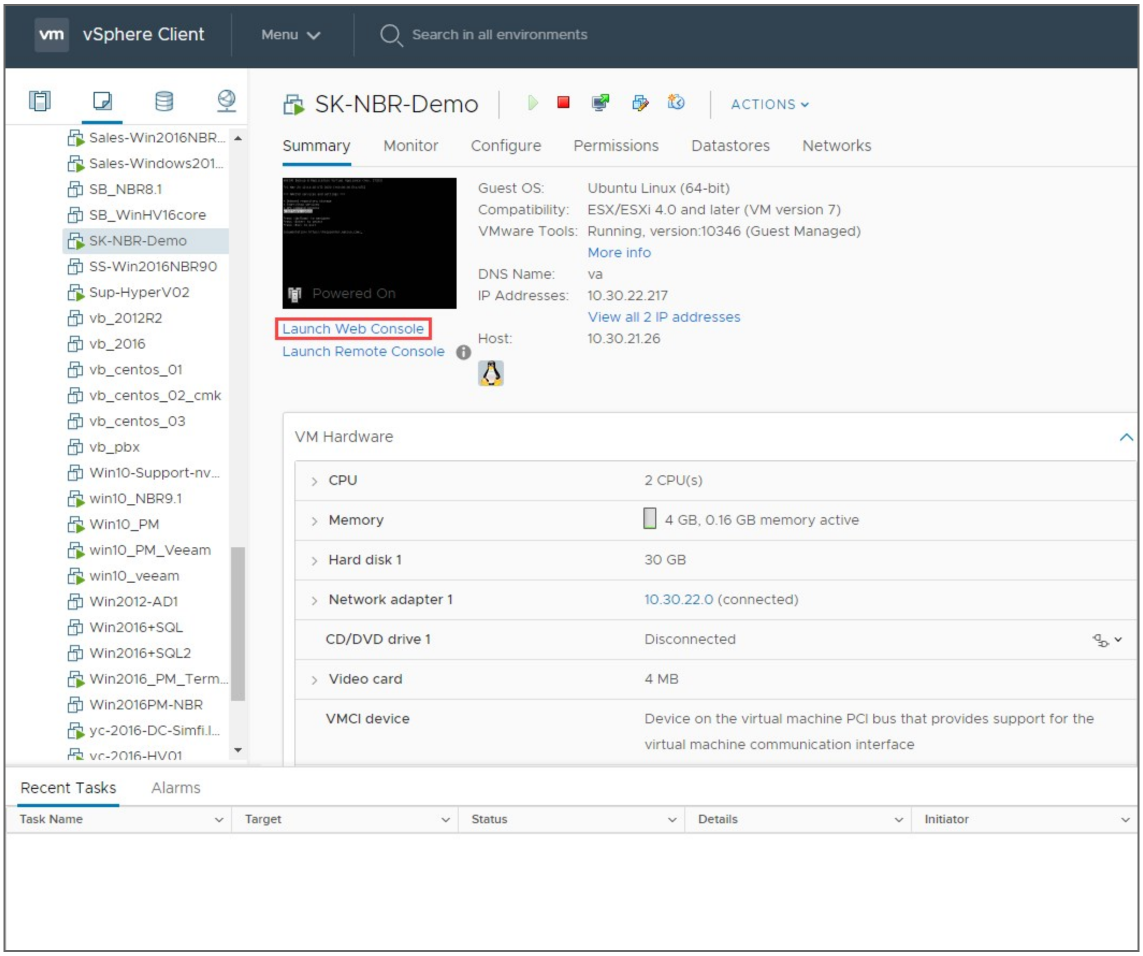
/opt/nakivo/updates/

Name	Size	Changed	Rights	Owner
..		Wed 23.12.20 4:49:22 PM	rwxr-xr-x	root
NAKIVO_Backup_&_Replication_v10.2.0.49807_Updater.sh	462,630 KB	Tue 05.01.21 12:56:22 PM	rw-r--r--	root

0 B of 451 MB in 0 of 1

4. Log out from the SSH client.

5. Log in to your vSphere client, navigate to your VA and click **Launch Web Console**.



Guest OS: Ubuntu Linux (64-bit)
Compatibility: ESX/ESXi 4.0 and later (VM version 7)
VMware Tools: Running, version:10346 (Guest Managed)
More info
DNS Name: va
IP Addresses: 10.30.22.217
View all 2 IP addresses
Host: 10.30.21.26

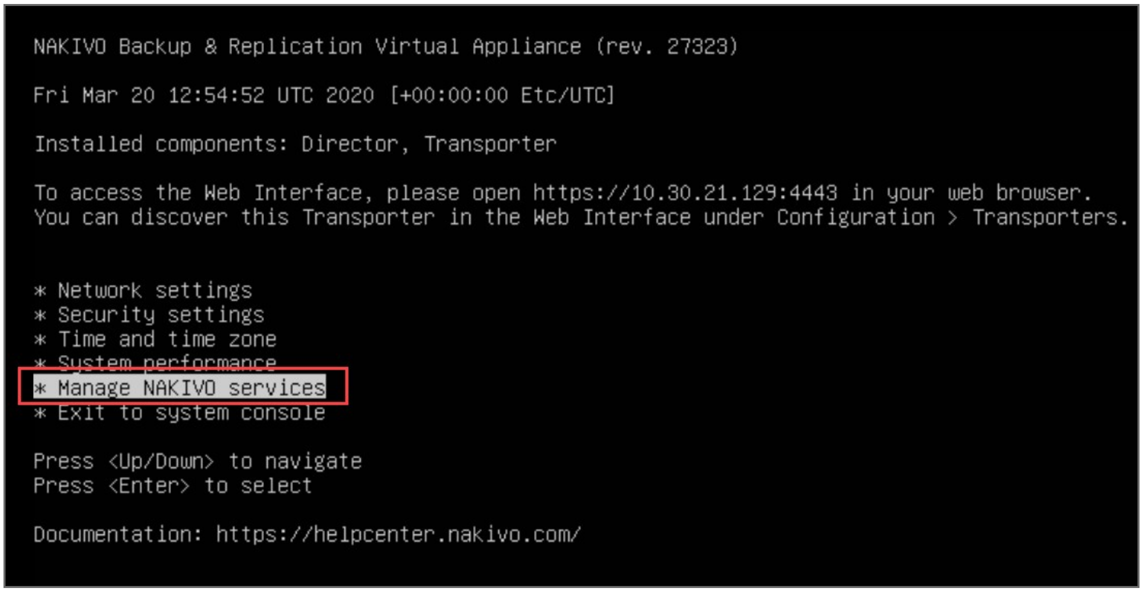
VM Hardware

CPU	2 CPU(s)
Memory	4 GB, 0.16 GB memory active
Hard disk 1	30 GB
Network adapter 1	10.30.22.0 (connected)
CD/DVD drive 1	Disconnected
Video card	4 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface

6. Do one of the following depending on the NAKIVO Backup & Replication version you use:

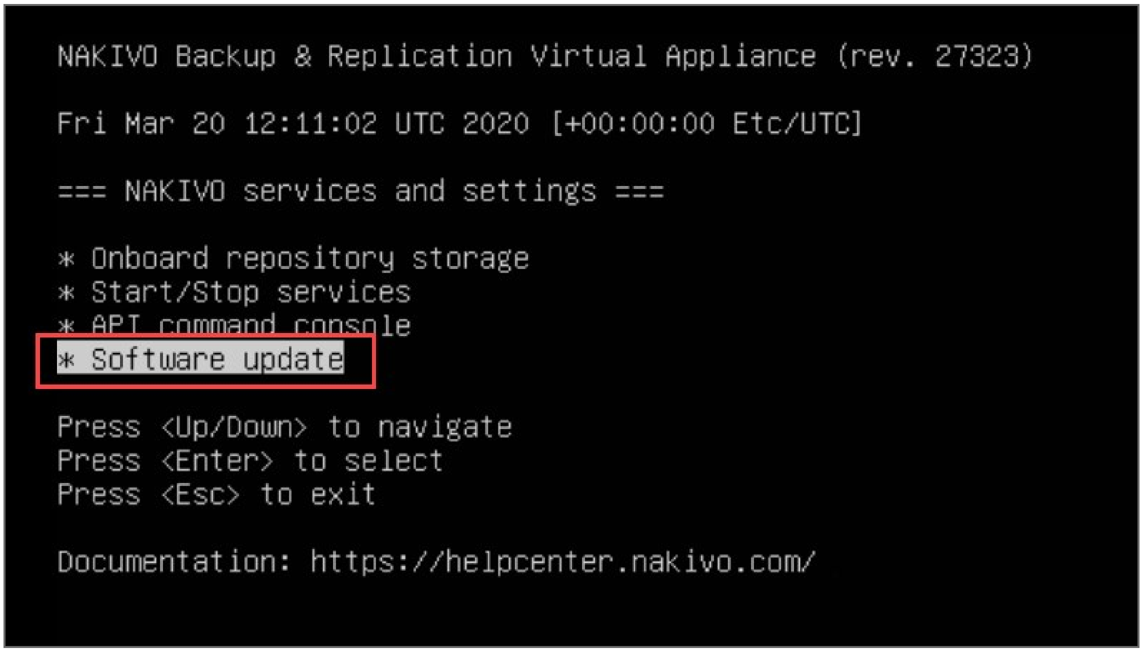
- For the product Version 8.1 and above:

  1. In the VA menu, select **Manage NAKIVO services** and press **Enter**.



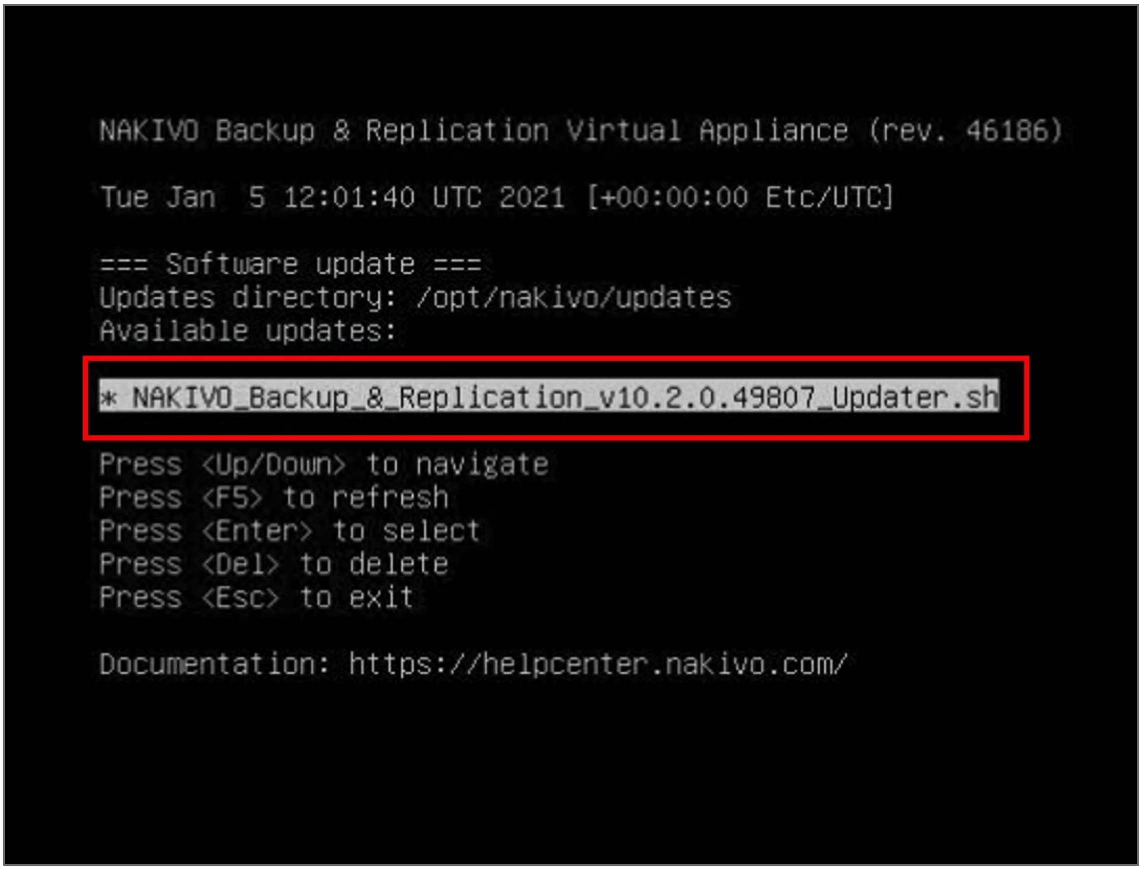
```
NAKIVO Backup & Replication Virtual Appliance (rev. 27323)

Fri Mar 20 12:54:52 UTC 2020 [+00:00:00 Etc/UTC]

Installed components: Director, Transporter

To access the Web Interface, please open https://10.30.21.129:4443 in your web browser.
You can discover this Transporter in the Web Interface under Configuration > Transporters.


* Network settings
* Security settings
* Time and time zone
* System performance
* Manage NAKIVO services
* Exit to system console

Press <Up/Down> to navigate
Press <Enter> to select

Documentation: https://helpcenter.nakivo.com/
```

  2. In the menu that opens, select **Software update** and press **Enter**.



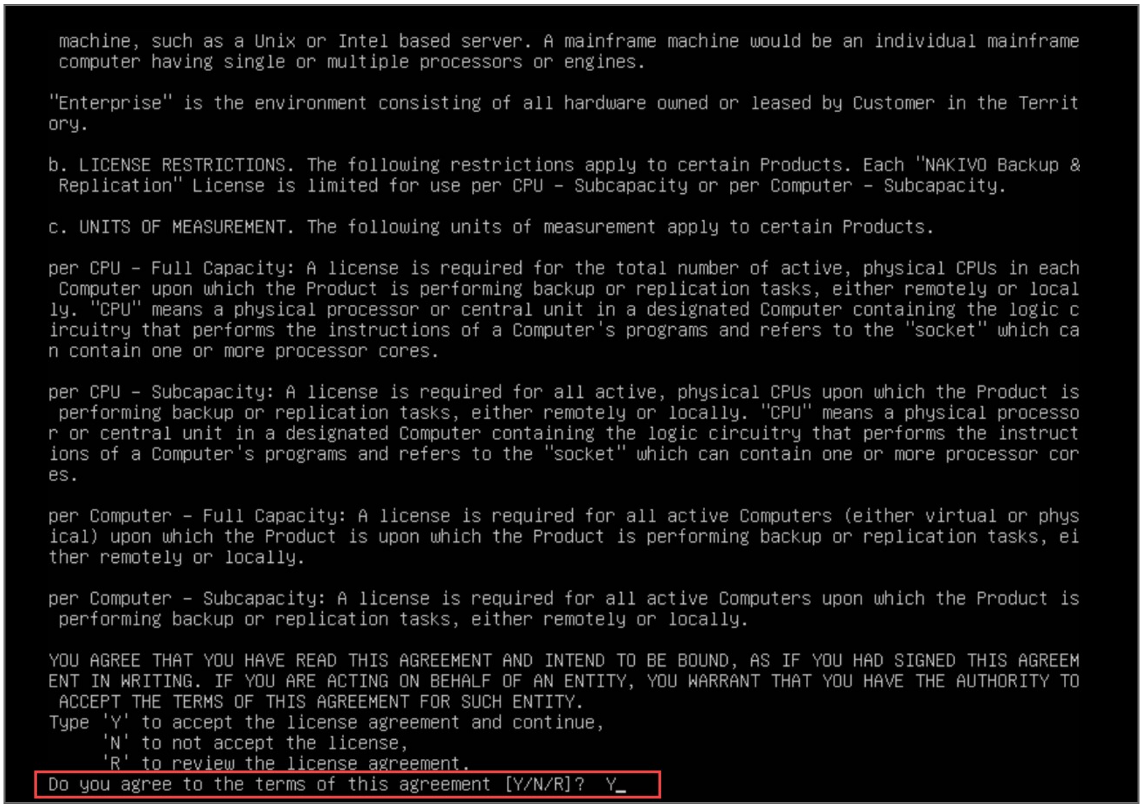
```
NAKIVO Backup & Replication Virtual Appliance (rev. 27323)

Fri Mar 20 12:11:02 UTC 2020 [+00:00:00 Etc/UTC]

=== NAKIVO services and settings ===

* Onboard repository storage
* Start/Stop services
* API command console
* Software update

Press <Up/Down> to navigate
Press <Enter> to select
Press <Esc> to exit

Documentation: https://helpcenter.nakivo.com/
```

3. Select the updater that you have downloaded and press **Enter**.



```
NAKIVO Backup & Replication Virtual Appliance (rev. 46186)

Tue Jan  5 12:01:40 UTC 2021 [+00:00:00 Etc/UTC]

=== Software update ===
Updates directory: /opt/nakivo/updates
Available updates:

* NAKIVO_Backup_&_Replication_v10.2.0.49807_Updater.sh

Press <Up/Down> to navigate
Press <F5> to refresh
Press <Enter> to select
Press <Del> to delete
Press <Esc> to exit

Documentation: https://helpcenter.nakivo.com/
```

    4. Review the End User License Agreement. Press **Space** to go to the bottom of it. If you agree to the terms of the agreement, type **Y** and then press **Enter** to begin the update process.



```
  machine, such as a Unix or Intel based server. A mainframe machine would be an individual mainframe
  computer having single or multiple processors or engines.

 "Enterprise" is the environment consisting of all hardware owned or leased by Customer in the Territ
 ory.

 b. LICENSE RESTRICTIONS. The following restrictions apply to certain Products. Each "NAKIVO Backup &
  Replication" License is limited for use per CPU - Subcapacity or per Computer - Subcapacity.

 c. UNITS OF MEASUREMENT. The following units of measurement apply to certain Products.

 per CPU - Full Capacity: A license is required for the total number of active, physical CPUs in each
  Computer upon which the Product is performing backup or replication tasks, either remotely or local
 ly. "CPU" means a physical processor or central unit in a designated Computer containing the logic c
 ircuitry that performs the instructions of a Computer's programs and refers to the "socket" which ca
 n contain one or more processor cores.

 per CPU - Subcapacity: A license is required for all active, physical CPUs upon which the Product is
  performing backup or replication tasks, either remotely or locally. "CPU" means a physical processo
 r or central unit in a designated Computer containing the logic circuitry that performs the instruct
 ions of a Computer's programs and refers to the "socket" which can contain one or more processor cor
 es.

 per Computer - Full Capacity: A license is required for all active Computers (either virtual or phys
 ical) upon which the Product is upon which the Product is performing backup or replication tasks, ei
 ther remotely or locally.

 per Computer - Subcapacity: A license is required for all active Computers upon which the Product is
  performing backup or replication tasks, either remotely or locally.

 YOU AGREE THAT YOU HAVE READ THIS AGREEMENT AND INTEND TO BE BOUND, AS IF YOU HAD SIGNED THIS AGREEM
 ENT IN WRITING. IF YOU ARE ACTING ON BEHALF OF AN ENTITY, YOU WARRANT THAT YOU HAVE THE AUTHORITY TO
  ACCEPT THE TERMS OF THIS AGREEMENT FOR SUCH ENTITY.
 Type 'Y' to accept the license agreement and continue,
      'N' to not accept the license,
      'R' to review the license agreement.
 Do you agree to the terms of this agreement [Y/N/R]?  Y_
```

- For earlier product versions:
    1. In the VA menu, select **Software update** and press **Enter.**
    2. Select the updater that you have downloaded and press **Enter.**
    3. Review the End User License Agreement. Press **Space** to go to the bottom of it. If you agree to the terms of the agreement, type **Y** and then press **Enter** to begin the update process.

7. When the update process is complete, a message will appear to inform you about it. Exit the VA console.
8. Update all machines on which you have deployed an additional Transporter.

Note

Updating your VA with versions prior to the previous major version (for example, updating VA version 6.1 to version 9.0) is prohibited. Please update your VA to the next major version first.

Updating on Windows

If auto-update within the NAKIVO Backup & Replication interface is not supported, follow the steps below to update the product manually:

1. Download the latest Windows updater from www.nakivo.com/resources/download/update/.
2. Make sure that no jobs or repository maintenance tasks are running in the product.
   If NAKIVO Backup & Replication is installed on a VM, create a snapshot of the VM before updating the product.
3. Run the updater on the machine on which the Director is installed, and also on all machines on which you have additionally deployed a Transporter.
4. Optionally, you can select the **Master password** checkbox and enter the password that will be used to generate a pre-shared key and secure the Transporter. This option is available only for the Transporter-only update.

   Notes

   - The master password must adhere to the following requirements:
     - Minimal length - 5 characters.
     - Maximum length - 50 characters.
   - The master password can be set and re-set manually by running the command on the machine housing the Transporter. Follow these steps:
     - Enter the following command `bhsvc -b P@ssword123`
     - Restart the Transporter service.
5. Optionally, you can select the **Transporter certificate** checkbox. This allows you to use a CA Certificate. Enter the path to the folder containing the certificate file in the field.

   Notes

   - When the checkbox is not selected, NAKIVO Backup & Replication automatically installs a self-signed certificate.
   - If the **Transporter Certificate** checkbox is not selected, a warning window appears prompting you to install it. Click **Continue** to proceed.
6. Click **Update**.
7. When the update is complete, click **Finish**.
8. If you have entered the new master password on step 4, do the following:
   a. Go to **Settings > Transporters** and click on the Transporter you have changed the master password for.
   b. Select **Edit**.
   c. Enter the new master password and click **Connect**.
   d. The **Certificate Acceptance** dialog box appears. Verify the certificate details, and click **Accept**.

e. Click **Apply** to save the changes.
f. Click on the sameTransporter once again and select **Refresh** to refresh the Transporter.

Updating on Linux

If updating on a Linux OS within the NAKIVO Backup & Replication interface is not supported, follow the steps below to update the product manually:

1. Download the latest Linux/VA updater from www.nakivo.com/resources/download/update/.
2. Upload the updater to the machine on which the Director is installed.

   Important

   Make sure you are using the *binary transfer mode* when uploading the updater to the machine with a Linux OS. For example:

   - Upload the installer from a Windows-based machine
   - Upload the product from a Linux-based machine: run the following command: `wget 'server_ip/shared/NAKIVO_Backup_Replication_vX.X.X_Updater.sh'`
3. Log in to the Linux machine and allow the execution of the updater file. For example: `chmod +x NAKIVO_Backup_Replication_vX.X.X_Updater.sh`
4. Make sure that no jobs or repository maintenance tasks are running in the product.

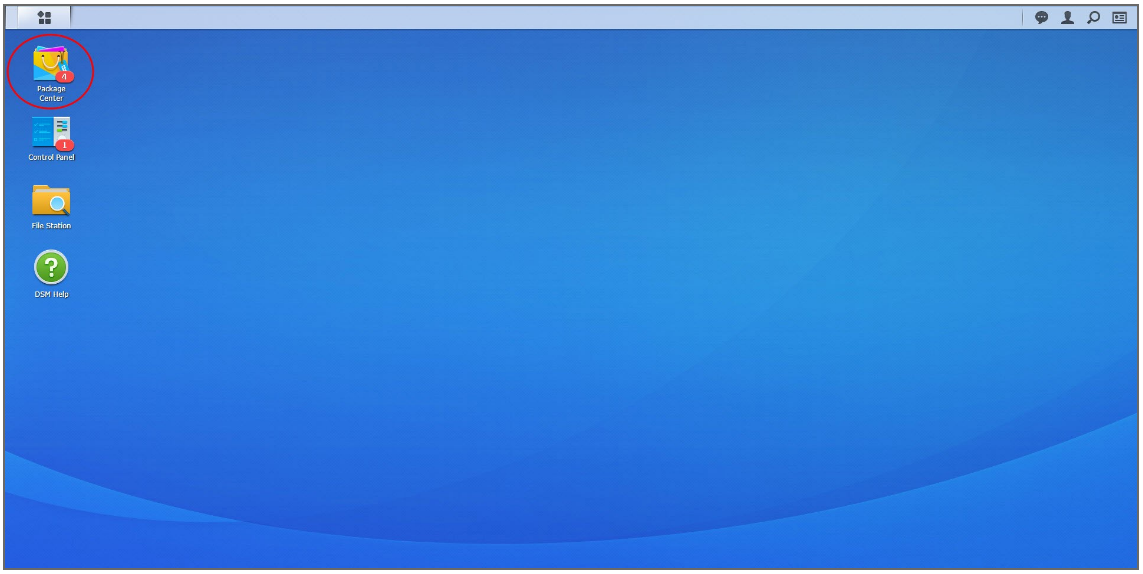
   If NAKIVO Backup & Replication is installed on a VM, create a snapshot of the VM prior to updating the product.
5. Run the updater file with root privileges. For example: `sudo ./NAKIVO_Backup_Replication_vX.X.X_Updater.sh`
6. Review the license agreement (press **Space** to go to the next page of the agreement). If you agree to the terms of the license agreement, press “Y” and then press **Enter**.
7. Enter the “Y” key and then press **Enter** to confirm that you wish to stop the services and begin the update process.
8. Update all machines on which you have additionally deployed a “Transporter” on page 61.

Updating on Synology NAS

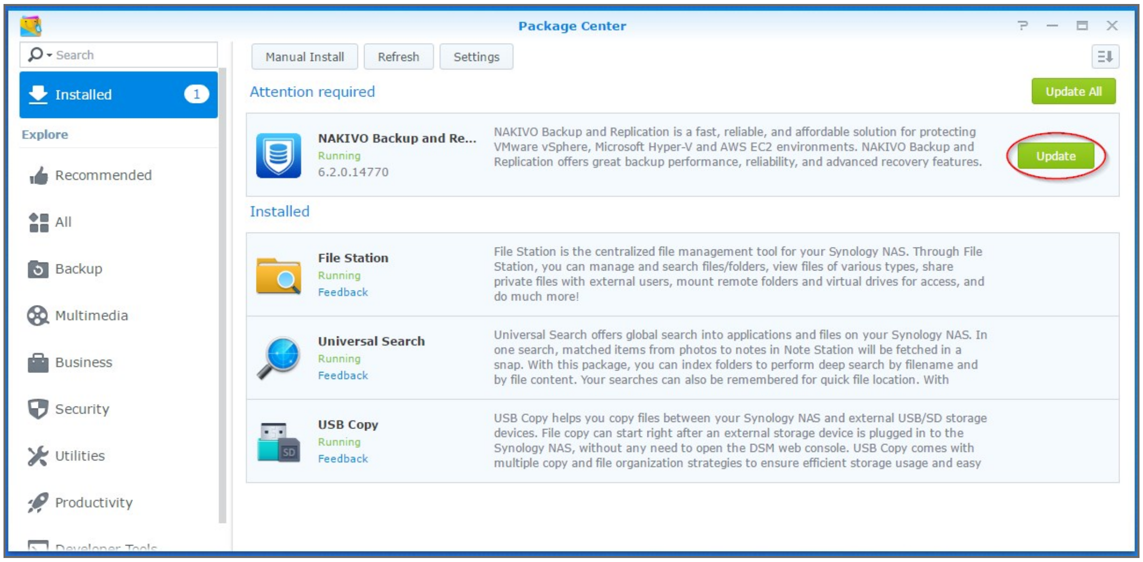
- Updating via Synology Package Center
- Updating Manually

Updating via Synology Package Center

1. Make sure that no jobs or repository maintenance tasks are running in the product.
2. In the Synology NAS management interface, open the **Package Center**.



3. Go to the **Installed** section.
4. If there is a new version of NAKIVO Backup & Replication available, you will see an **Update** button.



Attention required

NAKIVO Backup and Re...
Running
6.2.0.14770

NAKIVO Backup and Replication is a fast, reliable, and affordable solution for protecting VMware vSphere, Microsoft Hyper-V and AWS EC2 environments. NAKIVO Backup and Replication offers great backup performance, reliability, and advanced recovery features.

Installed

File Station
Running
Feedback

File Station is the centralized file management tool for your Synology NAS. Through File Station, you can manage and search files/folders, view files of various types, share private files with external users, mount remote folders and virtual drives for access, and do much more!

Universal Search
Running
Feedback

Universal Search offers global search into applications and files on your Synology NAS. In one search, matched items from photos to notes in Note Station will be fetched in a snap. With this package, you can index folders to perform deep search by filename and by file content. Your searches can also be remembered for quick file location. With

USB Copy
Running
Feedback

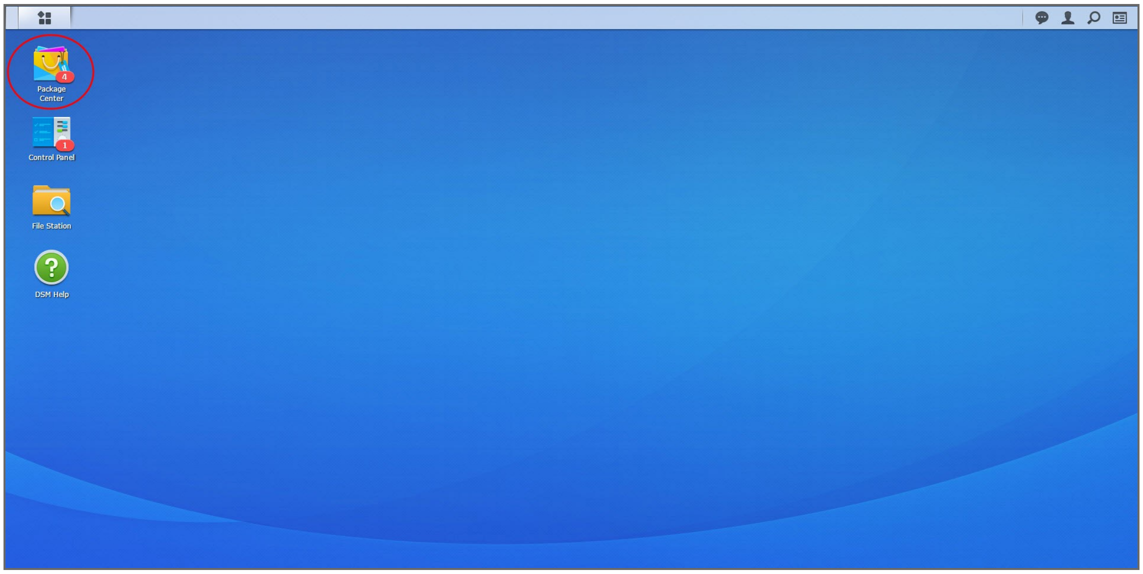
USB Copy helps you copy files between your Synology NAS and external USB/SD storage devices. File copy can start right after an external storage device is plugged in to the Synology NAS, without any need to open the DSM web console. USB Copy comes with multiple copy and file organization strategies to ensure efficient storage usage and easy

5. Click **Update**.

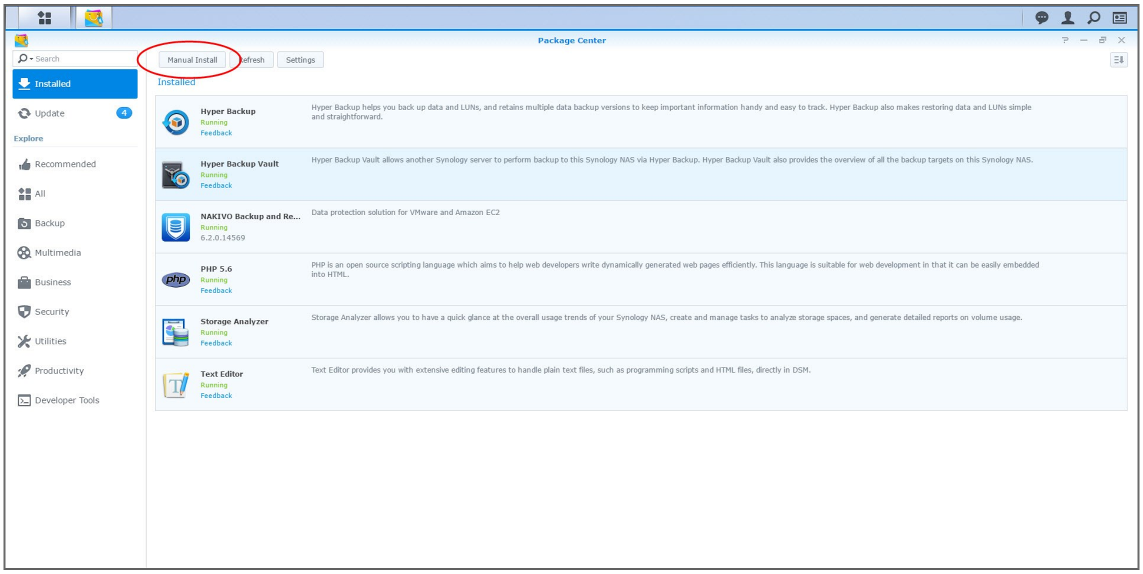
6. Wait until the update is complete.
7. Repeat these steps on all Synology NAS where you have also installed a Transporter.

Updating Manually

1. Download the latest Synology NAS updater from www.nakivo.com/resources/download/update/.
2. Make sure that no jobs or repository maintenance tasks are running in the product.
3. In the Synology NAS management interface, open the **Package Center**.



4. Click **Manual Install**.



Installed

Hyper Backup Running Feedback	Hyper Backup helps you back up data and LUNs, and retains multiple data backup versions to keep important information handy and easy to track. Hyper Backup also makes restoring data and LUNs simple and straightforward.
Hyper Backup Vault Running Feedback	Hyper Backup Vault allows another Synology server to perform backup to this Synology NAS via Hyper Backup. Hyper Backup Vault also provides the overview of all the backup targets on this Synology NAS.
NAKIVO Backup and Re... Running 6.2.0.14569	Data protection solution for VMware and Amazon EC2
PHP 5.6 Running Feedback	PHP is an open source scripting language which aims to help web developers write dynamically generated web pages efficiently. This language is suitable for web development in that it can be easily embedded into HTML.
Storage Analyzer Running Feedback	Storage Analyzer allows you to have a quick glance at the overall usage trends of your Synology NAS, create and manage tasks to analyze storage spaces, and generate detailed reports on volume usage.
Text Editor Running Feedback	Text Editor provides you with extensive editing features to handle plain text files, such as programming scripts and HTML files, directly in DSM.

5. Click **Browse**, navigate to the Synology NAS package that you have downloaded, select it, and click **Open**.
6. Click **Next**. the package is uploaded to your NAS.
7. Click **Apply**.
8. Run an appropriate updater on all machines on which you have also installed a Transporter.

Now, NAKIVO Backup & Replication has been updated.

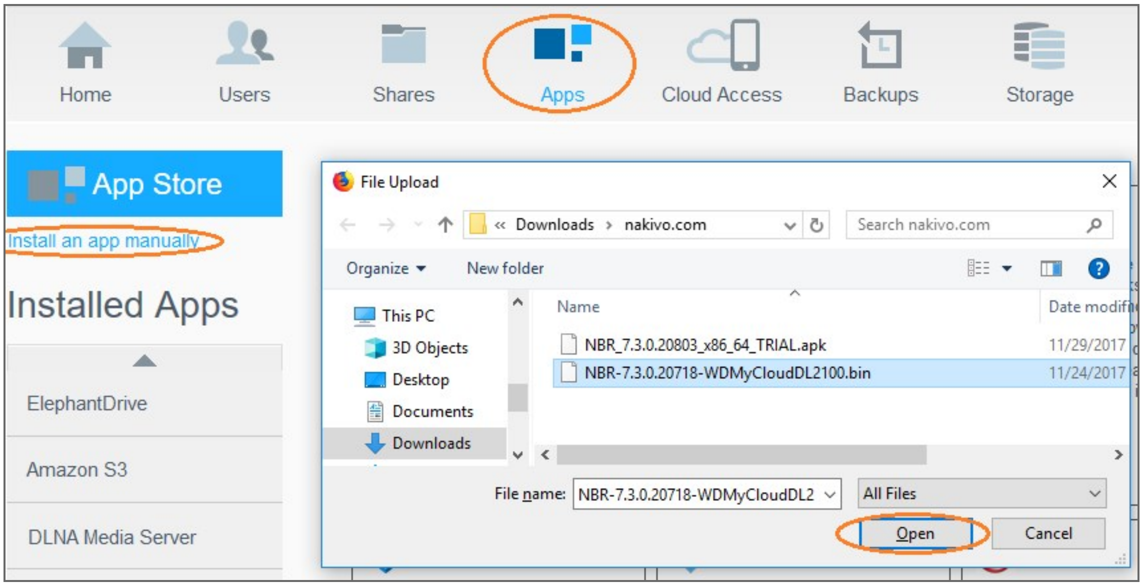
Updating on Western Digital NAS

Prior to updating NAKIVO Backup & Replication on Western Digital MyCloud NAS, make sure the following requirements have been met:

- You have access to the Western Digital NAS MyCloud Dashboard.
- NAKIVO Backup & Replication installer is available for your Western Digital NAS.

Please follow the steps below to update NAKIVO Backup & Replication on a Western Digital MyCloud NAS device:

1. In the **My Cloud** Dashboard, click **Apps**. The list of installed NAS applications opens on the left side of the page.
2. Above the list of NAS installed applications, click **Install an app manually**. The **File Upload** dialog opens.
3. In the **File Upload** dialog, navigate to your copy of the NAKIVO Backup & Replication installer for Western Digital NAS and click **Open**. The update progress bar opens.



4. Once the update has successfully finished, a dialog box opens with a message including said information. Click **OK** to close the dialog box.

Updating on Amazon EC2

The main installation of NAKIVO Backup & Replication (Director and Transporter) must be updated the way it is done on Linux.

Notes

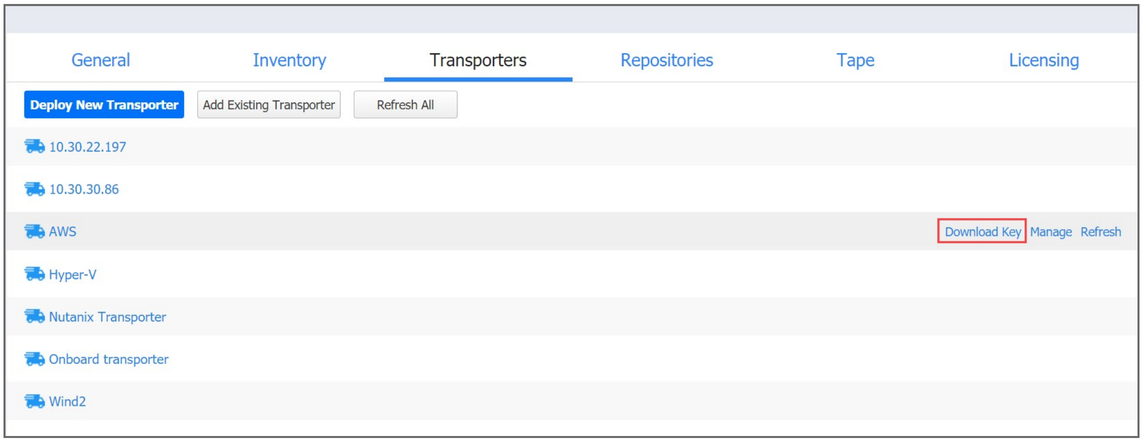
- You have to apply the **-e** argument for executing the installer, in order to avoid changing the Amazon EC2 Transporter with the regular Linux Transporter. Refer to "Installing on Linux" on page 127 for a description of the available arguments.
- Only the main installation of NAKIVO Backup & Replication needs to be updated manually. Transporters installed on Amazon EC2 instances are updated automatically.

Connecting to an Amazon EC2 Instance from Windows

You can use the following free tools to connect to your Amazon EC2 instance:

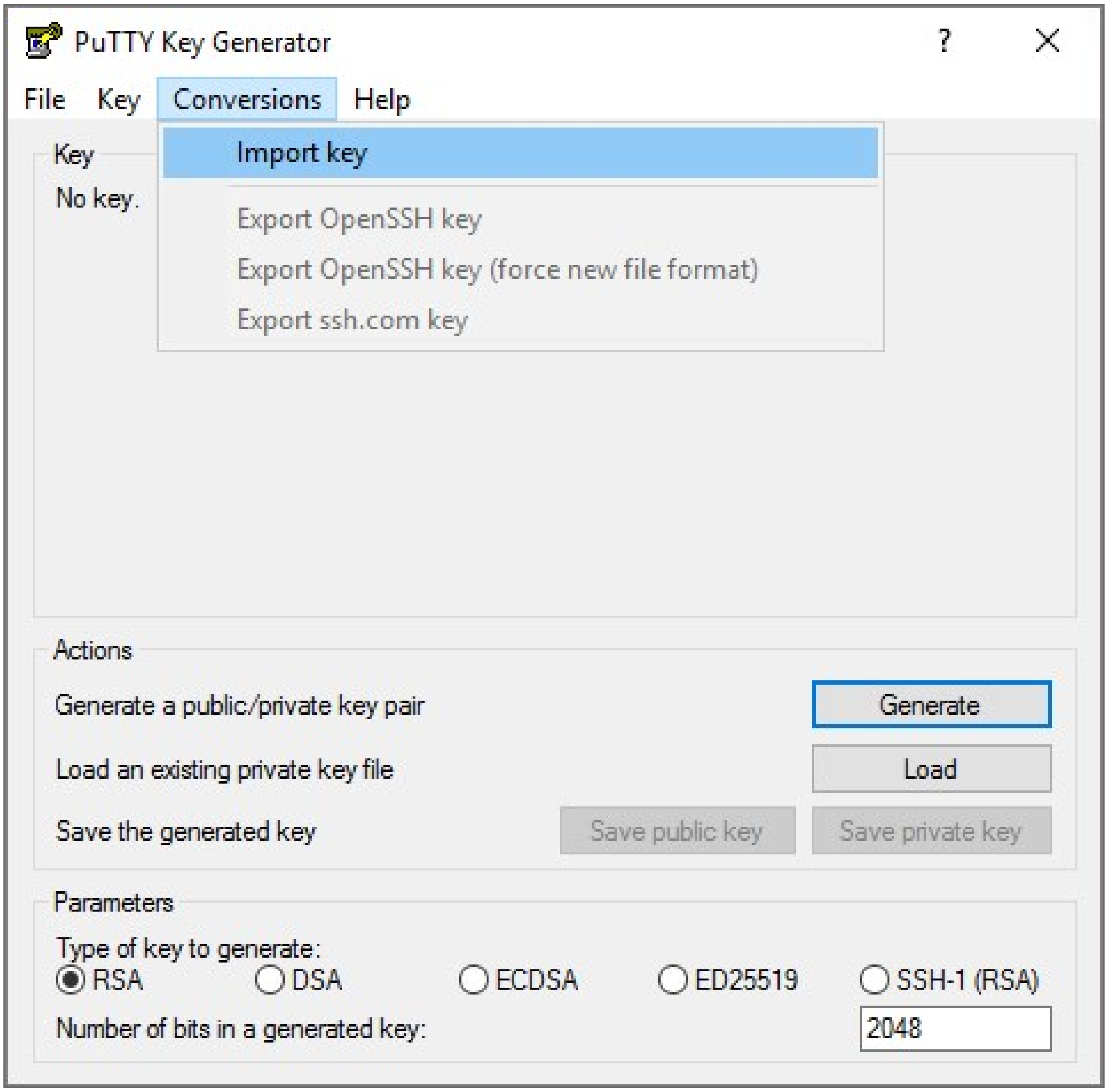
- WinSCP to upload the installer file.
- PuTTYgen tool to convert the private key.
- PuTTY tool to connect to an Amazon instance securely.

1. Log in to NAKIVO Backup & Replication.
2. Go to **Settings** > **Transporters**.
3. Download the keys of your Amazon instance.

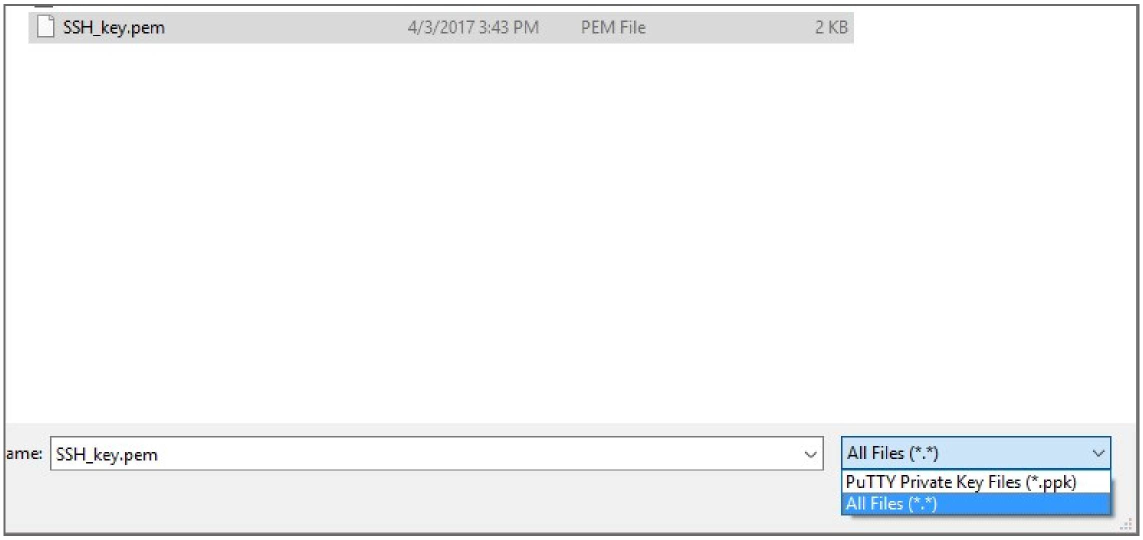


4. Click on the Transporter to view its details. Copy or remember the IP-address/hostname of the Amazon instance.
5. Unzip the folder with the key.
6. Convert the key using PuTTYgen:

1. In PuTTYgen menu, go to *Conversions* > *Import.*



   2. Locate the `SSH_key.pem` you just downloaded and unzipped. If you don't see it in the **Open**... dialogue box, change the file type to **All files**.



SSH_key.pem 4/3/2017 3:43 PM PEM File 2 KB

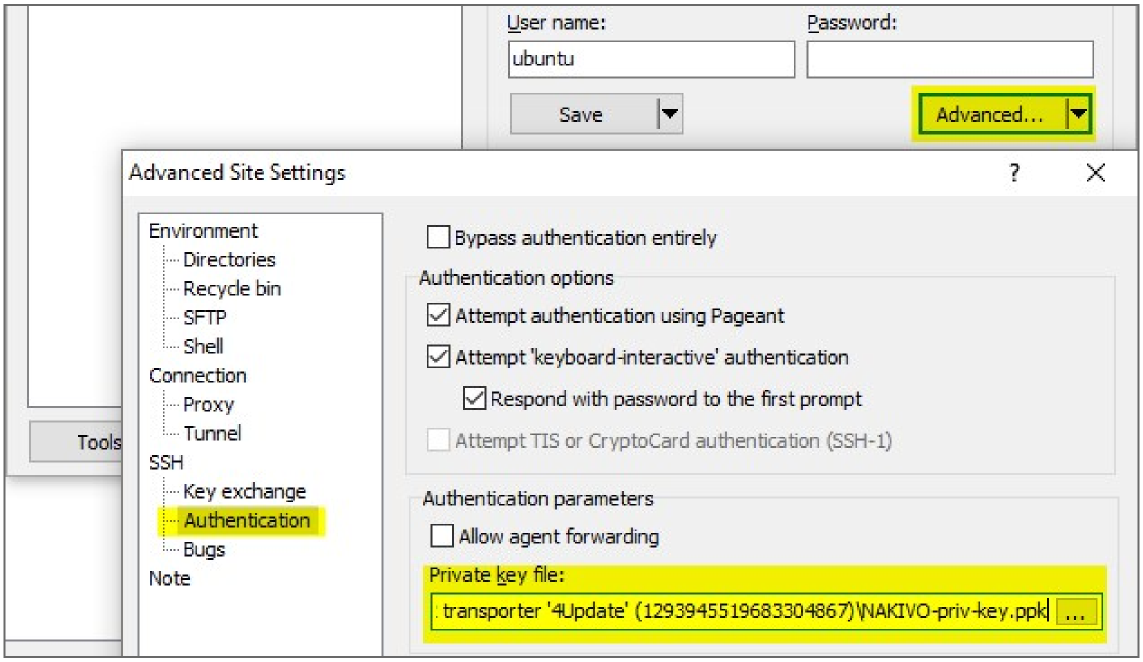
ame: SSH_key.pem

All Files (*.*)

   3. Click on **Save private key**. If PuTTYgen asks you to save the key without a passphrase, click **Yes**.

7. Open WinSCP.
8. Create a new session:
   1. Add the hostname or IP address of your Amazon instance you received on step 4 into the **Host Name** box.
   2. In the **Username** box, enter `ubuntu`.
   3. Leave the **Password** box empty.
   4. Add the private key to WinSCP:

   1. Click the **Advanced...** button.
   2. The **Advanced Site Settings** dialog box opens. Go to *SSH > Authentication > Private key file:* and select the key file you generated on step 6.



User name: ubuntu

Password:

Advanced Site Settings

☐ Bypass authentication entirely

Authentication options

☑ Attempt authentication using Pageant

☑ Attempt 'keyboard-interactive' authentication

☑ Respond with password to the first prompt

☐ Attempt TIS or CryptoCard authentication (SSH-1)

Authentication parameters

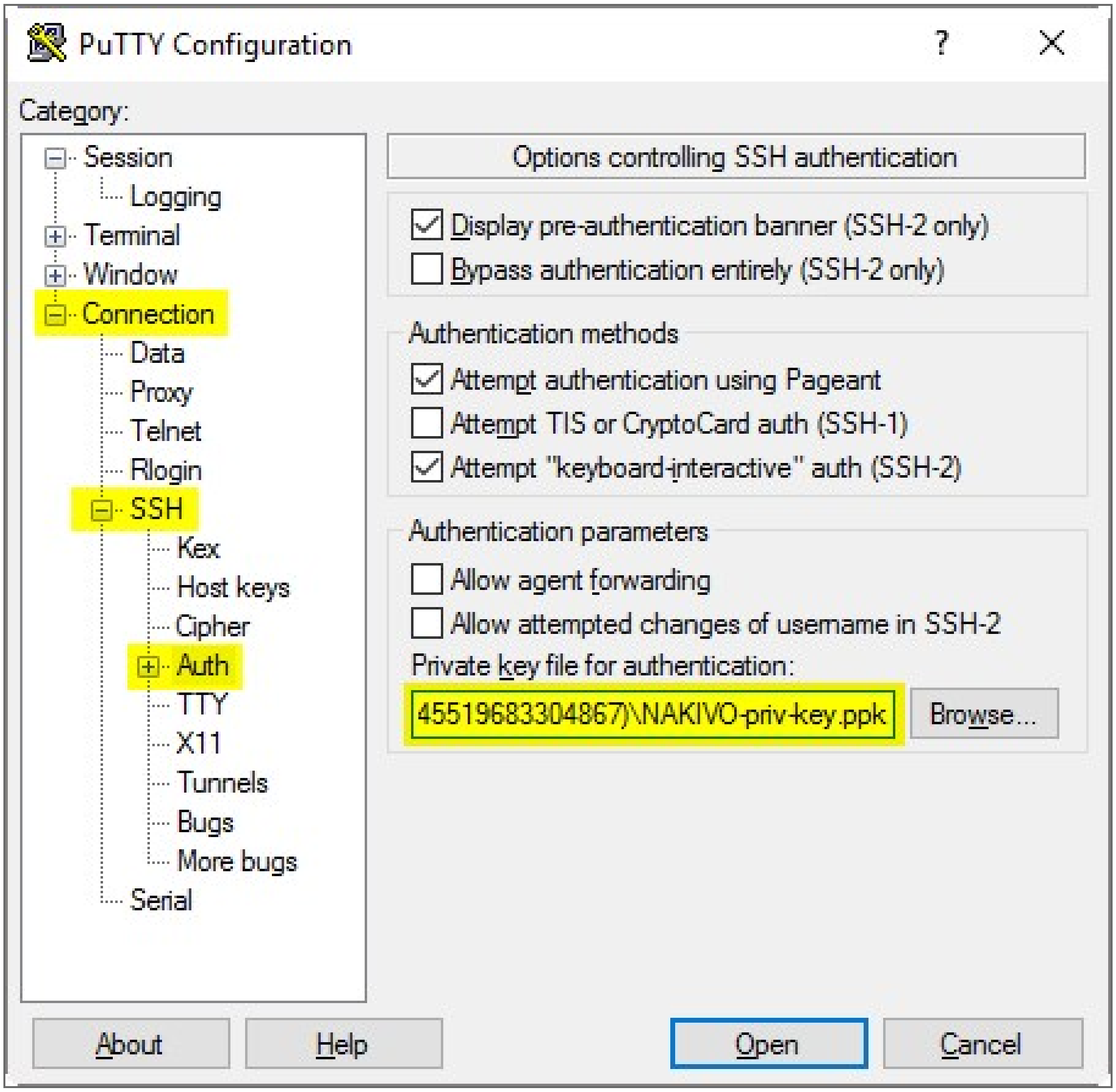
☐ Allow agent forwarding

Private key file: : transporter '4Update' (1293945519683304867)\NAKIVO-priv-key.ppk

   3. Click **OK**.

5. Click **Login**.
6. Upload the updater file.
7. Open PuTTY.
8. Enter the IP-address or hostname of the Amazon EC2 instance.

9. Go to *Connection* > *SSH* > *Auth* and add the private key in *Private key file for authentication:* box.



Options controlling SSH authentication

☑ Display pre-authentication banner (SSH-2 only)

☐ Bypass authentication entirely (SSH-2 only)

Authentication methods

☑ Attempt authentication using Pageant

☐ Attempt TIS or CryptoCard auth (SSH-1)

☑ Attempt "keyboard-interactive" auth (SSH-2)

Authentication parameters

☐ Allow agent forwarding

☐ Allow attempted changes of username in SSH-2

Private key file for authentication:

45519683304867)\NAKIVO-priv-key.ppk

10. Click **Open**.

11. In the command line prompt that opens: log in to the Amazon EC2 instance:
    1. For **login**, enter `ubuntu`
    2. For **password**, leave a blank line.

9. Update NAKIVO Backup & Replication following the instructions.

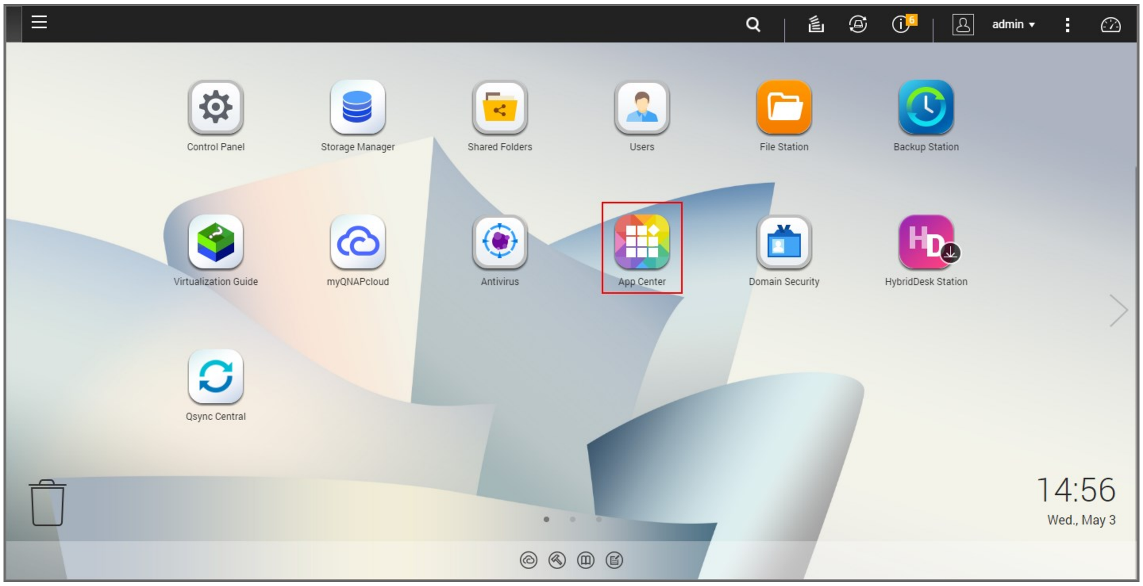
Updating on QNAP NAS

You can update NAKIVO Backup & Replication via QNAP AppCenter or manually. Refer to the following subtopics for details:

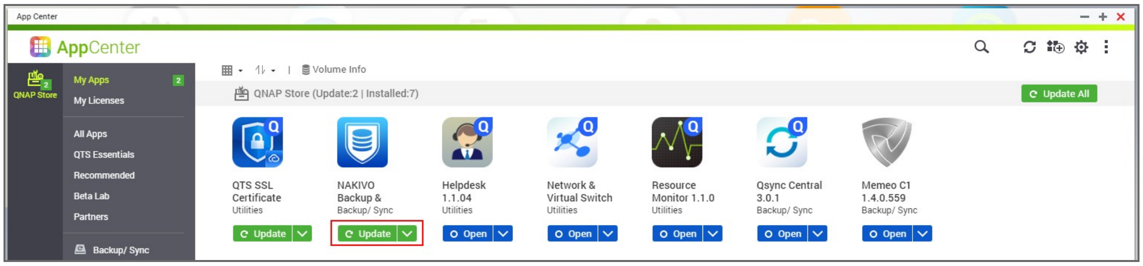
- Updating via QNAP AppCenter
- Updating Manually

Updating via QNAP AppCenter

1. Open the QNAP Desktop in your browser by entering the IP address of your QNAP NAS.



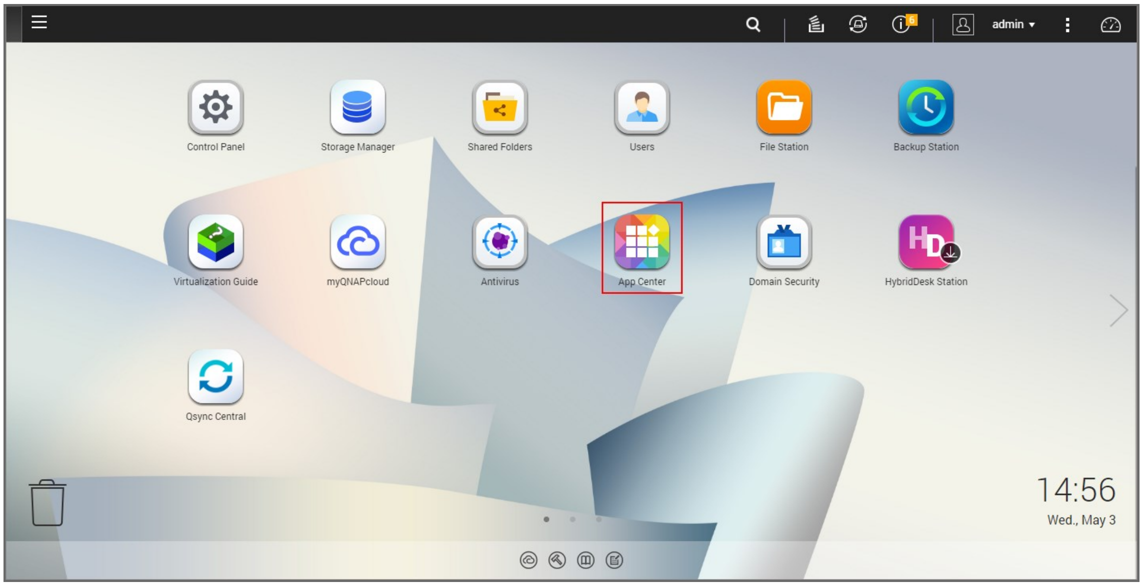
2. Go to **App Center**.
3. Select the *Backup/Sync* category and find NAKIVO Backup & Replication. Alternatively, use the search box at the top of the App Center window: click on the magnifier icon and enter "Nakivo".
4. If the new version of NAKIVO Backup & Replication is available in the QNAP App Center, you will see a green **Update** button.



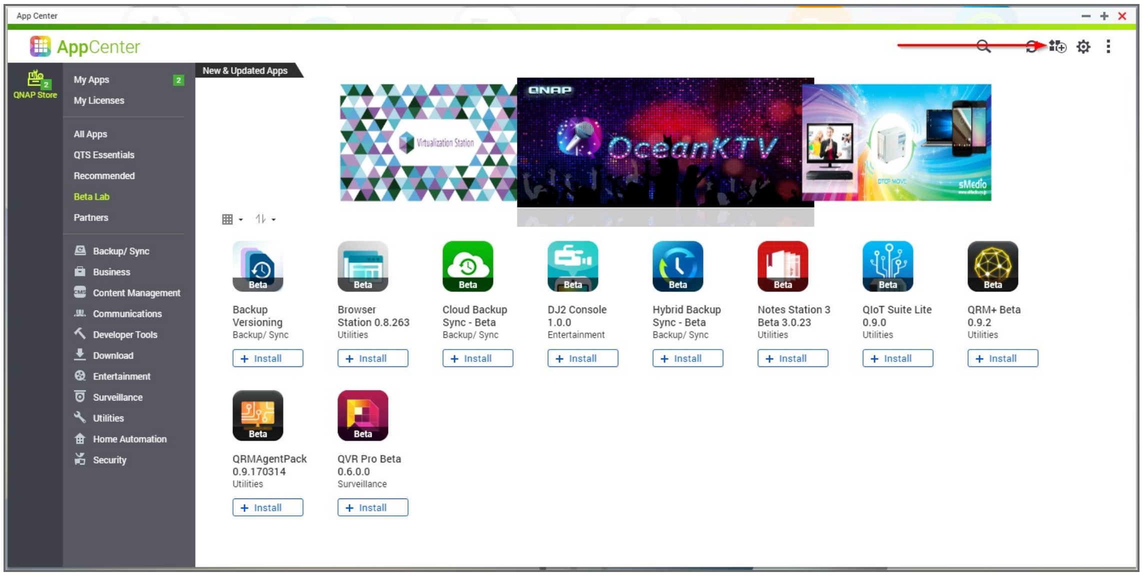
5. Click the **Update button** and wait till update finishes.

Updating Manually

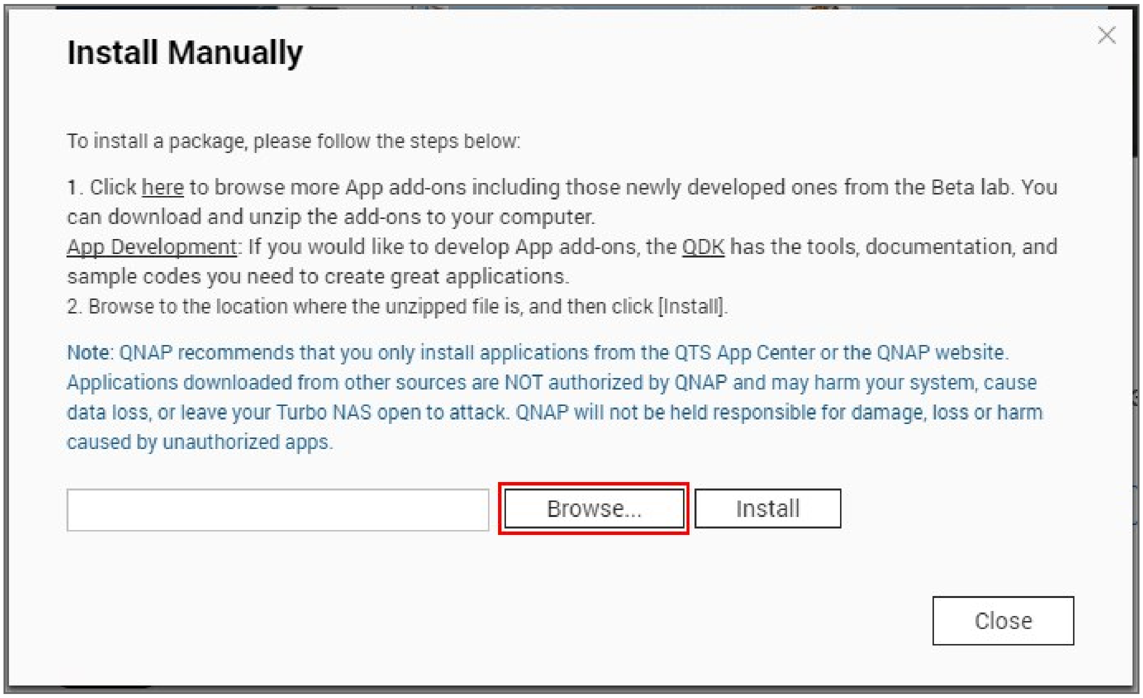
1. Download the update package from www.nakivo.com/resources/download/update/
2. Open the QNAP Desktop in your browser by entering the IP address of your QNAP NAS.



3. Go to **App Center**.
4. Click the **Install Manually** icon.


App Center
AppCenter
QNAP Store
My Apps 2
My Licenses
All Apps
QTS Essentials
Recommended
Beta Lab
Partners
Backup/ Sync
Business
Content Management
Communications
Developer Tools
Download
Entertainment
Surveillance
Utilities
Home Automation
Security
New & Updated Apps
OceanKTV
Backup Versioning Backup/ Sync + Install
Browser Station 0.8.263 Utilities + Install
Cloud Backup Sync - Beta Backup/ Sync + Install
DJ2 Console 1.0.0 Entertainment + Install
Hybrid Backup Sync - Beta Backup/ Sync + Install
Notes Station 3 Beta 3.0.23 Utilities + Install
QIoT Suite Lite 0.9.0 Utilities + Install
QRM+ Beta 0.9.2 Utilities + Install
QRMAgentPack 0.9.170314 Utilities + Install
QVR Pro Beta 0.6.0.0 Surveillance + Install

5. Click **Browse**. In the window appears, locate the installer (.qpkg file) on your computer.



Install Manually

To install a package, please follow the steps below:

1. Click here to browse more App add-ons including those newly developed ones from the Beta lab. You can download and unzip the add-ons to your computer.
App Development: If you would like to develop App add-ons, the QDK has the tools, documentation, and sample codes you need to create great applications.
2. Browse to the location where the unzipped file is, and then click [Install].

Note: QNAP recommends that you only install applications from the QTS App Center or the QNAP website. Applications downloaded from other sources are NOT authorized by QNAP and may harm your system, cause data loss, or leave your Turbo NAS open to attack. QNAP will not be held responsible for damage, loss or harm caused by unauthorized apps.

6. Click **Install**.
7. Wait until the update process is finished.

Updating on ASUSTOR NAS

- Updating on ASUSTOR NAS Manually
- Updating on ASUSTOR NAS via App Central

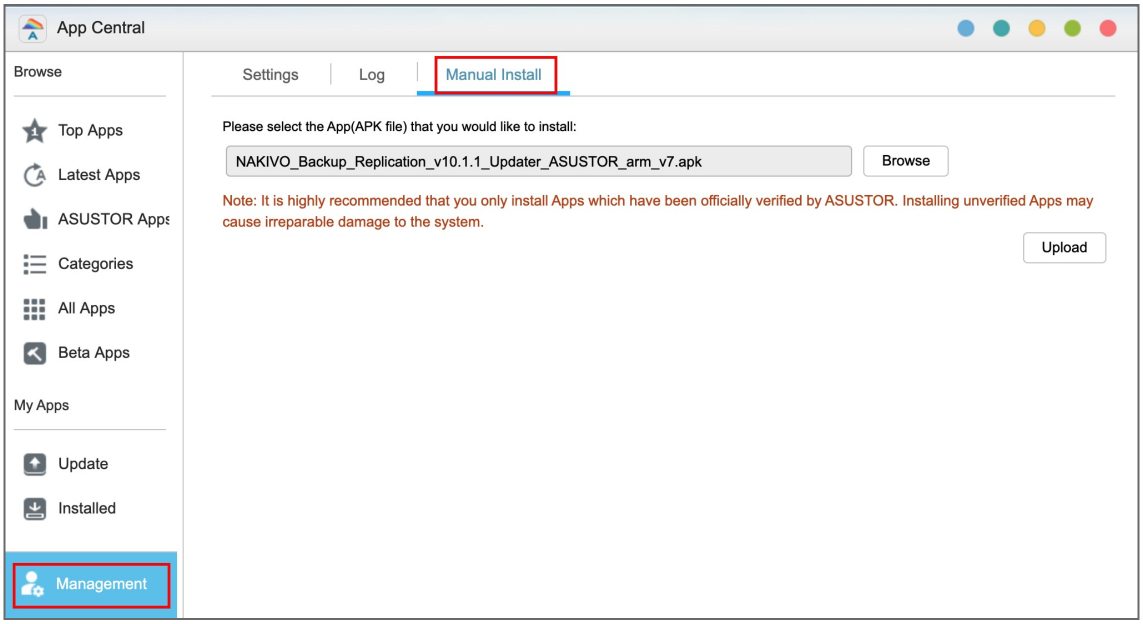
Updating on ASUSTOR NAS Manually

Prior to updating NAKIVO Backup & Replication on ASUSTOR NAS manually, make sure the following requirements are met:

- You have access to the ASUSTOR NAS.
- NAKIVO Backup & Replication installer is available for your ASUSTOR NAS.

Follow the steps below to update NAKIVO Backup & Replication on ASUSTOR NAS manually:

1. Open the **App Central** from the ASUSTOR NAS **Desktop**.
2. Click **Management** in the bottom left corner and click **Manual Install**.
3. The **Manual Install** pane opens to the right of the **App Central**. Click **Browse**.
4. The **Open** dialog box opens. Locate your copy of NAKIVO Backup & Replication installer for ASUSTOR NAS and click the **Open** button.
5. The **Open** dialog closes, and the **Upload** button becomes enabled. Click the **Upload** button.
6. When the upload finishes, the **About This App** dialog opens. If you are sure the requirements are met, click the **Next** button.
7. The **About This App** dialog opens a message asking you to review the summary of the NAKIVO Backup & Replication update. Select the checkbox **I understand the risks associated with installing unverified Apps** and click **Install**.
8. The **About This App** dialog closes, and the **Installed** pane of the **App Central** opens.
9. Wait until the update of NAKIVO Backup & Replication is complete.



Please select the App(APK file) that you would like to install:

NAKIVO_Backup_Replication_v10.1.1_Updater_ASUSTOR_arm_v7.apk

Note: It is highly recommended that you only install Apps which have been officially verified by ASUSTOR. Installing unverified Apps may cause irreparable damage to the system.

Updating on ASUSTOR NAS via App Central

Follow the steps below to update NAKIVO Backup & Replication on ASUSTOR NAS via App Central:

1. Open the **App Central** from the ASUSTOR NAS **Desktop**.
2. In the **Browse** menu to the left, click **All Apps**. The list of applications available in **the App Central** opens in the right pane.
3. In the search box in the upper right corner of the pane, enter "Nakivo". Installations of the NAKIVO Backup & Replication application that are available at App Central are now displayed.
4. Click the **Update** button below the required NAKIVO Backup & Replication application to start uploading the update.
5. When the update is uploaded successfully, the **About This App** dialog opens. Click the **Update** button if you are sure that all the requirements are met.
6. The **About This App** dialog closes, and the **Installed** pane of the **App Central** opens. Wait until the update of the NAKIVO Backup & Replication is completed.

Updating on NETGEAR ReadyNAS

- Updating on NETGEAR ReadyNAS Manually
- Updating on NETGEAR ReadyNAS via Available Apps

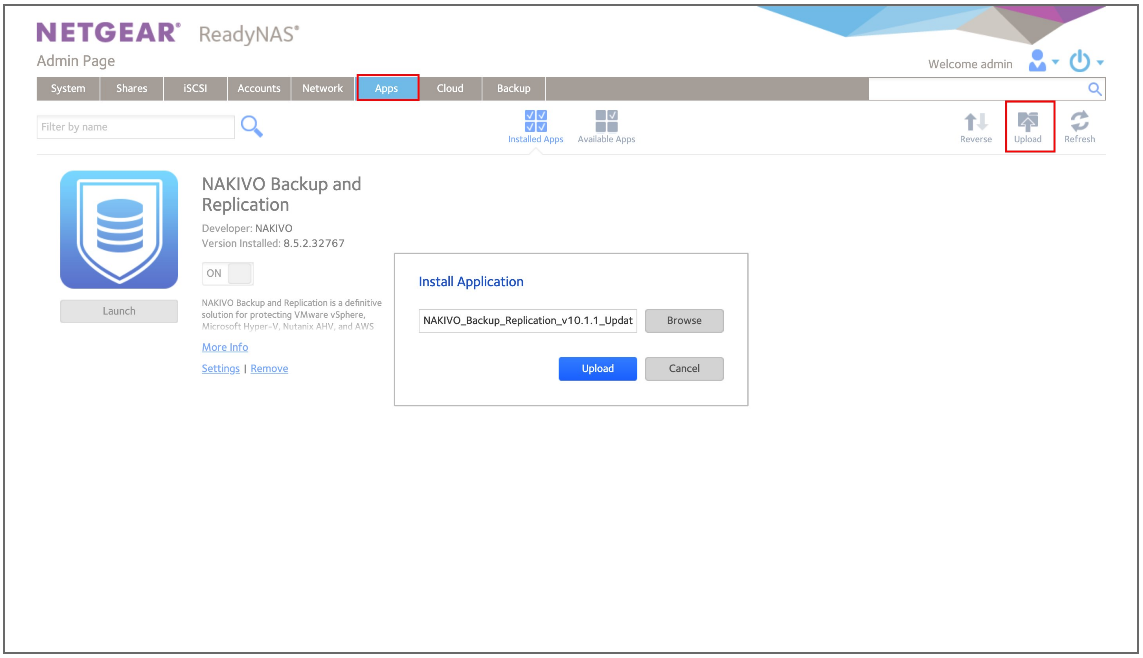
Updating on NETGEAR ReadyNAS Manually

Prior to updating NAKIVO Backup & Replication on NETGEAR ReadyNAS manually, make sure the following requirements have been met:

- You have access to the NETGEAR ReadyNAS.
- NAKIVO Backup & Replication update is available for your NETGEAR ReadyNAS.

Follow the steps below to update NAKIVO Backup & Replication on NETGEAR ReadyNAS manually:

1. Open the NETGEAR ReadyNAS **Admin Page** in your browser by entering the IP address of your NAS.
2. Go to **Apps** and click **Upload**.
3. The **Install Application** dialog box opens. Click **Browse**.
4. In the dialog box that opens, locate the downloaded installer (.deb file) and then click **Upload**.
5. Wait until the update is completed.



NAKIVO Backup and Replication

Developer: NAKIVO

Version Installed: 8.5.2.32767

NAKIVO Backup and Replication is a definitive solution for protecting VMware vSphere, Microsoft Hyper-V, Nutanix AHV, and AWS

NAKIVO_Backup_Replication_v10.1.1_Updat

Updating on NETGEAR ReadyNAS via Available Apps

Prior to updating NAKIVO Backup & Replication on NETGEAR ReadyNAS via Available Apps, make sure that you have access to NETGEAR ReadyNAS.

Follow the steps below to update NAKIVO Backup & Replication on NETGEAR ReadyNAS via Available Apps:

1. Open the NETGEAR ReadyNAS **Admin Page** in your browser by entering the IP address of your NAS.
2. Go to **Apps** > **Available Apps**.

3. Find **NAKIVO Backup & Replication** in the list of available applications. Alternatively, enter NAKIVO to the filtering box in the upper left corner of the **Admin Page**.
4. If a new version of NAKIVO Backup & Replication is available in the NETGEAR **Available Apps**, the **Update** button will be available below the application item. Click the **Update** button.
5. Wait until the update is complete.

Uninstalling NAKIVO Backup & Replication

Uninstalling on Windows

To uninstall NAKIVO Backup & Replication, run the uninstaller:

1. Go to **Start** -> **Control Panel** and run **Programs and Features**.
2. Select **NAKIVO Backup & Replication** and click **Uninstall**.
3. In the **NAKIVO Backup & Replication Uninstallation** wizard, click **Uninstall**.
4. Click **Close** when the uninstallation process is completed.

Uninstalling on Linux or Generic ARM-based NAS

Refer to the sections below to learn how to uninstall NAKIVO Backup & Replication on a Linux OS or a generic ARM-based NAS.

Uninstalling Director and Onboard Transporter on Linux or Generic ARM-based NAS

To uninstall the Director and Onboard Transporter, which is installed with the Director by default, follow the steps below:

1. Run the "uninstall" script which is located in the Ddirector folder inside the product installation folder. If the product is installed in the default location, run: /opt/nakivo/director/uninstall
2. Enter "U" and then press **Enter** to confirm uninstalling the application.

Uninstalling Transporter on Linux or Generic ARM-based NAS

To uninstall the Transporter, follow the steps below:

1. Run the "uninstall" script which is located in the transporter folder inside the product installation folder. If the product is installed in the default location, run: /opt/nakivo/transporter/uninstall

2. Enter "U" and then press **Enter** to confirm uninstalling the application.

Uninstalling on Synology NAS

Follow the steps below to uninstall NAKIVO Backup & Replication on a Synology NAS:

1. In the Synology NAS management interface, open the **Package Center**.
2. Click NAKIVO Backup & Replication.
3. Choose **Uninstall** from the **Actions** list.
4. Click **OK** in the message box that opens to confirm that you wish to uninstall the application.

When the uninstallation process is completed, NAKIVO Backup & Replication will be removed from the list of installed applications.

Uninstalling on Western Digital NAS

Follow the steps below to uninstall NAKIVO Backup & Replication on a Western Digital NAS:

1. Open the NAS My Cloud Dashboard and click **Apps**.
2. In the **Installed Apps** list, select NAKIVO Backup & Replication.
3. The NAKIVO Backup & Replication item opens to the right of the installed applications list. Click the **Uninstall** button.
4. The **Uninstall NAKIVO Backup and Replication** dialog opens. Click **OK** to confirm that you wish to uninstall the application and delete all application data and settings.
5. The **Updating** progress bar opens. Wait until the uninstallation completes.

When the uninstallation process is completed, NAKIVO Backup & Replication will be removed from the list of installed applications.

Uninstalling on QNAP NAS

Follow the steps below to uninstall NAKIVO Backup & Replication on a QNAP NAS:

1. Open the QNAP NAS Desktop and click **App Center**.
2. The **App Center** dialog opens. In the **My Apps** list, locate the NAKIVO Backup & Replication application and open the list of applicable actions by clicking the drop-down button.
3. In the list of applicable actions, click **Remove**.
4. In the dialog that opens, click **OK** to confirm removing the application and application-relevant user data.
5. Wait until the uninstallation is complete.

When the uninstallation process is completed, NAKIVO Backup & Replication will be removed from the list of installed applications.

Uninstalling on ASUSTOR NAS

Follow the steps below to uninstall NAKIVO Backup & Replication on a QNAP NAS:

1. Open the ASUSTOR NAS Desktop and click **App Central**.
2. In the list of installed applications, locate NAKIVO Backup & Replication, select it and then click the **Remove** button.
3. In the dialog that opens, click **OK** to confirm that you wish to remove the application.
4. The **Removing** progress bar opens. Wait until the uninstallation is completed.

When the uninstallation process is completed, NAKIVO Backup & Replication will be removed from the list of installed applications.

Uninstalling on NETGEAR ReadyNAS

Follow the steps below to uninstall NAKIVO Backup & Replication on NETGEAR ReadyNAS:

1. Open the NETGEAR ReadyNAS **Admin Page** and go to **Apps** > **Installed Apps**.
2. Locate **NAKIVO Backup & Replication** in the list of available applications. Alternatively, enter NAKIVO to the filtering box in the upper left corner of the **Admin Page**.
3. Click the **Remove** button below the application item.
4. The **Confirm Deletion** dialog box opens. Click **Yes** to confirm that you wish to uninstall NAKIVO Backup & Replication on NETGEAR ReadyNAS.
5. Wait until the uninstallation is completed.

When the uninstallation process is completed, NAKIVO Backup & Replication will be removed from the list of installed applications.

Terminating on Amazon EC2

Follow the steps below to terminate NAKIVO Backup & Replication that is launched as an Amazon EC2 instance:

1. Open AWS Management Console and go to **EC2 Dashboard**.
2. In the **Instances** menu, click **Instances**.
3. In the list of instances, locate the necessary NAKIVO Backup & Replication instance and select it.
4. In the **Actions** menu, go to **Instance State** and click **Terminate**.
5. In the **Terminate Instances** dialog, click **Yes, Terminate** to confirm that you wish to terminate your instance of NAKIVO Backup & Replication.
6. Wait until the instance is terminated.

In about 60 minutes, the terminated NAKIVO Backup & Replication instance will be removed from the list of Amazon EC2 instances.

Settings

This section covers the following topics:

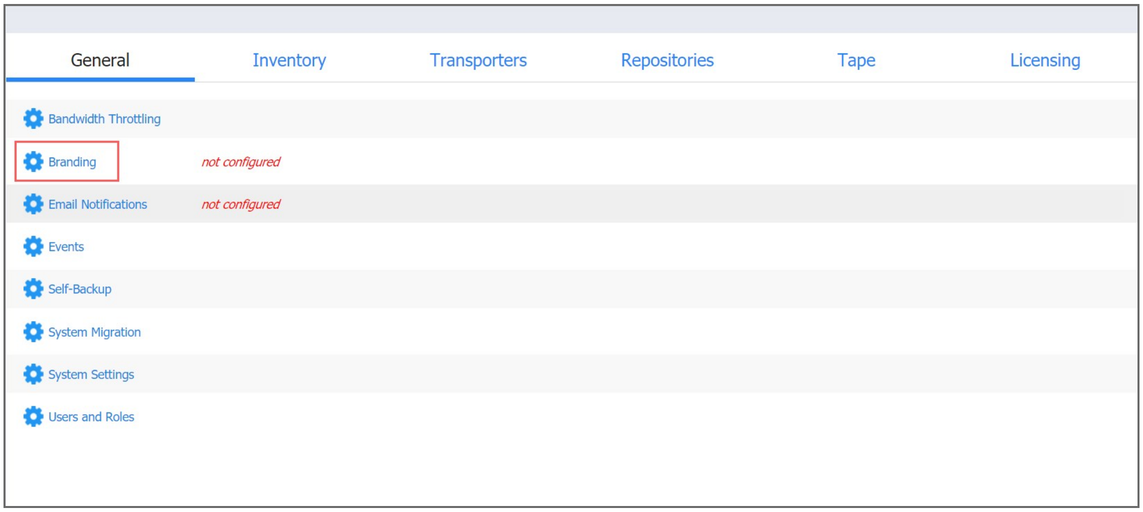
General

This section contains the following topics:

Branding Configuration

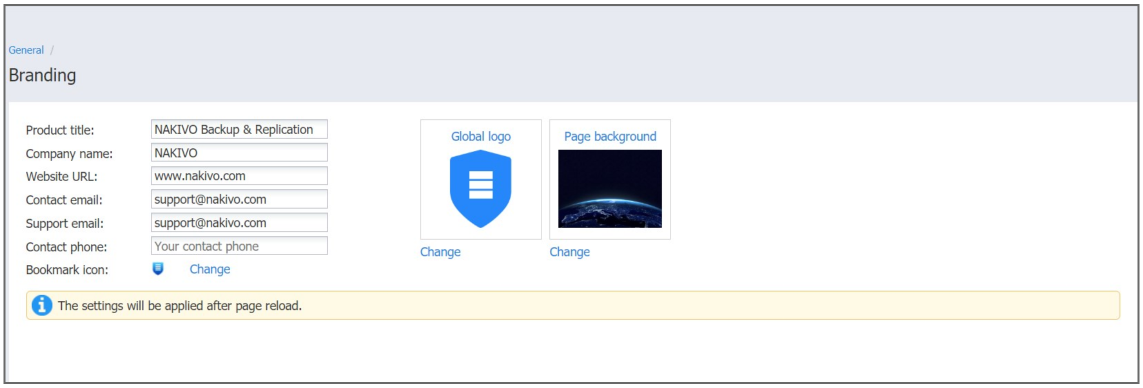
You can change the product branding settings such as product name, logo, background, and so on. To configure these product settings, follow the steps below:

1. Click **Settings** in the left pane of the product.
2. Go to the **General** tab and click **Branding**.



Bandwidth Throttling
Branding *not configured*
Email Notifications *not configured*
Events
Self-Backup
System Migration
System Settings
Users and Roles

3. Change the following, as appropriate:
   - Product title
   - Company name
   - Website URL
   - Contact email
   - Support email
   - Contact phone
   - Bookmark icon
   - Global logo
   - Page background



Product title: NAKIVO Backup & Replication
Company name: NAKIVO
Website URL: www.nakivo.com
Contact email: support@nakivo.com
Support email: support@nakivo.com
Contact phone: Your contact phone
Bookmark icon:

The settings will be applied after page reload.

4. Click **Apply**.

During upload, the logo and bookmark icon images are internally resized while preserving the aspect ratio. The background image is used as it is. To get the best image quality, follow the recommendations below.

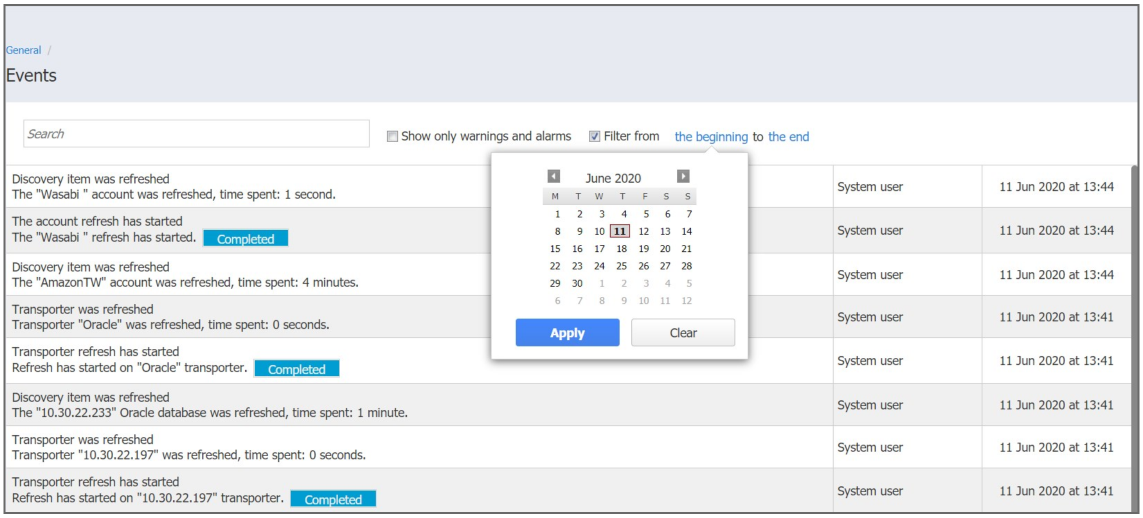
Image	Best format	Best resolution
Global logo	.png	40x40
Page background	.jpeg	1920x1440
Bookmark icon	.png	16x16

Configuring Events

NAKIVO Backup & Replication can store and display system events. By default, events are stored for 60 days; you can change the time period in **Settings**.

To view events, follow the steps below:

1. Click **Settings** in the left pane of the product.
2. Open the **General** tab and click **Events**. The **Events** page opens, displaying the NAKIVO Backup & Replication system events.
3. Optionally, you can enter a search string to the **Search** box. This allows you to see events related only to NAKIVO Backup & Replication items – Transporters, repositories, jobs, backups, and replicas,– contained in your search string.
4. Optionally, you can select **Show only warnings and alarms**. If selected, the events list displays only warnings and alarms.
5. Optionally, you can select **Filter by date** and enter the beginning and ending dates for events filtering. This allows you to limit the events list within a specific time period.
6. If required, navigate between pages by using the **Page** control.



General /

Events

Search ☐ Show only warnings and alarms ☑ Filter from the beginning to the end

Discovery item was refreshed The "Wasabi " account was refreshed, time spent: 1 second.	System user	11 Jun 2020 at 13:44
The account refresh has started The "Wasabi " refresh has started. Completed	System user	11 Jun 2020 at 13:44
Discovery item was refreshed The "AmazonTW" account was refreshed, time spent: 4 minutes.	System user	11 Jun 2020 at 13:44
Transporter was refreshed Transporter "Oracle" was refreshed, time spent: 0 seconds.	System user	11 Jun 2020 at 13:41
Transporter refresh has started Refresh has started on "Oracle" transporter. Completed	System user	11 Jun 2020 at 13:41
Discovery item was refreshed The "10.30.22.233" Oracle database was refreshed, time spent: 1 minute.	System user	11 Jun 2020 at 13:41
Transporter was refreshed Transporter "10.30.22.197" was refreshed, time spent: 0 seconds.	System user	11 Jun 2020 at 13:41
Transporter refresh has started Refresh has started on "10.30.22.197" transporter. Completed	System user	11 Jun 2020 at 13:41

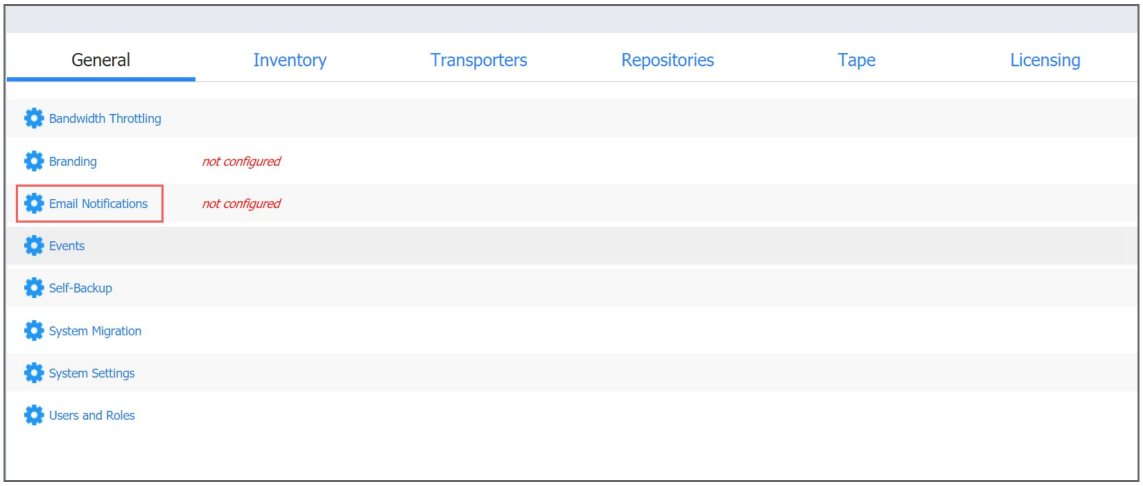
Email Notifications

NAKIVO Backup & Replication can send notifications and reports over email.

- Email Settings
- Email Notifications
- Automatic Reports

To receive automatic notifications, configure email settings by following the steps below:

1. Log in to NAKIVO Backup & Replication.
2. Click **Settings** in the left pane of the product.
3. Go to the **General** tab.
4. Click **Email notifications** to configure email settings, email notifications, and automatic reports section on the page that opens.



Email Settings

Important

If you use an email with two-factor authentication, grant access permissions to NAKIVO Backup & Replication via your account security settings and generate a unique password. As an example, use instructions for Google accounts provided in the Create & use App Passwords article. When configuring email setting of the product, enter this password in the **SMTP password** box.

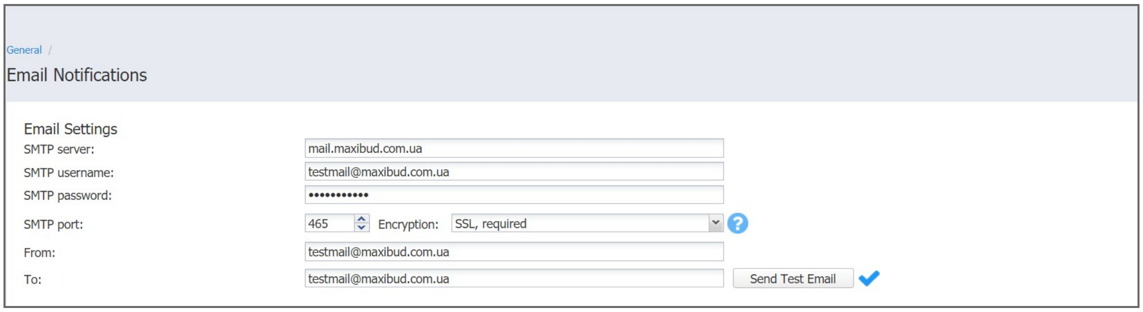
1. To set email settings, fill out the fields in the Email settings section:
    - **SMTP server**: The address of the server responsible for sending emails.
    - **SMTP username**: The username on the server (usually the same as the email username).
    - **SMTP password**: Usually the same as the password to your email.
    - **SMTP port**: Depends on encryption type.
    - **Encrypted connection**: Select the type of encryption:

- **Never**: Always use a plaintext connection. Not recommended.
- **TLS, if possible**: Start with plaintext, then use STARTTLS to switch to secure connection if supported by the server.
- **TLS, required**: Start with plaintext, then use STARTTLS to switch to secure connection; drop the connection if not supported by the server.
- **SSL, required**: Use the SSL-encrypted connection.

2. Click **Send Test Email** to verify that the settings are correct.

   Note

   If you want to use a Gmail account to receive email notifications, turn on the **Less secure apps access** setting by navigating to **Manage your Google Account>Security** in your Google account.



Email Notifications

Email Settings

SMTP server: mail.maxibud.com.ua

SMTP username: testmail@maxibud.com.ua

SMTP password: •••••••••••

SMTP port: 465 Encryption: SSL, required

From: testmail@maxibud.com.ua

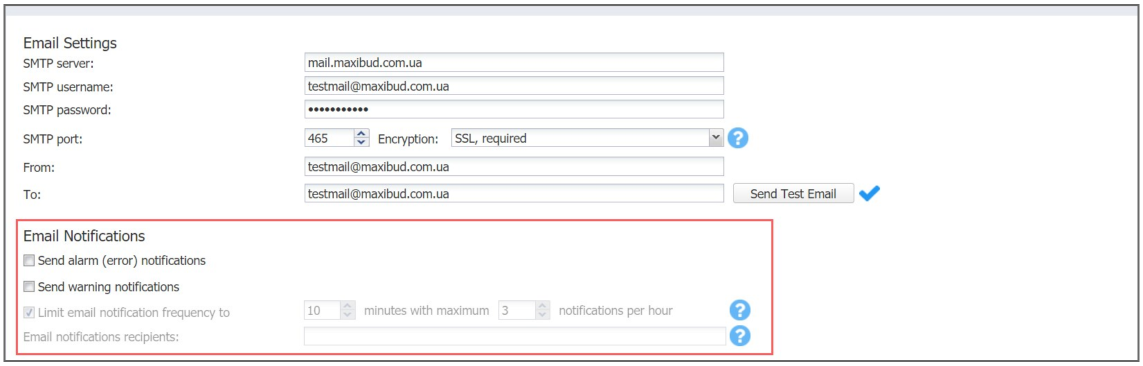
To: testmail@maxibud.com.ua

Email Notifications

To set Email notifications, fill out the fields in the *Email notifications* section:

- **Send alarm (error) notifications**: If this option is selected, NAKIVO Backup & Replication will send email notifications to the specified recipients in case an error (for example, a job failure) occurs in the product.
- **Send warning notifications**: If this option is selected, NAKIVO Backup & Replication will send email notifications to the specified recipients in case the product generates a warning message (for example, lost connection to a host or Backup Repository).
- **Limit email notification frequency**: This option provides you with the ability to set up a notification email frequency and hourly limit. If notification emails exceed the hourly limit, all new notifications will be delivered the next hour. If deselected, notification emails will be sent every 5 minutes with no hourly limit.
- **Email notification recipients**: Specify the recipients who will be receiving alarm and warning notifications (if

enabled).



Email Settings

SMTP server: mail.maxibud.com.ua

SMTP username: testmail@maxibud.com.ua

SMTP password: •••••••••••

SMTP port: 465 Encryption: SSL, required

From: testmail@maxibud.com.ua

To: testmail@maxibud.com.ua Send Test Email ✓

Email Notifications

□ Send alarm (error) notifications

□ Send warning notifications

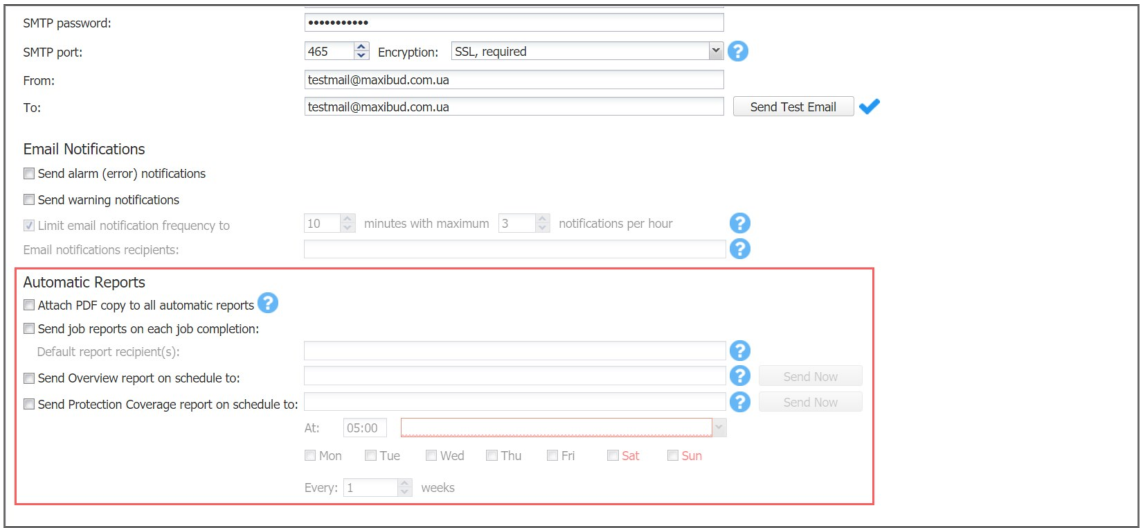
☑ Limit email notification frequency to 10 minutes with maximum 3 notifications per hour

Email notifications recipients:

Automatic Reports

To set automatic reports, fill out the fields in the *Automatic Reports* section:

- **Attach PDF copy to all automatic reports**: If selected, a PDF copy of the report will be attached to each automatic job report and to the Overview report. Note that this increases the size of email messages.
- **Send job reports on each job completion**: If this option is selected, NAKIVO Backup & Replication will send an HTML report after the completion of every job (regardless of the job success or failure) to email addresses specified in the text field. Use a semi-colon to separate multiple email addresses.
- **Send Overview report on schedule to**: If this option is selected, NAKIVO Backup & Replication will generate the Overview report (which includes information about all jobs and groups in the product) on the date and time specified in the scheduler and will send the report to the recipients specified in the text field. Use a semi-colon to separate multiple email addresses.
- **Send Protection Coverage report on schedule to**: If this option is selected, NAKIVO Backup & Replication will generate the Protection Coverage report. This includes information about all VMs & instances protected by backup and/or replication jobs as well as the information about all unprotected VMs & instances. The report will be sent to the recipients specified in the text field on the date and time specified in the scheduler. Use a semi-colon to separate multiple email addresses.



SMTP password: •••••••••••

SMTP port: 465 Encryption: SSL, required

From: testmail@maxibud.com.ua

To: testmail@maxibud.com.ua Send Test Email ✓

Email Notifications

□ Send alarm (error) notifications

□ Send warning notifications

☑ Limit email notification frequency to 10 minutes with maximum 3 notifications per hour

Email notifications recipients:

Automatic Reports

□ Attach PDF copy to all automatic reports

□ Send job reports on each job completion:

Default report recipient(s):

□ Send Overview report on schedule to: Send Now

□ Send Protection Coverage report on schedule to: Send Now

At: 05:00

□ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun

Every: 1 weeks

Click **Apply** when all settings are configured.

Self-Backup Configuration

The self-backup feature allows you to automatically protect configuration settings of your NAKIVO Backup & Replication instance. For more information, refer to "Self-Backup Feature" on page 8.

Note

Self-backup is not supported for the multi-tenant configuration.

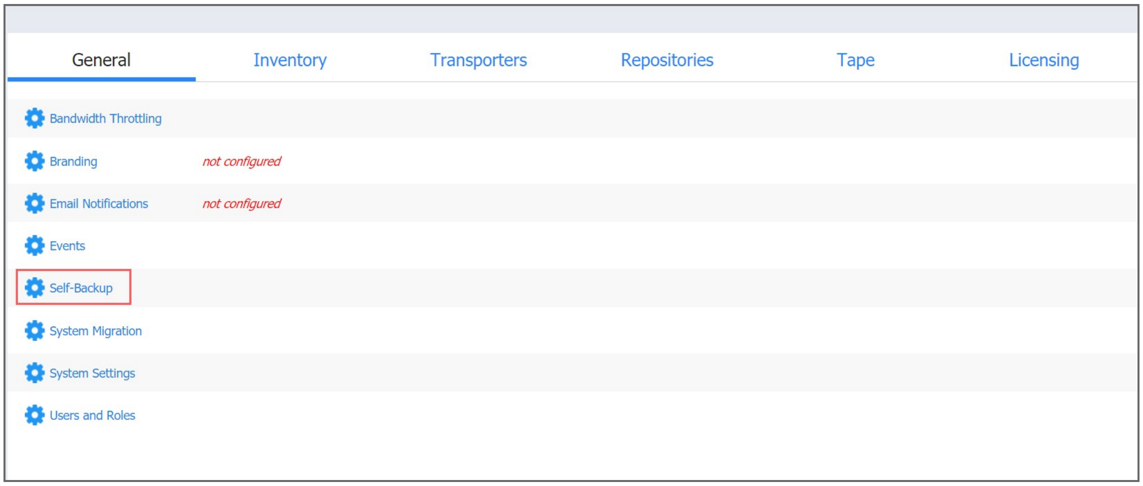
To configure self-backup options, proceed as described in the following sections:

- "Accessing Self-Backup Options" below
- "Setting Up Self-Backup Destination" below
- "Self-Backup Schedule" on page 201
- "Self-Backup Retention" on page 201
- "Recovering from Self-Backup" on page 202

Accessing Self-Backup Options

To access self-backup options, follow the steps below:

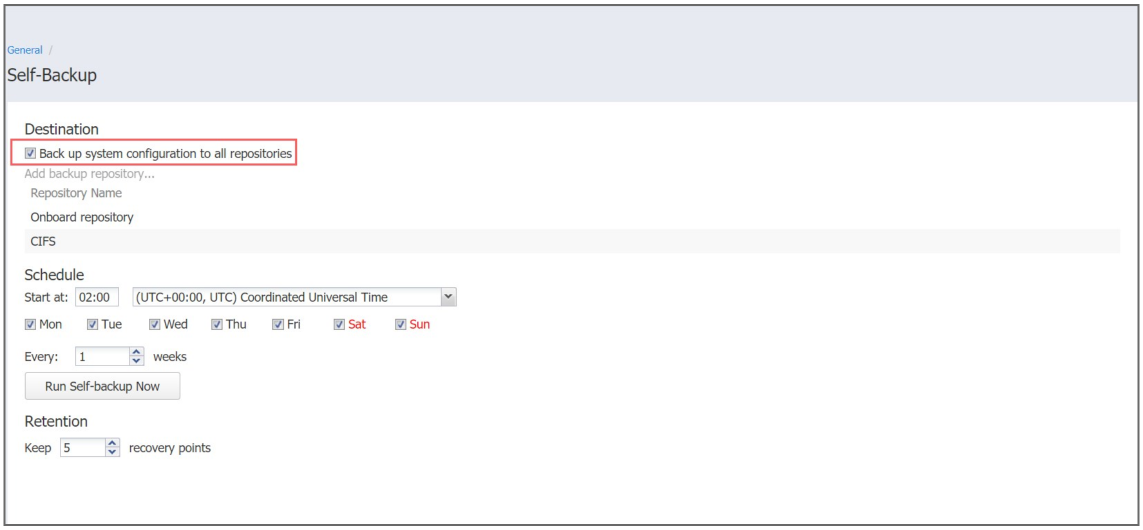
1. Click **Settings** in the left pane of NAKIVO Backup & Replication.
2. Go to the **General** tab and click **Self-backup**.



Setting Up Self-Backup Destination

To configure a self-backup destination, follow the steps below:

1. Select **Back up system configuration to all repositories** to enable all repositories in the list of repositories where system configuration will be backed up. If deselected, you can remove specific repositories from the list.



General /

Self-Backup

Destination

☑ Back up system configuration to all repositories

Add backup repository...

Repository Name
Onboard repository
CIFS

Schedule

Start at: 02:00 (UTC+00:00, UTC) Coordinated Universal Time

☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat ☑ Sun

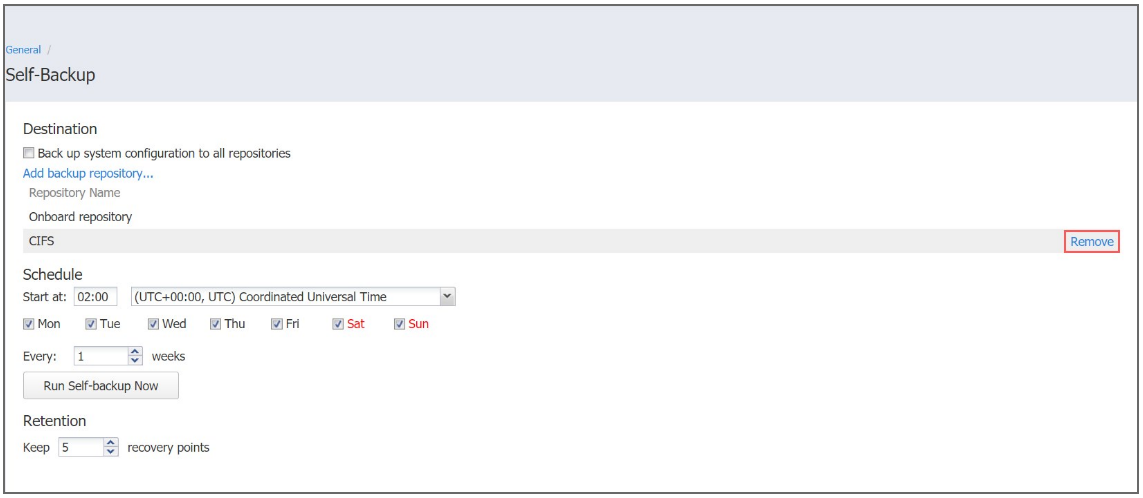
Every: 1 weeks

Run Self-backup Now

Retention

Keep 5 recovery points

2. If necessary, remove a Backup Repository from the list of repositories for self-backup:
    1. Hover the pointer over the header of the Backup Repository and then click **Remove**.
    2. In the dialog that opens, choose either of the following:
        - **Remove repository and keep self- backups**: Removes the selected Backup Repository from the list and keeps the self-backups.
        - **Remove repository and self-backups**: Removes both the selected Backup Repository and self-backups.
    3. Click **Remove** to confirm your operation.



General /

Self-Backup

Destination

□ Back up system configuration to all repositories

Add backup repository...

Repository Name	
Onboard repository	
CIFS	Remove

Schedule

Start at: 02:00 (UTC+00:00, UTC) Coordinated Universal Time

☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat ☑ Sun

Every: 1 weeks

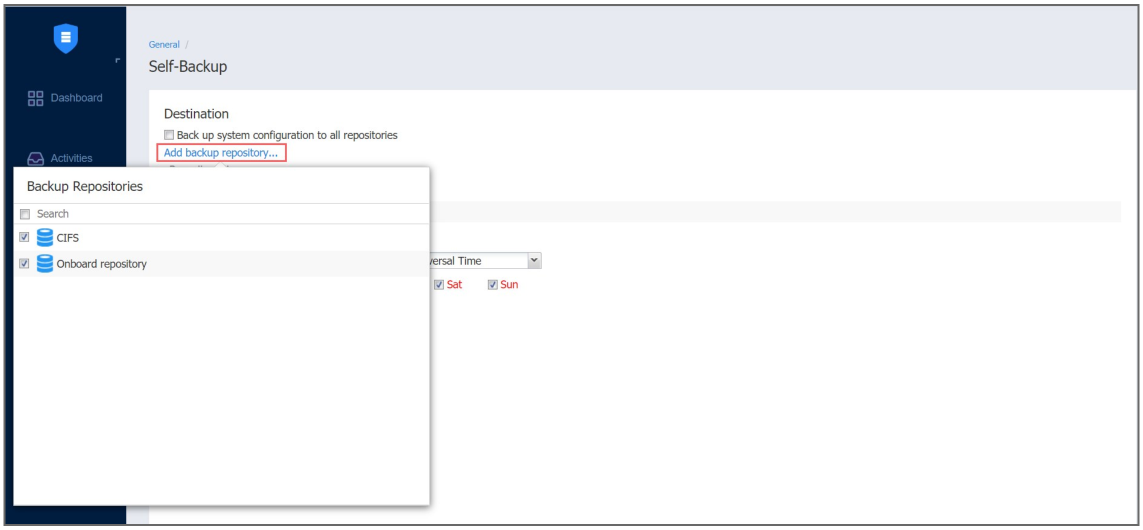
Run Self-backup Now

Retention

Keep 5 recovery points

3. If necessary, add a Backup Repository to the list:
    a. Click **Add backup repository** to add repositories to the list of repositories for system backing up.
    b. In the **Backup Repositories** dialog that opens, select the necessary repositories and close the

dialog.



General /

Self-Backup

Destination

☐ Back up system configuration to all repositories

Add backup repository...

Backup Repositories

☐ Search

☑ CIFS

☑ Onboard repository

ersal Time

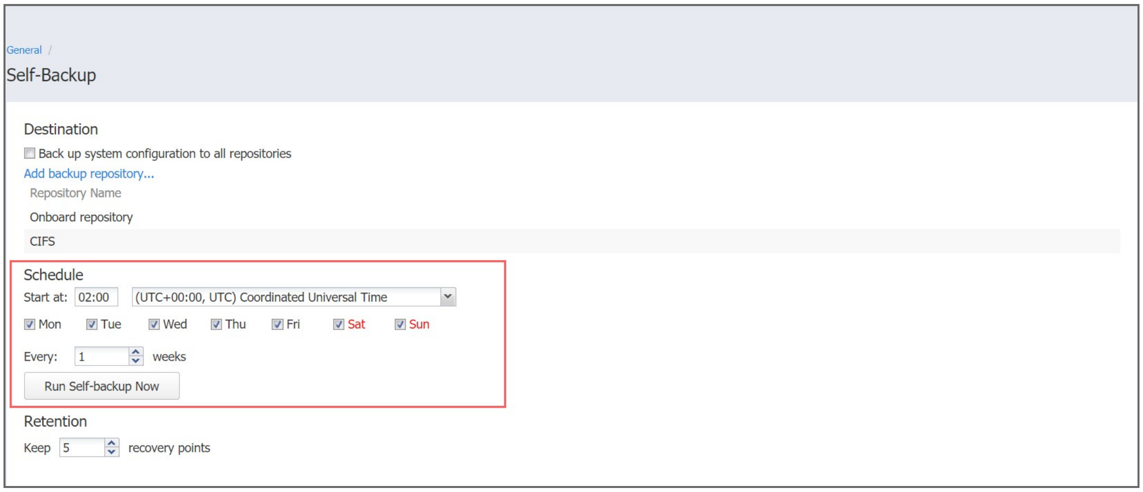
☑ Sat ☑ Sun

4. When ready with configuring the self-backup destination, click **Apply**.

Self-Backup Schedule

To configure the self-backup schedule, follow the steps below:

1. In the **Start at** group of boxes, enter time to trigger starting the self-backup. You can choose a specific time zone from the list, enter the hours and minutes of the day, and select the necessary days of the week.
2. If you need to start the self-backup immediately, click **Run Self-backup Now**.
3. When ready with configuring the self-backup schedule, click **Apply**.



General /

Self-Backup

Destination

☐ Back up system configuration to all repositories

Add backup repository...

Repository Name

Onboard repository

CIFS

Schedule

Start at: 02:00 (UTC+00:00, UTC) Coordinated Universal Time

☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat ☑ Sun

Every: 1 weeks

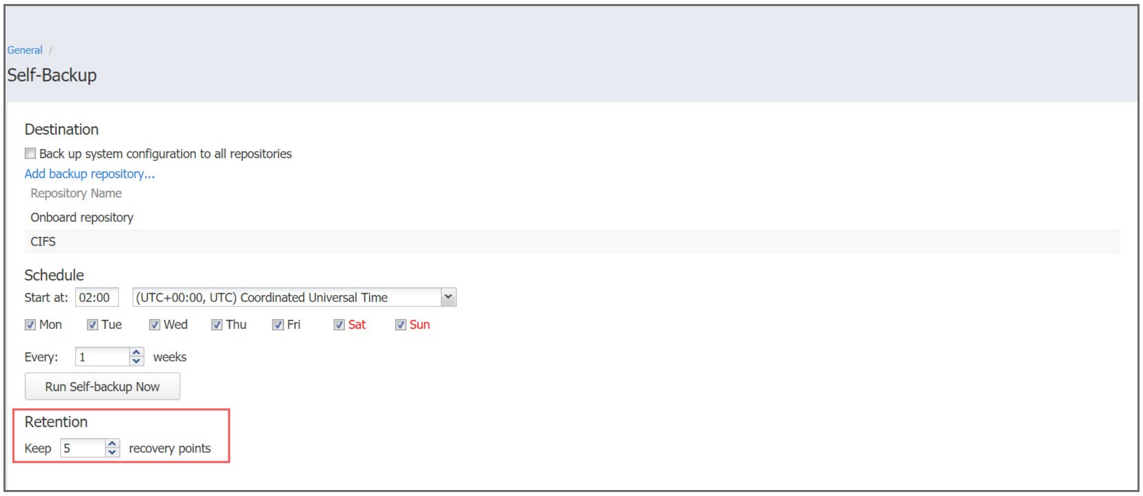
Run Self-backup Now

Retention

Keep 5 recovery points

Self-Backup Retention

In the **Retention** section of the self-backup settings, you can enter a number of recovery points to be kept for the self-backup. To apply your settings, click the **Apply** button.



Destination

☐ Back up system configuration to all repositories

Add backup repository...

Repository Name
Onboard repository
CIFS

Schedule

Start at: 02:00 (UTC+00:00, UTC) Coordinated Universal Time

☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat ☑ Sun

Every: 1 weeks

Retention

Keep 5 recovery points

Recovering from Self-Backup

To recover the configuration of NAKIVO Backup & Replication from a self-backup stored in a Backup Repository, do the following:

1. Go to **Settings** > **Repositories**.
2. Select one of the repositories that contain a self-backup.
3. Select the self-backup from the **Backups** list and click **Recover**.
4. Select a recovery point and click **Restore.**
5. Wait while the system configuration is restored. When the self-backup recovery process is completed, a message announcing success appears.

   Note

   If a selected recovery point was created from an encrypted self-backup, you will have to enter the password to it.

System Migration

NAKIVO Backup & Replication provides you with the ability to migrate all your settings (including inventory, jobs, credentials, transporter settings, and so on) to a new instance (copy) of the product.

Important

System configuration export and import are designed for migration purposes only, and not to serve as a system configuration backup. After you have exported system configuration from an old instance of the product, do not run jobs in that old instance. Doing so will result in failed jobs in the new instance after the migration. All jobs will have to be recreated, and full initial job run will be required.

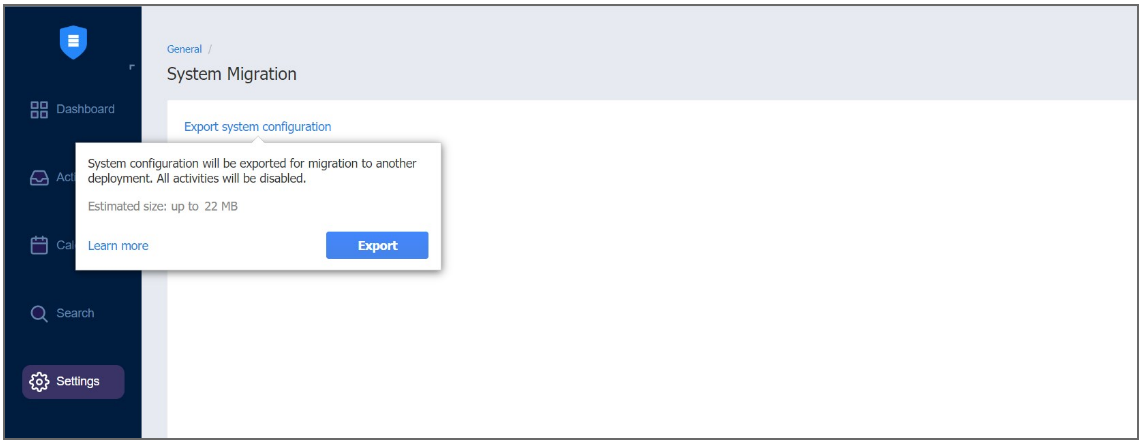
See the topics below for more information:

- Exporting System Configuration
- Importing System Configuration

Exporting System Configuration

To export system configuration from the old deployment, follow the steps below:

1. Click **Settings** in the left pane of the product.
2. Click **System Migration** in the **General** tab.
3. Click **Export system configuration**.
4. In the dialog window that appears, click **Export**.



System configuration will be exported for migration to another deployment. All activities will be disabled.

Estimated size: up to 22 MB

5. Click **Proceed** to confirm the operation.

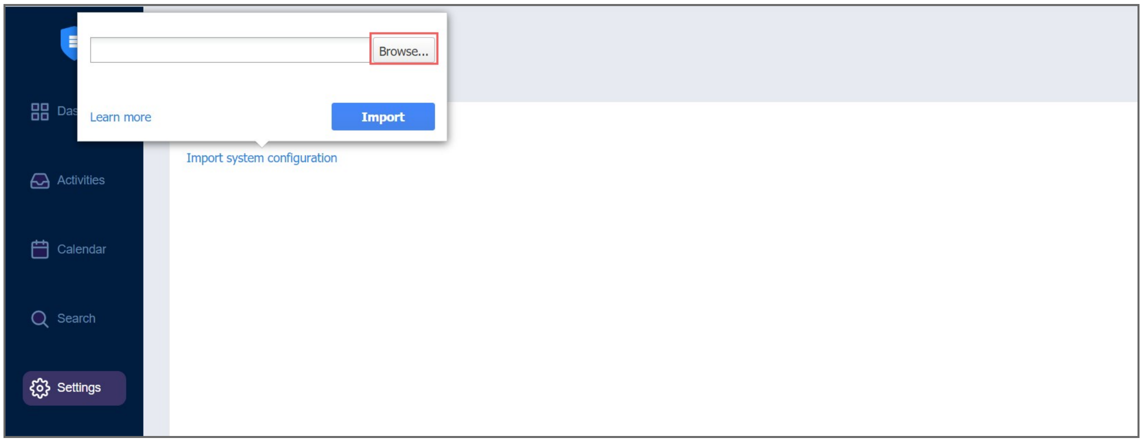
   Note

   All activities in the old instance (such as jobs and recovery sessions) will be automatically stopped and all jobs will be disabled.
6. Wait until the export is completed and download the export bundle.
7. Do not run jobs in the old instance.

Importing System Configuration

To import system configuration into a new instance of the product, follow the steps below:

1. Click **Settings** in the left pane of the product.
2. Click **System Migration** in the **General** tab.
3. Click **Import system configuration**.
4. In the dialog window that appears, locate the system configuration bundle using the **Browse** button.



5. Click **Import**.
6. Click **Proceed** to confirm the operation.

   Important

   - If there is any existing data in the new instance, it will be overwritten with the import operation.
   - If a physical configuration of your source deployment differs from a target deployment, a Backup Repository may become inaccessible after the bundle import is completed.
7. Wait until the import is completed, and close the dialog window.

Notes

- Backup Repositories are not migrated by the system configuration export and import. If you have a local Backup Repository on the old instance of the product, you may want to move it to the new location. After moving the Backup Repository, you may need to edit Backup Repository settings in the new instance, s that the new settings refer to the actual Backup Repository location.
- In case a custom TLS/SSL certificate of the Web server was used in the old instance, a manual service restart will be required in the new deployment.

System Settings

To configure the system settings, follow the steps below:

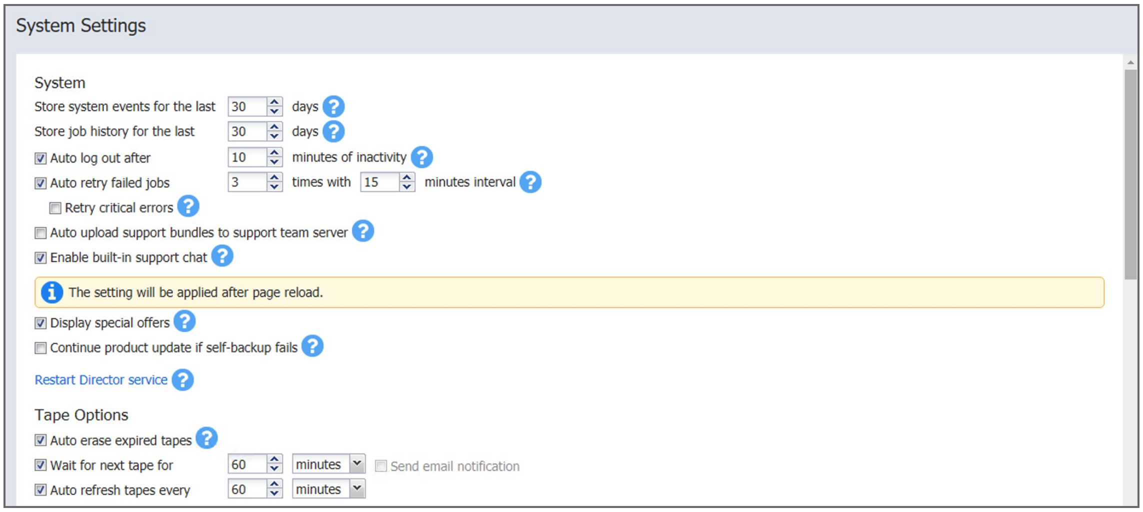
1. Click **Settings** in the main menu on the left.
2. Go to the **General** tab and click **System settings.**
3. Set the following options:
   - In the *System* section:
     - **Store system events for the last x days**: Events older than the specified number of days (can be from 10 to 365) will be deleted.
     - **Store job history for the last x days**: The history of the jobs older than the specified number of days (can be from 5 to 90) will be deleted.
     - **Auto log out after x minutes of inactivity**: When this option is selected, the current user will be automatically logged out of NAKIVO Backup & Replication after the specified period of inactivity.
     - **Auto retry failed jobs x times with y minutes interval**: When this option is selected, failed jobs will be automatically retried the specified number of times (from 2 to 10) and with the specified time interval (from 1 to 60). Jobs with failed backup, replication, and recovery remain in the "running" state until all retries have either succeeded or failed.
       - **Retry critical errors**: When this option is selected, NAKIVO Backup & Replication tries to automatically rerun jobs with critical and non-critical errors a specified number of times.
     - **Auto upload support bundles to support team server**: When this option is selected, NAKIVO Backup & Replication automatically creates, encrypts, and uploads support bundles once a day to a NAKIVO support server. The NAKIVO Support team may use this information to improve the product experience and to identify and resolve product issues faster.
     - **Enable built-in support chat**: When this option is selected, you can contact a NAKIVO representative via chat in the NAKIVO Backup & Replication interface. When selected in the multi-tenant mode, the built-in support chat is available to all tenants of the NAKIVO Backup & Replication instance.
     - **Display special offers**: When this option is enabled, the NAKIVO special offers toolbar appears in the NAKIVO Backup & Replication interface.
     - **Continue to update even if self-back fails**: When this option is selected, updates proceed even if self-backup cannot be performed.
     - You can click **Restart Director service** to stop all current activities and restart the Director. After clicking the link, a confirmation window appears. Click **Reboot** to confirm the restart.
   - In the *Tape Options* section:
     - **Auto erase expired tapes**: When this option is selected, expired tapes are erased automatically.

       Important

    If this option is selected, the following prerequisites must be met for a cartridge to be erased:

    - All recovery points within the tape cartridge are expired.
    - There are no dependent recovery points on other tape cartridges.
    - The product keeps at least one full chain of recovery points.

  - **Wait for next tape for**: Specify how long the system should wait for the next tape if there is no appropriate amount. Select the **Send email notification** checkbox to receive email notifications.
  - **Auto refresh tapes every**: Select how often the contents of the tapes are refreshed in minutes or hours. Deselect if refreshing is not required.



System Settings

System

Store system events for the last 30 days

Store job history for the last 30 days

☑ Auto log out after 10 minutes of inactivity

☑ Auto retry failed jobs 3 times with 15 minutes interval

□ Retry critical errors

□ Auto upload support bundles to support team server

☑ Enable built-in support chat

The setting will be applied after page reload.

☑ Display special offers

□ Continue product update if self-backup fails

Restart Director service

Tape Options

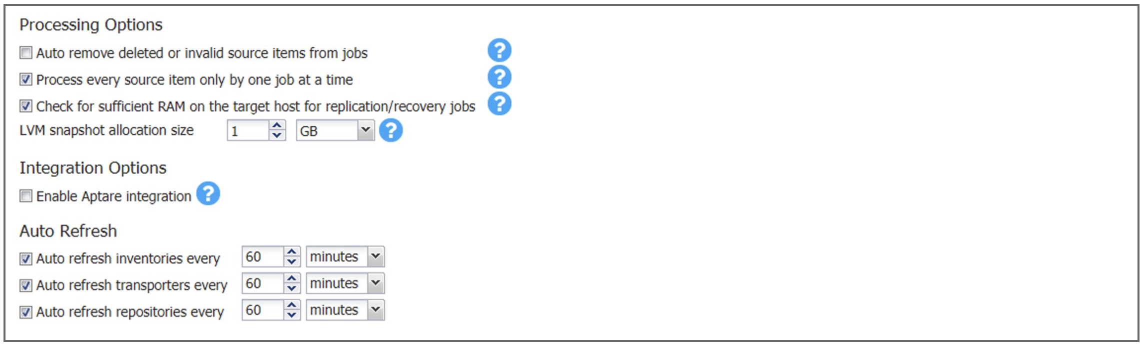
☑ Auto erase expired tapes

☑ Wait for next tape for 60 minutes □ Send email notification

☑ Auto refresh tapes every 60 minutes

- In the *Processing Options* section:
  - **Auto remove deleted VMs and instances from jobs**: This option applies to a protected container (such as a VMware cluster or EC2 region). When this option is selected, if NAKIVO Backup & Replication discovers (during the inventory refresh) that a VM(s) and/or EC2 instance(s) is no longer available in the protected container, NAKIVO Backup & Replication automatically removes these VMs and EC2 instances from all jobs.
  - **Process every source machine by one job at a time**: When this option is selected, all machines in backup and replication jobs are processed by one job at a time only. Running jobs and respective source objects will not be affected after changing this setting. For physical servers, this option is always enabled.
  - **Skip swap files and partitions during processing**: When this option is selected, swap files and partitions are skipped during backup and replication to reduce backup size.
  - **Check for sufficient RAM on the target host for replication/recovery jobs**: When this option is deselected, NAKIVO Backup & Replication does not check whether the amount of RAM on the target host is sufficient for replication and recovery jobs.
  - **LVM Snapshot allocation size**: This option allows you to set an LVM allocation snapshot size for a Linux physical server backup. The default size is 1 GB. The maximum size is 1000 GB.

- In the *Integration Options* section:
    - **Enable Aptare Integration**: Select this option to integrate APTARE storage resource management platform with NAKIVO Backup & Replication.
- In the *Auto Refresh* section:
    - **Auto refresh inventories every X minutes**: Specify how often you want your inventories to be refreshed.
    - **Auto refresh Transporters every X minutes**: Specify how often you want your Transporters to be refreshed.
    - **Auto refresh repositories every X minutes**: Specify how often you want your inventories to be refreshed.



Processing Options

☐ Auto remove deleted or invalid source items from jobs

☑ Process every source item only by one job at a time

☑ Check for sufficient RAM on the target host for replication/recovery jobs

LVM snapshot allocation size 1 GB

Integration Options

☐ Enable Aptare integration

Auto Refresh

☑ Auto refresh inventories every 60 minutes

☑ Auto refresh transporters every 60 minutes

☑ Auto refresh repositories every 60 minutes

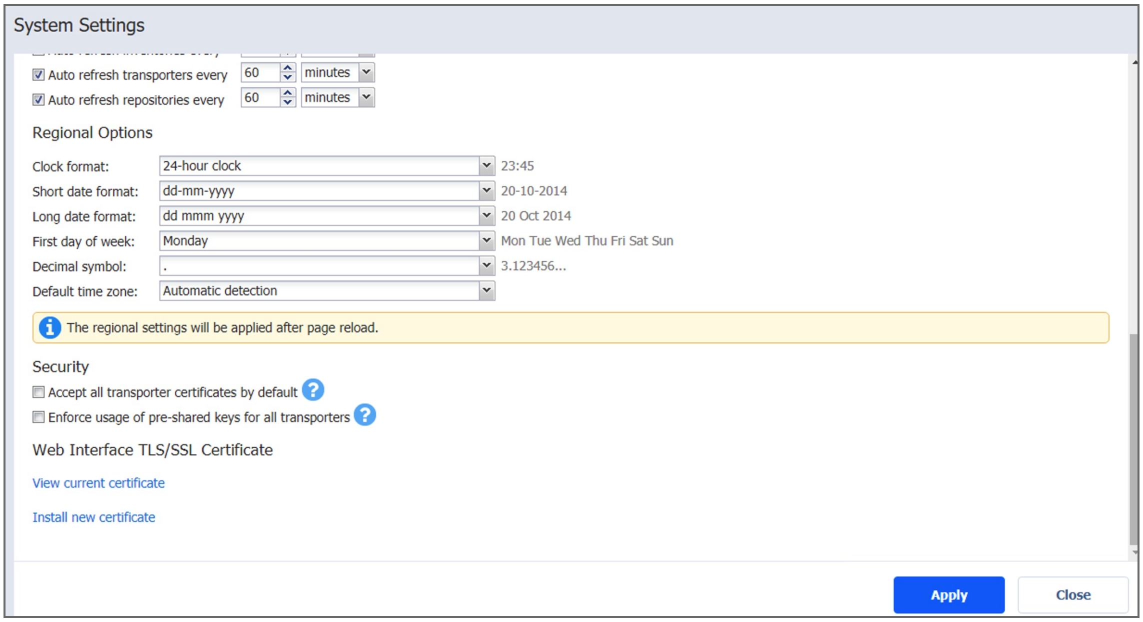
- In the *Regional options* section, set:
    - **Clock format**
    - **Short date format**
    - **Long date format**
    - **First day of week**
    - **Decimal symbol**
    - **Default time zone**

Note

If any time zone other than **(UTC+00:00, UTC) Coordinated Universal Time** is chosen, daylight savings times are honored.

- In the *Security section*you can enable the followin:
    - **Accept all transporter certificates by default**: When this option is selected, all Transporter certificates are accepted by default. Enabling this option is not recommended due to the security risks involved.
    - **Enforce usage of pre-shared keys for all transporters**: When this option is selected, all Transporters start requiring the pre-shared keys to function and become inaccessible

without them.



System Settings

☑ Auto refresh transporters every 60 minutes

☑ Auto refresh repositories every 60 minutes

Regional Options

Clock format: 24-hour clock 23:45

Short date format: dd-mm-yyyy 20-10-2014

Long date format: dd mmm yyyy 20 Oct 2014

First day of week: Monday Mon Tue Wed Thu Fri Sat Sun

Decimal symbol: . 3.123456...

Default time zone: Automatic detection

The regional settings will be applied after page reload.

Security

☐ Accept all transporter certificates by default

☐ Enforce usage of pre-shared keys for all transporters

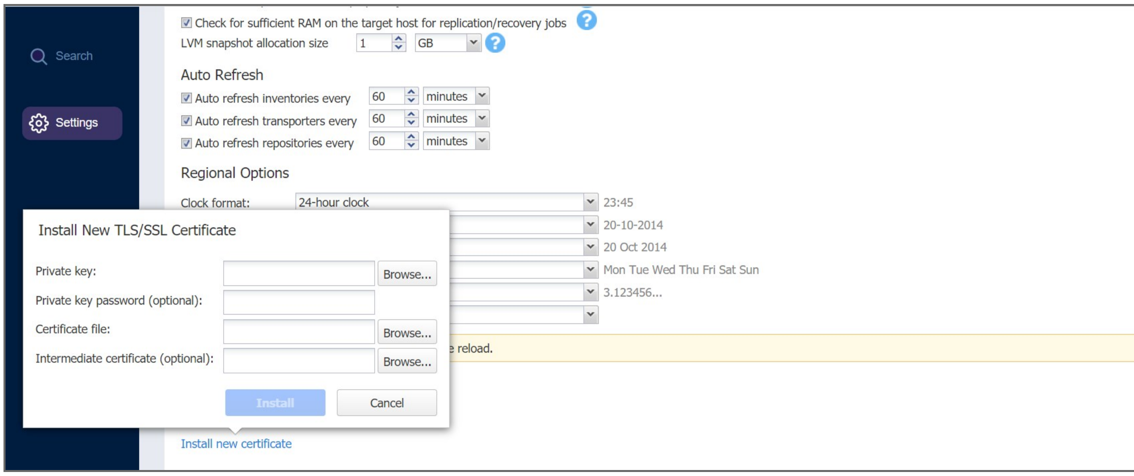
Web Interface TLS/SSL Certificate

View current certificate

Install new certificate

- In the *Web Interface TLS/SSL Certificate* section, you can either:
  - **View current certificate**: A dialog containing the current certificate information opens.
  - **Install new certificate**: A dialog opens allowing you to install a new TLS/SSL certificate for the NAKIVO Backup & Replication web interface. Certificates are generated either internally or through certification authorities. Proceed as follows to install a new certificate:
    - Click **Browse** and navigate to the location of either of the following certificate file types:
      - **Private key**: A file in the *.key format.
      - **Private key password (optional)**: A password for your private key.
      - **Certificate file**: A file in the *.pem, *.crt, *.cer, *.p7b, or *.p7s format.

- **Intermediate certificate (optional)**: A file in one of the following formats: *.pem, *.crt, *.cer, *.p7b, *.p7s.



☑ Check for sufficient RAM on the target host for replication/recovery jobs

LVM snapshot allocation size 1 GB

Auto Refresh

☑ Auto refresh inventories every 60 minutes

☑ Auto refresh transporters every 60 minutes

☑ Auto refresh repositories every 60 minutes

Regional Options

Clock format: 24-hour clock 23:45

20-10-2014

20 Oct 2014

Mon Tue Wed Thu Fri Sat Sun

3.123456...

e reload.

Install New TLS/SSL Certificate

Private key: Browse...

Private key password (optional):

Certificate file: Browse...

Intermediate certificate (optional): Browse...

Install Cancel

Install new certificate

4. Click **Install**.

Notes

- NAKIVO Backup & Replication supports Certificates with the RSA algorithm only.
- In the *Web Interface TLS/SSL Certificate* section, you can see a notification about imminent TLS/SSL Certificate expiration in 30 days and onwards. If your certificate has expired, you will be asked to install a valid certificate.

Users and Roles

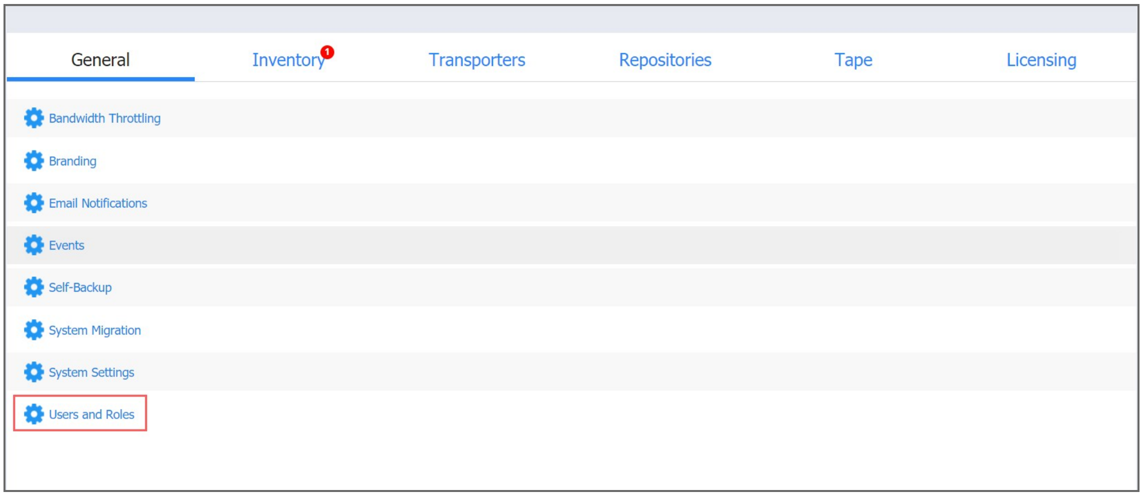
Accessing NAKIVO Backup & Replication is possible either with a user account created in the product or with an account added to the product from Active Directory. Each user in the product is assigned a role, which is a set of specific permissions.

- Managing Users and Roles
- Navigating Users View
- Navigating AD Groups View

Managing Users and Roles

Managing users and roles can be done by following these steps:

1. Log in to NAKIVO Backup & Replication.
2. Click **Settings** (cog icon) in the left pane of the product.
3. Go to the **General** tab and click **Users and Roles**.



Navigating Users View

To see the list of all local users, select the **Users** view from the drop-down list in the upper-left pane. On this page of the solution you can do the following:

- See the list of all local users added to NAKIVO Backup & Replication.
- Sort the list by **Name**, **Role**, **2FA**, or **Group** by clicking on the respective name of the column.
- Filter the list of users by entering the name of the user fully or partially into the **Search** bar or by selecting the **Filter** option.
  - Clicking **Filter** opens a new window that allows you to filter the list of local users according to **Name**, **User name**, **Email**, **Group**, **Role**, and **Status**.
- Add a new local user by clicking **Add User**.
- Integrate Active Directory account by clicking **AD Integration**.

- Edit, delete, disable, enable Two-factor authentication, and assign a new role to the local user individually. This can also be done in bulk by checking the box in the upper left pane to select all users and clicking **Bulk Action**.

  Note

  When selecting all local users to apply a bulk action, NAKIVO Backup & Replication selects only those users that are displayed on the screen.
- Edit the role assigned to the local use by clicking on the name of the role in the respective column.

Navigating AD Groups View

To see the list of all Active Directory groups, select the **AD Groups** view from the drop-down list in the upper-left pane. On this page of the solution you can do the following:

- See the list of all AD groups added to NAKIVO Backup & Replication.
- Sort the list by **Name**, **Users**, **2FA**, or **Role** by clicking on the respective name of the column.
- Filter the list of users by entering the name of the user fully or partially into the **Search** bar or by selecting the **Filter** option.
  - Clicking **Filter** opens a new window that allows you to filter the list of local users according to **Name**, **Role**, and **Status**.
- Add a new AD group by clicking **Add AD group**.
- Integrate Active Directory account by clicking **AD Integration**.
- Edit, delete, disable, enable Two-factor authentication, and assign a new role to the AD group individually. This can also be done in bulk by checking the box in the upper left pane to select all groups and clicking **Bulk Action**.

  Note

  When selecting all AD groups to apply a bulk action, NAKIVO Backup & Replication selects only those groups that are displayed on the screen.
- Edit the role assigned to the local use by clicking on the name of the role in the respective column.

For details, refer to the following sections:

- “Managing Active Directory Users” on page 212
- “Managing Local Users” on page 219
- “Managing User Roles” on page 227
- Configuring Two-Factor Authentication

Managing Active Directory Users

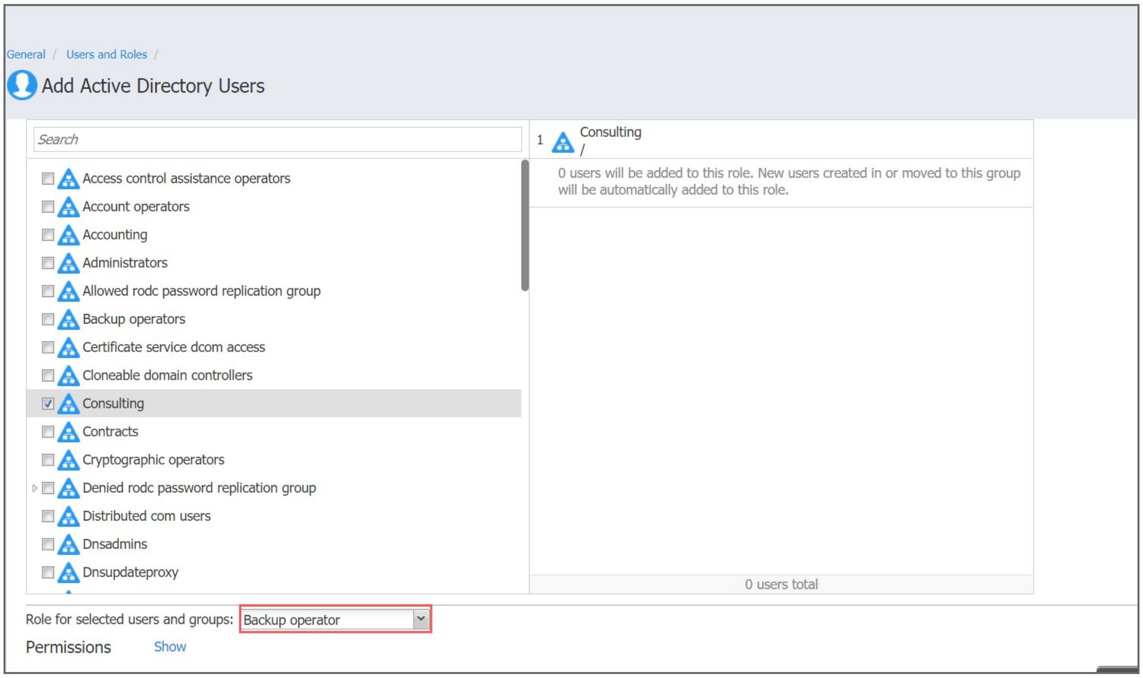
With NAKIVO Backup & Replication, you can configure Active Directory integration at any time. You can also freely add, edit, disable, delete AD users, or assign a role to them. For details, refer to the topics below:

- "Adding Active Directory User" on page 213
- "Assigning Role to Active Directory User" on page 214
- "Configuring Active Directory Integration" on page 215
- "Deleting Active Directory User" on page 216
- "Disabling Active Directory User" on page 217
- "Editing Active Directory User" on page 218

Adding Active Directory User

After configuring AD integration in the **Active Directory Configuration** wizard, you can proceed with adding AD user(s). Proceed as follows:

1. Optionally, you can filter the tree of Active Directory users by entering a string to the **Search** box. You can enter a section or the whole name of the item.
2. Select Active Directory users and groups by placing a checkmark to their left.
3. The selected items appear in the right pane of the page. If necessary, reorder the selected items by dragging them to a new position. By doing so, you can specify to add the most important users and groups first.
4. Review the list of selected items. If necessary, remove a selected user or group from the list in either of the following ways:
   - Deselect the item in the left pane. This will remove the item from the right pane.
   - In the right pane, hover the pointer over the item you wish to remove and click the **Remove** button. This will deselect the item in the left pane.
5. In the **Role** list, choose a user role to be assigned to the users.



General / Users and Roles /

Add Active Directory Users

Search

□ Access control assistance operators
□ Account operators
□ Accounting
□ Administrators
□ Allowed rodc password replication group
□ Backup operators
□ Certificate service dcom access
□ Cloneable domain controllers
☑ Consulting
□ Contracts
□ Cryptographic operators
□ Denied rodc password replication group
□ Distributed com users
□ Dnsadmins
□ Dnsupdateproxy

1 Consulting
/

0 users will be added to this role. New users created in or moved to this group will be automatically added to this role.

0 users total

Role for selected users and groups: Backup operator

Permissions Show

6. To unhide permissions granted to the users based on the role assigned, click the **Show** button beside the **Permissions** label. To hide the user permissions again, click **Hide**.
7. In the lower right corner of the page, click **Add**. Active Directory users appear in the NAKIVO Backup & Replication list of users.

Assigning Role to Active Directory User

Follow the steps below to assign a role to an Active Directory user:

1. Go to **Settings > General > Users & Roles**.
2. The **Users and Roles** page opens in the **Users** view. Hover over the Active Directory user, and then click **Manage** in the rightmost column of the row.
3. In the menu that opens, click **Assign role**.
4. In the dialog box that opens, select a new user role from the **Role** list and then click **Save**.

The Active Directory user appears in the list of users with the assigned role.

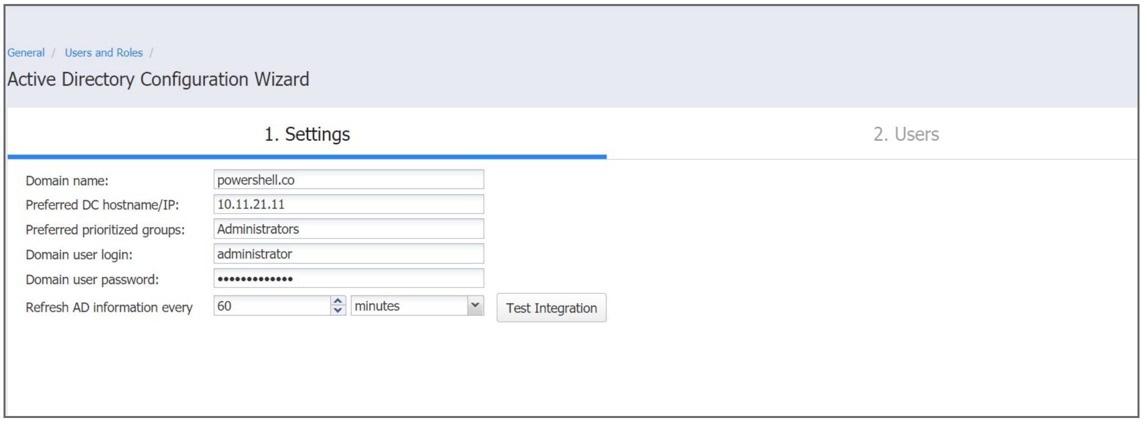
Configuring Active Directory Integration

To configure Active Directory integration, follow these steps:

1. Go to **Settings > General > Users & Roles**.
2. The **Users & Roles** page opens in the **Users** view. Click the **Configure AD Integration** button.
3. The **Active Directory Configuration Wizard** opens on the **Settings** page. Proceed as follows:
    a. In the **Domain name** box, enter the domain name.
    b. In the **Preferred DC hostname/IP** box, enter the name of the preferred domain controller or its IP address.
    c. Optionally, you can enter the name of the preferred Active Directory groups in the **Preferred prioritized groups** box.

       Note

       If a user is a member of two or more Active Directory groups, enter the prioritized group's name in this field.
    d. In the **Domain user login** box, enter the username that will be applied when integrating Active Directory.
    e. In the **Domain user password** box, enter the user password that will be applied when integrating Active Directory.
    f. **Refresh AD information every**: Specify a periodicity of refreshing Active Directory information.
    g. Click the **Test Integration** button to verify the successful integration with Active Directory.


General / Users and Roles /
Active Directory Configuration Wizard
1. Settings
2. Users
Test Integration

Domain name: powershell.co
Preferred DC hostname/IP: 10.11.21.11
Preferred prioritized groups: Administrators
Domain user login: administrator
Domain user password: •••••••••••••
Refresh AD information every 60 minutes

    h. If Active Directory integration is tested successfully, a checkmark appears beside the **Test Integration** button. Then click **Next** to go to the next page of the wizard. If you fail to connect to the AD domain, refer to the Knowledge Base article for possible causes.
    i. On the **Users** page of the wizard, proceed with adding an Active Directory user.

When the wizard closes, the **Users & Roles** page opens, displaying the newly-added Active Directory users in the list of users.

Deleting Active Directory User

Follow the steps below to delete an Active Directory user:

1. Go to **Settings > General > Users & Roles**.
2. The **Users and Roles** page opens in the **Users** view. Hover over the Active Directory user you want to delete, and then click **Manage** in the rightmost cell of the row.
3. In the menu that opens, click **Delete**.
4. In the dialog box that opens, click **Delete** to confirm that you wish to delete the AD user.

The Active Directory user disappears from the list of users.

Disabling Active Directory User

Follow the steps below to disable an Active Directory user:

1. Go to **Settings > General > Users & Roles**.
2. The **Users and Roles** page opens in the **Users** view. Hover over the Active Directory user you want to disable, and then click **Manage** in the rightmost column of the row.
3. In the menu that opens, click **Disable**.
4. In the dialog box that opens, click **Disable** to confirm that you want to disable the Active Directory user.

The Active Directory user appears dimmed in the list of users.

Editing Active Directory User

Follow the steps below to edit an Active Directory user:

1. Go to **Settings > General > Users & Roles**.
2. The **Users and Roles** page opens in the **Users** view. In the list of users, do either of the following:
    a. Locate the Active Directory user and click its name.
    b. Hover over the Active Directory user, click **Manage** in the rightmost column of the row.
    c. Click **Edit**.
3. The **Edit Active Directory User** page opens. Edit the Active Directory user properties if necessary:
    a. In the **Description** box, edit the user description.
    b. In the **Role** list, edit the user role.
    c. To unhide permissions granted to the user based on the role assigned, click the **Show** button beside the **Permissions** label. To hide the user permissions again, click **Hide**.
    d. Click **Save** to save your modifications to the Active Directory user.

Managing Local Users

With NAKIVO Backup & Replication, you can freely add, edit, disable, delete local users, or assign a role to them. For details, refer to the topics below:

- "Adding Local Users" on page 220
- "Assigning Role to Local User" on page 222
- "Deleting Local User" on page 223
- "Disabling Local User" on page 224
- "Editing Local User" on page 225

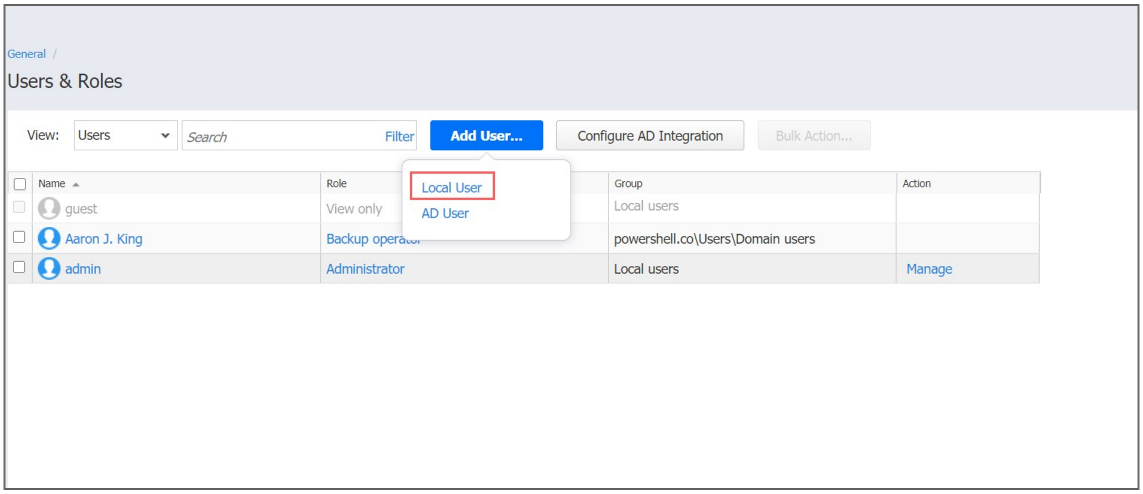
The application has the following built-in local users:

- **admin**: This user has the **Administrator** role assigned. You cannot delete it, disable it, or assign another role.
- **guest**: This user has the **View only** role assigned, with configurable file and object recovery permissions. By default, the account is disabled.

Adding Local Users

Follow the steps below to add a local user:

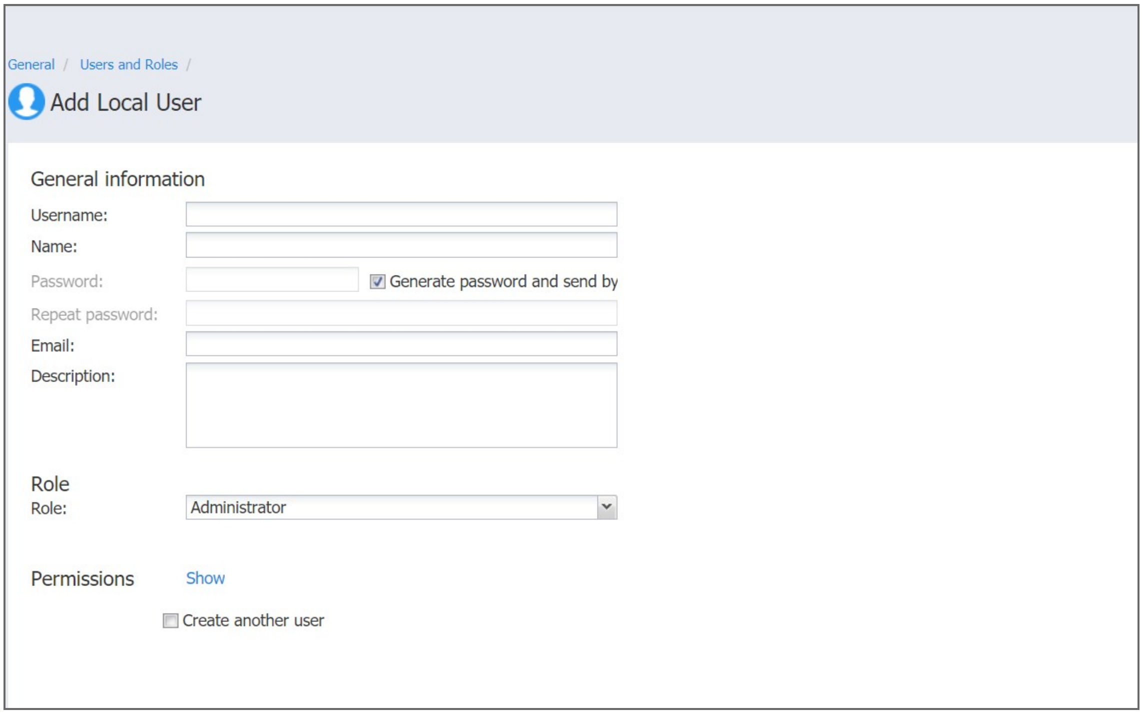
1. Go to **Settings > General > Users and Roles**
2. The **Users and Roles** page opens in the **Users** view. Click **Add User**.
3. In the menu that opens, click **Local User**.



□	Name	Role	Group	Action
□	guest	View only	Local users	
□	Aaron J. King	Backup opera	powershell.co\Users\Domain users	
□	admin	Administrator	Local users	Manage

4. The **Add Local User** page opens. Proceed as follows:
   a. In the **Username** box, enter the user name.
   b. In the **Name** box, enter the user's real name.
   c. In the **Password** box, enter the user password. To generate a password automatically and send it to the user, select **Generate password and send by**.
   d. In the **Repeat password** box, re-enter the user password.
   e. In the **Email** box, enter the user's email address.
   f. In the **Description** box, optionally enter a user description.
   g. In the **Access level** dropdown list, select an access level for the new user (for multi-tenant solutions only).
   h. In the **Role** dropdown list, select a user role. Refer to "Managing User Roles" on page 227 for more details about user roles.
   i. To unhide permissions granted to the user based on the role assigned, click the **Show** button beside the **Permissions** label. To hide the user permissions again, click **Hide**.
   j. To proceed with creating another user after creating the current one, select **Create another user**.

k. In the lower right corner of the page, click **Add**.



General / Users and Roles /

Add Local User

General information

Username:

Name:

Password: ☑ Generate password and send by

Repeat password:

Email:

Description:

Role

Role: Administrator

Permissions Show

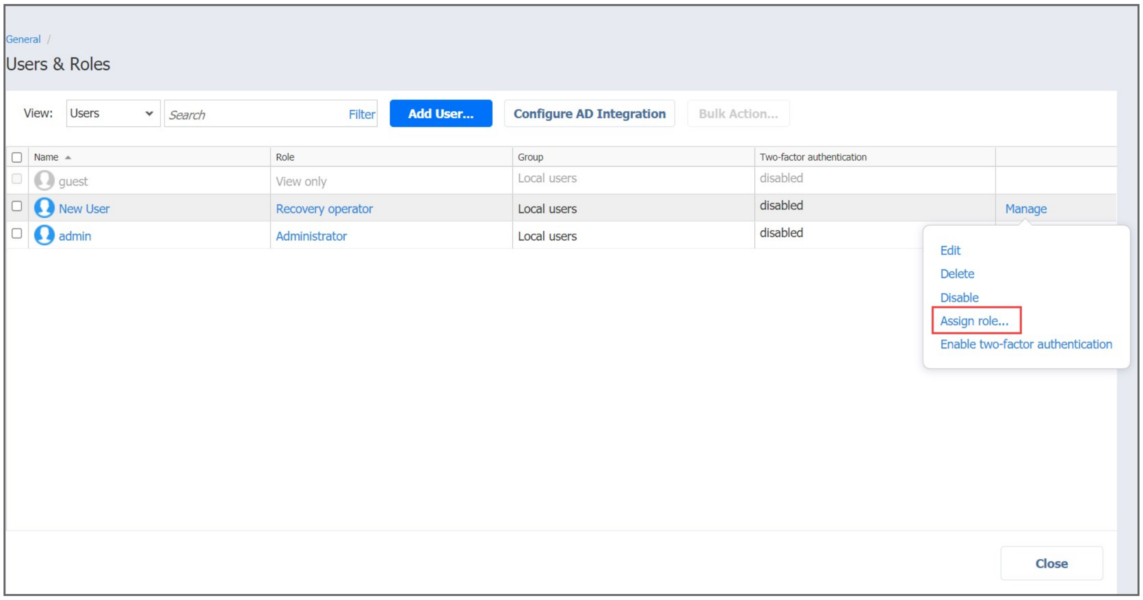
□ Create another user

The local user appears in the list of users.

Assigning Role to Local User

Follow the steps below to assign a role to a local user:

1. Go to **Settings > General > Users & Roles**.
2. The **Users and Roles** page opens in the **Users** view. Hover over the local user, and then click **Manage** in the rightmost column of the row.
3. In the menu that opens, click **Assign role**.
4. In the dialog box that opens, select a new user role from the **Role** drop-down list and then click **Save**.



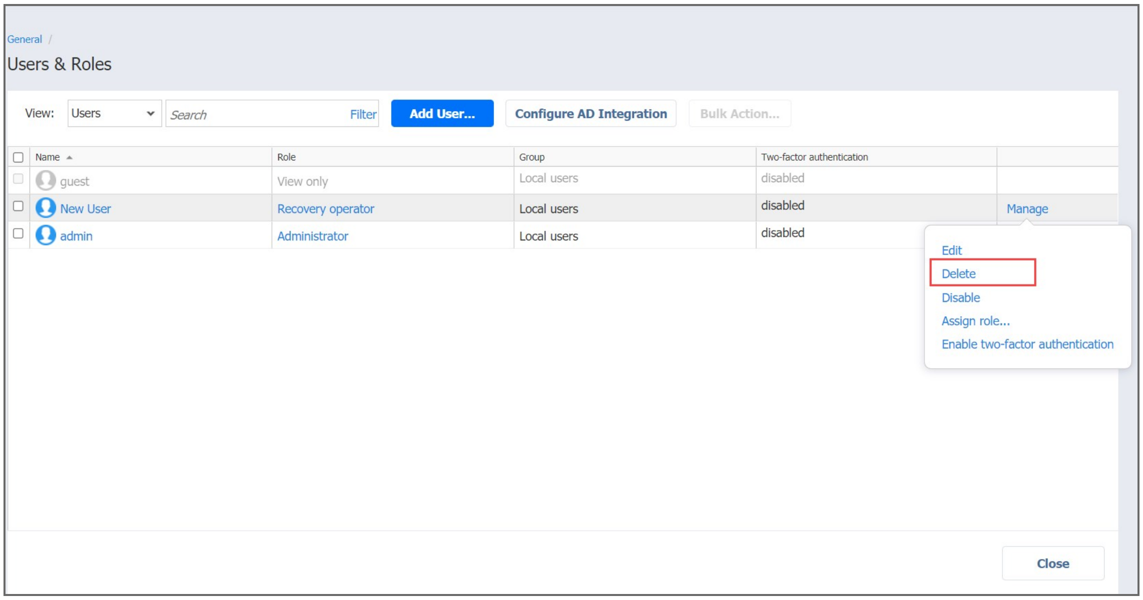
☐	Name	Role	Group	Two-factor authentication	
☐	guest	View only	Local users	disabled	
☐	New User	Recovery operator	Local users	disabled	Manage
☐	admin	Administrator	Local users	disabled	

The local user appears in the list of users with the assigned role.

Deleting Local User

Follow the steps below to delete a local user:

1. Go to **Settings > General > Users & Roles**.
2. The **Users and Roles** page opens in the **Users** view. Hover over the local user you wish to be deleted, and then click **Manage** in the rightmost cell of the row.
3. In the menu that opens, click **Delete**.
4. In the dialog box that opens, click **Delete** to delete the local user.



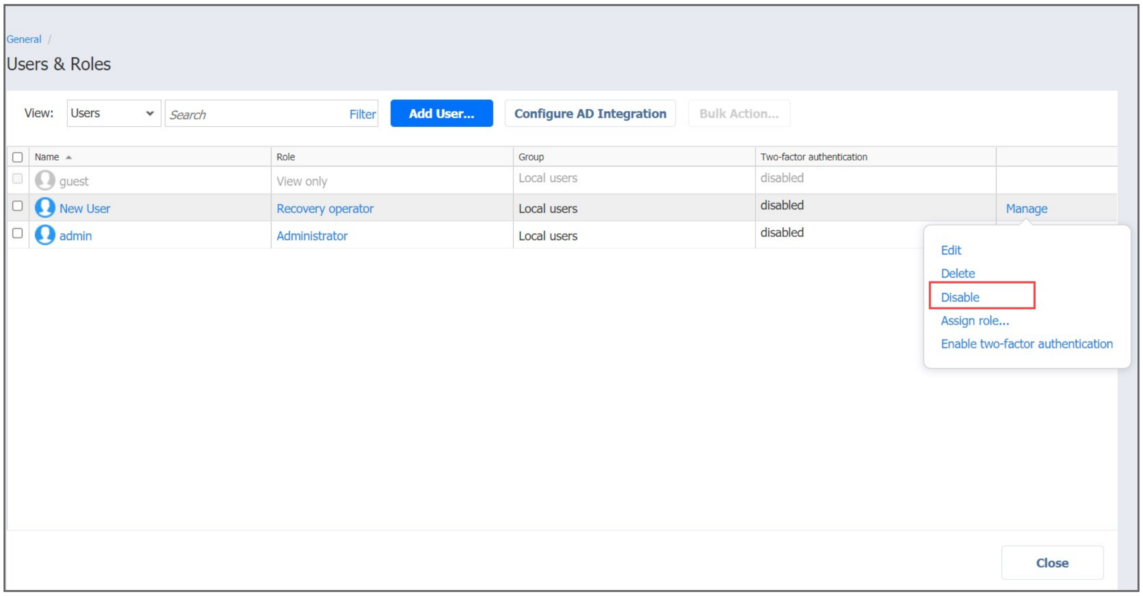
☐	Name	Role	Group	Two-factor authentication	
☐	guest	View only	Local users	disabled	
☐	New User	Recovery operator	Local users	disabled	Manage
☐	admin	Administrator	Local users	disabled	

The deleted user disappears from the list of users.

Disabling Local User

Follow the steps below to disable a local user:

1. Go to **Settings > General > Users & Roles**.
2. The **Users and Roles** page opens in the **Users** view. Hover over the local user you wish to be disabled, and then click **Manage** in the rightmost column of the row.
3. In the menu that opens, click **Disable**.
4. In the dialog box that opens, click **Disable** to disable the local user.



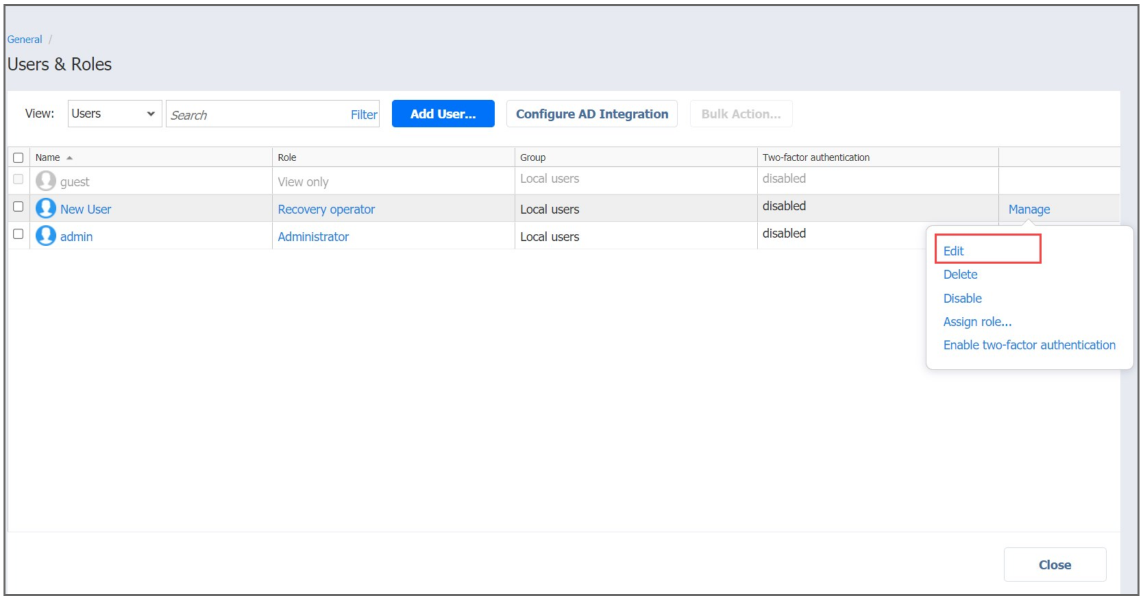
□	Name	Role	Group	Two-factor authentication	
□	guest	View only	Local users	disabled	
□	New User	Recovery operator	Local users	disabled	Manage
□	admin	Administrator	Local users	disabled	

The disabled user appears dimmed in the list of local users.

Editing Local User

Please follow the steps below to edit a local user:

1. Go to **Settings > General > Users & Roles**.
2. The **Users and Roles** page opens in the **Users** view. In the list of users, do either of the following:
   a. Locate the local user that you want to edit.
   b. Hover over the local user, click **Manage** in the rightmost column of the row and then click **Edit**.



□	Name	Role	Group	Two-factor authentication	
□	guest	View only	Local users	disabled	
□	New User	Recovery operator	Local users	disabled	Manage
□	admin	Administrator	Local users	disabled	

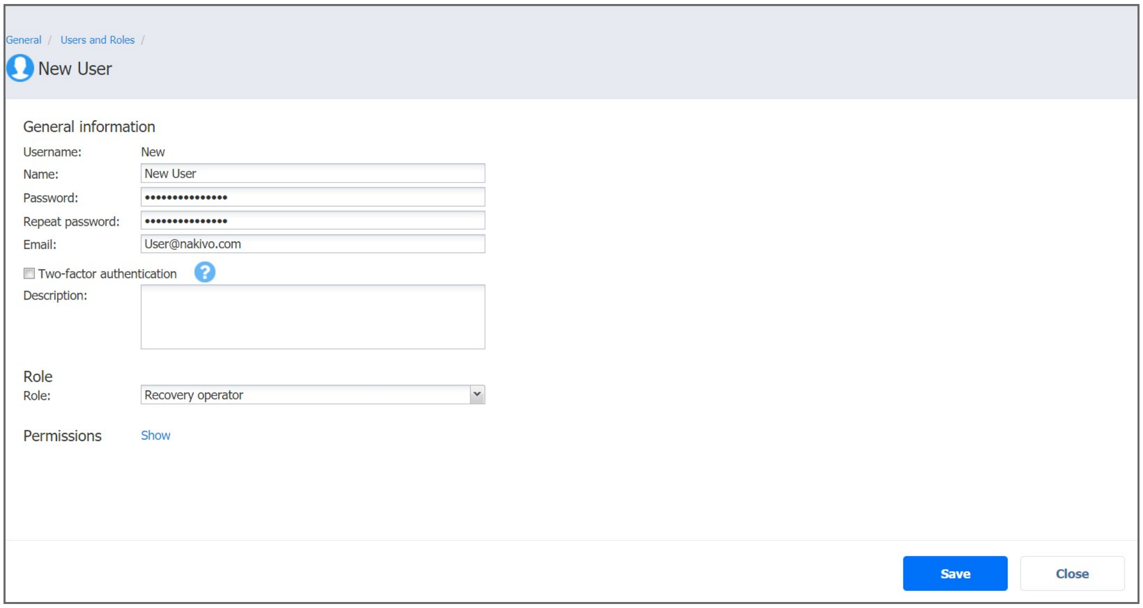
3. The **Edit User** page opens. Edit the local user properties if needed:
   a. In the **Name** box, edit the user name.
   b. In the **Password** box, edit the user password.
   c. If you edited the user password, re-enter the user password in the **Repeat password** box.
   d. In the **Email** box, edit the user's email address.
   e. Optionally, enable **Two-factor authentication**.

   Note

   This feature is disabled when no email address has been provided for the user.

   f. In the **Description** box, edit the user description.
   g. In the **Role** list, edit the user role.
   h. To unhide permissions granted to the user based on the role assigned, click the **Show** button beside the **Permissions** label. To hide the user permissions again, click **Hide**.

i. Click **Save** to save your modifications to the local user.



General information

Username:	New
Name:	New User
Password:	•••••••••••••••
Repeat password:	•••••••••••••••
Email:	User@nakivo.com

□ Two-factor authentication

Description:

Role

Role: Recovery operator

Permissions

Managing User Roles

A user role with full access to the **User management** permission is assigned to your user profile to manage user roles. You cannot edit or delete the user role that is assigned to your user profile. The following topics describe how to manage roles of NAKIVO Backup &Replication users in detail:

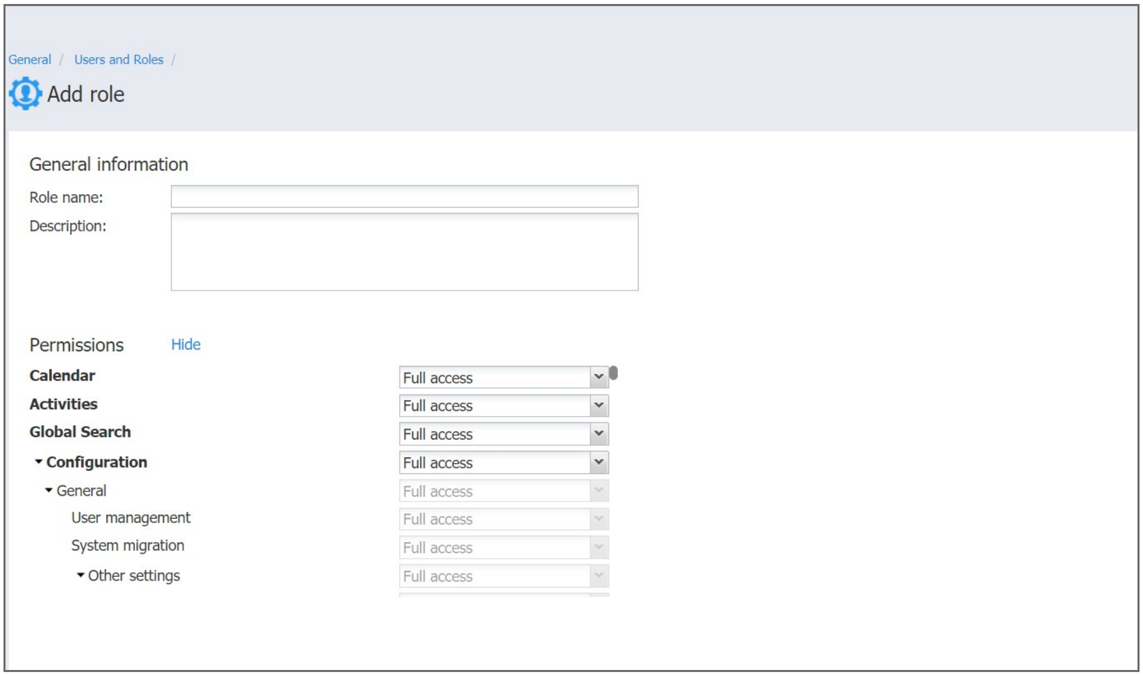
- "Overview of User Roles" on page 233
- "Adding User Role" on page 228
- "Editing User Role" on page 231
- "Cloning User Role" on page 229
- "Deleting User Role" on page 230

Adding User Role

Follow the steps below to add a user role:

1. Go to **Settings > General > Users & Roles**.
2. On the **Users & Roles** page, switch to the **Roles** view.
3. Click **Add Role**.
4. The **Add Role** page opens. Proceed as follows:
    a. In the **Role name** box, enter the role name.
    b. If you are working with a multi-tenant environment, choose either a tenant, master tenant, or all tenants, from the **Access level** list.
    c. In the **Description** box, optionally enter a user description.
    d. To unhide permissions to be granted to the role, click the **Show** button beside the **Permissions** label.
    e. A list of permissions opens. Specify necessary permissions for the user role.
    f. Click **Add** in the lower right corner of the page.

The user role appears in the list of roles.



General information

Role name:

Description:

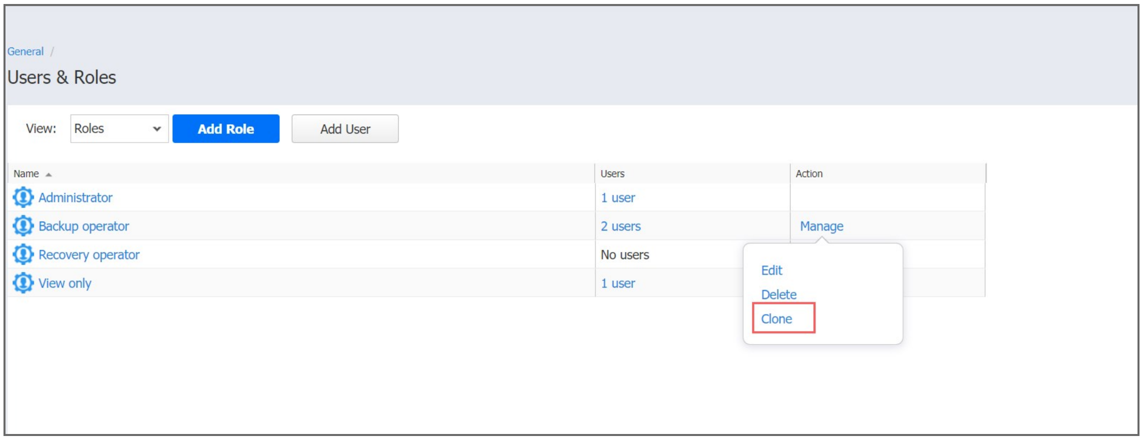
Permissions

Calendar	Full access
Activities	Full access
Global Search	Full access
▾ **Configuration**	Full access
▾ General	Full access
User management	Full access
System migration	Full access
▾ Other settings	Full access

Cloning User Role

Follow the steps below to clone a user role:

1. Go to **Settings > General > Users & Roles**.
2. On the **Users & Roles** page, switch to the **Roles** view.
3. Hover over the user role, click **Manage** in the rightmost column of the row and then click **Clone**.
4. A dialog opens asking you to enter the name of the new user role. Enter the name of the new user role and click **Save**.



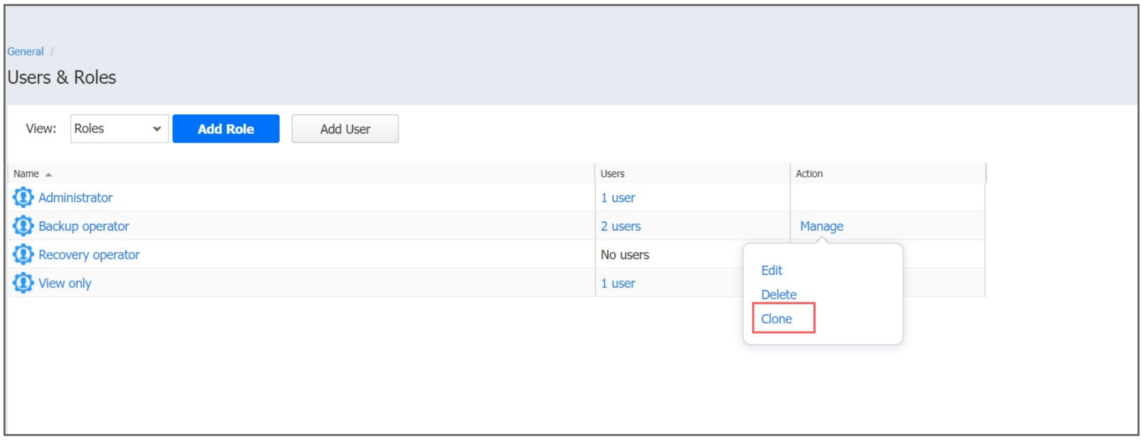
Name	Users	Action
Administrator	1 user	
Backup operator	2 users	Manage
Recovery operator	No users	
View only	1 user	

The new user role appears in the list of roles.

Deleting User Role

Follow the steps below to delete a user role:

1. Go to **Settings > General > Users & Roles**.
2. On the **Users & Roles** page, switch to the **Roles** view.
3. Hover over the user role, click **Manage** in the rightmost column of the row and then click **Delete.**
4. In the dialog box that opens, click **Delete** to confirm deleting the local user.



General /

Users & Roles

View: Roles

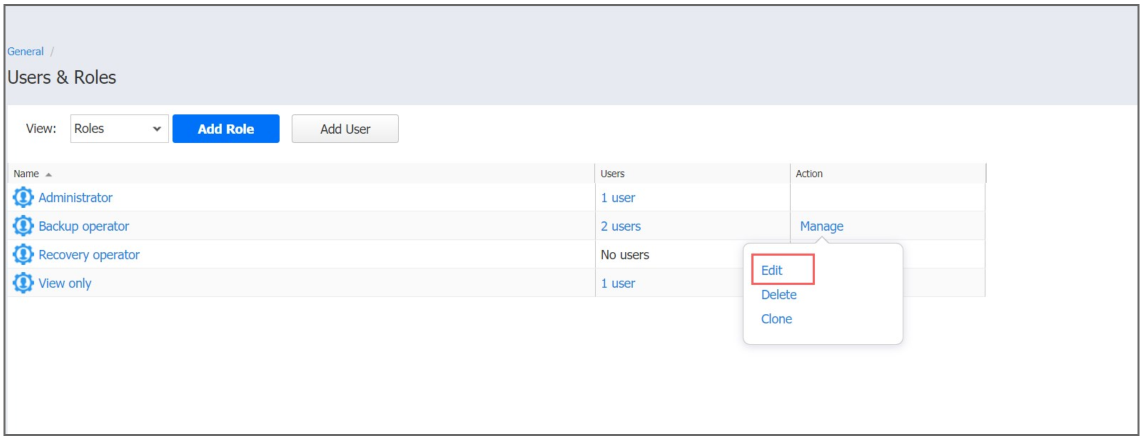
Name	Users	Action
Administrator	1 user	
Backup operator	2 users	Manage
Recovery operator	No users	
View only	1 user	

The user role disappears from the list of roles.

Editing User Role

Follow the steps below to edit a user role:

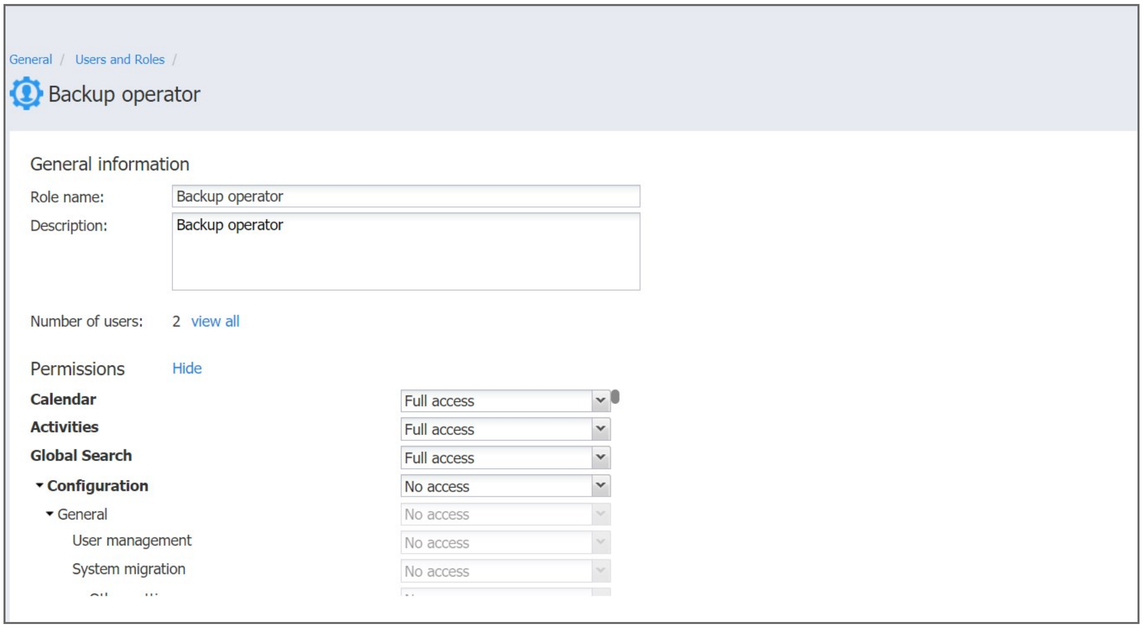
1. Go to **Settings > General > Users & Roles**.
2. On the **Users & Roles** page, switch to the **Roles** view.
3. In the list of roles, do either of the following:
    a. Locate the user role and click on it.
    b. Hover over the user role, click **Manage** in the rightmost column of the row.
    c. Click **Edit**.



Name	Users	Action
Administrator	1 user	
Backup operator	2 users	Manage
Recovery operator	No users	
View only	1 user	

4. The **Edit User Role** page opens. Edit the user role properties if needed:
    a. In the **Role name** box, edit the user role name.
    b. If you are working with a multi-tenant environment, you can change the access level for this role by choosing another tenant, master tenant, or all tenants in the **Access level** list.
    c. In the **Description** box, edit the user description.
    d. You can view the **Number of users** assigned with this role and click **view all**to see their full list on a new page.
    e. To unhide permissions to be granted to the role, click the **Show** button beside the **Permissions** label.
    f. A list of permissions opens. Edit necessary permissions for the user role.

g. When ready to save the user role, click **Save** in the lower right corner of the page.



Backup operator

General information

Role name: Backup operator

Description: Backup operator

Number of users: 2 view all

Permissions

Calendar	Full access
Activities	Full access
Global Search	Full access
▾ **Configuration**	No access
▾ General	No access
User management	No access
System migration	No access

Overview of User Roles

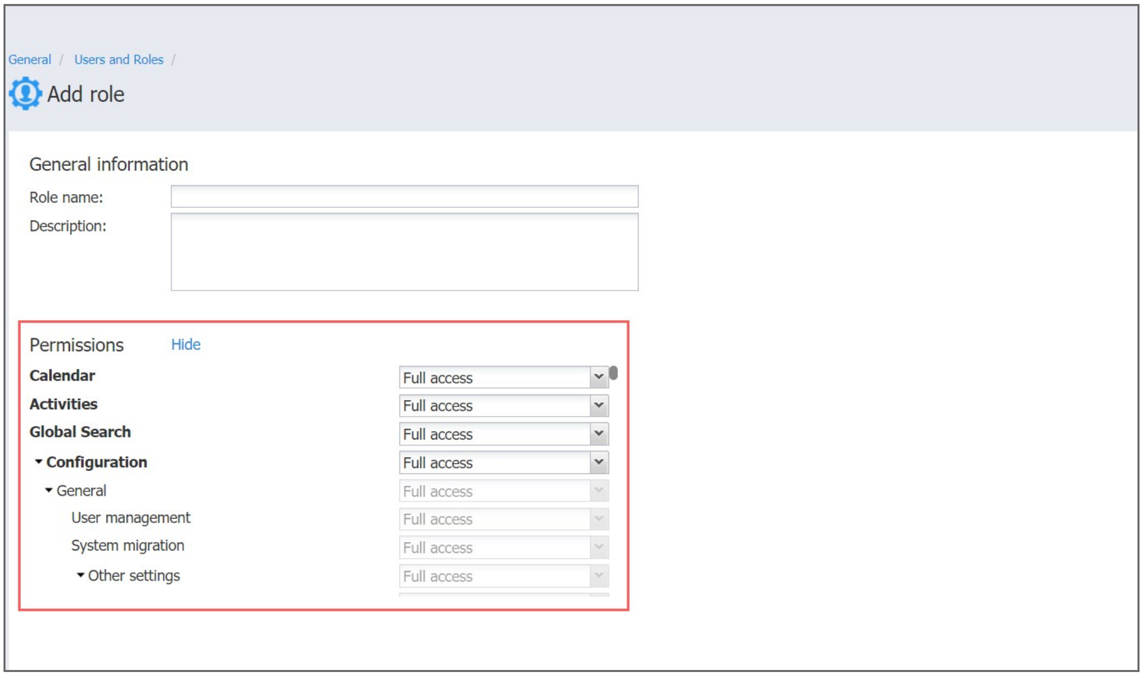
NAKIVO Backup & Replication allows you to assign roles and grant specific permissions to users of the product.

- User Roles
- Access Levels
- Built-in User Roles

User Roles

A user role consists of a set of permissions that can be granted to a NAKIVO Backup & Replication user. Available permissions are grouped by the following product objects:

- **Calendar**: Contains permissions for accessing the Calendar dashboard.
- **Activities**: Contains permissions for accessing the Activities dashboard.
- **Global Search**: Contains permissions for accessing Global Search.
- **Configuration**: Contains a series of permissions for accessing configuration of NAKIVO Backup & Replication.
- **Jobs**: Contains a series of permissions for managing jobs.
- **User profile**: Contains a series of permissions for managing user profile.
- **Help and Support**: Contains a series of permissions for accessing email support, online help center, chat support, and system information.
- **Aptare Report Generation**: Contains permissions for managing Aptare report generation.



General information

Role name:

Description:

Permissions Hide

Calendar	Full access
Activities	Full access
Global Search	Full access
Configuration	Full access
General	Full access
User management	Full access
System migration	Full access
Other settings	Full access

Access Levels

There are the following access levels that can be set up for particular permission:

- **No access**: The user cannot view, edit, and run the commands, neither from the graphical interface nor from the command line.
- **View only**: The user can view the commands in the graphical interface but cannot edit or run them; using the command line, the user can only run the commands that do not change NAKIVO Backup & Replication objects.
- **Run only**: The user can only view and run commands, both from the graphical interface and the command line.
- **Full access**: The user can view, edit, and run the commands, both from the graphical interface and the command line.
- **Custom**: A custom set of permissions is configured for a product object.

Built-In User Roles

The product offers you a number of built-in user roles:

- Backup operator
- Recovery operator
- Self-service administrator
- Self-service user
- View only

Built-in user roles can be used for performing typical user management tasks. If you need an extra level of security, you can add a new user role or take a built-in user role as a starting point by cloning it.

The user profile can only have a single role assigned.

Inventory

Prior to creating backup, replication, or recovery jobs, you need to add your virtual/cloud infrastructure to the product’s Inventory. The discovered infrastructure is added to the internal product database, which is refreshed every 1 hour by default. Refer to the following sections to learn more:

- “Adding Microsoft 365 Accounts” on page 236
- “Managing Credentials” on page 247
- “Managing Inventory” on page 242

Adding Microsoft 365 Accounts

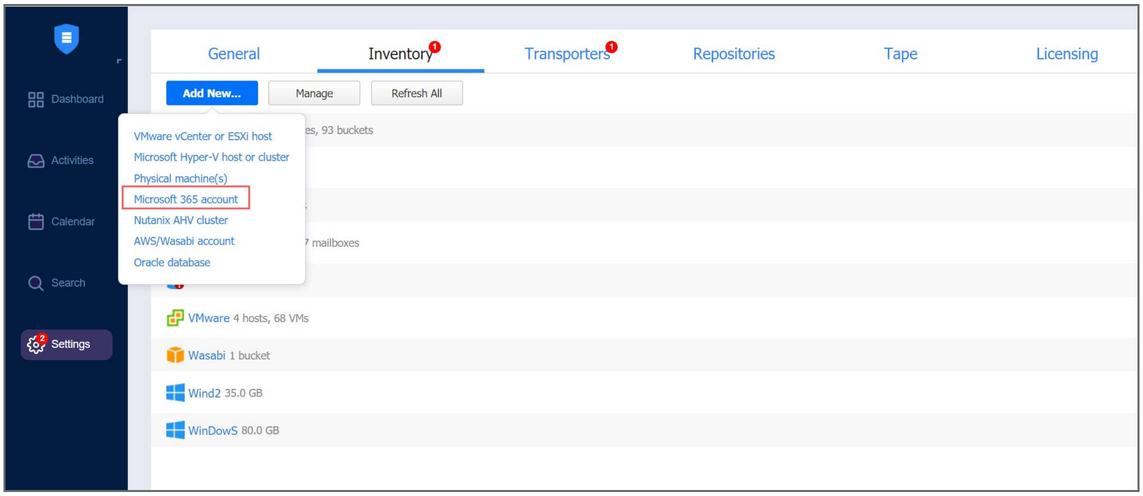
Before you start backing up items from your Microsoft 365 account, you need to add the Microsoft 365 account to the NAKIVO Backup & Replication inventory.

- Adding Microsoft 365 Account to Inventory
- Obtaining Microsoft 365 Credentials

Adding Microsoft 365 Account to Inventory

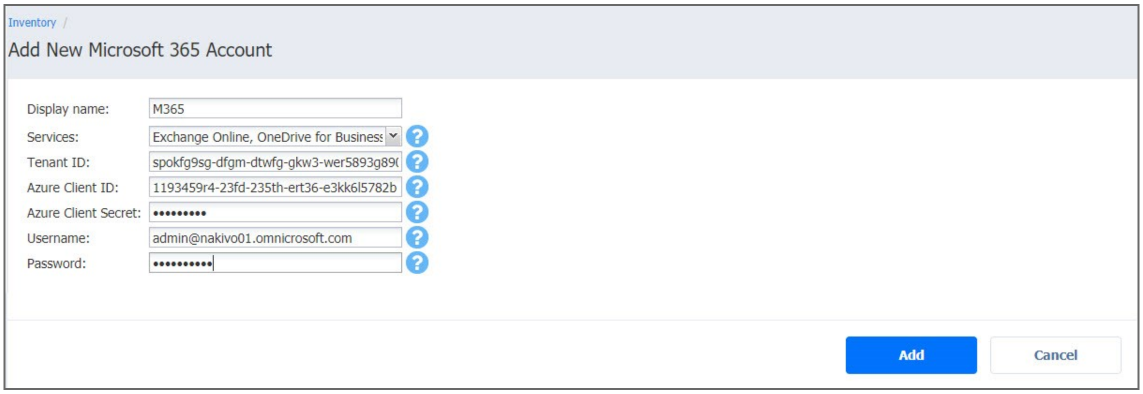
To add a Microsoft 365 account to the inventory, do the following:

1. Check if you meet Microsoft 365 requirements.
2. Click **Settings** in the left pane of the product.
3. Go to the **Inventory** tab and click **Add New**.
4. In the dialog that opens, click **Microsoft 365 account**.



5. The **Add New Microsoft 365 Account** page opens. Provide the following information:
   - **Display name:** Enter the preferred name for the account.
   - **Services**: Select one or several Microsoft 365 services that you want to back up:
     - **Exchange Online**
     - **OneDrive for Business**
     - **SharePoint**
   - **Tenant ID**: Enter your Azure Tenant ID created when registering your Microsoft 365 account in the Azure Portal.
   - **Azure Client ID**: Enter your Azure Client ID created when registering your Microsoft 365 account in the Azure Portal.
   - **Azure Client Secret**: Enter your Azure Client Secret obtained from the Azure Portal. For more information on obtaining the Azure credentials, refer to the Obtaining Microsoft 365 Credentials section.

- **Username**: Provide the administrator username required for SharePoint Online support. If left empty, SharePoint Online data will not be discovered.
- **Password**: Provide the password required for SharePoint Online support. If left empty, SharePoint Online data will not be discovered.



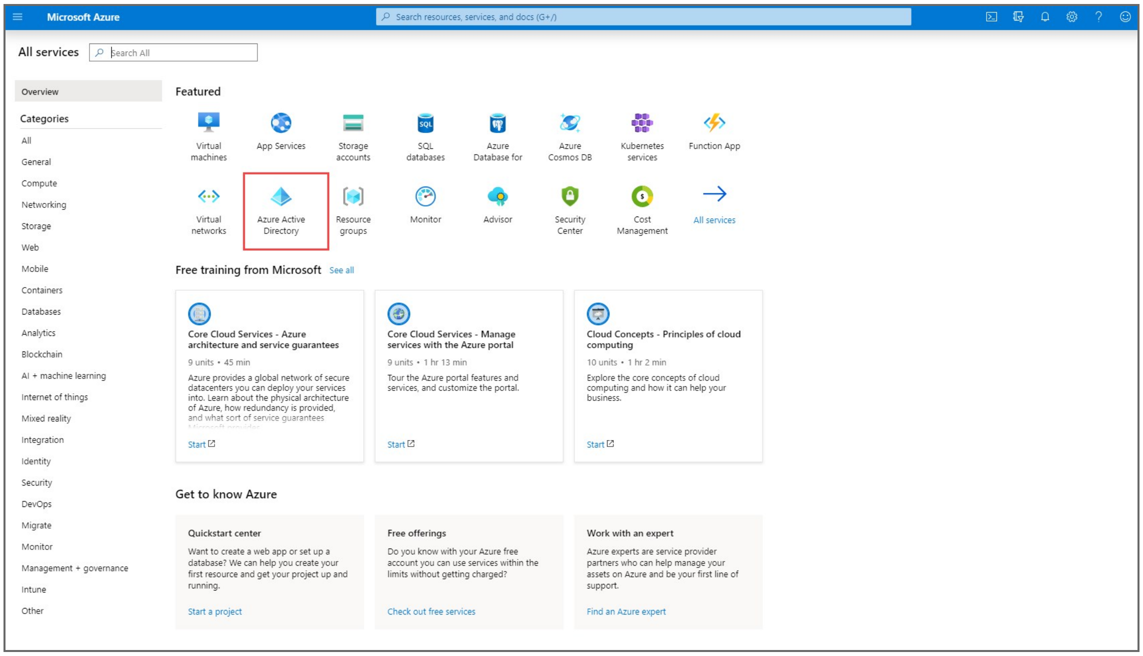
Display name: M365
Services: Exchange Online, OneDrive for Business
Tenant ID: spokfg9sg-dfgm-dtwfg-gkw3-wer5893g89(
Azure Client ID: 1193459r4-23fd-235th-ert36-e3kk6l5782b
Azure Client Secret: •••••••••
Username: admin@nakivo01.omnicrosoft.com
Password: ••••••••••

6. Click **Add**. The Microsoft 365 account has been added to the inventory.

Obtaining Microsoft 365 Credentials

To obtain the credentials required to add a Microsoft 365 account to the NAKIVO Backup & Replication inventory, follow the steps below:

1. Open the Azure Portal by going to portal.azure.com
2. Sign in to Microsoft Azure with your Microsoft 365 account credentials.
3. Select **Azure Active Directory** from the Dashboard or from the Portal Menu.



Core Cloud Services - Azure architecture and service guarantees
9 units • 45 min
Azure provides a global network of secure datacenters you can deploy your services into. Learn about the physical architecture of Azure, how redundancy is provided, and what sort of service guarantees Microsoft provides
Start

Core Cloud Services - Manage services with the Azure portal
9 units • 1 hr 13 min
Tour the Azure portal features and services, and customize the portal.
Start

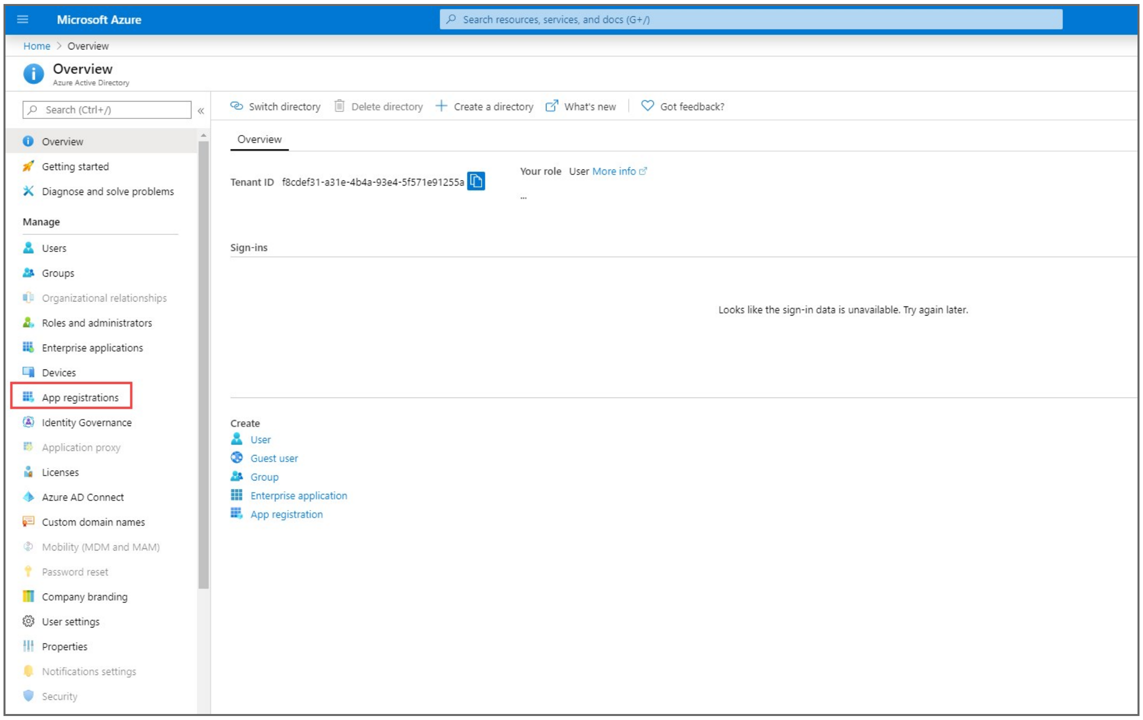
Cloud Concepts - Principles of cloud computing
10 units • 1 hr 2 min
Explore the core concepts of cloud computing and how it can help your business.
Start

Quickstart center
Want to create a web app or set up a database? We can help you create your first resource and get your project up and running.
Start a project

Free offerings
Do you know with your Azure free account you can use services within the limits without getting charged?
Check out free services

Work with an expert
Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support.
Find an Azure expert

4. In the left menu, click **App registrations**.

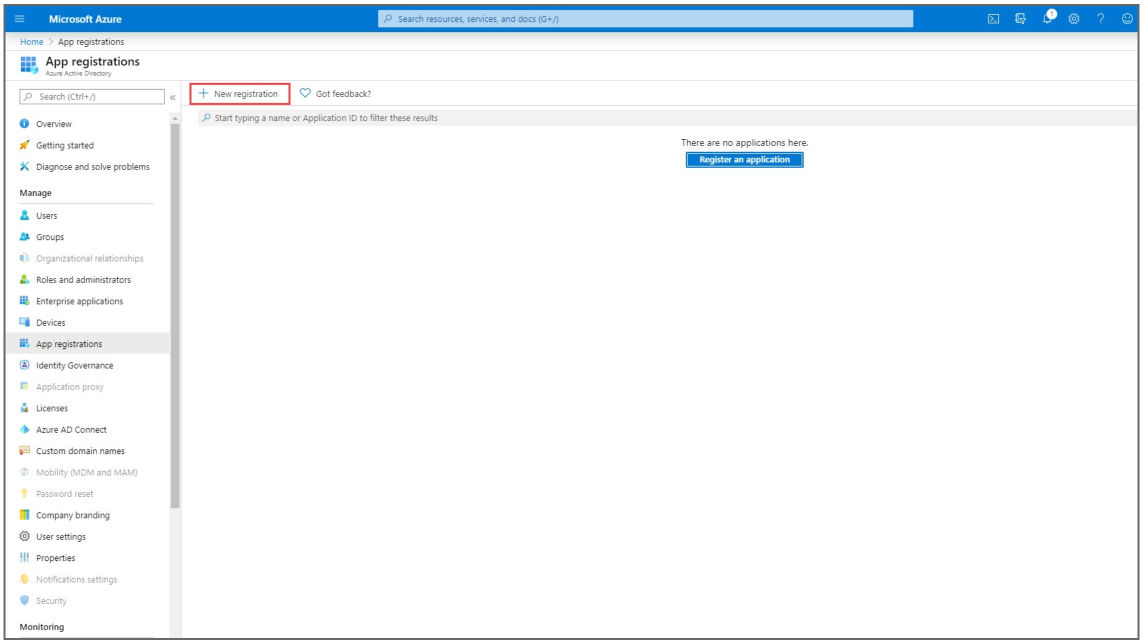


Tenant ID f8cdef31-a31e-4b4a-93e4-5f571e91255a

Your role User More info

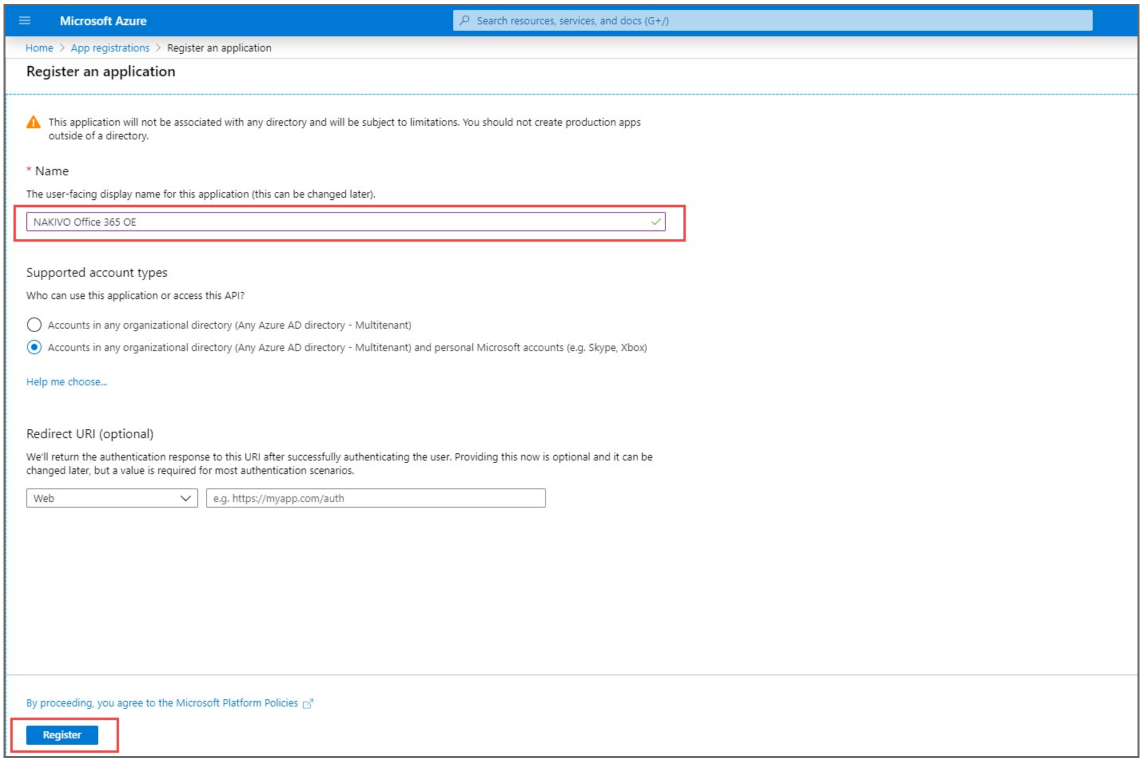
Looks like the sign-in data is unavailable. Try again later.

5. Click **New registration** on the **App registrations** page.



There are no applications here.

6. On the **Register an application** page, enter a name for the application and click **Register**.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > App registrations > Register an application

Register an application

This application will not be associated with any directory and will be subject to limitations. You should not create production apps outside of a directory.

* Name

The user-facing display name for this application (this can be changed later).

NAKIVO Office 365 OE

Supported account types

Who can use this application or access this API?

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

● Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

Help me choose...

Redirect URI (optional)

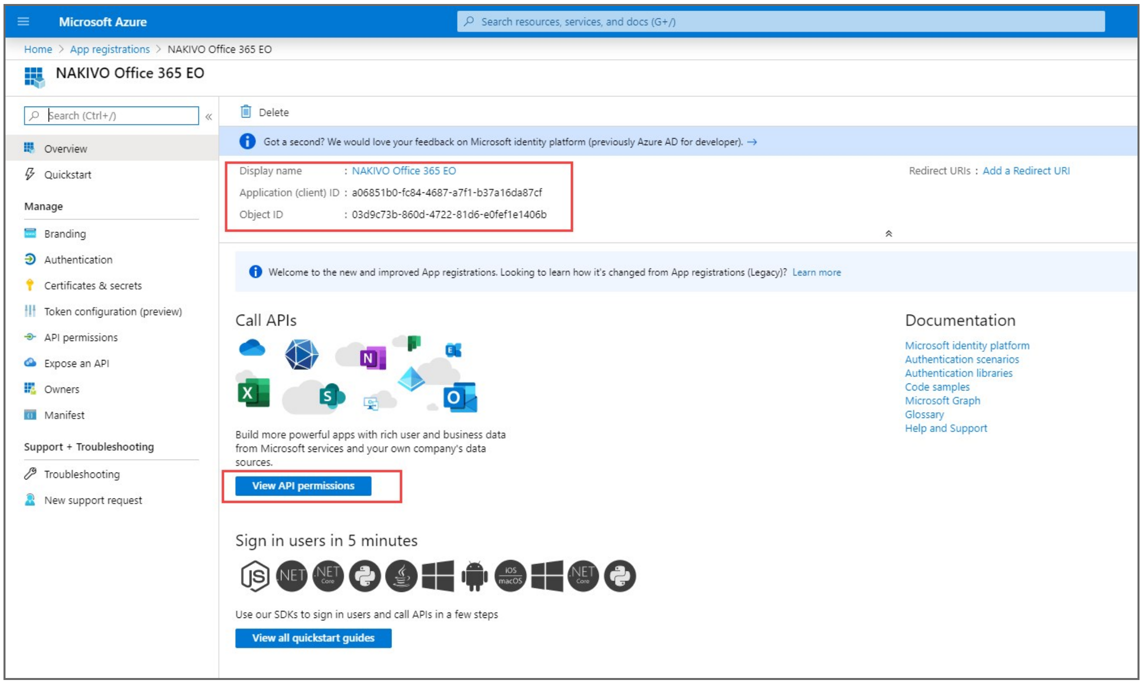
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web | e.g. https://myapp.com/auth

By proceeding, you agree to the Microsoft Platform Policies

The application has been successfully registered and **Tenant ID** and **Azure Client ID** are displayed (**Directory (tenant) ID** and **Application (client) ID** respectively).

7. Click **View API Permissions** to add the necessary permissions.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > App registrations > NAKIVO Office 365 EO

NAKIVO Office 365 EO

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Display name : NAKIVO Office 365 EO

Application (client) ID : a06851b0-fc84-4687-a7f1-b37a16da87cf

Object ID : 03d9c73b-860d-4722-81d6-e0fef1e1406b

Redirect URIs : Add a Redirect URI

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more

Call APIs

Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

Sign in users in 5 minutes

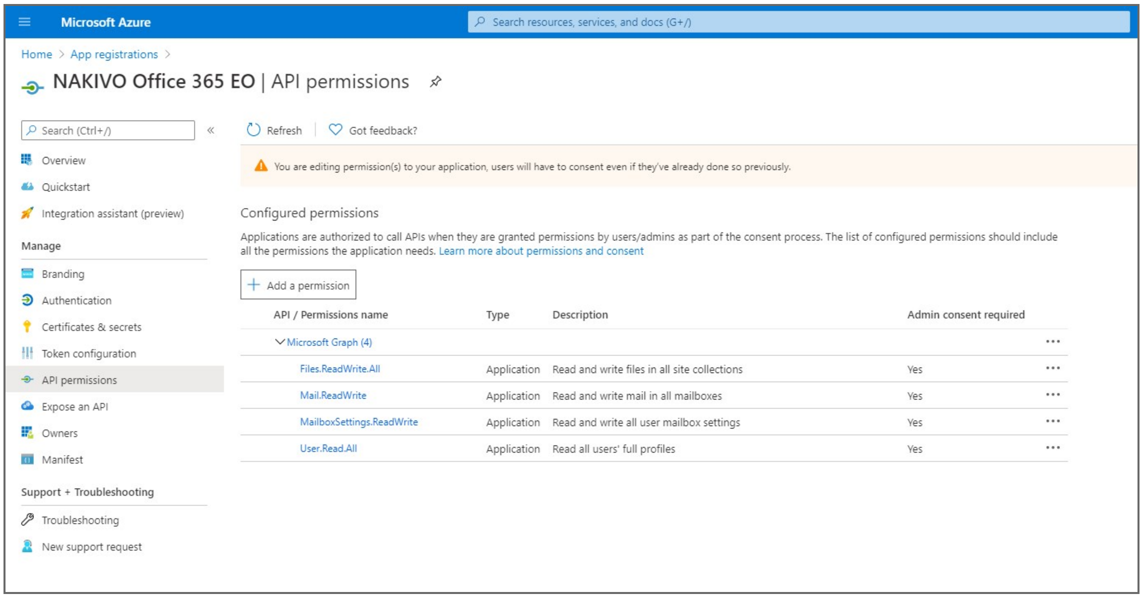
Use our SDKs to sign in users and call APIs in a few steps

8. Click **Microsoft Graph**.
9. Click on the **Application permissions** tab.
10. Provide the necessary API Permissions. Refer to Required API Permissions from Microsoft 365 for details.

Notes

- To skip discovering Exchange Online mailboxes, OneDrives or SharePoint sites in the inventory, disable the API permissions for the corresponding service.
- If the necessary Microsoft Exchange Online/OneDrive/Shaepoint API permissions are not provided, the corresponding service will not be discovered by NAKIVO Backup & Replication.
- If the necessary API permissions for Microsoft Exchange Online contact and calendar items are not provided, the items will not be supported for backup and recovery operations.
- o recover messages and contacts containing a lot of content, you also need to enable full_ access_as_app for Office 365 Exchange Online in **APIs my organization uses**.

11. Click **Update Permissions**.



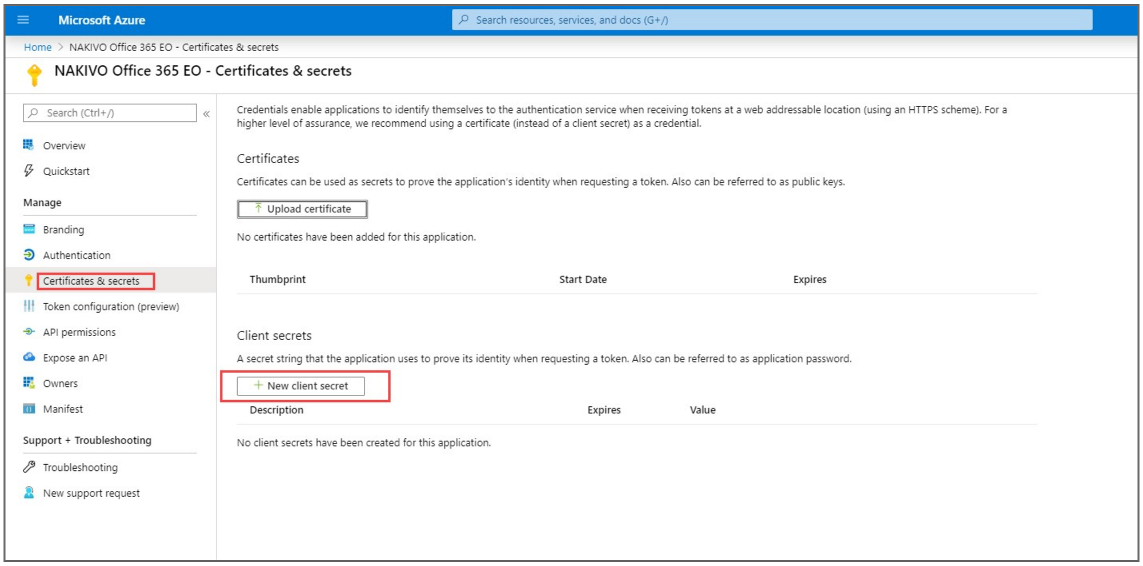
You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent required
Microsoft Graph (4)			
Files.ReadWrite.All	Application	Read and write files in all site collections	Yes
Mail.ReadWrite	Application	Read and write mail in all mailboxes	Yes
MailboxSettings.ReadWrite	Application	Read and write all user mailbox settings	Yes
User.Read.All	Application	Read all users' full profiles	Yes

12. Click **Certificates & secrets>New client secret** to create a new client secret for your app.



Credentials enable applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

No certificates have been added for this application.

Thumbprint	Start Date	Expires

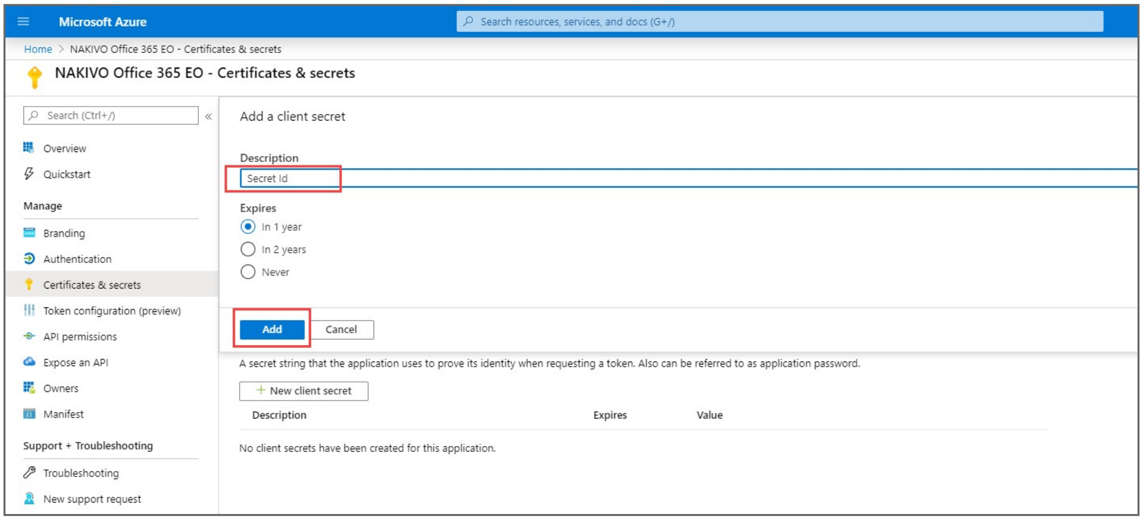
Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value

No client secrets have been created for this application.

13. Enter a description for the client secret, select the expiration period, and click **Add**.



NAKIVO Office 365 EO - Certificates & secrets

Add a client secret

Description: Secret Id

Expires

● In 1 year

○ In 2 years

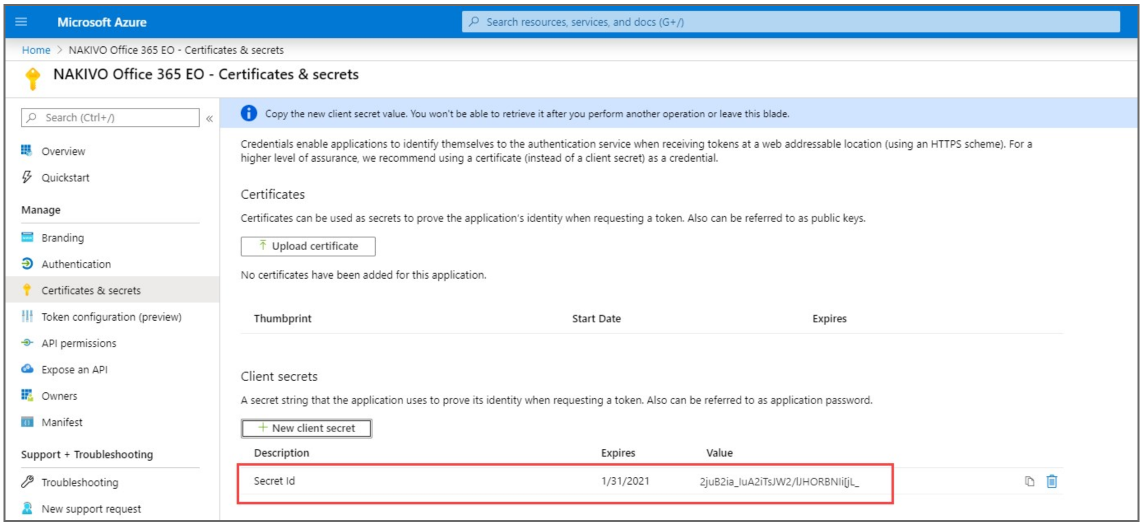
○ Never

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value

No client secrets have been created for this application.

The new **Client secret** is generated.



NAKIVO Office 365 EO - Certificates & secrets

Copy the new client secret value. You won't be able to retrieve it after you perform another operation or leave this blade.

Credentials enable applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

No certificates have been added for this application.

Thumbprint	Start Date	Expires

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value
Secret Id	1/31/2021	2juB2ia_IuA2iTsJW2/lJHORBNIi[jL_

Make sure you jot down the client secret id somewhere safe; If you lose it, you will need to generate a new one.

Managing Inventory

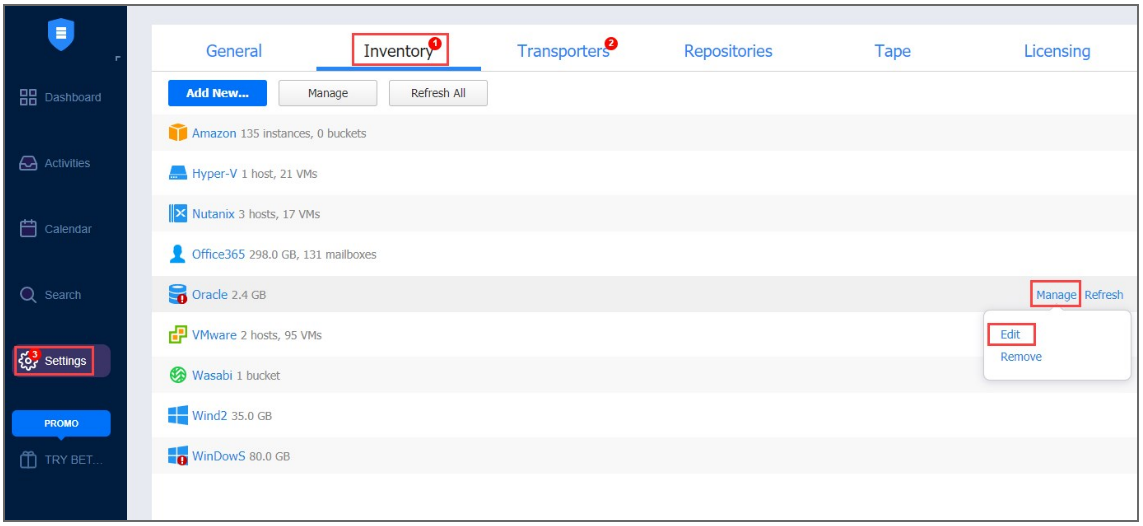
Refer to the following topics:

- “Refreshing Inventory” on page 244
- “Editing Inventory Items” on page 243
- “Removing Items from Inventory” on page 246

Editing Inventory Items

If the credentials of an inventory item are no longer correct, the connection to the inventory item will be lost. To re-establish a connection, update the required fields in the product by following the steps below:

1. Click **Settings** in the left pane of the product.
2. Go to the **Inventory** tab.
3. Click the item you want to edit.
4. In the title of the item, click **Manage** and then click **Edit**.



Amazon 135 instances, 0 buckets
Hyper-V 1 host, 21 VMs
Nutanix 3 hosts, 17 VMs
Office365 298.0 GB, 131 mailboxes
Oracle 2.4 GB
VMware 2 hosts, 95 VMs
Wasabi 1 bucket
Wind2 35.0 GB
WinDowS 80.0 GB

5. Update the appropriate fields and click **Apply**.

Refreshing Inventory

NAKIVO Backup & Replication keeps the information about the discovered infrastructure in its internal database, which is refreshed every 1 hour by default. During the inventory refresh, the product collects all required information about your virtual infrastructure, such as a list of hosts and VMs, their power state, and so on.

Only one item can be refreshed at a time. If you have added multiple items to the inventory, they will remain in the queue until they are able to be refreshed.Refer to the sections below to learn how to refresh the discovered infrastructure.

- Changing Inventory Refresh Frequency
- Manually Refreshing All Inventory
- Manually Refreshing a Discovered Item

Changing Inventory Refresh Frequency

1. Click **Settings** in the left pane of the product.
2. Go to the **Inventory** tab.
3. Do either of the following:
   - To prevent the product from automatically refreshing the inventory, deselect the **Refresh inventory every X [time period]** checkbox.
   - To change the inventory refresh frequency, enter a new value in the **Refresh inventory every X [time period]** field (from 1 to 60 minutes or from 1 to 24 hours).

Note

New setting are applied instantly and do not need to be saved.

Manually Refreshing All Inventory

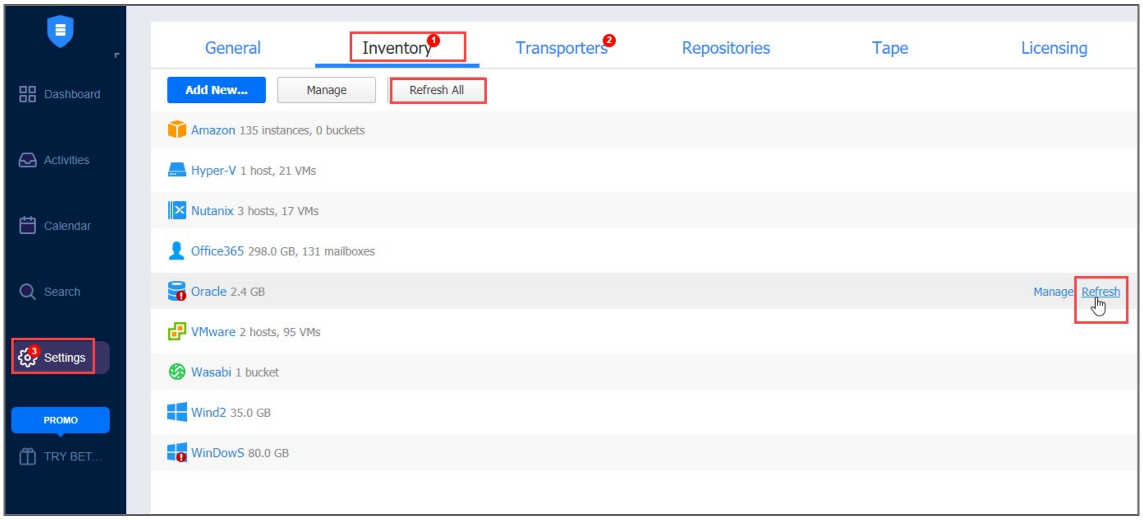
To update all inventory items, follow the steps below:

1. Click **Settings** in the left pane of the product and go to the **Inventory** tab.
2. Click **Refresh All**.

Manually Refreshing a Discovered Item

To update a single discovered item, follow the steps below:

1. Click **Settings** in the left pane of the product and go to the **Inventory** tab.
2. Click the item that you would like to update.
3. In the title of the item, click **Refresh**.



Amazon 135 instances, 0 buckets

Hyper-V 1 host, 21 VMs

Nutanix 3 hosts, 17 VMs

Office365 298.0 GB, 131 mailboxes

Oracle 2.4 GB

VMware 2 hosts, 95 VMs

Wasabi 1 bucket

Wind2 35.0 GB

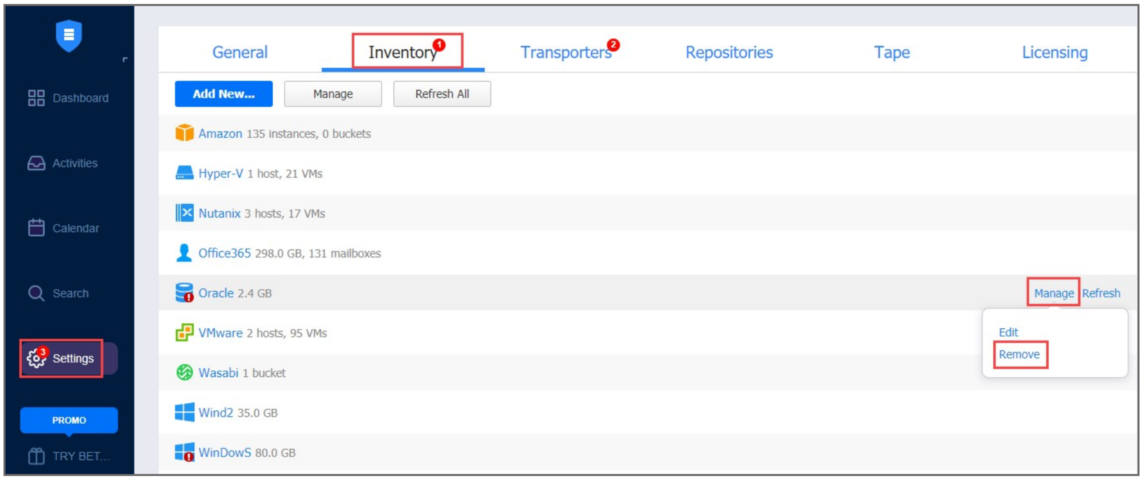
WinDowS 80.0 GB

Removing Items from Inventory

You cannot remove an inventory item if there is at least one backup or replication job that uses the item or its children. In order to remove such items from the inventory, you first need to delete (or edit) the corresponding jobs so no VMs/Instances are backed up or replicated on the host/server/account being removed.

To remove an item from the inventory, follow the steps below:

1. Click **Settings** in the left pane of the product and go to the **Inventory** tab.
2. Click the item that you wish to remove from inventory.
3. In the item title, click **Manage**, and then click **Remove**.
4. In the dialog that opens, click **Remove**.



Managing Credentials

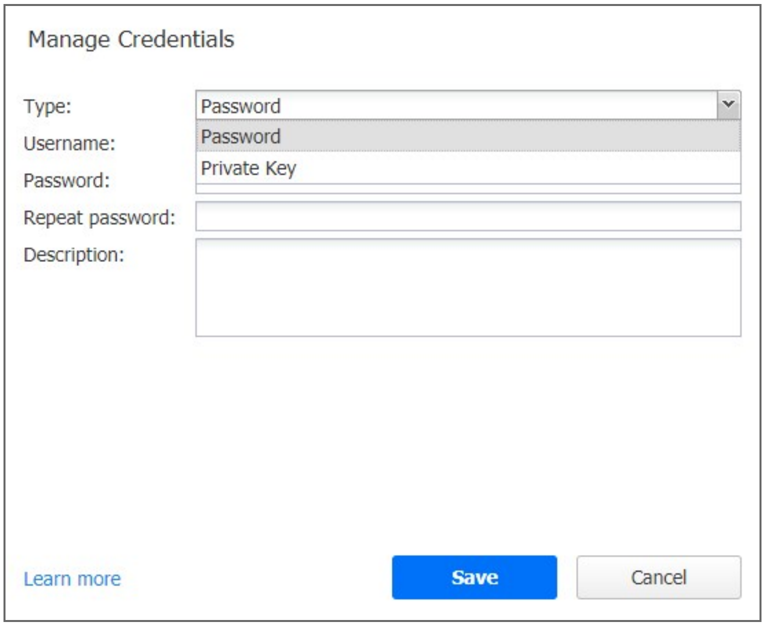
NAKIVO Backup & Replication provides you with the ability to store your OS login and password, Amazon EC2 instance private keys or shh keys to your Linux machines. Refer to the following topics:

- Adding Credentials
- Editing Credentials
- Deleting Credentials

Adding Credentials

To add new credentials, do the following:

1. Click **Settings** in the left pane of the product.
2. Go to the **Inventory** tab.
3. Click **Manage**.
4. In the dialog that opens, click **Manage Credentials**.
5. In the **Manage Credentials** dialog that opens, click **Add Credentials**.



Type: Password

6. Then do the following:
   - **Type**: Select the type of credentials:
     - To add a username and password, fill out the **Username**, **Password**, and **Description** fields and click **Save**.
     - To add a private key to an Amazon EC2 instance or a Linux physical machine, do the following:
       a. **Private key**:Select a private key from the Type menu.
       b. **Username**: Enter a username for the private key.

c. **Password**: Create a password for the private key.

d. **Repeat password**: Repeat password.

   Note

   If you generated your key with a passphrase, you have to enter this passphrase into the **password** and **repeat password** boxes.

e. Locate and select the private key.

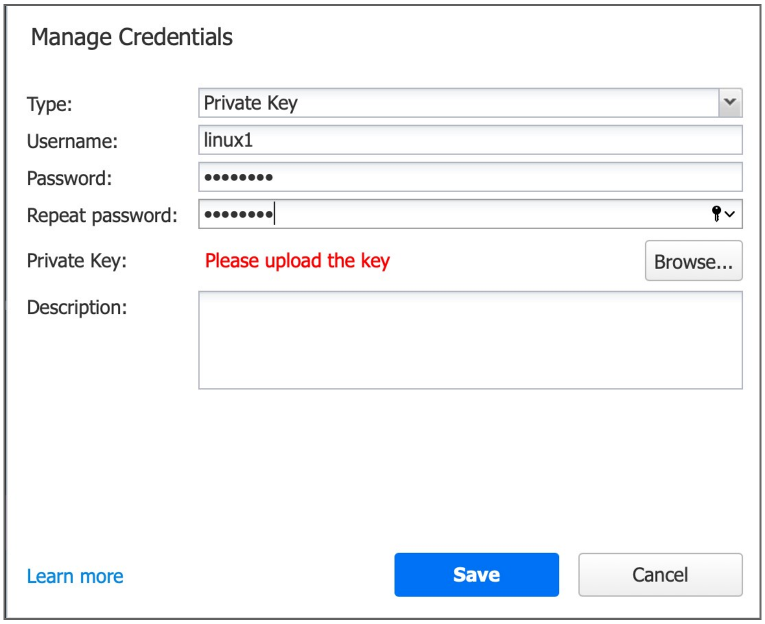
   Information

   Supported key formats: RSA, DSA

   Supported file extensions: no extension, .pem, .key, .cer, .der, .txt

f. Fill out the **Description** box.

g. Click **Save.**



Manage Credentials

Type: Private Key

Username: linux1

Password: ••••••••

Repeat password: ••••••••

Private Key: Please upload the key

Description:

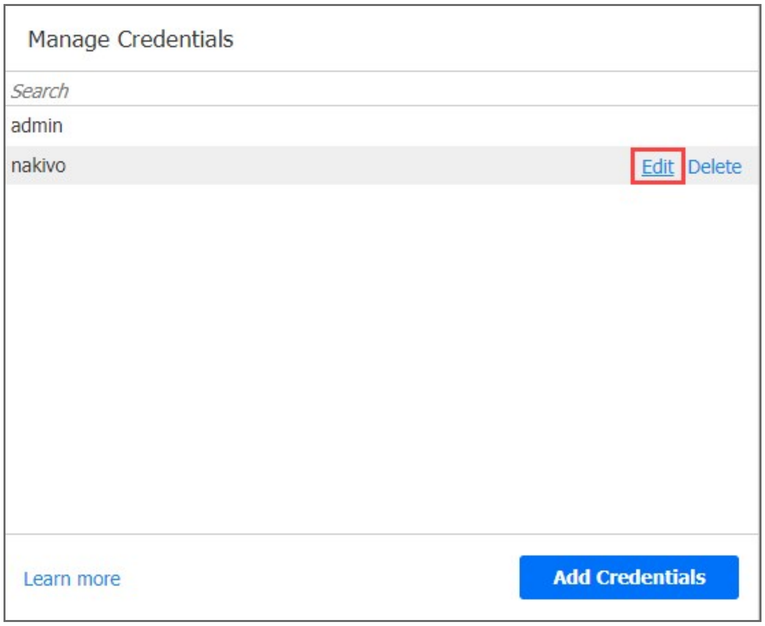
You can now assign the credentials while creating jobs.

Editing Credentials

To edit credentials, do the following:

1. Click **Settings** in the left pane of the product.
2. Go to the **Inventory** tab.
3. Click **Manage credentials**.

4. Hover the mouse pointer over the record that you would like to edit, and click **Edit.**

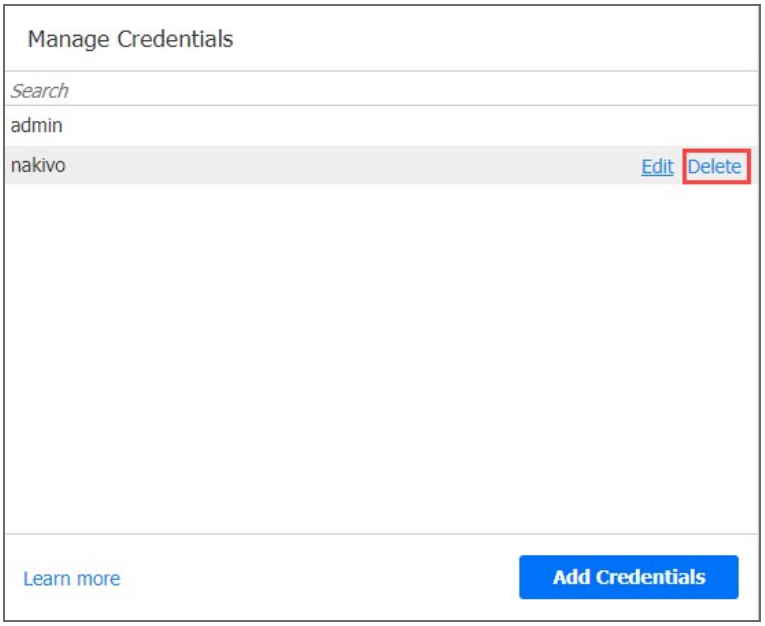


5. Make any required changes, and then click **Save**.

Deleting Credentials

Do the following:

1. Click **Settings** in the left pane of the product.
2. Go to the **Inventory** tab.
3. Click **Manage credentials**.
4. Hover the mouse pointer over the record that you would like to delete, and click **Delete.**



5. Click **Delete** in the confirmation dialog that opens.

Transporters

The Transporter is one of NAKIVO Backup & Replication component that does all of the heavy-lifting: it performs backup, replication, and recovery, as well as data compression, deduplication, and encryption. To learn how to add an additional Transporter and how to manage it, refer to the topics below:

- "Adding Installed Transporters" on page 251
- "Managing Transporters" on page 268

Adding Installed Transporters

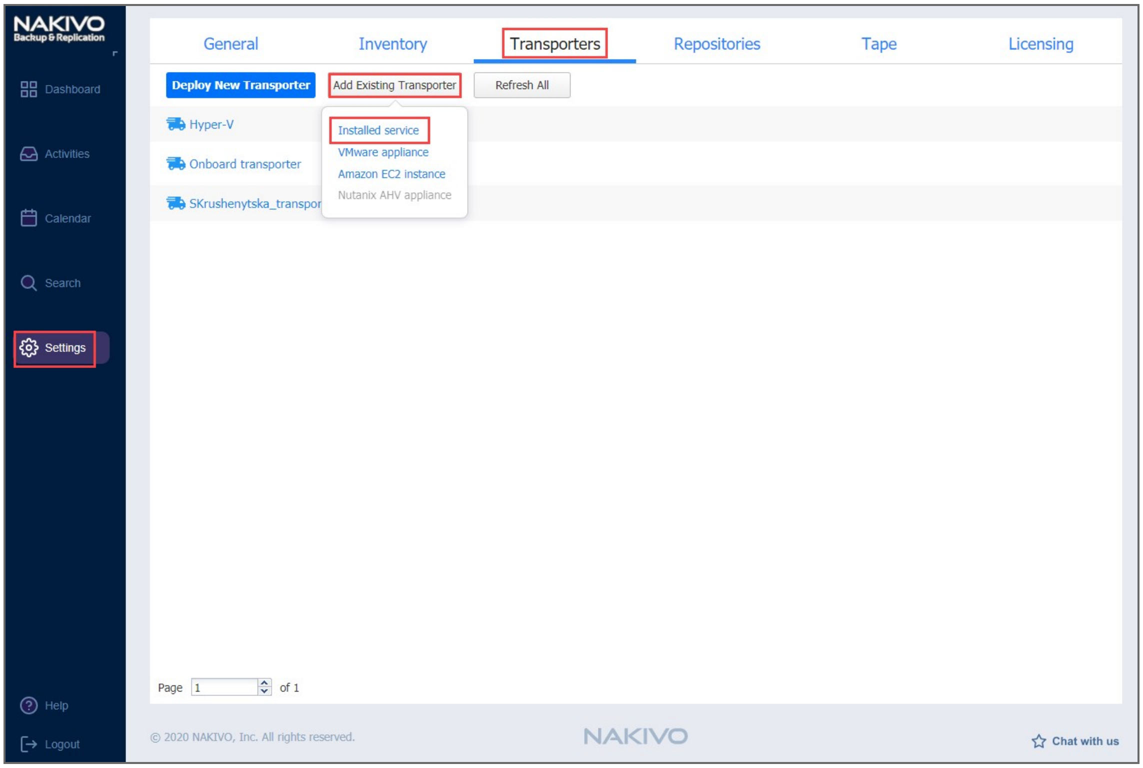
After you have installed a Transporter, you need to add it to NAKIVO Backup & Replication so that the Transporter can be used for backup, replication, and recovery tasks. Refer to the following topics:

- Installed Service
- VMware Appliance
- Amazon EC2 Instance
- Nutanix AHV Appliance

Installed Service

Please follow the steps below to add a Transporter that is installed as a service:

1. Click **Settings** in the left pane of the product dashboard and go to the **Transporters** tab.
2. Click **Add Existing Transporter** and then click **Installed service** in the dialog that opens.



3. The **Add Existing Transporter - Installed Service** dialog opens. In the **Hostname or IP** box, enter the IP address or a hostname of the machine on which the Transporter is installed.

   Note

   If you are adding the Transporter by a DNS name, make sure this DNS name can be resolved on the machines on which the Director and any other Transporters (which you plan to use in conjunction with the current one) are installed.
4. Click **More options** and fill out the following fields:

- In the *Security* section:
    - **Master Password**: Optionally, you can set a password to secure the connection. The set password must match the one configured on the Transporter. Note that setting a master password is required when the **Enable Direct Connect** for this Transporter option is enabled. Proceed as follows:
        a. After entering the password, click **Connect**.
        b. The **Certificate Acceptance** dialog box appears. Verify the certificate details, and click **Accept**.

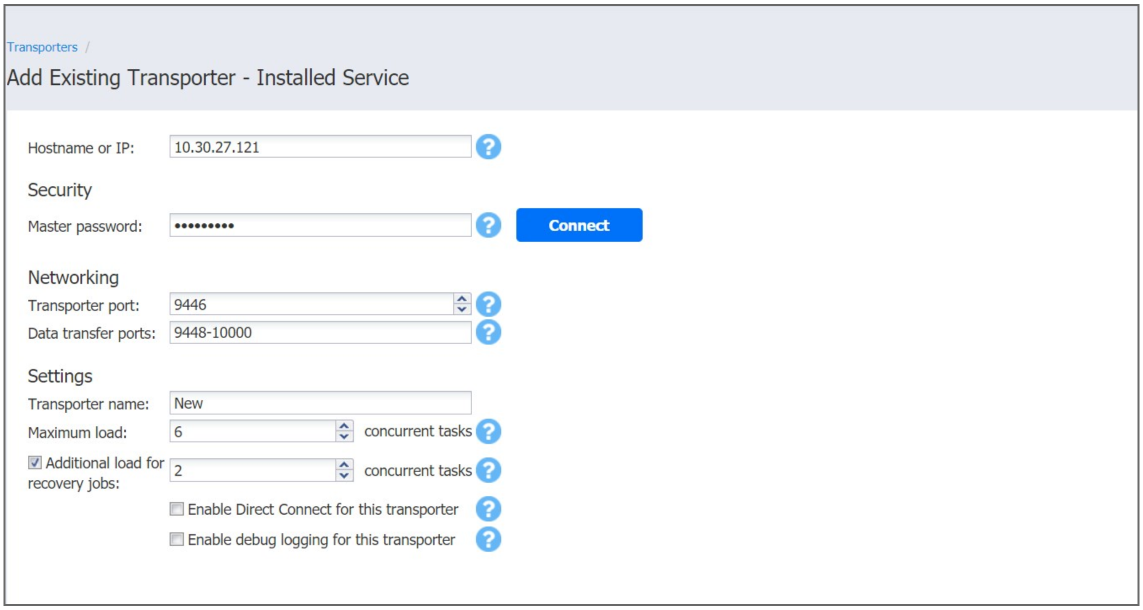
        Notes

        - The master password must adhere to the following requirements:
            - Minimal length - 5 characters.
            - Maximum length - 50 characters.
        - The master password can be set and re-set manually by running the command on the machine housing the Transporter. Follow these steps:
            - Enter the following command `bhsvc -b P@ssword123`
            - Restart the Transporter service.
- In the *Networking* section:
    - **Transporter port**: Specify the port number that will be used to connect to the Transporter.
    - **Data transfer ports**: Specify a range of port numbers (from 1 to 65535) that will be used to transfer data. The range you specify should contain at least 100 ports. Make sure that the ports you specify are open in your firewall.
- In the *Settings* section:
    - **Transporter name**: Specify a display name for the Transporter.
    - **Maximum load**: Specify the maximum number of tasks that the Transporter should process simultaneously. A task, for example, is a backup or replication of a single VM disk, or one granular recovery session.
    - **Additional load for recovery jobs**: If selected, the specified amount of tasks will be added to set maximum transporter load to be used for recovery jobs exclusively. This allows running the specified amount of concurrent recovery jobs along with other types of jobs without the need to wait for their completion.
    - **Enable Direct Connect for this transporter**: When this option is enabled, you can access remote resources via a single port connection without establishing a VPN connection. The following conditions must be met at the remote infrastructure to enable this feature:
        - The NAKIVO Transporter must be installed.
        - A master password must be set for security reasons. A pre-shared key is generated based on the entered master password.

- The Transporter port on the local machine must be exposed to be externally available via the internet.

- **Enable debug logging for this transporter**: If needed, enable debug level logging for the current transporter. It is not recommended to use this option on a permanent basis.

5. Click **Add**.



Transporters /

Add Existing Transporter - Installed Service

Hostname or IP: 10.30.27.121

Security

Master password: •••••••••

Networking

Transporter port: 9446

Data transfer ports: 9448-10000

Settings

Transporter name: New

Maximum load: 6 concurrent tasks

☑ Additional load for recovery jobs: 2 concurrent tasks

□ Enable Direct Connect for this transporter

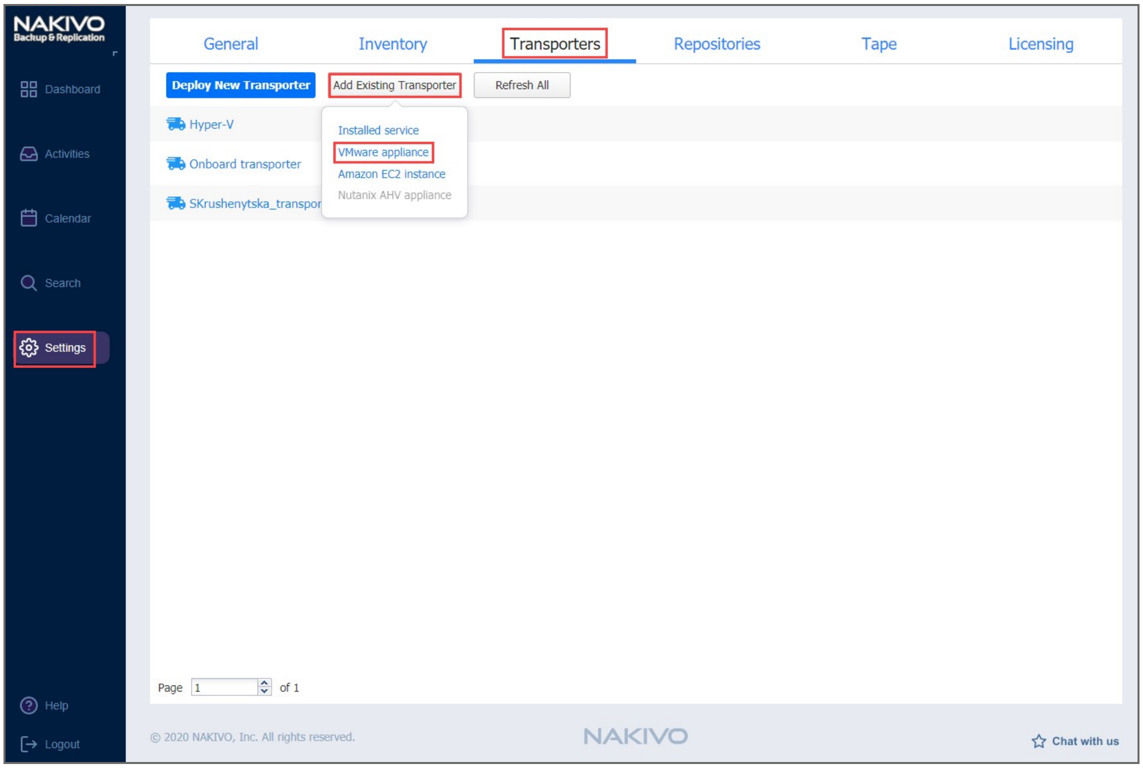
□ Enable debug logging for this transporter

The Transporter is added to the product and is ready to be used for backup, replication, and recovery.

VMware Appliance

Please follow the steps below to add a Transporter that is deployed as a VMware appliance:

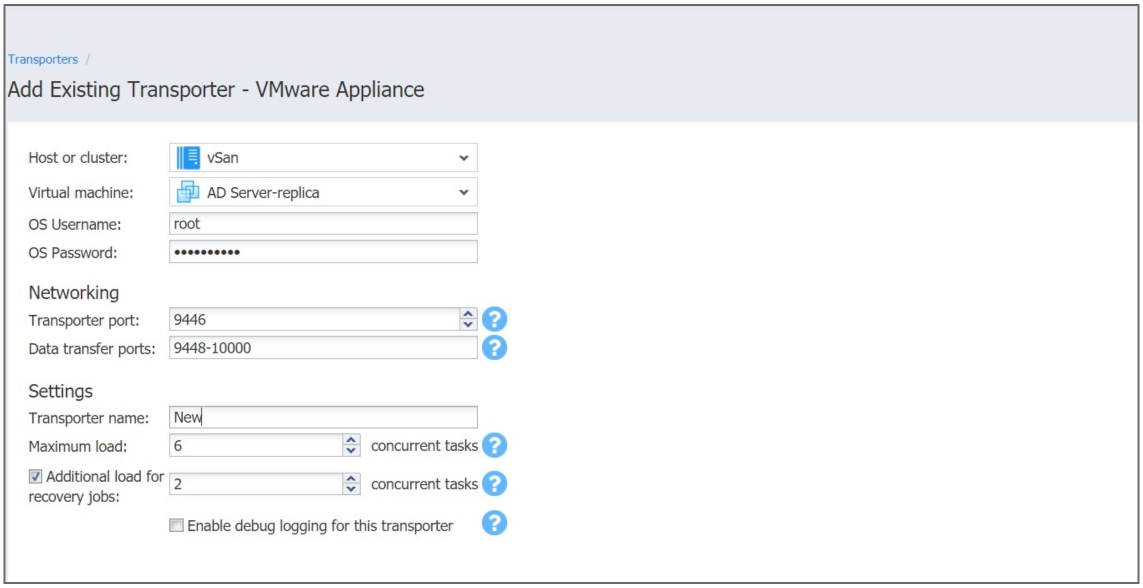
1. Click **Settings** in the left pane of the product dashboard and go to the **Transporters** tab.
2. Click **Add Existing Transporter** and then click **VMware appliance** in the dialog that opens.



3. The `VMware Appliance` dialog opens. Fill out the fields as described below:
   - In the **Host or cluster** box, enter the IP address or name of the host or the cluster where the corresponding virtual machine is deployed.
   - In the **Virtual machine** box, specify the virtual machine on which the Transporter is installed.
   - In the **OS Username** and **OS Password** fields, specify credentials for accessing the virtual machine.
   - Click **More options** and fill out the following fields:
     - In the *Networking* section:
       - **Transporter port**: Specify the port number that will be used to connect to the Transporter.
       - **Data transfer ports**: Specify a range of port numbers (from 1 to 65535) that will be used to transfer data. The range you specify should contain at least 100 ports. Make sure that the ports you specify are open in your firewall.
     - In the *Settings* section:
       - **Transporter name**: Specify a display name for the Transporter.
       - **Maximum load**: Specify the maximum number of tasks that the Transporter should process simultaneously. A task, for example, is a backup or replication of a single VM disk, or one granular recovery session.
       - **Additional load for recovery jobs**: Selecting this option reserves the Transporter's resources exclusively for recovery jobs. This allows you to run recovery jobs concurrently with other types of jobs without the need to wait for their completion. The Transporter resources will be reserved according to the specified number.

- **Enable debug logging for this transporter**: If needed, enable debug level logging for the current transporter. It is not recommended to use this option on a permanent basis.

4. Click **Add**.



Transporters /

Add Existing Transporter - VMware Appliance

Host or cluster: vSan

Virtual machine: AD Server-replica

OS Username: root

OS Password: ••••••••••

Networking

Transporter port: 9446

Data transfer ports: 9448-10000

Settings

Transporter name: New

Maximum load: 6 concurrent tasks

☑ Additional load for recovery jobs: 2 concurrent tasks

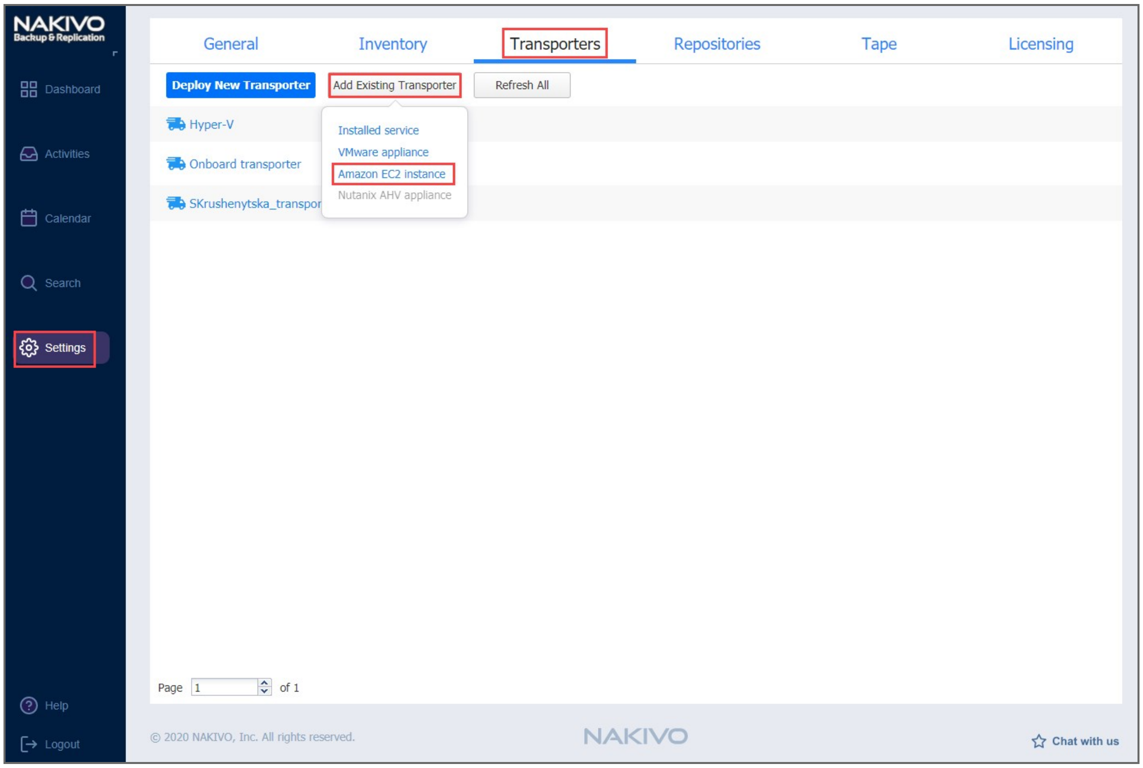
□ Enable debug logging for this transporter

The Transporter is added to the product and is ready to be used for backup, replication, and recovery.

Amazon EC2 Instance

If you have already deployed a Transporter in Amazon EC2 and now wish to re-import the Transporter in a new instance of NAKIVO Backup & Replication, do the following:

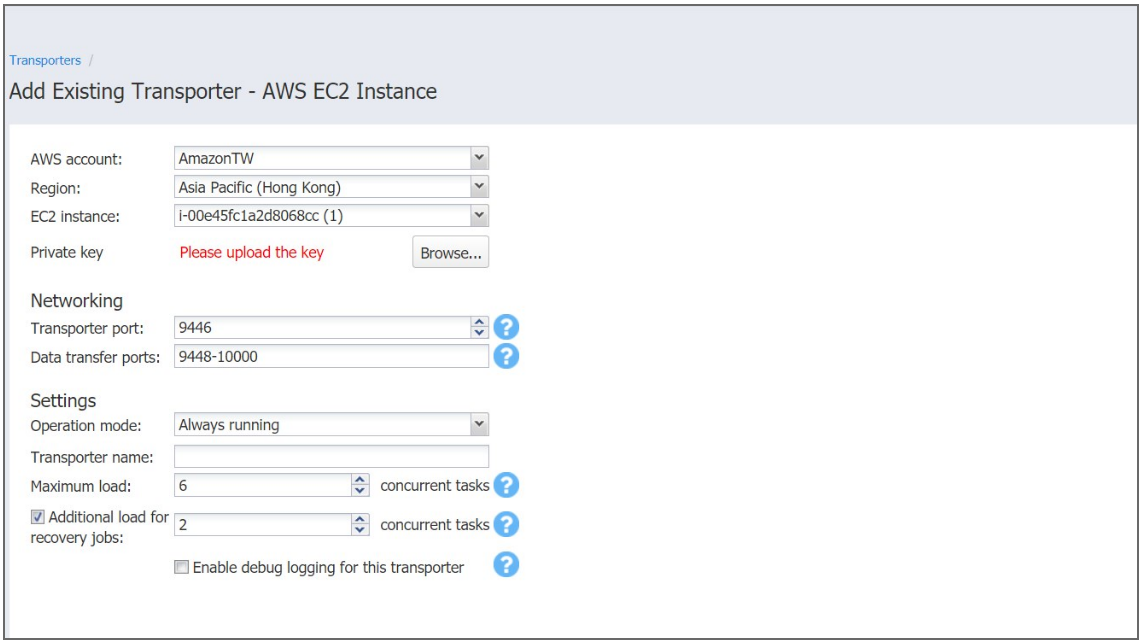
1. Click **Settings** in the left pane of the product dashboard and go to the **Transporters** tab.
2. Click **Add Existing Transporter** and then click **Amazon EC2 instance** in the popup that opens.



3. The **Amazon EC2 Instance** dialog opens. Fill out the fields as described below:
   - **AWS account**: Choose an appropriate Amazon AWS Account from the list of Amazon AWS Accounts added to the Inventory.
   - **Region**: Choose a region in which an AWS EC2 instance with the Transporter is deployed.
   - **EC2 Instance**: Select the Amazon EC2 Instance with the Transporter that you wish to add to the product.
   - **Private key**: Click the **Browse** button to locate and upload the Private key for the Transporter Instance that was created when you deployed the Transporter in the cloud.
   - Click **More options** and fill out the following fields:
     - In the *Networking* section:
       - **Transporter port**: Specify the port number that will be used to connect to the Transporter.
       - **Data transfer ports**: Specify a range of port numbers (from 1 to 65535) that will be used to transfer data. The range you specify should contain at least 100 ports. Make sure that the ports you specify are open in your firewall.
     - In the *Settings* section:
       - **Operation mode**: Choose either of the following Transporter operation modes:
         - **Always running**
         - **Running while required**
       - **Transporter name**: Specify a display name for the Transporter.
       - **Maximum load**: Specify the maximum number of tasks that the Transporter should process simultaneously. A task, for example, is a backup or replication of a single VM disk, or one granular recovery session.

- **Additional load for recovery jobs**: If selected, the specified amount of tasks will be added to set maximum transporter load to be used for recovery jobs exclusively.
- **Enable debug logging for this Transporter**: If needed, enable debug level logging for the current transporter. It is not recommended that you use this option on a permanent basis.

4. Click **Add**.



Transporters /

Add Existing Transporter - AWS EC2 Instance

AWS account: AmazonTW

Region: Asia Pacific (Hong Kong)

EC2 instance: i-00e45fc1a2d8068cc (1)

Private key Please upload the key Browse...

Networking

Transporter port: 9446

Data transfer ports: 9448-10000

Settings

Operation mode: Always running

Transporter name:

Maximum load: 6 concurrent tasks

☑ Additional load for recovery jobs: 2 concurrent tasks

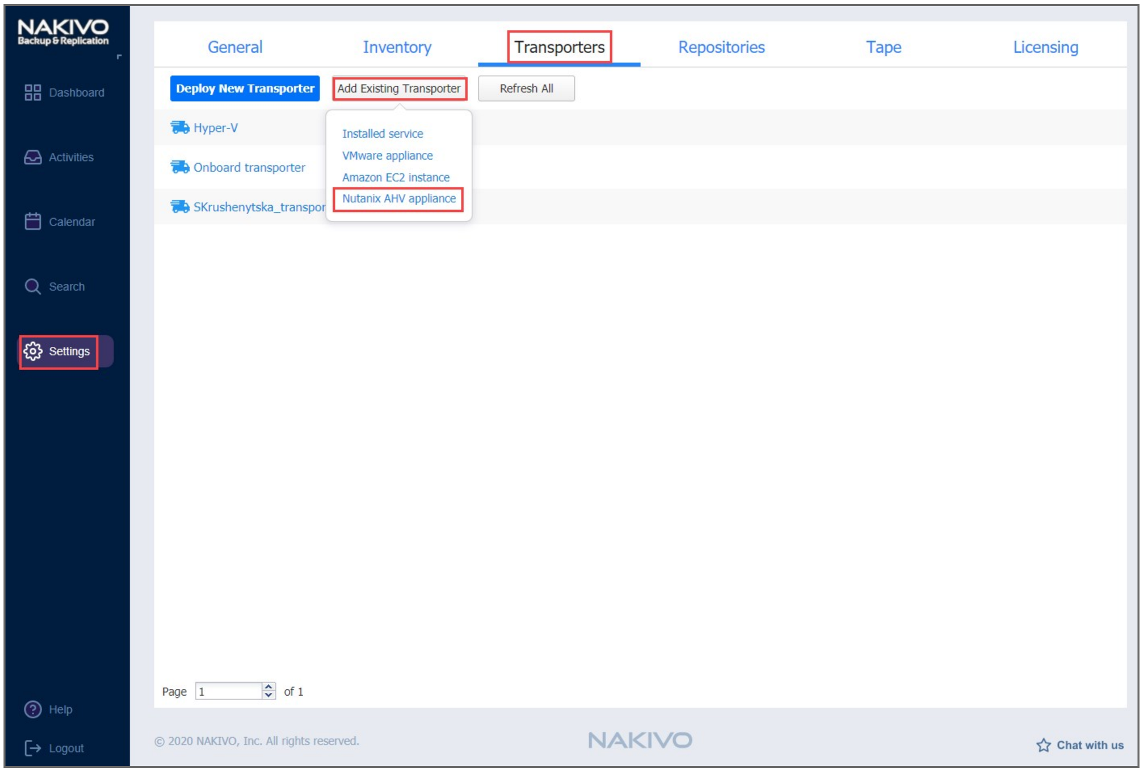
☐ Enable debug logging for this transporter

The Transporter is added to the product and is ready to be used for backup, replication, and recovery tasks.

Nutanix AHV Appliance

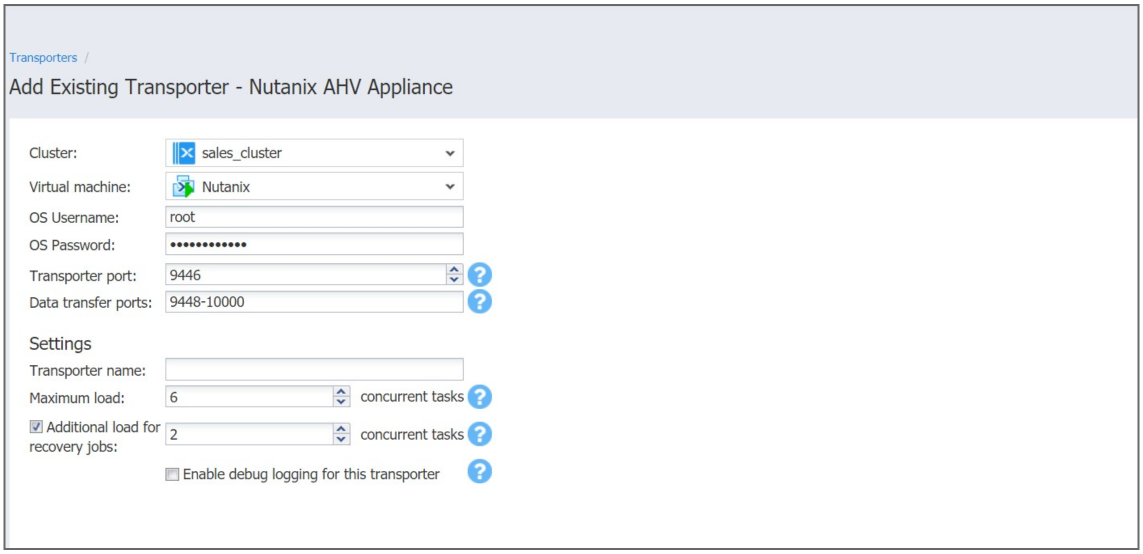
Please follow the steps below to add a Transporter that is deployed as a Nutanix AHV appliance:

1. Click **Settings** in the left pane of the product dashboard and go to the **Transporters** tab.
2. Click **Add Existing Transporter** and then select **Nutanix AHV Appliance**.



3. In the **Add Existing Transporter - Nutanix AHV Appliance** dialog, enter the following options:
    - **Cluster**: Select a cluster where the corresponding virtual machine is deployed.
    - **Virtual machine**: Select the virtual machine on which the Transporter is installed.
    - **Username/Password**: Enter credentials for accessing the virtual machine where the Transporter is installed.
    - **Transporter port**: Enter the port number that will be used to connect to the Transporter.
    - **Data transfer ports**: Enter a range of port numbers (from 1 to 65535) that will be used to transfer data. The range you specify should contain at least 100 ports. Make sure that the ports you specify are open in your firewall.
    - **Transporter name**: Enter a display name for the Transporter.
    - **Maximum load**: Select the maximum number of tasks that the Transporter should process simultaneously. A task, for example, is a backup or replication of a single VM disk, or one granular recovery session.
    - **Additional load for recovery jobs**: If selected, the specified amount of tasks will be added to set maximum transporter load to be used for recovery jobs exclusively.
    - **Enable debug logging for this transporter**: If needed, enable debug level logging for the current

transporter. It is not recommended that you use this option on a permanent basis.



Transporters /

Add Existing Transporter - Nutanix AHV Appliance

Cluster: sales_cluster

Virtual machine: Nutanix

OS Username: root

OS Password: ••••••••••••

Transporter port: 9446

Data transfer ports: 9448-10000

Settings

Transporter name:

Maximum load: 6 concurrent tasks

☑ Additional load for recovery jobs: 2 concurrent tasks

□ Enable debug logging for this transporter

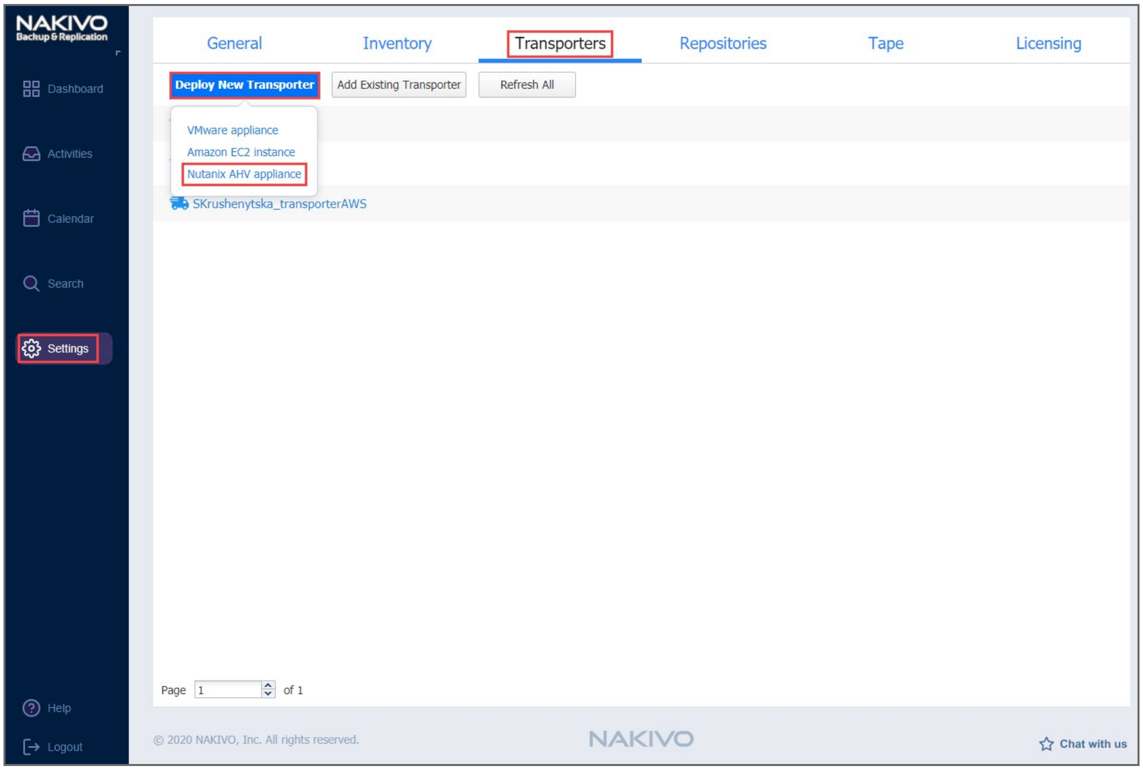
4. Click **Add**. The Transporter is added to the product and can be used for backup, replication, and recovery.

Deploying Transporter as Nutanix AHV Appliance

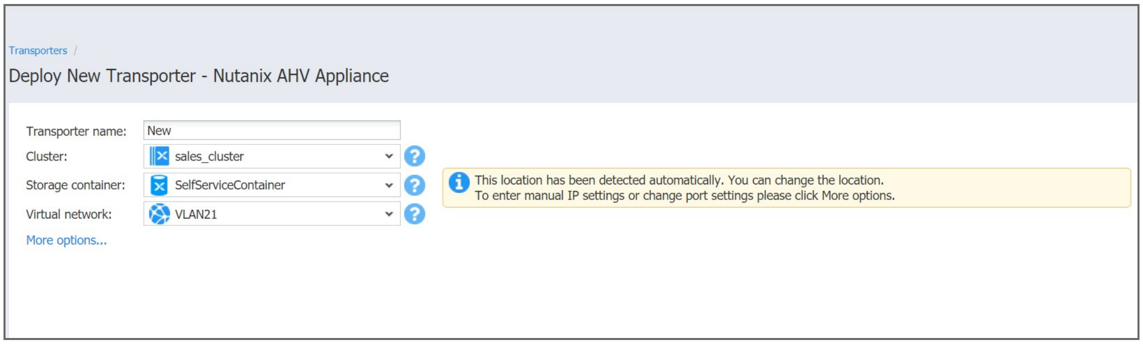
To enable NAKIVO Backup & Replication to create and run jobs within a Nutanix AHV cluster, a dedicated Transporter must be deployed as a Nutanix appliance in that cluster.

Please follow the steps below to add a transporter as a Nutanix appliance:

1. Go to **Settings > Transporters** tab.
2. On the **Transporters** tab, click **Deploy New Transporter** and select **Nutanix AHV Appliance** from the drop-down list.



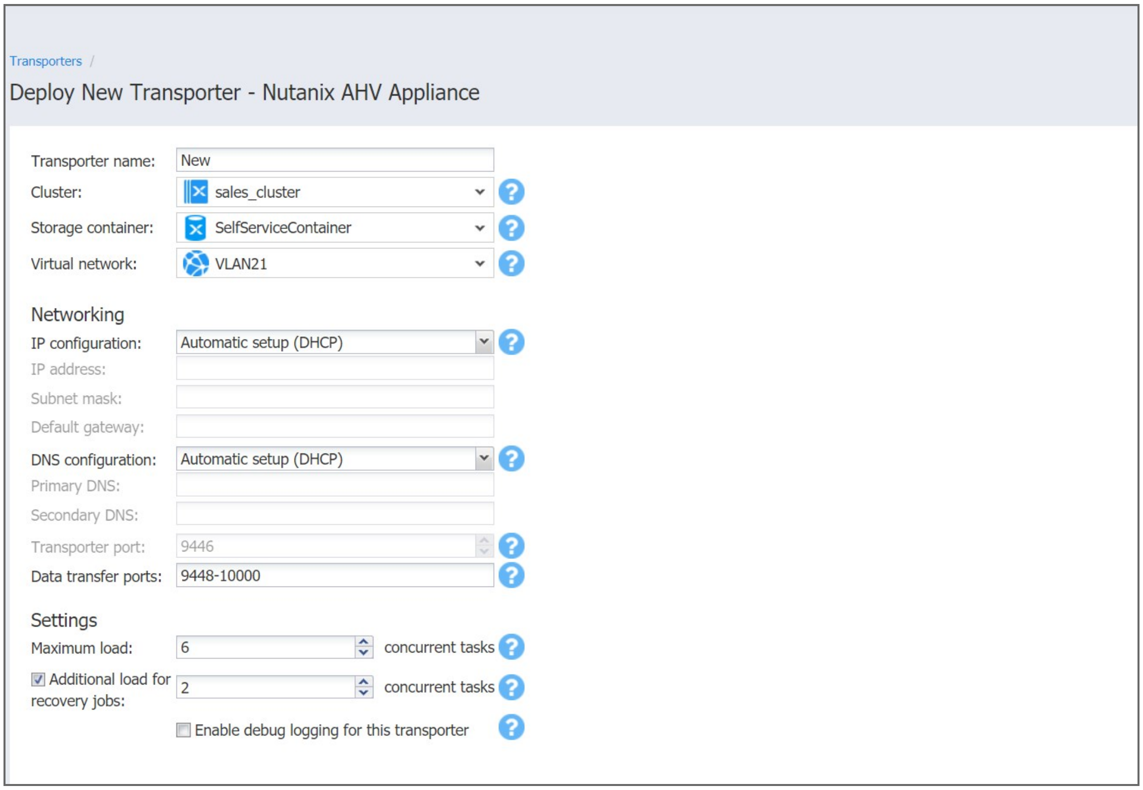
3. In the **Deploy New Transporter - Nutanix AHV Appliance** dialog, specify the following options:
   - **Transporter name**: Enter a name for the new Transporter.
   - **Cluster**: Select a cluster where the transporter VM will run.
   - **Storage container**: Select a storage container where the transporter VM will be located.
   - **Virtual network**: Select a virtual network where the transporter VM will be connected.



Transporter name: New
Cluster: sales_cluster
Storage container: SelfServiceContainer
Virtual network: VLAN21

This location has been detected automatically. You can change the location.
To enter manual IP settings or change port settings please click More options.

4. Click **Deploy** if you want to go with the automatically selected networking options and default Transporter load configuration.
5. Alternatively, click **More options** if you wish to manually set the following options:
    - **IP configuration**: Can be either **Automatic setup (DHCP)** or **Manual setup**. With manual setup selected, specify an **IP address**, **Subnet mask** and **Default gateway**.
    - **DNS configuration**: Can be either **Automatic setup (DHCP)** or **Manual setup**. With manual setup selected, specify **Primary** and **Secondary DNS**.
    - **Transporter port**: Enter a communication port for your Transporter.
    - **Data transfer ports**: Enter a port range that will be used by your Transporter for actual data transfer.
    - **Maximum load**: Specify the maximum number of tasks that the Transporter should process simultaneously. A task, for example, is a backup or replication of a single VM disk, or one granular recovery session.
    - **Additional load for recovery jobs**: If selected, the specified quantity of tasks will be added to set the maximum Transporter load to be used for recovery jobs exclusively. This allows for running the specified amount of concurrent recovery jobs along with other types of jobs without the need to wait for their completion.
    - **Enable debug logging for this transporter**: If needed, enable debug level logging for the current transporter. Using this option on a permanent basis is not recommended.



Transporters /

Deploy New Transporter - Nutanix AHV Appliance

Transporter name: New
Cluster: sales_cluster
Storage container: SelfServiceContainer
Virtual network: VLAN21

Networking
IP configuration: Automatic setup (DHCP)
IP address:
Subnet mask:
Default gateway:
DNS configuration: Automatic setup (DHCP)
Primary DNS:
Secondary DNS:
Transporter port: 9446
Data transfer ports: 9448-10000

Settings
Maximum load: 6 concurrent tasks
☑ Additional load for recovery jobs: 2 concurrent tasks
☐ Enable debug logging for this transporter

6. Click **Deploy**. The deployment process starts. Successfully deployed Transporter is displayed in the **Transporters** tab.

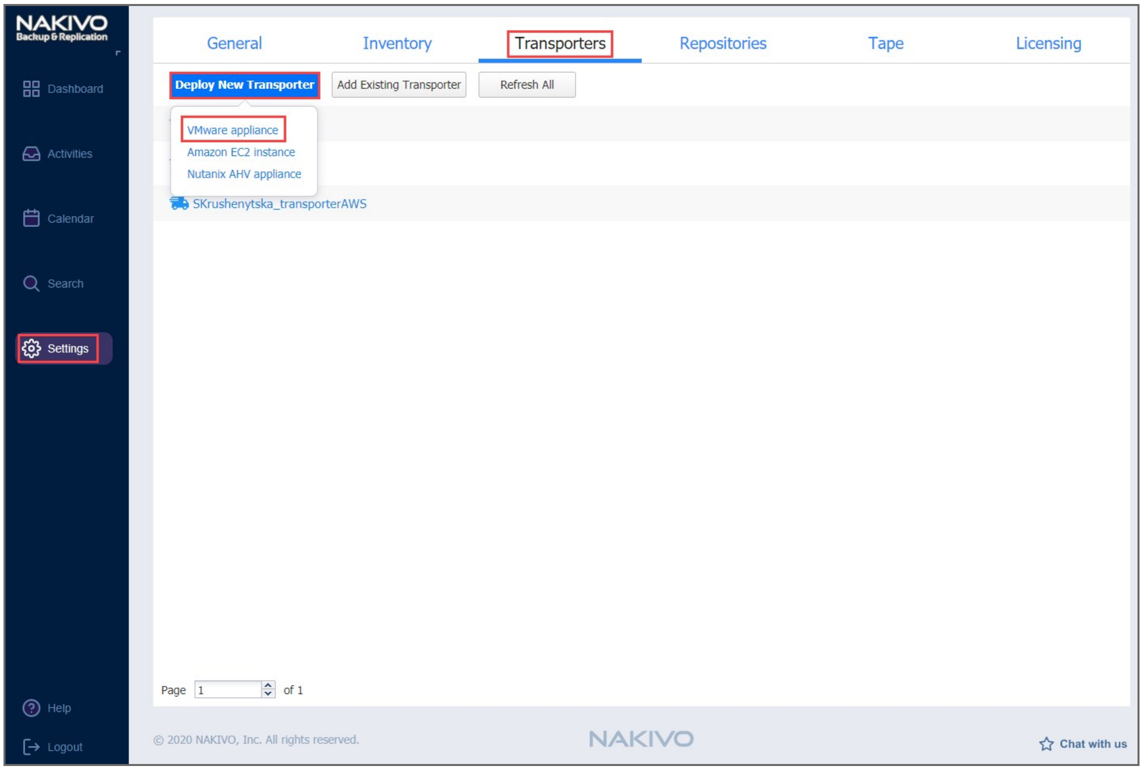
Deploying Transporter as VMware Appliance

Note

If your instance of NAKIVO Backup & Replication is installed on ARM-based NAS, an external Transporter needs to be deployed to work with VMware vCenters and ESXi hosts. This is because certain features are not supported by ARM-based NASes.

Please follow the steps below to deploy a Transporter that supports VMware vCenter:

1. Go to **Settings** > **Transporters** and then click **Deploy New Transporter**.
2. In the dialog that opens, click **VMware appliance**.



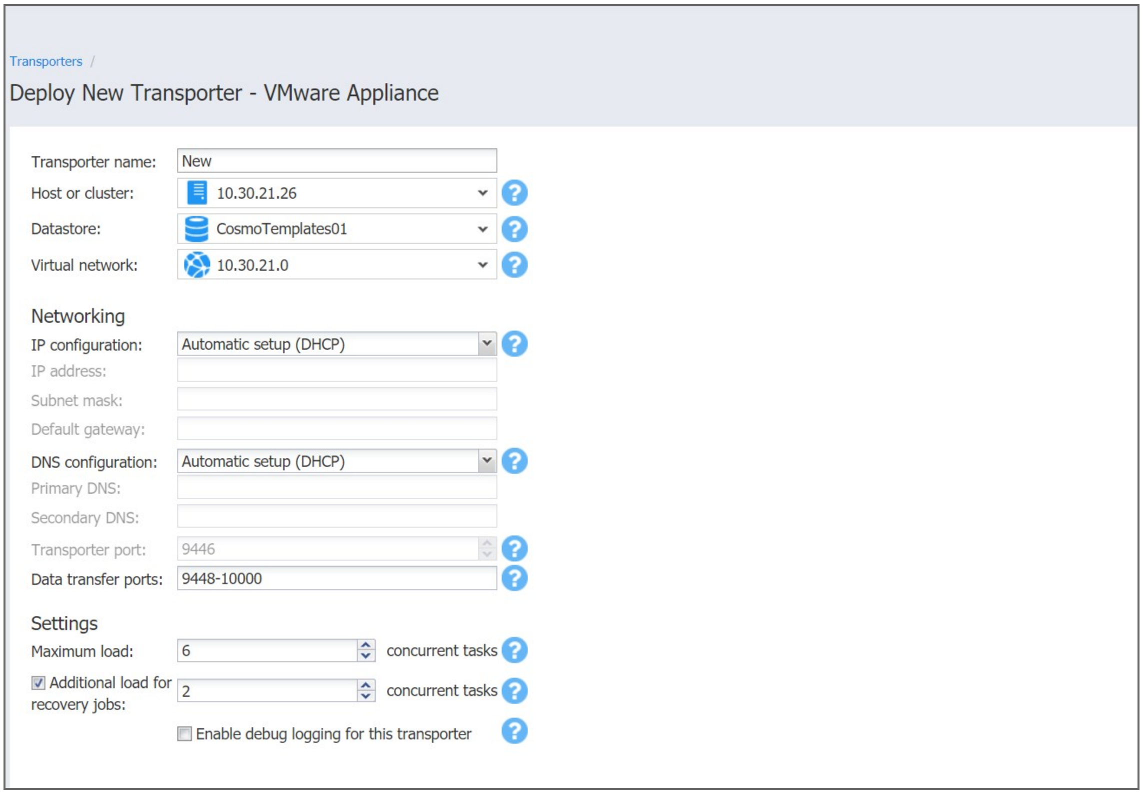
3. In the **Deploy New Transporter - VMware Appliance** dialog that opens, proceed as follows:
   - **Transporter name**: Enter a name for your Transporter.
   - **Host or cluster**: Select a target host or cluster.
   - **Datastore**: Select a target datastore.
   - **Virtual network**: Select a target virtual network.

     Note

     An internet connection is required to deploy a new Transporter as a VMware appliance on the target host or cluster.
   - If necessary, access the advanced options for your Transporter by clicking **More options** and then entering data for the following parameters:

- In the *Networking* section:
    - **IP configuration**: It can be either **Automatic setup (DHCP)**, or **Manual setup**.
    - **IP address**: If you have chosen **Manual setup** for the IP configuration, enter a Transporter IP address.
    - **Subnet mask**: If you have chosen **Manual setup** for the **IP configuration**, enter a subnet mask.
    - **Default gateway**: If you have chosen **Manual setup** for the **IP configuration**, enter a default gateway.
    - **DNS configuration**: It can be either **Automatic setup (DHCP)**, or **Manual setup**.
    - **Primary DNS**: If you have chosen **Manual setup** for the **DNS configuration**, enter a primary DNS server IP address.
    - **Secondary DNS**: If you have chosen **Manual setup** for the **DNS configuration**, enter a secondary DNS server IP address.
    - **Transporter port**: Enter a communication port for your transporter.
    - **Data transfer ports**: Enter a port range that will be used by your transporter for actual data transfer.
- In the *Settings* section:
    - **Maximum load**: A number of tasks concurrently processed by the Transporter.
    - **Additional load for recovery jobs**: If selected, the specified amount of tasks will be added to set maximum transporter load to be used for recovery jobs exclusively. This allows for running the specified amount of concurrent recovery jobs along with other types of jobs without the need to wait for their completion.
    - **Enable debug logging for this transporter**: When selected, it enables debug level logging for the Transporter. It is not recommended to have this option selected on a permanent basis.

4. Click **Deploy** to confirm deploying the Transporter.



Transporters /

Deploy New Transporter - VMware Appliance

Transporter name:	New
Host or cluster:	10.30.21.26
Datastore:	CosmoTemplates01
Virtual network:	10.30.21.0

Networking

IP configuration:	Automatic setup (DHCP)
IP address:	
Subnet mask:	
Default gateway:	
DNS configuration:	Automatic setup (DHCP)
Primary DNS:	
Secondary DNS:	
Transporter port:	9446
Data transfer ports:	9448-10000

Settings

Maximum load:	6 concurrent tasks
☑ Additional load for recovery jobs:	2 concurrent tasks
	☐ Enable debug logging for this transporter

When deployment of the new Transporter finishes successfully, a message appears informing you about it.

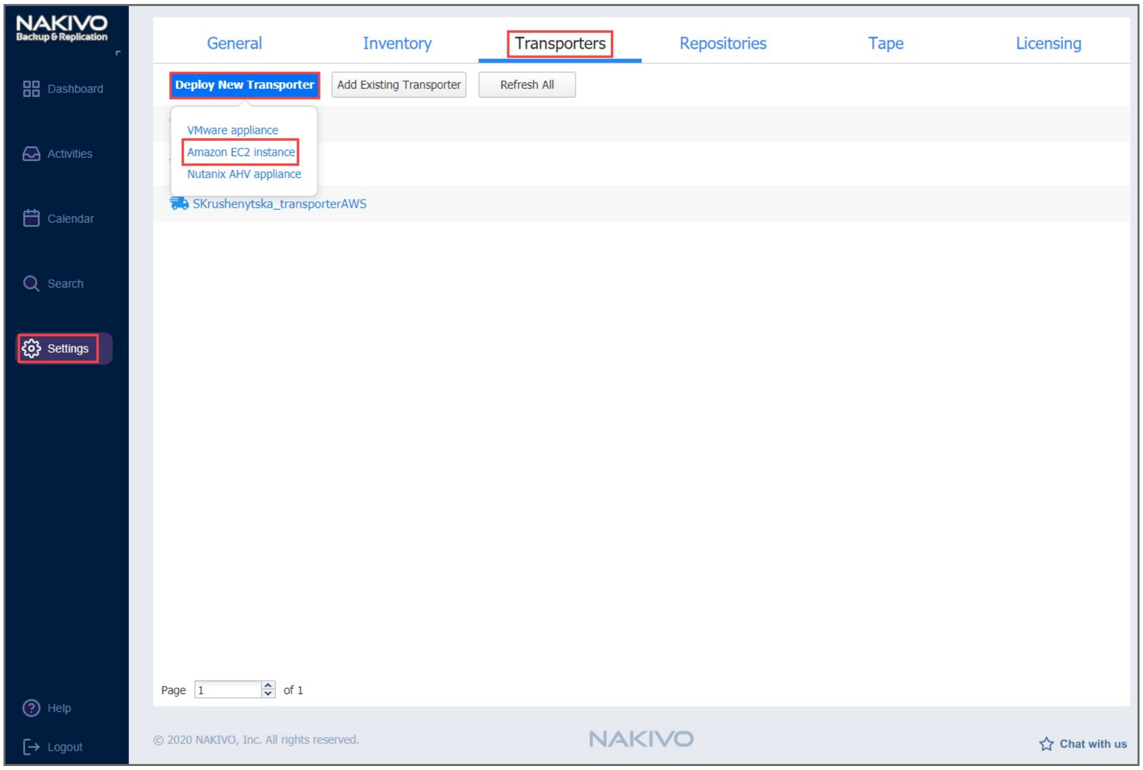
Deploying Transporters in Amazon EC2

You need to deploy a Transporter in Amazon EC2 to enable the following features:

- Backing up VMware VMs and/or Amazon EC2 Instances to a backup repository located in Amazon EC2.
- Backing up Amazon EC2 Instances in a particular Amazon EC2 Region.

NAKIVO Backup & Replication automates deploying a Transporter in Amazon EC2. To deploy a Transporter in Amazon EC2 within the product interface, follow the steps below:

1. Click **Settings** in the left pane of the product dashboard and then go to the **Transporters** tab.
2. Click **Deploy New Transporter** and then click **Amazon EC2 instance**.



3. The **Amazon EC2 instance** dialog opens. Fill out the fields as described below:
   - **Transporter name**: Enter a name for the Transporter.
   - **Region**: Select an Amazon EC2 region where you wish to deploy the Transporter. This will enable you to create a backup repository in the region as well as back up Amazon EC2 Instances available in the region.
   - **Instance type**: Choose a type of Amazon EC2 Instance (for example, "t2.medium") that will be used to deploy the Transporter. Note that more powerful Instances may be able to process data faster, but will cost more to run on Amazon EC2.
   - Click **More options** and do the following:
     - In the *Networking* section:
       - **Automatically configure VPC for this transporter**: If selected, a new VPC with a single public subnet will be created and used to deploy this transporter. If you want to deploy the Transporter into a different VPC and subnet, deselect this option.

        - **Network**: Select a network to which the Amazon EC2 instance with the Transporter will be connected.
        - **Subnet**: Select a subnet for the Amazon EC2 Instance with the Transporter.
    - **Allowed traffic from**: Enter the IP addresses of the machines that can connect to the Amazon EC2 instance with the Transporter. Access from other IP addresses will be restricted.

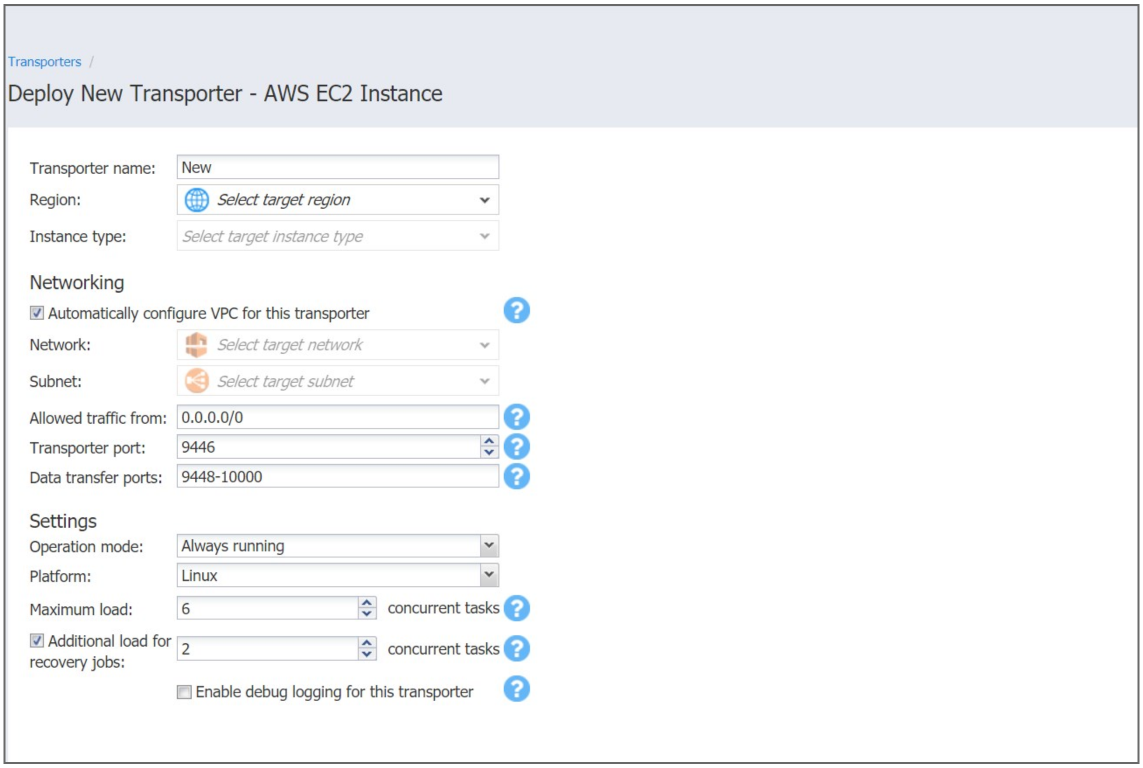
      Important

      By default, the Amazon EC2 security group is not restricted, that is, the Transporter can be accessed by and receive tasks from any machine. For security purposes, restrict traffic only to trusted IP addresses.
    - **Transporter Port**: Specify the port number that will be used to connect to the Transporter.
    - **Data transfer ports**: Specify a range of port numbers (from 1 to 65535) that will be used to transfer data. The range you specify should contain at least 100 ports. Make sure that the ports you specify are open in your firewall.
- In the *Settings* section:
    - **Operation mode**: If you select the **Running while required** option, the Amazon EC2 Instance with the Transporter will be powered on only when the Transporter is required to run a backup, replication, and recovery tasks.
    - **Platform**: Choose an OS for the instance where the Transporter will be deployed.
    - **Maximum load**: Specify the maximum number of tasks that the Transporter should process simultaneously. An example of a task is processing a single VM disk or a single file recovery session.
    - **Additional load for recovery jobs**: If selected, the specified amount of tasks will be added to set the maximum Transporter load to be used for recovery jobs exclusively. This allows for running the specified quantity of concurrent recovery jobs along with other types of jobs without the need to wait for their completion.
    - **Enable debug logging for this Transporter**: Enables debug level logging for the current Transporter. Since this feature slows down Transporter performance, it is recommended that you enable debug logging only for the investigation of support issues.

Note

Refer to “Amazon EC2 Concepts” on page 11 for the definitions of Amazon EC2-related terms.

4. Click **Deploy**.



Transporters /

Deploy New Transporter - AWS EC2 Instance

Transporter name:	New
Region:	Select target region
Instance type:	Select target instance type

Networking

☑ Automatically configure VPC for this transporter

Network:	Select target network
Subnet:	Select target subnet
Allowed traffic from:	0.0.0.0/0
Transporter port:	9446
Data transfer ports:	9448-10000

Settings

Operation mode:	Always running
Platform:	Linux
Maximum load:	6 concurrent tasks
☑ Additional load for recovery jobs:	2 concurrent tasks

☐ Enable debug logging for this transporter

Important

- After you have deployed a Transporter in Amazon EC2, you need to download the Transporter Keys. The Transporter Keys are used by NAKIVO Backup & Replication to access and manage the Transporter in Amazon EC2. If you lose the current instance of NAKIVO Backup & Replication and install a new copy of the product, you will need to provide the Transporter Keys to access the Transporter.
- You may be additionally charged for using a 3rd-party resource. Please refer to the 3rd-party resource provider documentation for details.

Managing Transporters

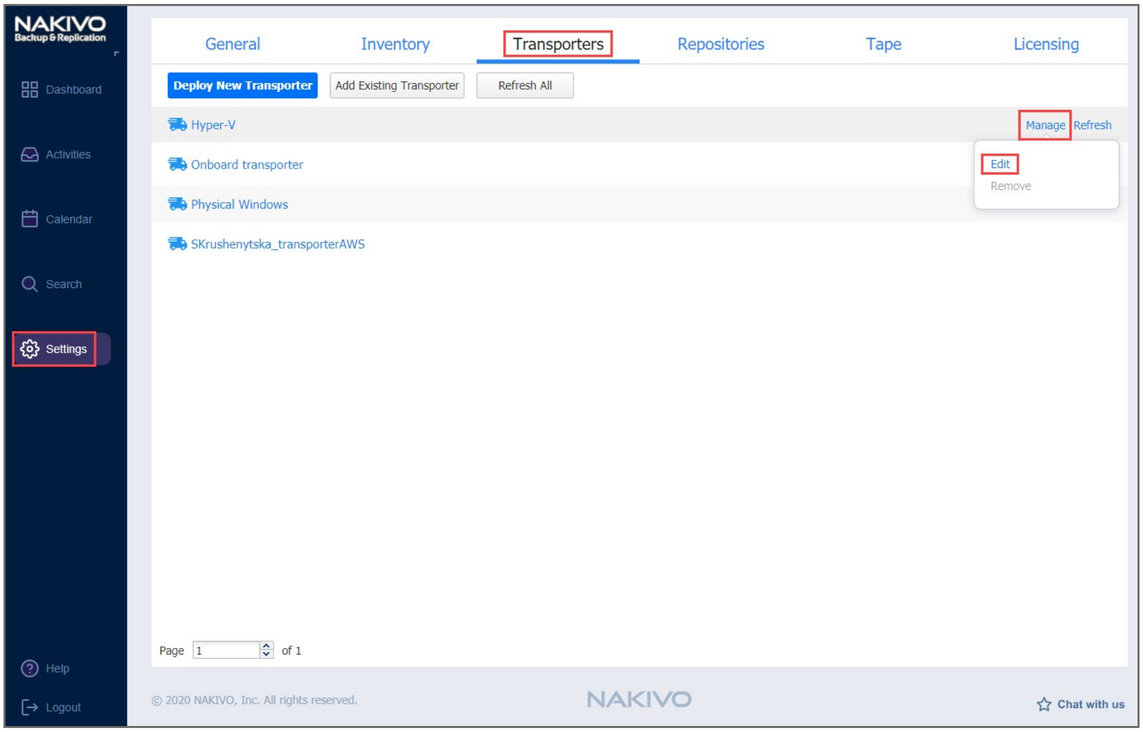
Refer to the following topics:

- “Editing Transporters” on page 269
- “Refreshing Transporter Details” on page 271
- “Downloading Transporter's Credentials” on page 274
- “Removing (Deleting) Transporters” on page 273

Editing Transporters

To modify the settings of an existing Transporter, follow the steps below:

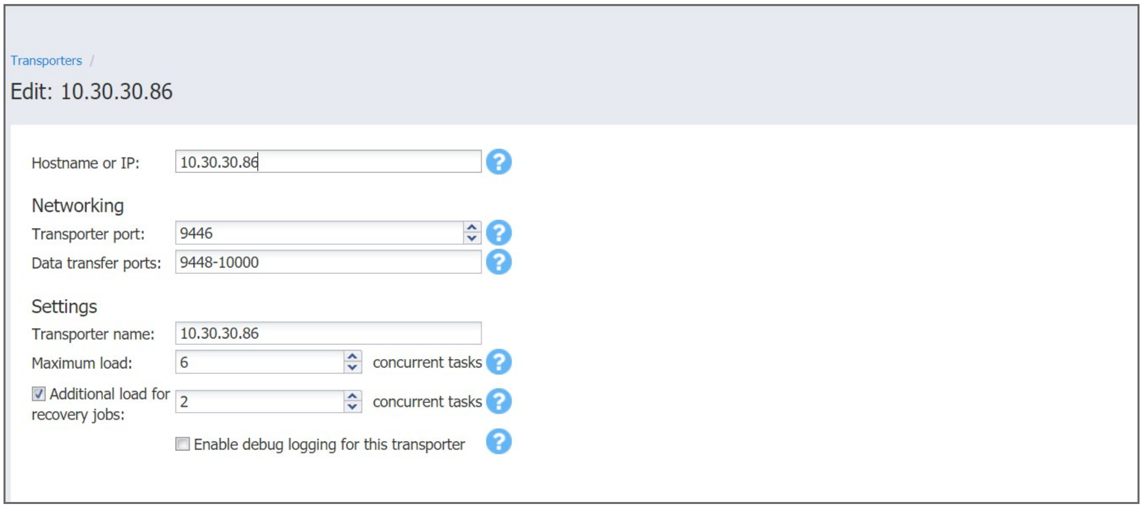
1. Click **Settings** in the left pane of the product.
2. Go to the **Transporters** tab and click on the Transporter you would like to edit.
3. In the Transporter title, click **Manage** and then click **Edit**.



4. A dialog opens for editing the Transporter settings. Edit the settings as required:
   - **Hostname or IP**: Here you can edit the IP address or hostname of the machine on which the Transporter is installed.
     - In the *Networking* section:
       - **Transporter port**: Enter a communication port for your Transporter.
       - **Data transfer ports**: Enter a port range that will be used by your Transporter for actual data transfer.
     - In the *Settings* section:
       - **Transporter name**: Edit the name of your Transporter.
       - **Maximum load**: Edit the number of tasks concurrently processed by the Transporter.
       - **Additional load for recovery jobs**: If selected, the specified amount of tasks will be added to the set maximum Transporter load to be used for recovery jobs exclusively. This allows for running the specified amount of concurrent recovery jobs along with other types of jobs without the need to wait for their completion.

- **Enable debug logging for this transporter**: Enable/disable debug level logging for the Transporter. Having this option enabled on a permanent basis is not recommended.

5. Click **Appy** to save your changes.



Transporters /

Edit: 10.30.30.86

Hostname or IP: 10.30.30.86

Networking

Transporter port: 9446

Data transfer ports: 9448-10000

Settings

Transporter name: 10.30.30.86

Maximum load: 6 concurrent tasks

☑ Additional load for recovery jobs: 2 concurrent tasks

☐ Enable debug logging for this transporter

The changes you have made are applied to the Transporter.

Refreshing Transporter Details

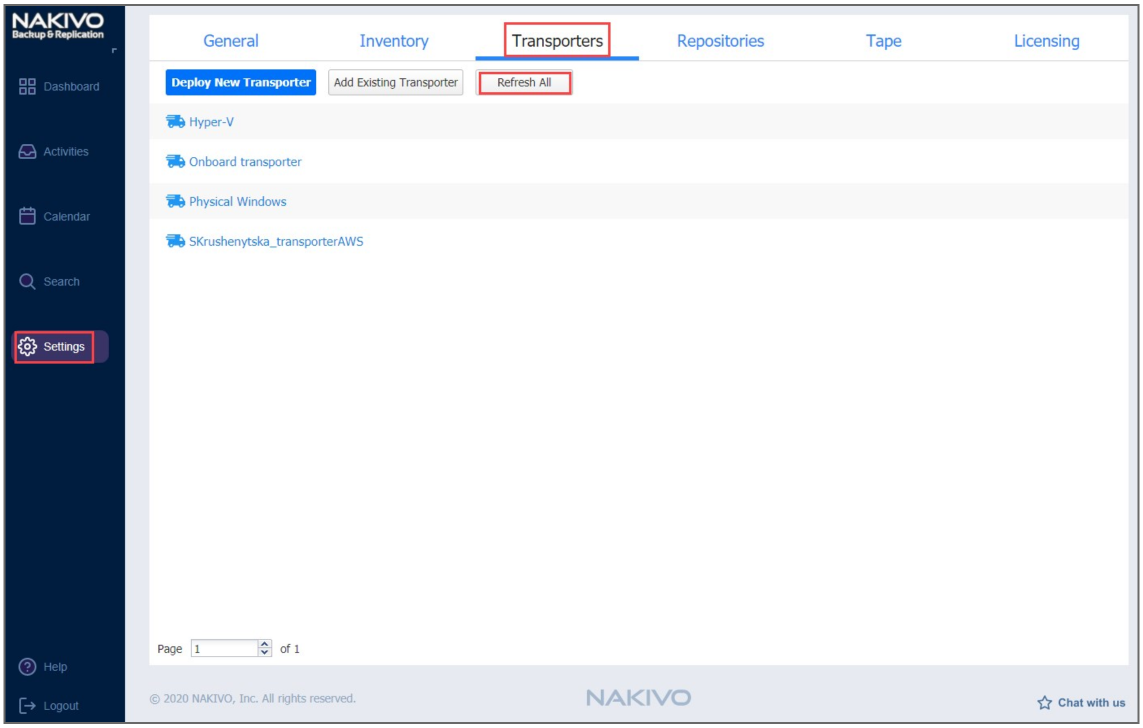
By default, NAKIVO Backup & Replication refreshes the information about Transporters every hour. During the refreshing process, the product collects all the required information about all Transporters. Only one Transporter can be refreshed at a time. If you have more than one Transporter, all others will remain in the queue until they are able to be refreshed.

- Manually Refreshing All Transporters
- Manually Refreshing a Single Transporter

Manually Refreshing All Transporters

To update all Transporters, follow the steps below:

1. Click **Settings** in the left pane of the product and go to the **Transporters** tab.
2. Click **Refresh All.**



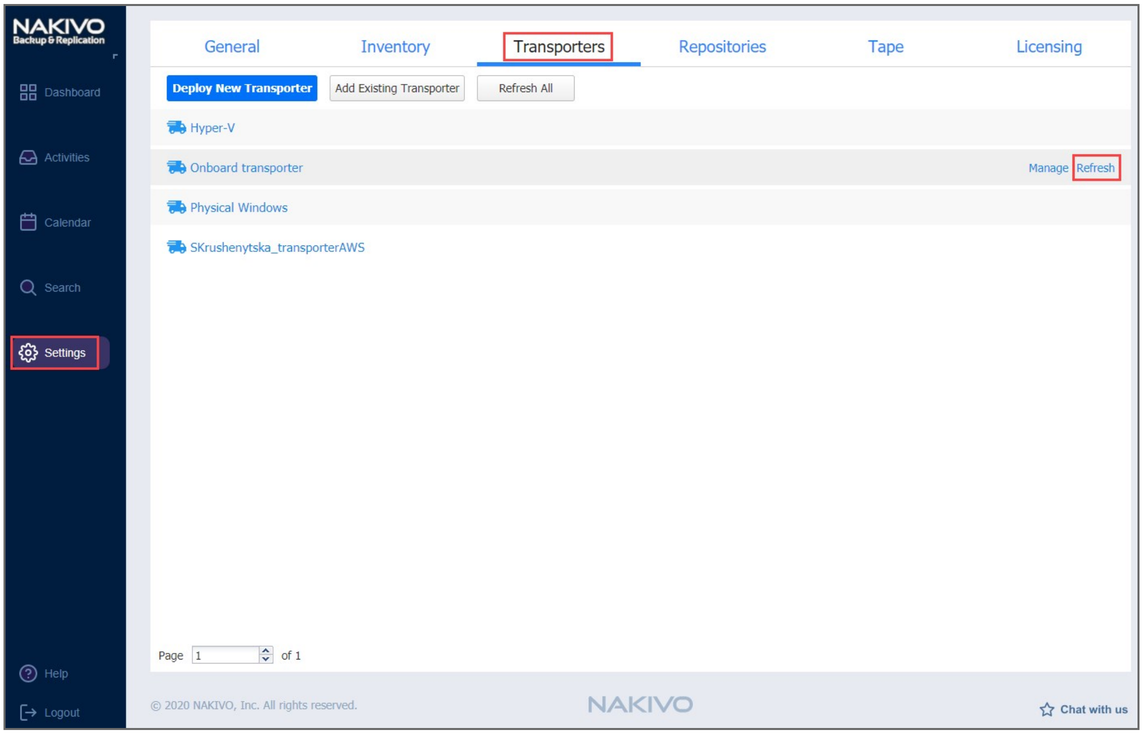
The update of all Transporters starts.

Manually Refreshing a Single Transporter

To update a single Transporter, follow the steps below:

1. Click **Settings** in the left pane of the product.
2. Go to the **Transporters** tab.
3. Select the Transporter you would like to update.

4. In the title of the Transporter, click **Refresh.**

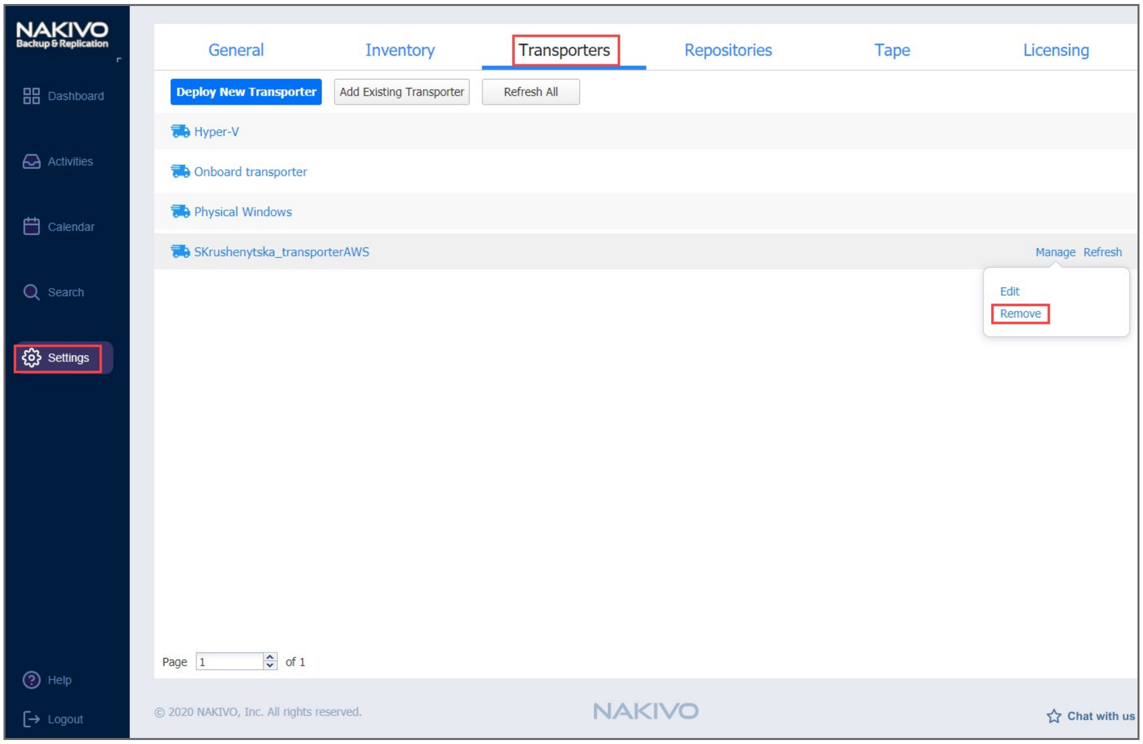


The Transporter refresh starts.

Removing (Deleting) Transporters

To remove a Transporter from NAKIVO Backup & Replication, follow the steps below:

1. Click **Settings** in the left pane of the product.
2. Go to the **Transporters** tab.
3. Select the Transporter you would like to remove.
4. In the Transporter title, click **Manage** and then click **Remove.**



5. Click **Remove** in the message that appears.

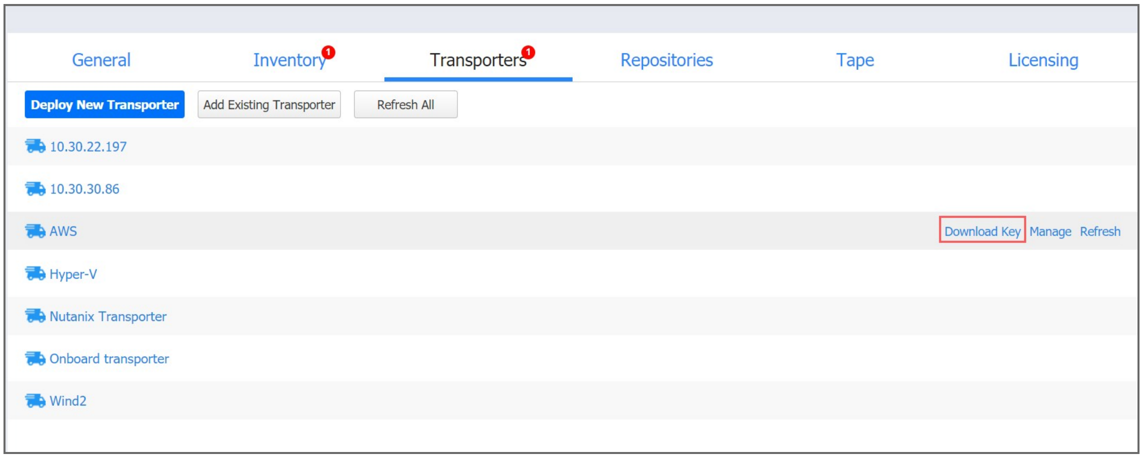
Important

The following Transporters cannot be removed:

- The Onboard Transporter (which is installed with the "Director" on page 59 by default)
- Transporters manually assigned to a job
- Transporters assigned to the backup repositories in Amazon Cloud.

Downloading Transporter's Credentials

If you want to re-import an Amazon EC2 or VMware Transporter into another installation of the NAKIVO Backup & Replication, you need to have the Transporter's credentials. To obtain the credentials, click the **Download key** link next to the corresponding Transporter.



Clicking the link downloads the ZIP file containing the Transporter's credentials.

Backup Repositories

A Backup Repository is one of the key components of NAKIVO Backup & Replication and is a regular folder where the product stores backups and backup metadata. For more detailed information, refer to "Backup Repository" on page 65.

This section covers repository-related topics such as creation, management, etc. of Backup Repositories and contains the following articles:

- "Adding Existing Backup Repositories" on page 276
- "Viewing Backup Repository Details" on page 288
- "Managing Backup Repositories" on page 278

Adding Existing Backup Repositories

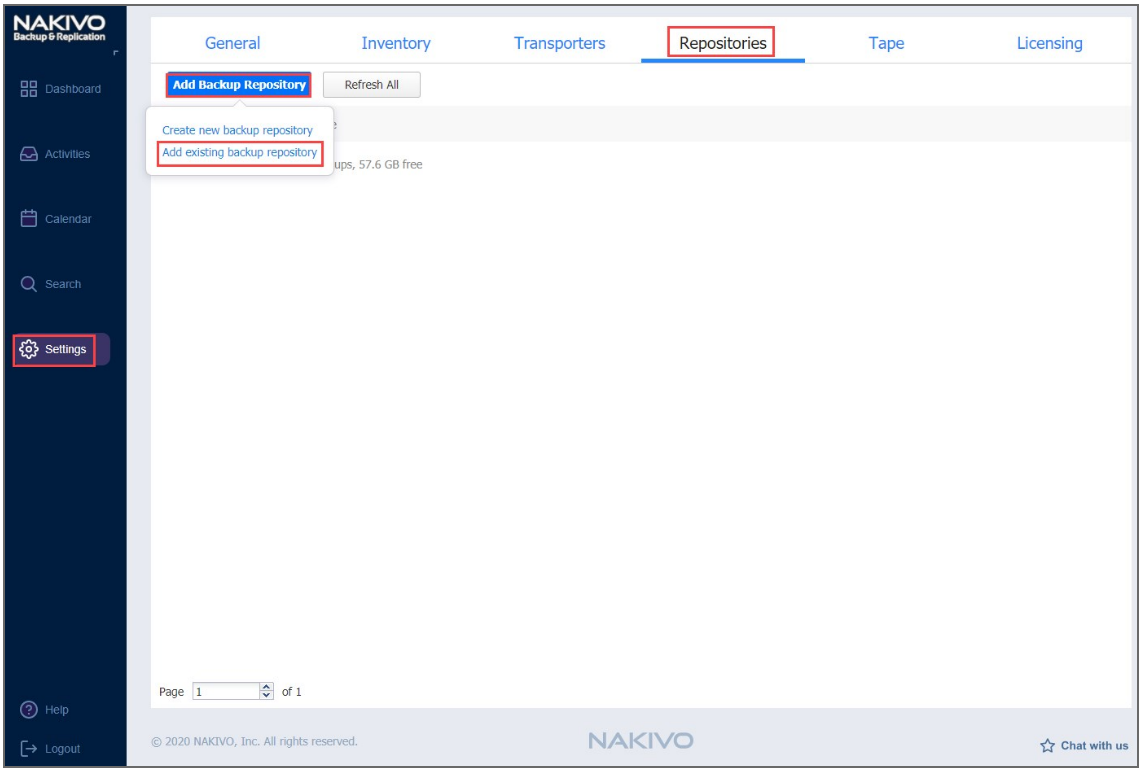
NAKIVO Backup & Replication provides you with the ability to add an existing Backup Repository to a new copy of the product.

Important

During the import process, NAKIVO Backup & Replication searches for the "`NakivoBackup`" folder in the specified location, so if your Backup Repository is located in `E:\backup\NakivoBackup`, you need to specify the following path: `E:\backup`

To import an existing Backup Repository, do the following:

1. Go to the main menu and click **Settings**.
2. Go to the **Repositories** tab and click **Add Backup Repository**.
3. Click **Add existing backup repository** in the dialog that opens.



4. The **Add Existing Backup Repository** wizard opens. On the **Type** page of the wizard, select the following Backup Repository :
   - **SaaS**
5. On the **Name & Location** page of the wizard, fill out all the necessary fields the way it's described in the article for the corresponding Backup Repository type.
6. On the **Options** page of the wizard, the following options can be available for configuration:

- **Detach this repository on schedule**: Select this option if you want to detach and then reattach the Backup Repository on a schedule. Detaching a Backup Repository saves the Backup Repository data and metadata in a consistent state and stops the product interaction with the Backup Repository (so that the Backup Repository can be copied or moved). You can use this feature, for example, for the disk-to-disk-to-tape (D2D2T) data protection approach, in which backups are stored on a disk for fast operational recovery, and copied to a tape (while the repository is detached) for archiving and long-term storage.
  - **Delete and re-create the repository on attach**: If this option is selected, all data in the Backup Repository will be erased prior to attaching it to the product. As a result, jobs that write to this Backup Repository will create full VM backups. You can use this option, for example, to create full daily, weekly, or monthly VM backups and write them to tape or removable media.

7. Click **Finish**. The Backup Repository is imported.

Managing Backup Repositories

Refer to the following topics:

- “Attaching Backup Repositories” on page 281
- “Detaching Backup Repositories” on page 282
- “Editing Backup Repositories” on page 283
- “Refreshing Backup Repositories” on page 284
- “Removing and Deleting Backup Repositories” on page 286

SaaS Backup Repository

Choose this type of Backup Repository for all your Microsoft 365 related activities.

Important

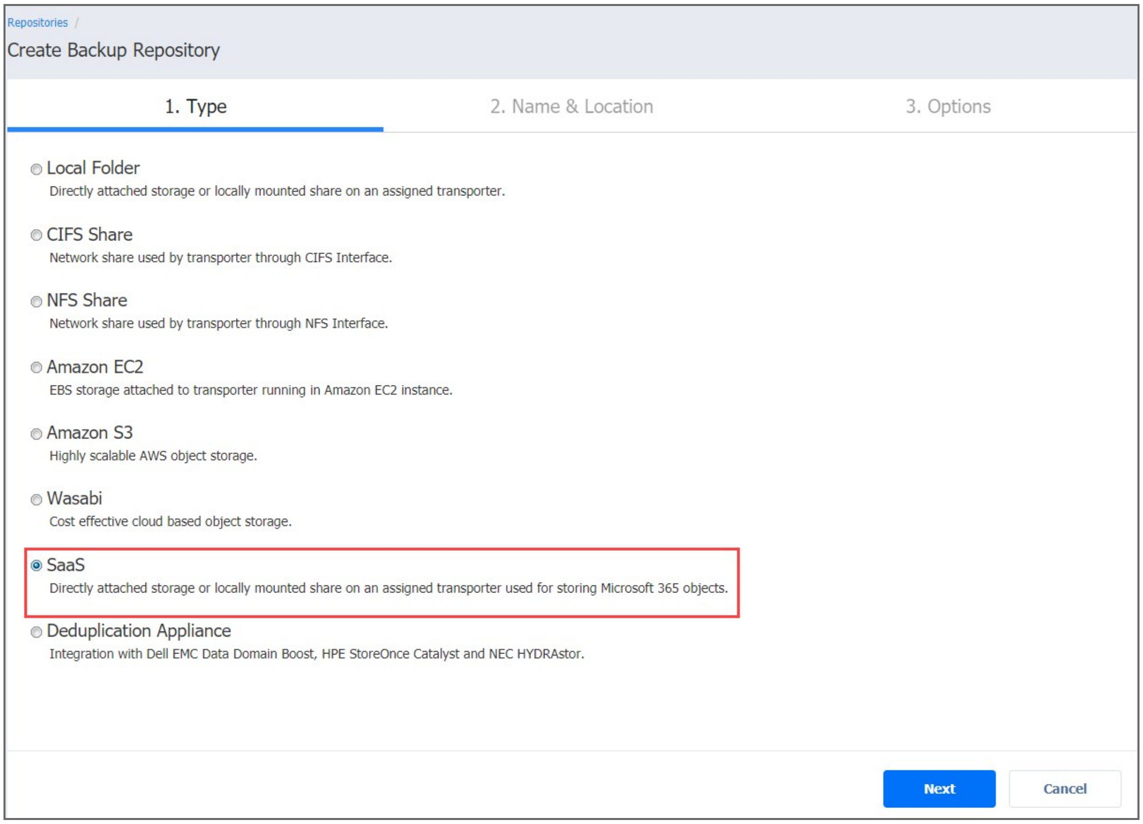
- For SaaS repositories, only local folders are supported as a location.
- ARM-based (x32) NAS devices are not supported for SaaS Backup Repository creation.
- Synology NAS devices with ARMv8 architecture are not supported for SaaS Backup Repository creation.
- Before creating a SaaS repository, provide read and write permissions to the local folder where the repository will be located.

To create a SaaS Backup Repository, proceed as described in the following sections:

- Create Backup Repository: Type
- Create Backup Repository: Name and Location
- Create Backup Repository: Options

Create Backup Repository: Type

On the **Type** page of the **Create Backup Repository** wizard, select **SaaS** and click **Next** to go to the next page of the wizard.



Repositories /

Create Backup Repository

1. Type | 2. Name & Location | 3. Options

○ Local Folder
Directly attached storage or locally mounted share on an assigned transporter.

○ CIFS Share
Network share used by transporter through CIFS Interface.

○ NFS Share
Network share used by transporter through NFS Interface.

○ Amazon EC2
EBS storage attached to transporter running in Amazon EC2 instance.

○ Amazon S3
Highly scalable AWS object storage.

○ Wasabi
Cost effective cloud based object storage.

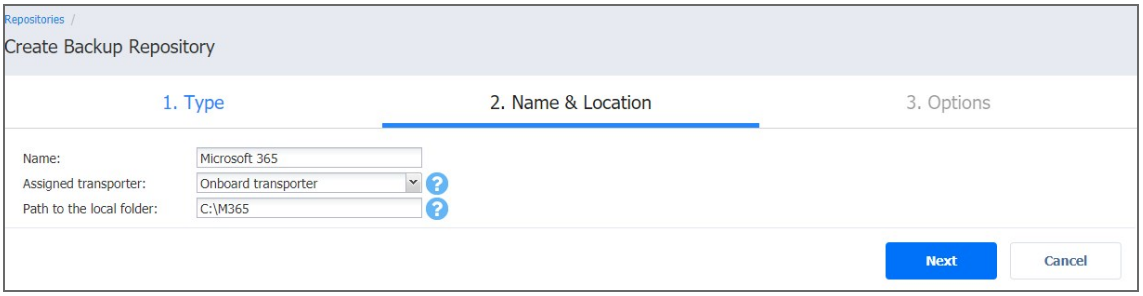
● SaaS
Directly attached storage or locally mounted share on an assigned transporter used for storing Microsoft 365 objects.

○ Deduplication Appliance
Integration with Dell EMC Data Domain Boost, HPE StoreOnce Catalyst and NEC HYDRAstor.

Create Backup Repository: Name and Location

On the **Name & Location** page of the wizard, do the following:

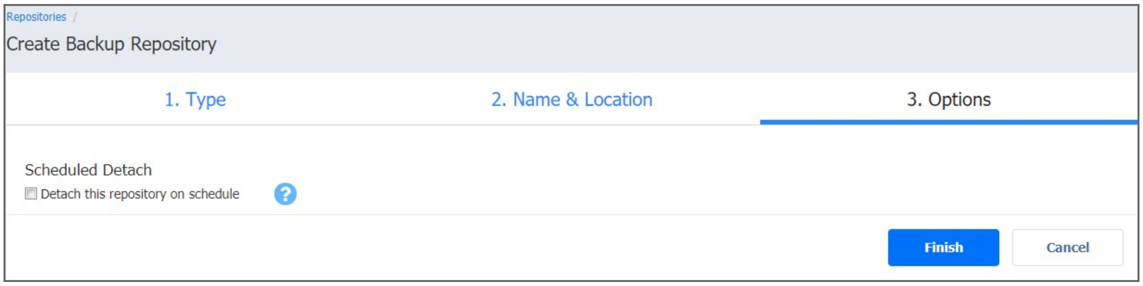
1. Enter the name of the Backup Repository in the **Name** box.
2. Select the Transporter from the **Assigned transporter** drop-down list.
3. Enter a path to the local folder in the corresponding box.
4. Click **Next** to go to the next page of the wizard.


Repositories /
Create Backup Repository
1. Type 2. Name & Location 3. Options
Name: Microsoft 365
Assigned transporter: Onboard transporter
Path to the local folder: C:\M365

Create Backup Repository: Options

On the **Options** page:

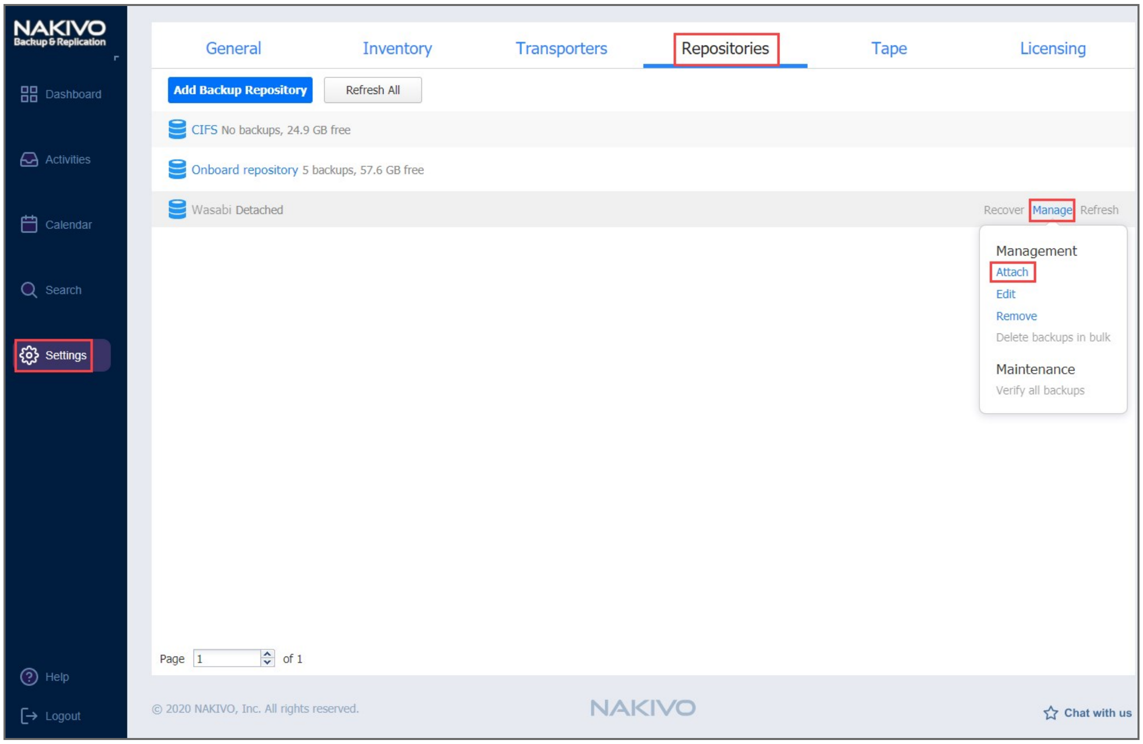
1. Schedule detaching of the Backup Repository
   - **Detach this repository on schedule:** Select this option if you want to detach and then attach the Backup Repository on a schedule. Detaching a Backup Repository saves the Backup Repository data and metadata in a consistent state and then stops the product's interaction with the Backup Repository (so that the Backup Repository can be copied or moved). You can use this feature, for example, for the disk-to-disk-to-tape (D2D2T) data protection approach, in which backups are stored on a disk for fast operational recovery, and copied to a tape (while the repository is detached) for archiving and long-term storage.
     - **Delete and re-create the repository on attach:** If this option is selected, all data in the Backup Repository will be erased prior to attaching it to the product. As a result, jobs that write to this Backup Repository will create full VM backups. You can use this option, for example, to create full daily, weekly, or monthly VM backups and write them to tape or removable media.
2. Click **Finish** to finish creating the Backup Repository.


Repositories /
Create Backup Repository
1. Type 2. Name & Location 3. Options
Scheduled Detach
☐ Detach this repository on schedule

Attaching Backup Repositories

If you have detached a Backup Repository, you can reattach it to the product by following the steps below:

1. Go to the main menu of NAKIVO Backup & Replication and click **Settings**.
2. Go to the **Repositories** tab and click a Backup Repository.
3. In the Backup Repository title, click **Manage** and then click **Attach.**



The Backup Repository is reattached to NAKIVO Backup & Replication. You can now back up to the attached Backup Repository.

Detaching Backup Repositories

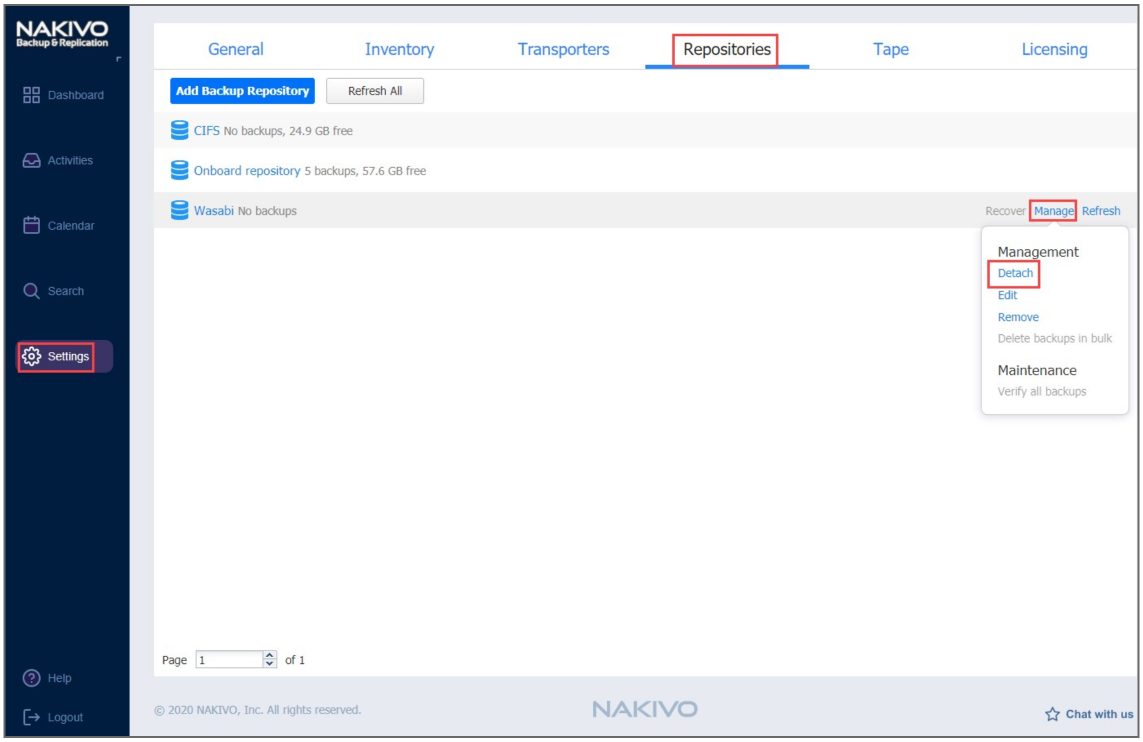
Detaching a Backup Repository saves the Backup Repository data and metadata in a consistent state and then stops the product's interaction with the Backup Repository (such as read and write of data and metadata, and so on). You may want to detach a Backup Repository in order to move it to a different location or to put the storage with the Backup Repository on maintenance.

Important

Since the product stops working with detached backup repositories, jobs that back up VMs to a detached Backup Repository will fail.

To detach a Backup Repository, follow the steps below:

1. Go to the main menu and click **Settings**.
2. Go to the **Repositories** tab and choose a Backup Repository.
3. In the Backup Repository title, click **Manage** and then click **Detach.**



Note

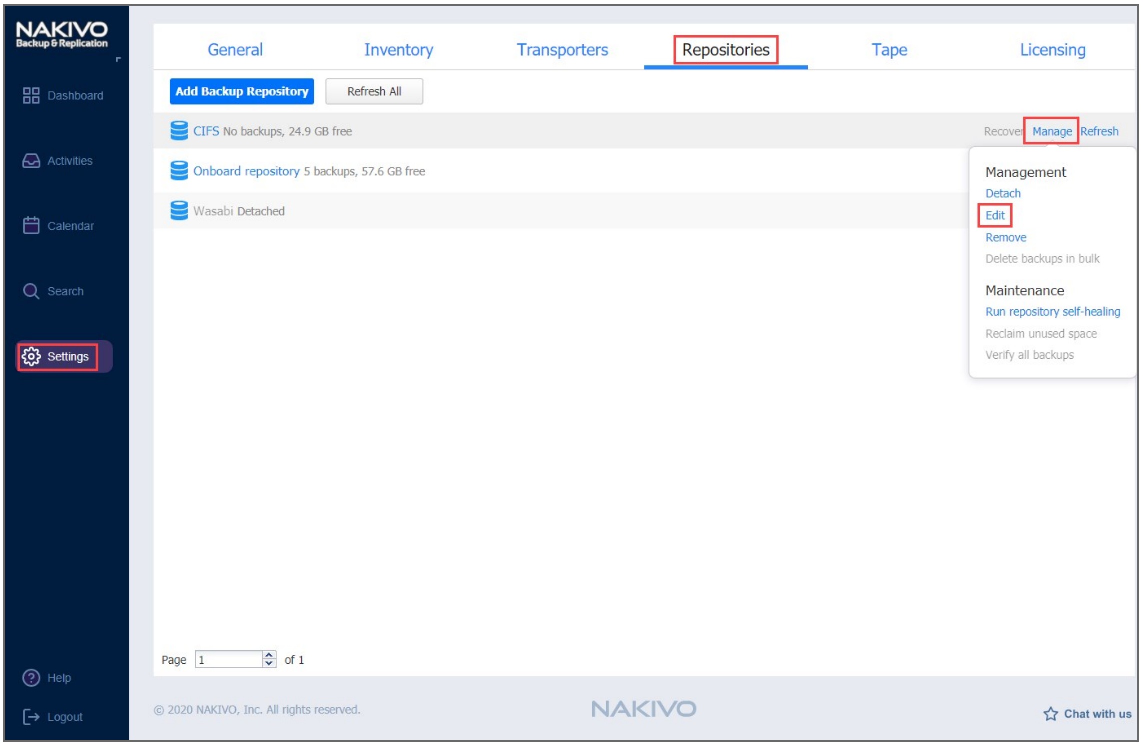
A Backup Repository cannot be detached if a job that backs up to this Backup Repository is running.

The Backup Repository is detached from the product. You can reattach the Backup Repository to NAKIVO Backup & Replication when needed.

Editing Backup Repositories

To modify the settings of an existing Backup Repository, follow the steps below:

1. Go to the main menu of NAKIVO Backup & Replication and click **Settings**.
2. Go to the **Repositories** tab and choose a Backup Repository.
3. In the Backup Repository title, click **Manage** and then click **Edit**.



CIFS No backups, 24.9 GB free

Onboard repository 5 backups, 57.6 GB free

Wasabi Detached

Note

A Backup Repository cannot be edited if there is a job that backs up to this Backup Repository is concurrently running.

4. Update the fields as necessary.
5. Click **Apply**. Changes you have made are applied and the Backup Repository update starts.

Refreshing Backup Repositories

By default, NAKIVO Backup & Replication refreshes information about Backup Repositories every hour. During the refreshing process, the product collects all required information about Backup Repositories (such as the amount of free space, number of backups and recovery points, and so on).

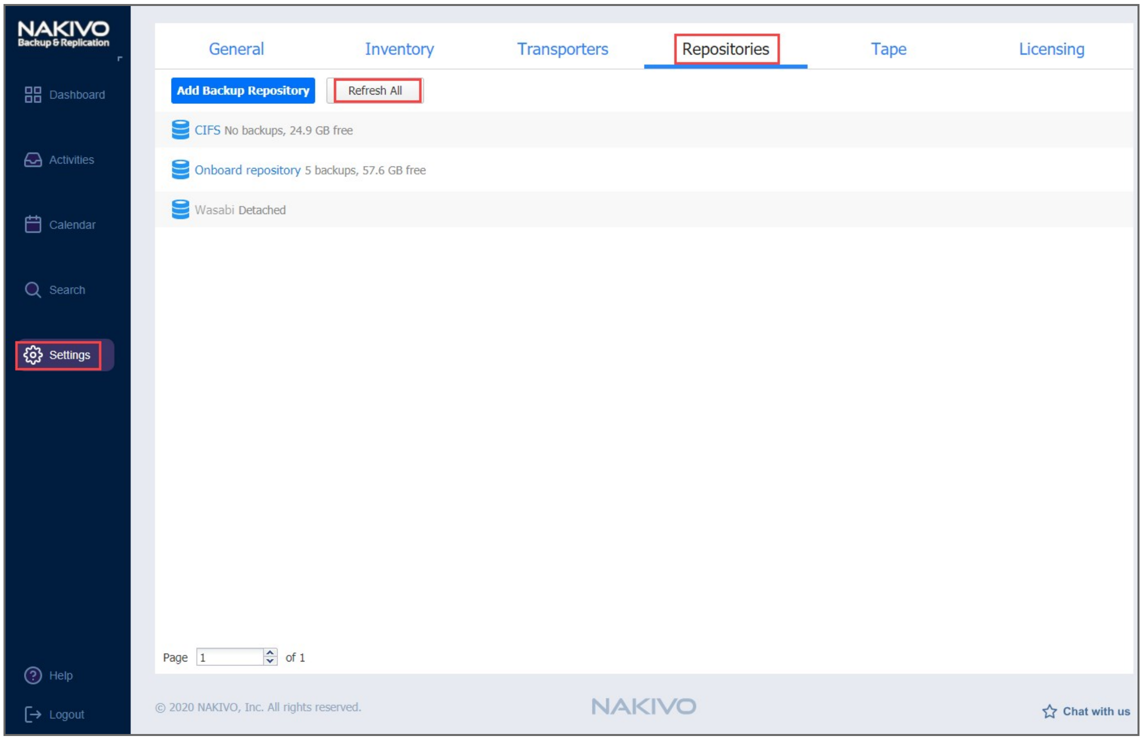
Only one Backup Repository is refreshed at a time. Therefore, if you have more than one Backup Repository, all others will remain in a queue.

- Refreshing All Backup Repositories
- Refreshing a Single Backup Repository

Refreshing All Backup Repositories

To refresh all backup repositories, follow the steps below:

1. Go to the main menu of NAKIVO Backup & Replication and click **Settings**.
2. Go to the **Repositories** tab.
3. Click **Refresh All.**

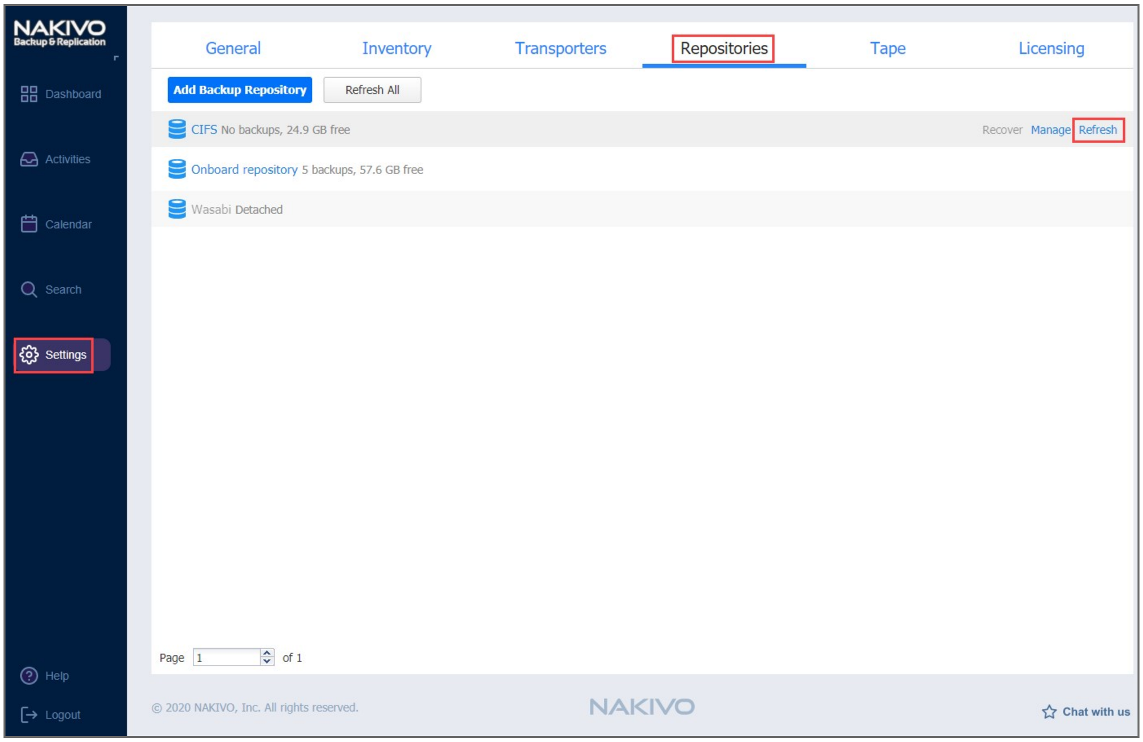


The Backup Repositories refresh starts.

Refreshing a Single Backup Repository

To update a single Backup Repository, follow the steps below:

1. Go to the main menu of NAKIVO Backup & Replication and click **Settings**.
2. Go to the **Repositories** tab.
3. Click the Backup Repository that you wish to update.
4. In the title of the Backup Repository, click **Refresh.**



CIFS No backups, 24.9 GB free

Onboard repository 5 backups, 57.6 GB free

Wasabi Detached

The Backup Repository refresh starts.

Removing and Deleting Backup Repositories

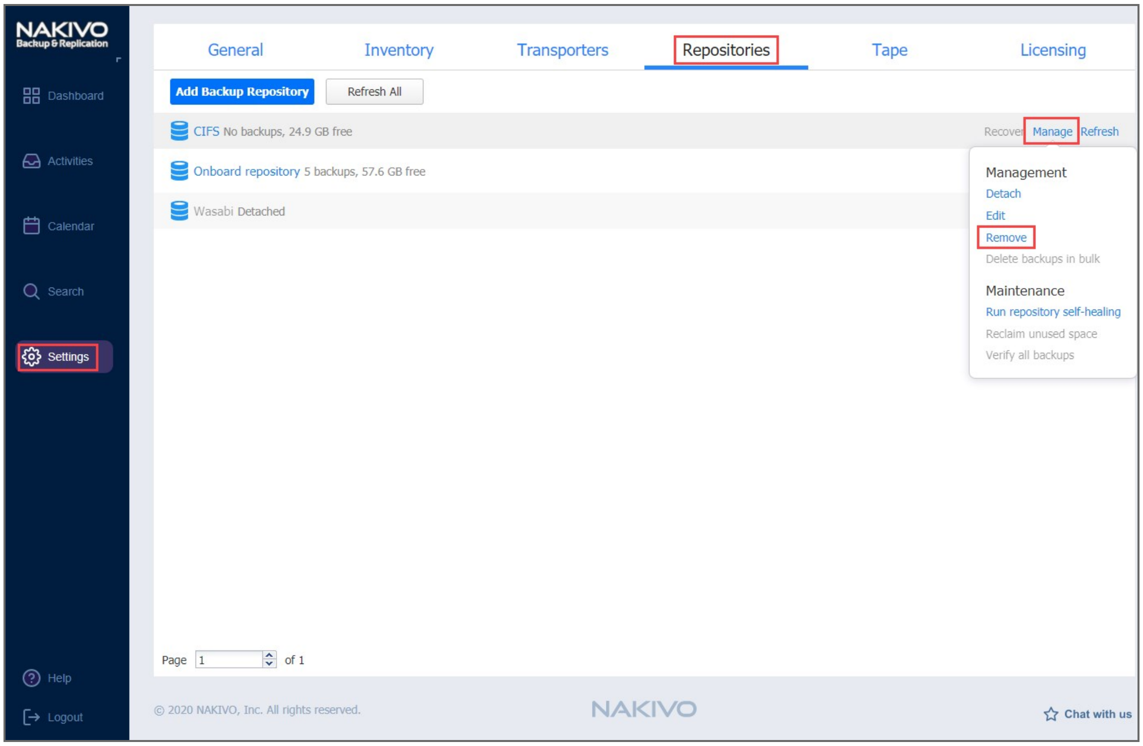
In NAKIVO Backup & Replication, you can either permanently delete a Backup Repository and all of its data or remove only the Backup Repository from the product while maintaining all of its data. After removing a Backup Repository you will be able to import it into the same or a new instance of the product.

Important

You will not be able to remove a Backup Repository if there is a job that backs up to this Backup Repository. To remove such a Backup Repository, you first need to delete (or edit) the corresponding jobs so no items are backed up to the Backup Repository that is being removed.

To permanently delete or remove a Backup Repository from the product, follow the steps below:

1. Go to the main menu of NAKIVO Backup & Replication and click **Settings**.
2. Go to the **Repositories** tab.
3. Click a Backup Repository.
4. In the Backup Repository title, click **Manage** and then click **Remove.**



5. Do the following when the confirmation message appears:
   - To remove the Backup Repository from NAKIVO Backup & Replication and keep the Backup Repository on a disk, click the **Remove Repository and Keep Backups** button.

     Note

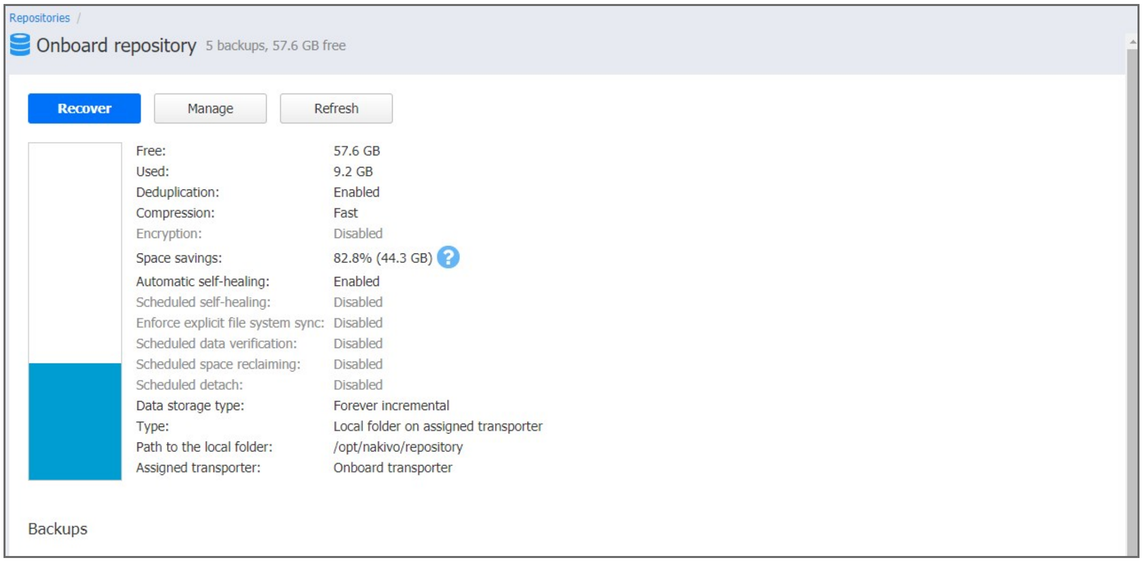
     You can import the removed Backup Repository back to the same or to new product installation.

- To permanently delete the Backup Repository and all its data, click the **Remove Repository and Delete Backups** button.
  Important
  This operation will permanently delete the Backup Repository and all VM backups.

Viewing Backup Repository Details

To view Backup Repository details, follow the steps below:

1. Go to the main menu of NAKIVO Backup & Replication and click **Settings**.
2. Go to the **Repositories** tab.
3. Click a Backup Repository.
4. The following data is displayed:



Repositories /

Onboard repository 5 backups, 57.6 GB free

Free:	57.6 GB
Used:	9.2 GB
Deduplication:	Enabled
Compression:	Fast
Encryption:	Disabled
Space savings:	82.8% (44.3 GB)
Automatic self-healing:	Enabled
Scheduled self-healing:	Disabled
Enforce explicit file system sync:	Disabled
Scheduled data verification:	Disabled
Scheduled space reclaiming:	Disabled
Scheduled detach:	Disabled
Data storage type:	Forever incremental
Type:	Local folder on assigned transporter
Path to the local folder:	/opt/nakivo/repository
Assigned transporter:	Onboard transporter

Backups

- **Free**: The amount of free space currently available for the Backup Repository.
- **Used**: The amount of space that the Backup Repository occupies on a disk. The amount of space that can be reclaimed is displayed in parentheses.
- **Deduplication**: The status of deduplication in the current Backup Repository.
- **Compression**: The compression level specified for the current Backup Repository.
- **Encryption**: The status of encryption in the current Backup Repository.
- **Space savings**: The estimated percentage and amount of space saved by compression and deduplication. For example, if 200 GB of data were backed up and the size of the backup was reduced to 50 GB, the ratio is calculated as 75%.
- **Automatic self-healing**: The current state of the automatic self-healing option for the Backup Repository.
- **Scheduled self-healing**: The current state of the scheduled self-healing option for the Backup Repository.
- **Enforce explicit file system sync**: The current state of the enforce explicit file system sync option for the Backup Repository.
- **Scheduled data verification**: The current state of the scheduled data verification option for the Backup Repository.
- **Scheduled space reclaiming**: The current state of the scheduled space reclaiming option for the Backup Repository.
- **Scheduled detach**: The current state of the scheduled detach option for the Backup Repository.

- **Data storage type**: The type of Backup Repository, which can be one of the following:
    - **Forever incremental**: After the initial full backup, all subsequent backups will transfer and store only changed data (increments) to the backup repository.
    - **Incremental with full backups**: After the initial full backup, backup jobs will store changed data (increments) in separate files and will periodically create full backups as specified in the job settings. Backup deduplication is not available when this option is selected.
- **Type**: The location of the Backup Repository, which can be one of the following:
    - **Local folder on the assigned Transporter**
    - **Remote CIFS Share**
    - **Remote NFS Share**
    - **Amazon EC2**
    - **SaaS**
    - **Amazon S3**
    - **Wasabi**
    - **Deduplication Appliance**
- **Path to the folder**: The path to the Backup Repository folder.
- **Assigned transporter**: The Transporter that manages the Backup Repository (i.e. reads data from and writes data to the Backup Repository).
- **Backups**: List of available backups in the Backup Repository.

Viewing Backup Details

Here you can view the details of the backups stored in the Backup Repository. The following information is displayed:

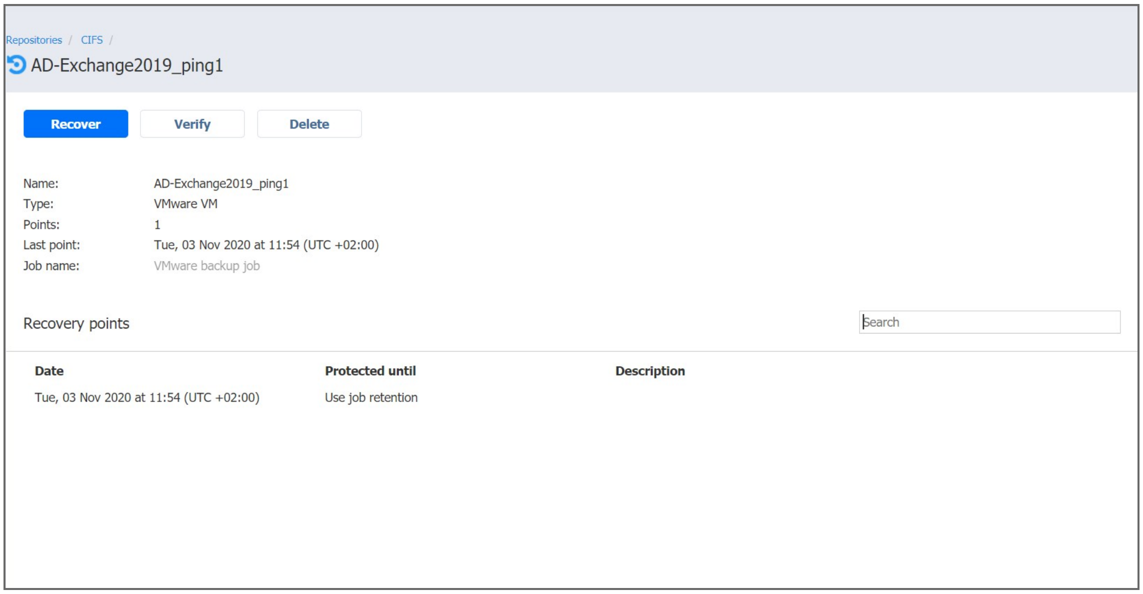
- **Name**: Name of the backup.
- **Job**: The job type that created this backup.

Hover over the name of the backup to select one of the following options that appear on the right side of the screen:

- **Recover**: Select this option to proceed with recovery.
- **Verify**: Select this option to verify the backup.
- **Delete**: Select this option to delete the backup from the repository.

Click on the backup name to view more information about the backup and see the recovery points available. The following information is displayed:

- **Name**: Name of the job.
- **Type**: Type of the job.
- **Points**: Number of recovery points available.
- **Last point**: Date of the latest recovery point.
- **Job name**: Name of the job.



Repositories / CIFS /

AD-Exchange2019_ping1

Name: AD-Exchange2019_ping1
Type: VMware VM
Points: 1
Last point: Tue, 03 Nov 2020 at 11:54 (UTC +02:00)
Job name: VMware backup job

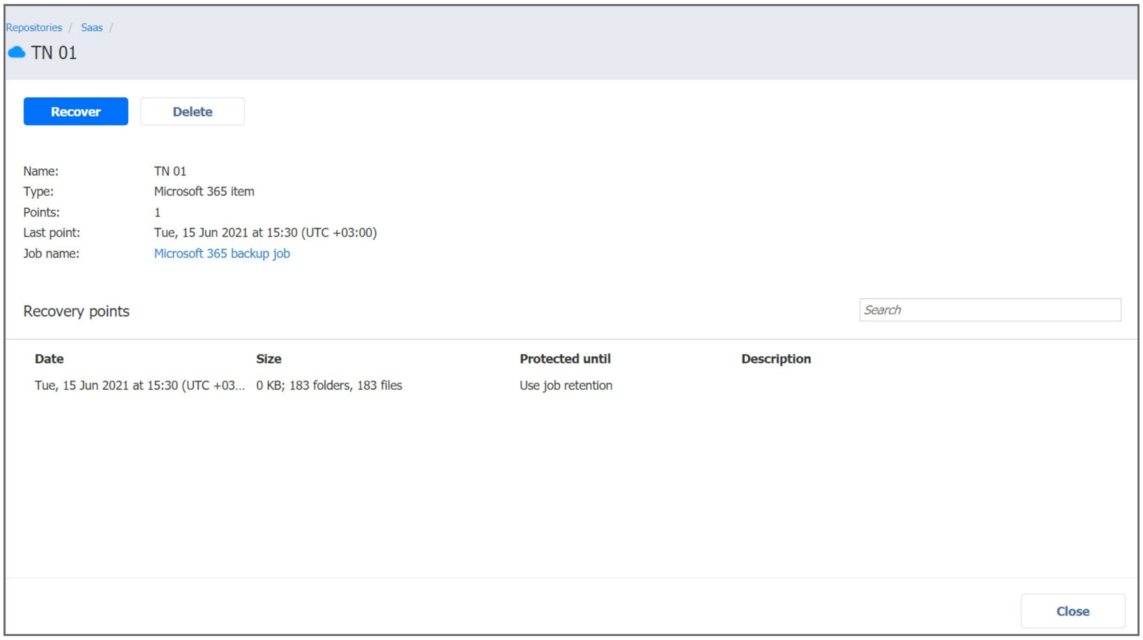
Recovery points

Date	Protected until	Description
Tue, 03 Nov 2020 at 11:54 (UTC +02:00)	Use job retention	

Viewing Recovery Point Details

You can view the details of the recovery point in the lower part of the screen. The following information is displayed:

- **Date**: Date of the recovery point.
- **Size**: Size of the recovery point.
- **Type**: Type of the backup used for this recovery point.
- **Protected until**: The date until which the recovery point remains protected.
- **Description**: Description of the recovery point.



Repositories / Saas /

TN 01

Name: TN 01
Type: Microsoft 365 item
Points: 1
Last point: Tue, 15 Jun 2021 at 15:30 (UTC +03:00)
Job name: Microsoft 365 backup job

Recovery points

Date	Size	Protected until	Description
Tue, 15 Jun 2021 at 15:30 (UTC +03...	0 KB; 183 folders, 183 files	Use job retention	

Note

Size and **Type** are displayed only if the Backup Repository has **Incremental with full backup data storage** type selected.

Date, Type, and Description can also be viewed when selecting recovery points in Recovery Job Wizard. Hover over the name of the recovery point to select one of the following options that appear on the right side of the screen:

- **Recover**: Select this option to proceed with recovery.
- **Edit**: Select this option to edit the recovery point. Do the following:
    - Optionally, you can add the **description** to your recovery point.
    - Choose the date until which the recovery point should remain protected. The following options are available:
        - **Use job retention**: Choose this option to use the retention settings selected in the job for this recovery point.
        - **Keep forever**: Choose this option to keep this recovery point forever.
        - **Protect until**: Choose this option to protect this recovery point until a specific date. After selecting this option, choose the date in the calendar.
- **Delete**: Select this option to delete the recovery point from the repository.

Virtual Appliance Configuration

This section covers the following topics:

- “Configuring Network Settings of Virtual Appliance” on page 293
- “Increasing Backup Repository Size on Virtual Appliance” on page 294
- “Removing the Disk with Backup Repository from Virtual Appliance” on page 295

Configuring Network Settings of Virtual Appliance

To configure networking on the Virtual Appliance (VA), follow the steps below:

1. Open the VA console.
2. On the main menu, select the **Network Settings** option and press **Enter**.
3. Do either of the following:
    - To change the Virtual Appliance hostname, select the **Hostname** option, press **Enter**, enter a new hostname, and press **Enter** again.
    - To configure a network card, select it and press **Enter**. Press **Enter** to switch between DHCP and manual network settings. If you set the **DHCP** option to **disabled**, you can manually set up network settings by selecting an option, pressing **Enter**, entering a new value, and pressing **Enter** again. Press **F10** to save your changes and exit.

Increasing Backup Repository Size on Virtual Appliance

A Backup Repository on a Virtual Appliance (VA) is located in a logical volume (that can spread across multiple physical volumes). To extend the Backup Repository size on the VA, you need to add a new disk to the VA and then use the VA console to extend the Backup Repository to the new disk.

The Backup Repository size on the VA cannot be increased by extending existing VA disks.

The backup repository size on the VA cannot be increased by extending existing VA disks. To increase the size of the backup repository on the Virtual Appliance, follow the steps below:

1. Attach a new disk to the VA.
2. Open the VA console in your hypervisor's client.
3. Run the following commands in the VA console depending on the NAKIVO Backup & Replication version you use:
   - For the product Version 8.1 and higher:
     a. Select **Manage NAKIVO services** in the main menu and press **Enter**.
     b. Select **Onboard repository storage** and press **Enter**.
   - For earlier product versions, select **Backup storage** in the main menu and press **Enter**.
4. Refresh the list of disks by pressing **F5**.
5. Select the disk that you have created and press **Enter**.
6. Press **Enter** again to confirm the procedure. The disk is formatted and added to the Backup Repository on the VA.

Removing the Disk with Backup Repository from Virtual Appliance

The Virtual Appliance (VA) comes with a 500 GB disk on which a Backup Repository is created. If you have deployed the Virtual Appliance disks using the **Thin Provision** option, then the disk does not consume 500 GB of space on your datastore – only the space occupied by VM backups is consumed.

If you still would like to delete the 500GB disk after you have deployed the Virtual Appliance, follow the steps below:

1. Log in to NAKIVO Backup & Replication.
2. Go to the **Configuration** > **Repositories** tab.
3. Click **Onboard repository**
4. Click **Manage** and choose **Remove** from the menu.
5. In the message that opens, click the **Remove Repository and Delete Backups** button.
6. Click **Remove** to confirm that you wish to remove the Backup Repository.
7. Open the vSphere client and launch the console of the VA.
8. In the Virtual Appliance interface, select the **Exit to system console** option and press **Enter**.
9. Enter a login and password (default are `root/roo`t).
10. Run the following command to unmount the volume on which the Backup Repository is located: `umount /opt/nakivo/repository`
11. Open the configuration file with the `nano` editor by running the following command: `nano/etc/fstab`
12. In the editor, delete the line: `dev/mapper/Volume_Group_Backup_Repository_500GB/Logical_Volume_Backup_Repository_500GB /opt/nakivo ext4 defaults 0 2`
13. Save changes by pressing **Ctrl+O**, and then pressing **Enter**.
14. Exit the editor by pressing **Ctrl+X**.
15. Power off the VA and delete the 500 GB disk.

Multi-Tenant Mode Configuration

This section covers the following topics:

Changing Login and Password in Multi-Tenant Mode

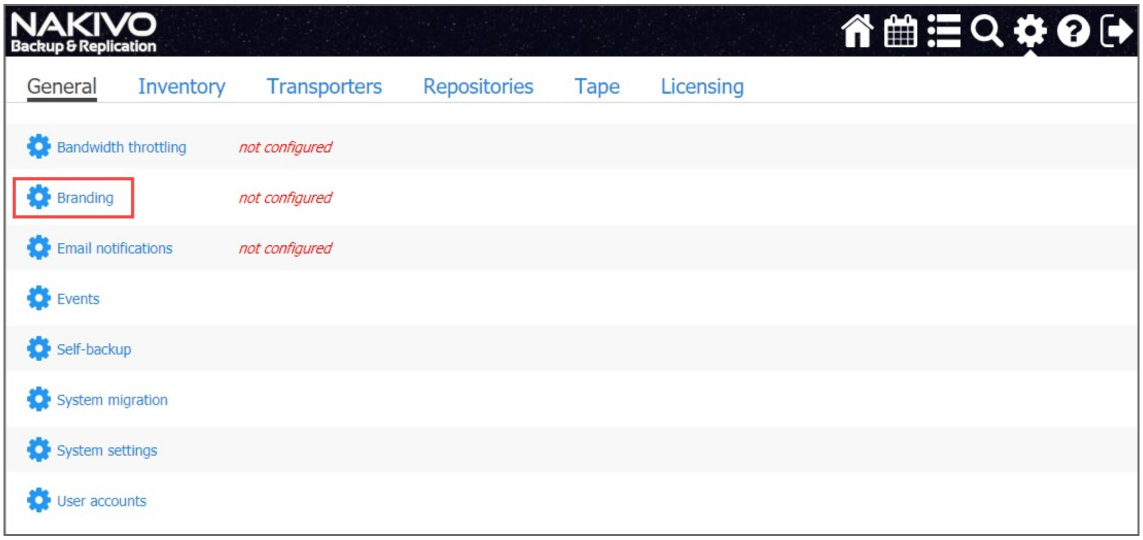
To change the login and password of the Master Admin, follow the steps below:

1. Log in to NAKIVO Backup & Replication as a Master Admin.
2. Click **Configuration** in the upper right corner of the product.
3. Go to the **General** tab and click **Users and Roles**.
4. In the list of users that opens, click the Master Admin user.
5. For the Master Admin, enter data in the **Login, Password**, **Confirm Password**, and **Admin email** boxes and click **Apply.**

Configuring Branding Settings in Multi-Tenant Mode

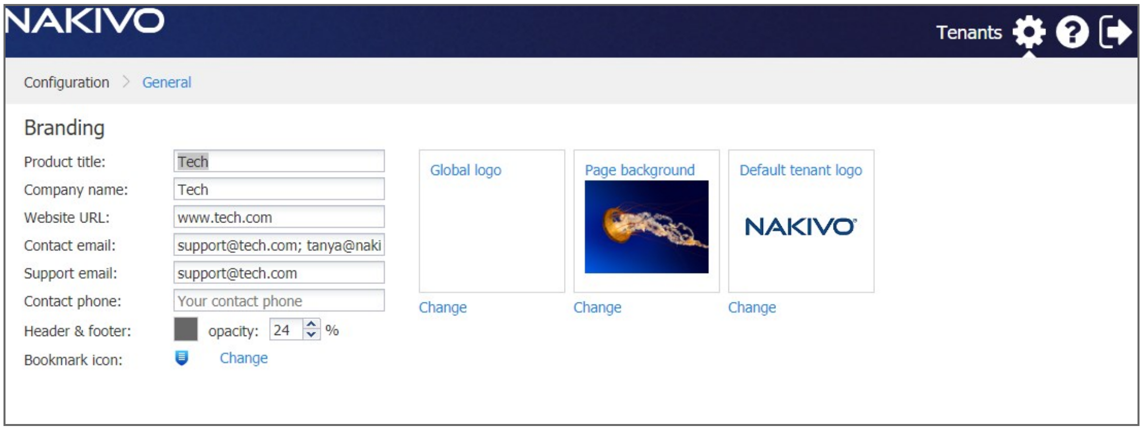
In the multi-tenant mode, you can change the product branding settings such as product name, logo, background, and so on. To configure the system settings, follow the steps below:

1. Log in to NAKIVO Backup & Replication as a Master Admin.
2. Click **Configuration** in the upper right corner of the product.
3. Go to the **General** tab and click **Branding**.



Bandwidth throttling	*not configured*
Branding	*not configured*
Email notifications	*not configured*
Events	
Self-backup	
System migration	
System settings	
User accounts	

4. Do the following:
   - To change the product title, company name, website URL, contact email, support email, and contact phone, type a new value in the appropriate field
   - To change the product logo, background, and default tenant logo, click **Change** under the appropriate box, select a new image, and click **Open**.



Branding

Product title:	Tech
Company name:	Tech
Website URL:	www.tech.com
Contact email:	support@tech.com; tanya@naki
Support email:	support@tech.com
Contact phone:	Your contact phone
Header & footer:	■ opacity: 24 %
Bookmark icon:	Change

5. Click **Apply**.

NOTE: During upload, the logo and bookmark icon images are resized internally while preserving the aspect ratio. The background image is used as it is. To get the best image quality, follow the recommendations below:

Image	**Best format**	**Best resolution**
Global logo	.png	40x40
Page background	.jpeg	1920x1440
Bookmark icon	.png	16x16
Default tent logo	.png	120x95

Configuring Email Notifications in Multi-Tenant Mode

NAKIVO Backup & Replication can send notifications and reports over email. To configure the email notifications, follow the steps below:

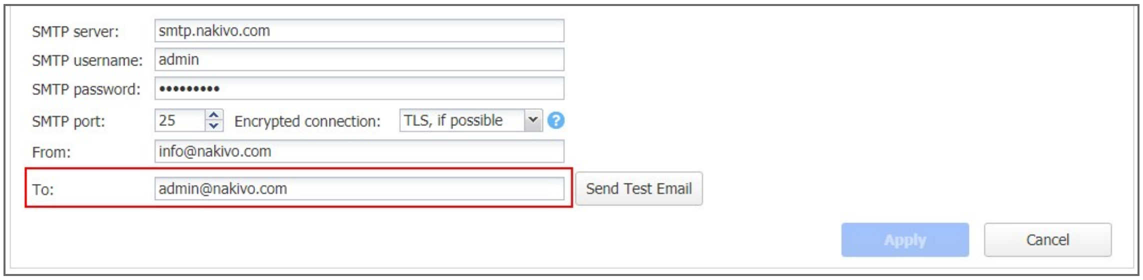
1. Make sure you have configured your email settings.
2. Log in to NAKIVO Backup & Replication as a Master Admin.
3. Click **Configuration** in the upper right corner of the product and go to the **General** tab.
4. Click **Email settings**.
5. In the **Email Notifications** section, select the options as appropriate:
   a. **Send alarm (error) notifications**: If selected, this will send notifications about a job, repository, infrastructure, connection, and other failures to email addresses specified in the text field. Use a semicolon to separate multiple email addresses.
   b. **Send warning notifications**: If selected, this will send warning notifications on non-critical events, such as infrastructure change, to email addresses specified in the text field. Use a semicolon to separate multiple email addresses.
   c. **Limit email notification frequency to**: Set a limit to how often email notifications are sent.
6. In the **Automatic Reports** section, select or deselect the following automatic reports options:
   - **Attach PDF copy to automatic reports**: Specify whether you wish to include a copy of the PDF report with notifications.
   - **Send tenant Overview reports on schedule to**: If this option is selected, NAKIVO Backup & Replication will generate an Overview report (which includes information about all jobs and groups in the product) on the date and time specified in the scheduler and will send the report to the recipients specified in the text field. Use a semicolon to separate multiple email addresses.
   - **Send tenant Protection Coverage reports on schedule to**: If this option is selected, NAKIVO Backup & Replication will generate the Protection Coverage report (which includes information about all VMs & instances protected by backup and/or replication jobs as well as the information about all unprotected VMs & instances) on the date and time specified in the scheduler and will send the report to the recipients specified in the text field. Use a semicolon to separate multiple email addresses.
   - Click **Apply**.

Configuring Email Settings in Multi-Tenant Mode

Configure email settings so that NAKIVO Backup & Replication can send email notifications as well as reports over email. If email settings are not configured, tenants will not be able to configure email notifications for their jobs. To configure email settings**,** follow the steps below:

1. Log in to NAKIVO Backup & Replication as a Master Admin.
2. Click **Configuration** in the upper right corner of the product.
3. Go to the **General** tab and click **Email notifications**.
4. In the **Email Settings** section, enter data in the boxes, and click **Send Test Email** to verify the settings are correct.

After the email settings are configured, you can configure the product email notifications.



SMTP server: smtp.nakivo.com

SMTP username: admin

SMTP password: •••••••••

SMTP port: 25 Encrypted connection: TLS, if possible

From: info@nakivo.com

To: admin@nakivo.com

Configuring System Settings in Multi-Tenant Mode

To configure the system settings, follow the steps below:

1. Log in to NAKIVO Backup & Replication as a Master Admin.
2. Click **Configuration** in the upper right corner of the product.
3. Go to the **General** tab and click **System settings**.
4. Select or deselect the following options:
    - **Store system events for the last X days**: This option specifies the time period (from 10 to 365 days) during which the application events will be kept. Older events are automatically deleted.
    - **Auto log out after X minutes of inactivity**: If this option is selected, the current user will be automatically logged out of the product after the specified period of inactivity.
    - **Auto upload support bundles to support team server**: If this option is enabled, NAKIVO Backup & Replication will automatically create, encrypt, and upload support bundles once a day to a NAKIVO support server during the evaluation period. The NAKIVO Support team may use this information to improve the product experience and will be able to identify and resolve product issues faster.
    - **Enable built-in support chat:** If selected, this will allow you to chat with the NAKIVO support team.
    - **Display special offers**: If selected, this will show a toolbar with special offers in the GUI.
    - **Continue product update if self-backup fails**: If selected, product update will proceed even if automatic self-backup cannot be performed.
    - **Tape options**: These present you with setting options for tape devices:
        - **Auto erase expired tapes**: If selected, expired tape cartridges will be erased automatically.
        - **Wait for next tape for**: Specify for how long the system needs to wait for the next tape cartridge if there is no appropriate one. Select the **Send email notification** checkbox to allow you to receive email notifications.
        - **Auto refresh tapes every**: Select how often the contents of tape cartridges are to be refreshed in minutes or hours. Deselect if no refreshing is required.
    - **Regional options**: Set the clock format, short date format, long date format, first day of the week, decimal symbol, and default time zone in the corresponding fields.

- In the **Web Interface TLS/SSL Certificate** section, you can either**:**
    - **View current certificate**: A dialog containing the current certificate information opens.
    - **Install new certificate**: A dialog opens, allowing you to install a new TLS/SSL certificate for the NAKIVO Backup & Replication web interface. Certificates are generated either internally or through certification authorities. Proceed as follows to install a new certificate:
        - Click **Browse** and navigate to the location of either of the following certificate file types:
            - **Private key**: A file in the *.key format.
            - **Private key password (optional)**: A password for your private key.
            - **Certificate file**: A file in the *.pem, *.crt, *.cer, *.p7b, or *.p7s format.

    - **Intermediate certificate (optional)**: A file in the *.pem, *.crt, *.cer, *.p7b, *.p7s format.
- Click Install.

Note

In the Web Interface TLS/SSL Certificate section, you can see a notification about imminent TLS/SSL certificate expiration in 30 days and onwards. If your certificate has expired, you will be asked to install a valid certificate.

Exporting and Importing Configuration in Multi-Tenant Mode

System configuration export and import are recommended for easy migration to new product deployment. System configuration, such as jobs, user credentials, inventory items, Transporter and Backup Repository settings, is all exported into a single export bundle.

The export bundle can be applied to a new deployment.

To export system configuration from the old deployment, follow the steps below:

1. Open **Configuration** of the old deployment.
2. Go to the **General** tab and click **System migration**.
3. Click **Export system configuration**.
4. In the dialog box that opens, click **Export**.
5. Click **Proceed** to confirm the operation.

   Note

   All activities in the old deployment (such as jobs and recovery sessions) will be automatically stopped and disabled.
6. Wait until the export is completed, and download the export bundle.

To import system configuration into the new deployment, follow the steps below:

1. Open **Configuration** of the new deployment.
2. Go to the **General** tab and click **System migration**.
3. Click **Import system configuration**.
4. In the dialog window that appears, locate the export bundle using the **Browse** button.
5. Click **Import**.
6. Click **Proceed** to confirm the operation.

   Note

   If there is any existing data in the new deployment, it will be overwritten with the import operation.
7. Wait until the import is completed, and close the dialog box.

Notes

- Data contained in backup repositories is not migrated to the new location automatically. If you are using a locally attached Backup Repository, the physical data must be copied or moved to the new location manually. After moving the files you may need to edit the Backup Repository settings in the new deployment so that the new settings refer to the actual Backup Repository location.
- If a custom TLS/SSL certificate of the Web server was used in the old deployment, a manual service restart will be required in the new deployment.

Support Bundles

NAKIVO Backup & Replication provides you with the ability to create support bundles – a zipped collection of the product logs and system information. Sending a support bundle to the NAKIVO Support Team allows them to quickly identify the root cause of issues and suggest a proper solution.

- Creating Support Bundles
- Sending Support Bundles

Creating Support Bundles

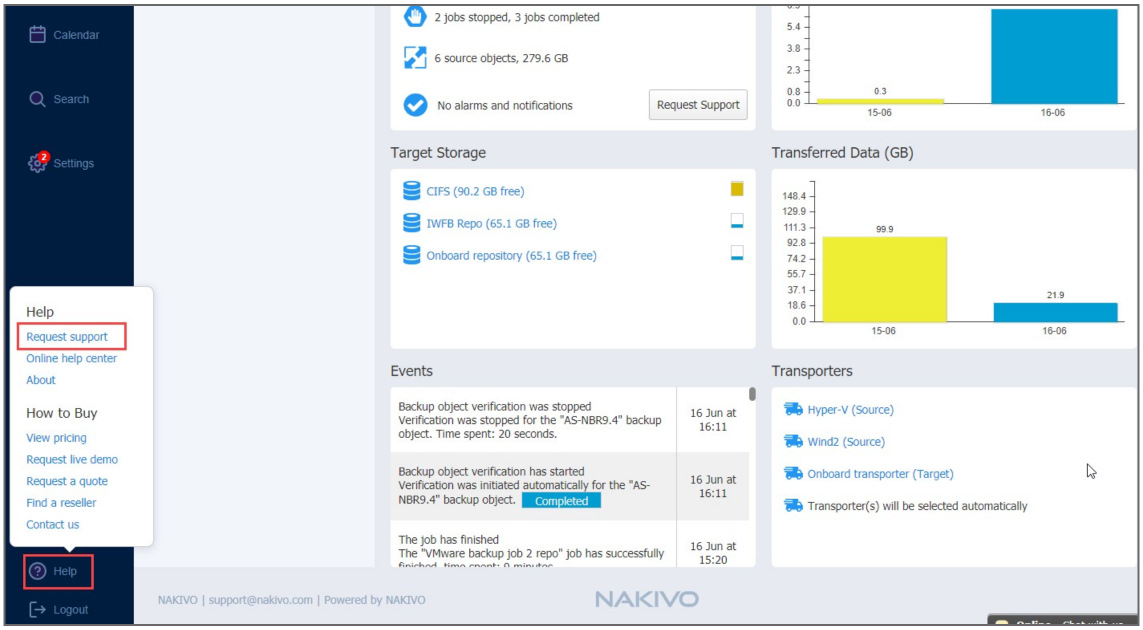
To create a support bundle, follow the steps below:

Important

Before creating a support bundle, make sure Email settings are configured.

1. Click the **"?" (help)** icon in the lower-left corner of the web UI.
2. Select and click **Request support** . The dialog box will appear.
3. Enter a description of your problem in the **Please describe the problem you're experiencing** box.
4. Enter your email address in the **Contact email** box.
5. If necessary, upload an attachment by clicking **Browse**.
6. Select **Include logs of all tenants** if you wish to include log files of all tenants to the support bundle.
7. Select **Include main database** if you want to include your main database.
8. Select **Include tenant databases** if you wish to include tenant databases containing most of the tenant configuration, including inventory, transporters, repositories, and jobs.
9. Click **Create & Send Support Bundle** to send the support bundle to NAKIVO Support Team. You will receive an answer from the NAKIVO Support Team within one business day.

10. Optionally, click **Download** to save the support bundle on your machine.



2 jobs stopped, 3 jobs completed

6 source objects, 279.6 GB

No alarms and notifications

CIFS (90.2 GB free)

IWFB Repo (65.1 GB free)

Onboard repository (65.1 GB free)

Backup object verification was stopped
Verification was stopped for the "AS-NBR9.4" backup object. Time spent: 20 seconds.
16 Jun at 16:11

Backup object verification has started
Verification was initiated automatically for the "AS-NBR9.4" backup object. Completed
16 Jun at 16:11

The job has finished
The "VMware backup job 2 repo" job has successfully
16 Jun at 15:20

Hyper-V (Source)

Wind2 (Source)

Onboard transporter (Target)

Transporter(s) will be selected automatically

NAKIVO | support@nakivo.com | Powered by NAKIVO

Sending Support Bundles Manually

Some support bundles may become overly large in size. This can occur due to large log files or file dumps. In such cases, it is recommended to upload these files manually.

To do this, follow these steps:

1. Open the Upload Files to NAKIVO Supportpage.
2. In the *Files* section, click **Browse** and select up to three files. You can select more than three files by clicking **Add Another File**.

   Note

   You can upload any files relevant to your issue: logs, file dumps, or the support bundles that you have manually downloaded from the product's UI.
3. Enter your email address in the **Contact email** field.
4. You can also enter the ID of your support ticket in the **Ticket ID** field if you have one opened.
5. Optionally, enter a description in the **Description** field.
6. Click **Upload** when you’re done uploading the file(s).

   Note

   Wait for a successful upload notification before closing the page.

Built-in Support Chat

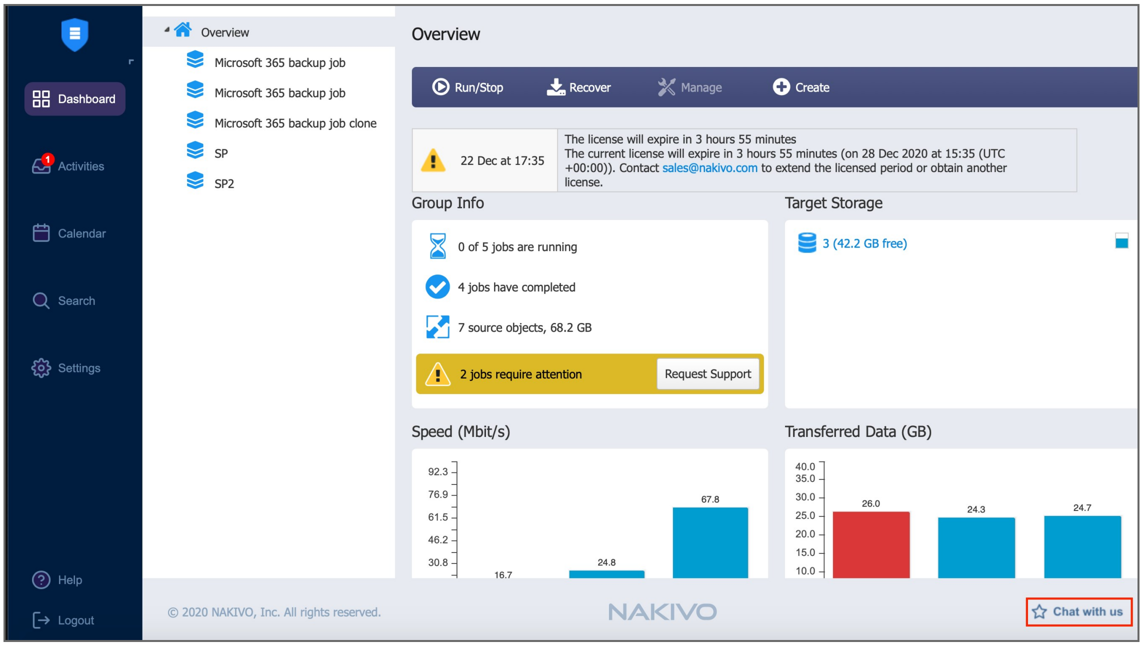
You have the possibility to contact a NAKIVO representative via chat in the NAKIVO Backup & Replication interface.

- Opening Built-in Support Chat
- Sending Files in Built-in Support Chat
- Sending Feedback to Built-in Support Chat
- Sending Email Transcript of Built-in Support Chat
- Disabling/Enabling Sound Notifications
- Disabling Built-in Support Chat

Opening Built-in Support Chat

To open Built-in Support Chat, follow the steps below:

1. In the lower right corner of the NAKIVO Backup & Replication interface, click the chat button.



22 Dec at 17:35

The license will expire in 3 hours 55 minutes

The current license will expire in 3 hours 55 minutes (on 28 Dec 2020 at 15:35 (UTC +00:00)). Contact sales@nakivo.com to extend the licensed period or obtain another license.

0 of 5 jobs are running

4 jobs have completed

7 source objects, 68.2 GB

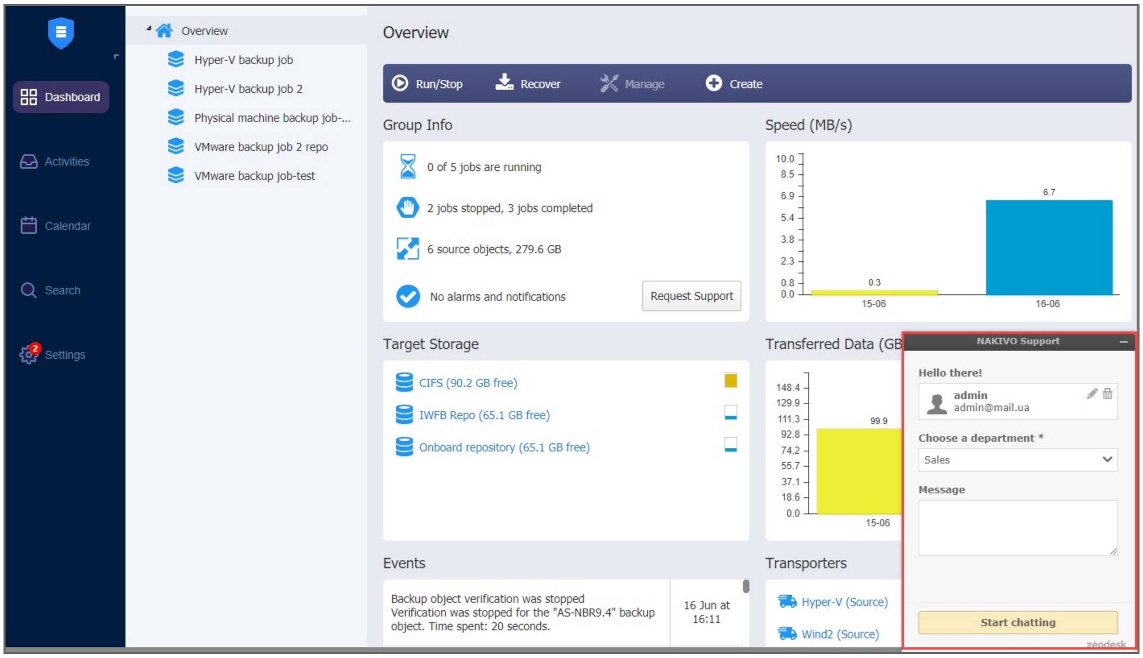
2 jobs require attention

3 (42.2 GB free)

© 2020 NAKIVO, Inc. All rights reserved.

2. The **NAKIVO Support** dialog box opens. Introduce yourself by providing the following information:
   a. In the upper box of the dialog box, enter your name.
   b. In the box below, enter your email address.
3. Choose a department from the list of available departments.

4. Enter your message text and click **Start Chatting**.



0 of 5 jobs are running

2 jobs stopped, 3 jobs completed

6 source objects, 279.6 GB

No alarms and notifications

CIFS (90.2 GB free)

IWFB Repo (65.1 GB free)

Onboard repository (65.1 GB free)

Backup object verification was stopped
Verification was stopped for the "AS-NBR9.4" backup object. Time spent: 20 seconds.
16 Jun at 16:11

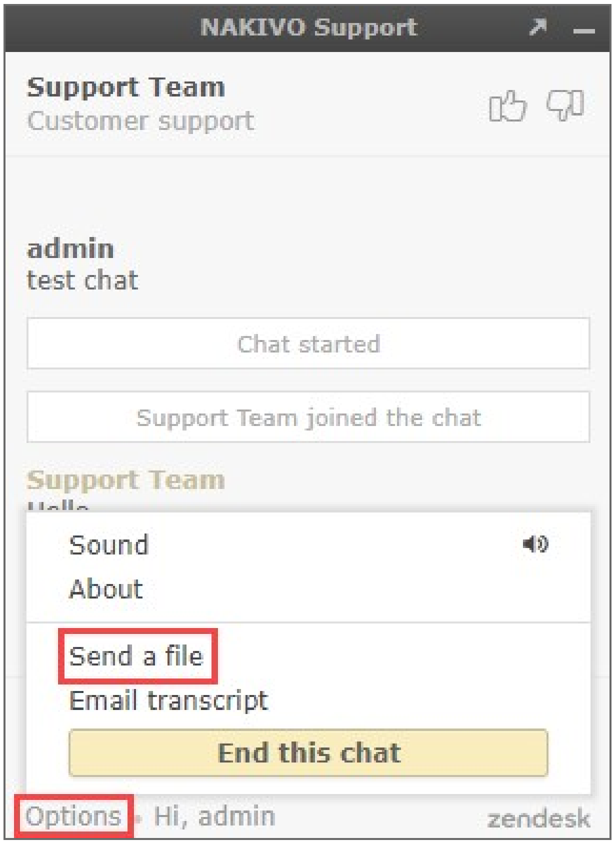
5. Your message is sent to a NAKIVO representative and will be processed as soon as possible. If needed, click the **Send Another** button to proceed with sending another chat message.

Sending Files in Built-in Support Chat

Please use either of the following ways to send your files in Built-in Support Chat:

- Drag and drop: open **Windows File Explorer**, select necessary files, and then drag them and drop to the chat dialog.
- Built-in Support Chat interface:
  1. In the upper left corner of the Built-in Support Chat dialog, click **Options**.
  2. In the dialog that opens, click **Send a file**.

3. The **Open** dialog opens. Navigate to the location of your files, select them and then click **Open**.



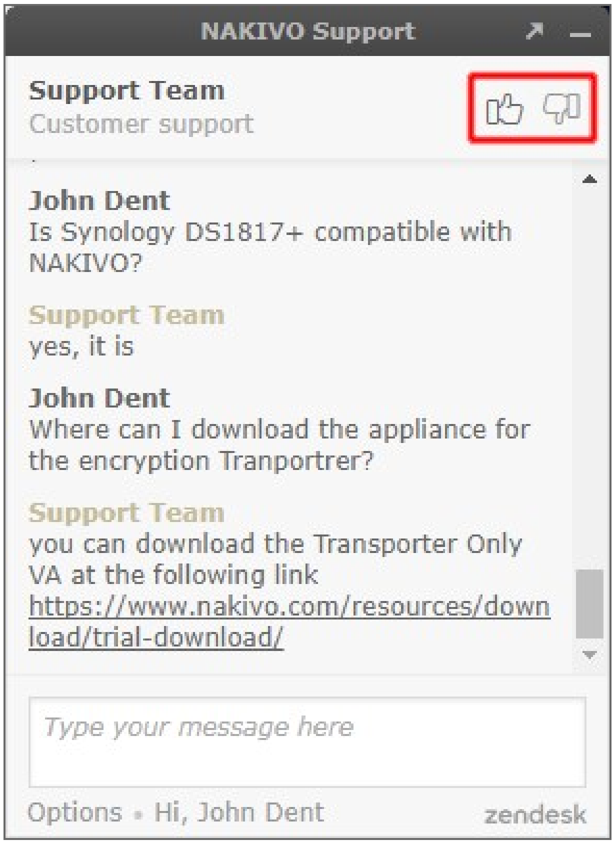
Note

The following file formats are allowed: `.pdf, .png, .jpeg, .gif, .txt`. The maximum file size is 20 MB.

Sending Feedback to Built-in Support Chat

You have the possibility of sending feedback to Built-in Support Chat: in the upper right corner of the dialog, click **Good** or **Bad**, as you deem appropriate.

If appropriate, leave a comment for NAKIVO Support Team: click **Leave a comment** and in the text box that opens, enter your comment about the chat service. Then click **Send**.



NAKIVO Support

Support Team
Customer support

John Dent
Is Synology DS1817+ compatible with NAKIVO?

Support Team
yes, it is

John Dent
Where can I download the appliance for the encryption Tranportrer?

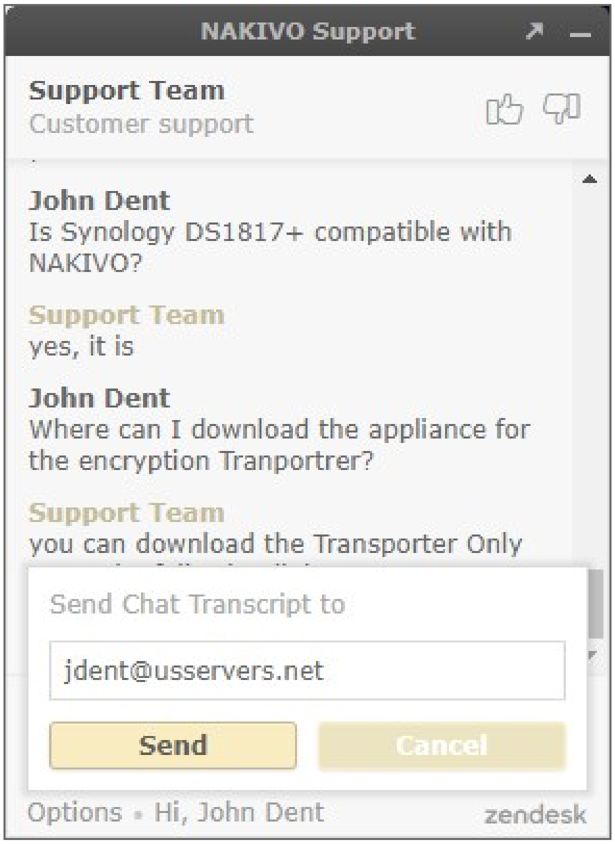
Support Team
you can download the Transporter Only VA at the following link https://www.nakivo.com/resources/download/trial-download/

Sending Email Transcript of Built-in Support Chat

Follow the steps below to send the transcript of your Built-in Support Chat session:

1. In the upper left corner of the Built-in Support Chat dialog, click **Options**.
2. In the dialog that opens, click **Email transcript**.
3. In the dialog that opens, make sure the email address of the recipient is correct, and then click **Send**.

Your Built-in Support Chat transcript will be sent to the specified email recipient.



John Dent
Is Synology DS1817+ compatible with NAKIVO?

Support Team
yes, it is

John Dent
Where can I download the appliance for the encryption Tranportrer?

Support Team
you can download the Transporter Only

Send Chat Transcript to

jdent@usservers.net

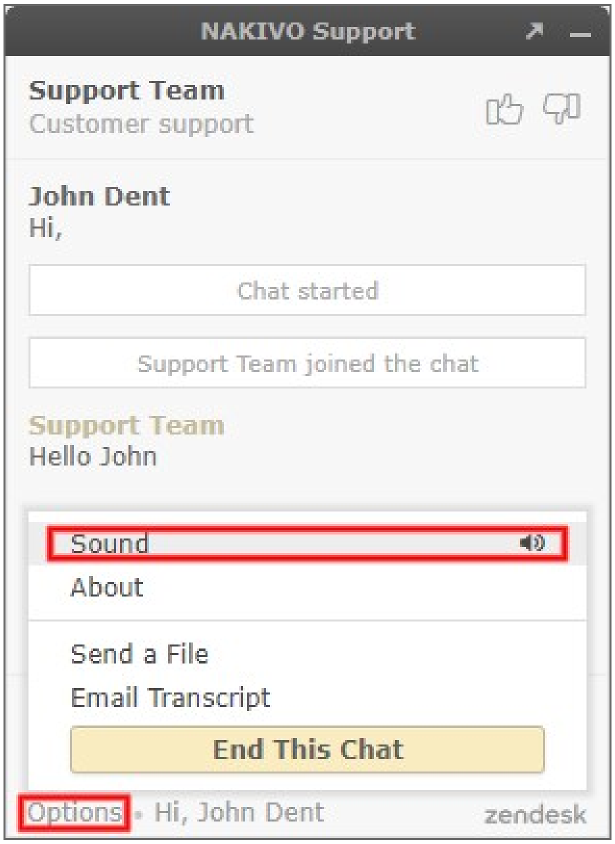
Disabling/Enabling Sound Notifications

By default, sound notifications are enabled for Built-in Support Chat.

Do the following to disable sound notifications in Built-in Support Chat:

1. In the upper left corner of the Built-in Support Chat dialog, click **Options**.
2. In the dialog that opens, click **Sound**.
3. Close the options dialog.

Sound notifications will be disabled for Built-in Support Chat.



NAKIVO Support

Support Team
Customer support

John Dent
Hi,

Chat started

Support Team joined the chat

Support Team
Hello John

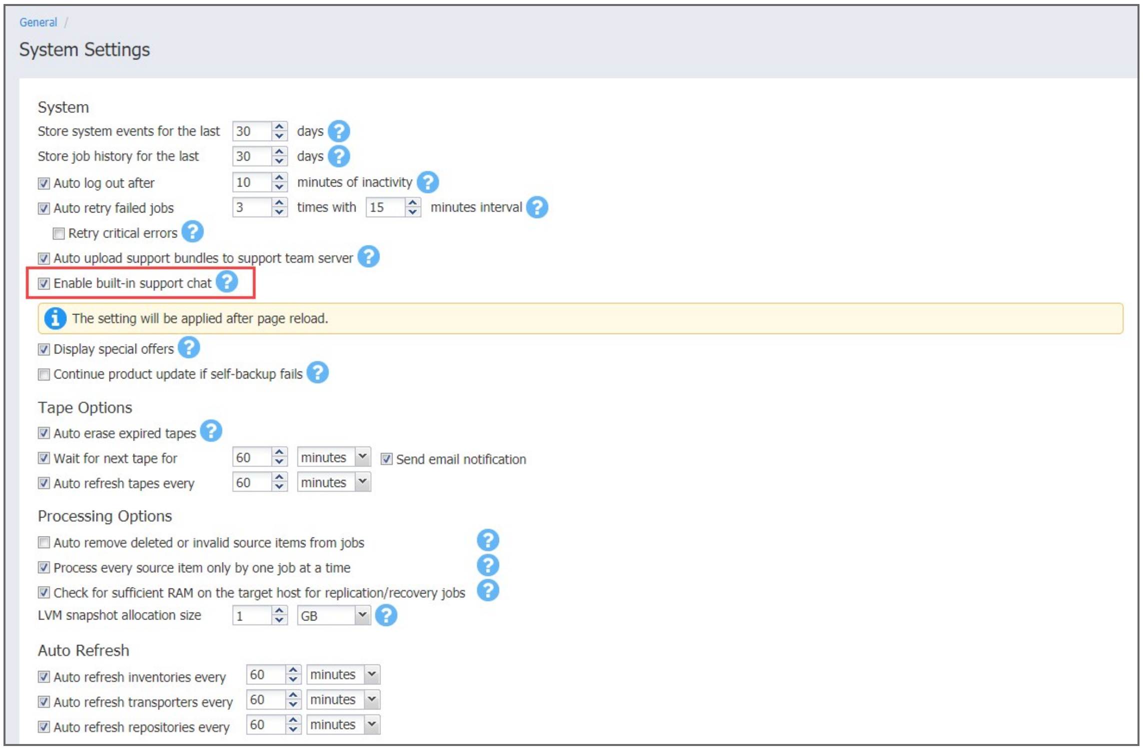
Disabling Built-in Support Chat

By default, the built-in support chat is enabled in your instance of NAKIVO Backup & Replication.

Do the following to disable built-in support chat:

1. Go to **Settings** > **General** > **System settings**.
2. Click **Edit** to make system settings editable and then deselect the **Enable built-in support chat** checkbox.

3. Click the **Apply** button.



General /

System Settings

System

Store system events for the last 30 days

Store job history for the last 30 days

☑ Auto log out after 10 minutes of inactivity

☑ Auto retry failed jobs 3 times with 15 minutes interval

□ Retry critical errors

☑ Auto upload support bundles to support team server

☑ Enable built-in support chat

The setting will be applied after page reload.

☑ Display special offers

□ Continue product update if self-backup fails

Tape Options

☑ Auto erase expired tapes

☑ Wait for next tape for 60 minutes ☑ Send email notification

☑ Auto refresh tapes every 60 minutes

Processing Options

□ Auto remove deleted or invalid source items from jobs

☑ Process every source item only by one job at a time

☑ Check for sufficient RAM on the target host for replication/recovery jobs

LVM snapshot allocation size 1 GB

Auto Refresh

☑ Auto refresh inventories every 60 minutes

☑ Auto refresh transporters every 60 minutes

☑ Auto refresh repositories every 60 minutes

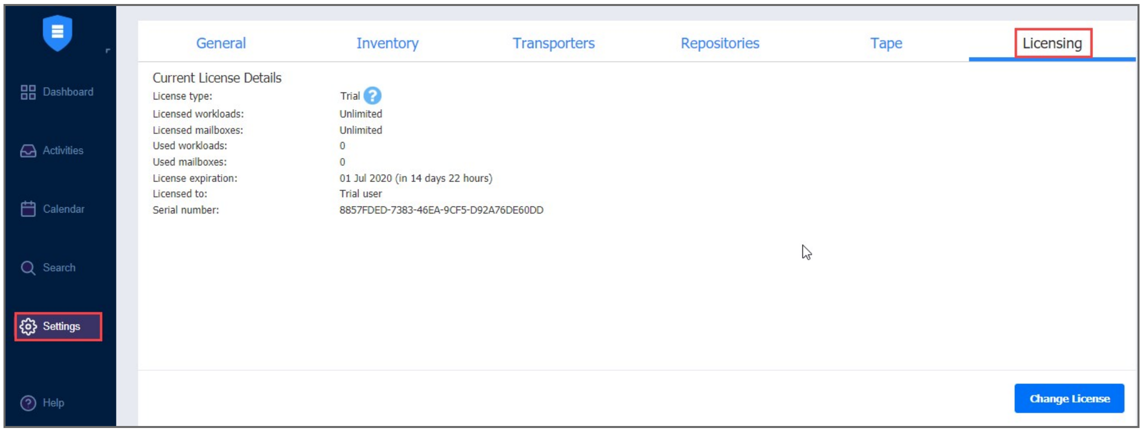
Note

When disabled, the Built-in Support Chat will not be available in all tenants of the NAKIVO Backup & Replication instance in multi-tenant mode.

Replacing License

To change your current license, follow the steps below:

1. Go to the main menu of NAKIVO Backup & Replication and click **Settings**.
2. Go to the **Licensing** tab and click **Change License**.



Current License Details

License type:	Trial
Licensed workloads:	Unlimited
Licensed mailboxes:	Unlimited
Used workloads:	0
Used mailboxes:	0
License expiration:	01 Jul 2020 (in 14 days 22 hours)
Licensed to:	Trial user
Serial number:	8857FDED-7383-46EA-9CF5-D92A76DE60DD

3. Locate and open the license file in the window that appears.

Upgrading from Free License

If your current license type is **Free** and the **Trial** license has not yet been applied to the current deployment of NAKIVO Backup & Replication, you can try the full functionality of the solution for 15 days. To do that:

1. Open the **Help Menu**
2. Select the **Try full functionality** option. A new popup window appears.
3. **Click Start Free Trial.**

Note

Once the **Trial** license expires, the product automatically goes back to using your **Free** license.

Backup

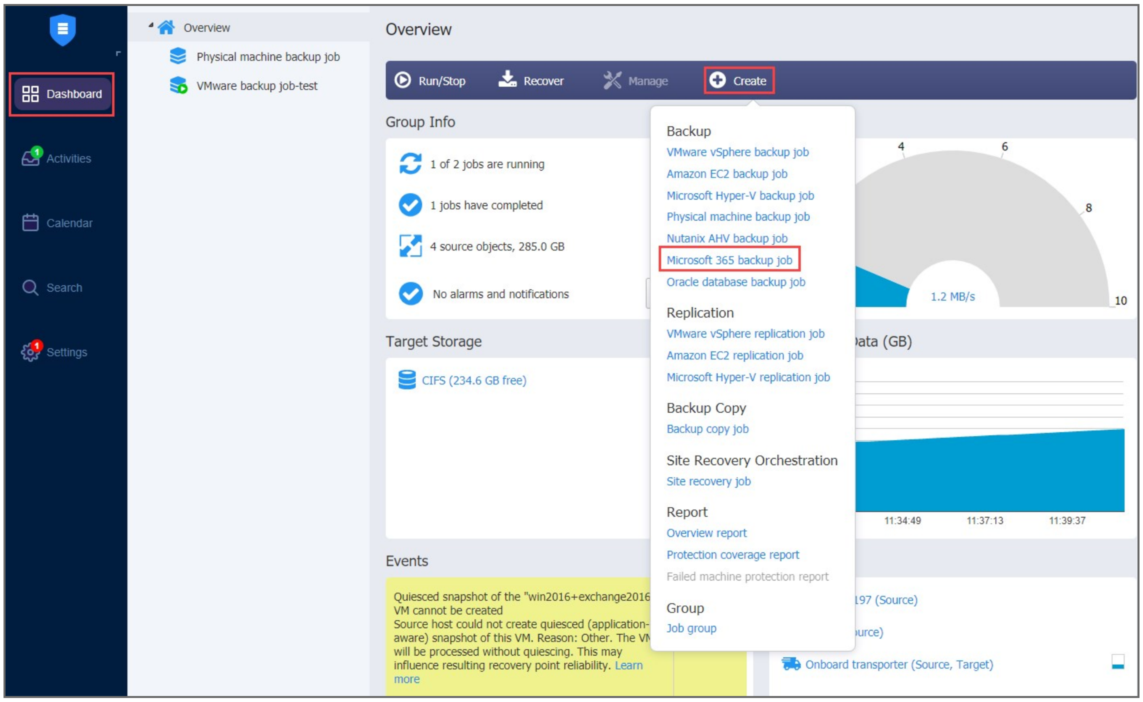
This section contains the following topics:

Creating Microsoft 365 Backup Jobs

With NAKIVO Backup & Replication, you can back up an entire Microsoft 365 account or individual mailboxes, emails, folders, files, OneDrive instances, and SharePoint sites within that account. When creating a back job for your Microsoft 365 account(s), you can specify which items to back up, where to store the backups, how often the backup job will run, and other backup options. To create a backup job, click **Create** on the **Dashboard**, and then click **Microsoft 365 backup job**.

Important

- Before creating a Microsoft 365 backup job, you must add a “SaaS Backup Repository” on page 279.
- Refer to Required API Permissions for Microsoft 365 to see the list of required permissions for backing up Microsoft 365 objects.
- Refer to Microsoft 365 Platform Limitations of the latest Release Notes for the full list of Microsoft 365 items that are not supported.



Quiesced snapshot of the "win2016+exchange2016 VM cannot be created
Source host could not create quiesced (application-aware) snapshot of this VM. Reason: Other. The V will be processed without quiescing. This may influence resulting recovery point reliability. Learn more

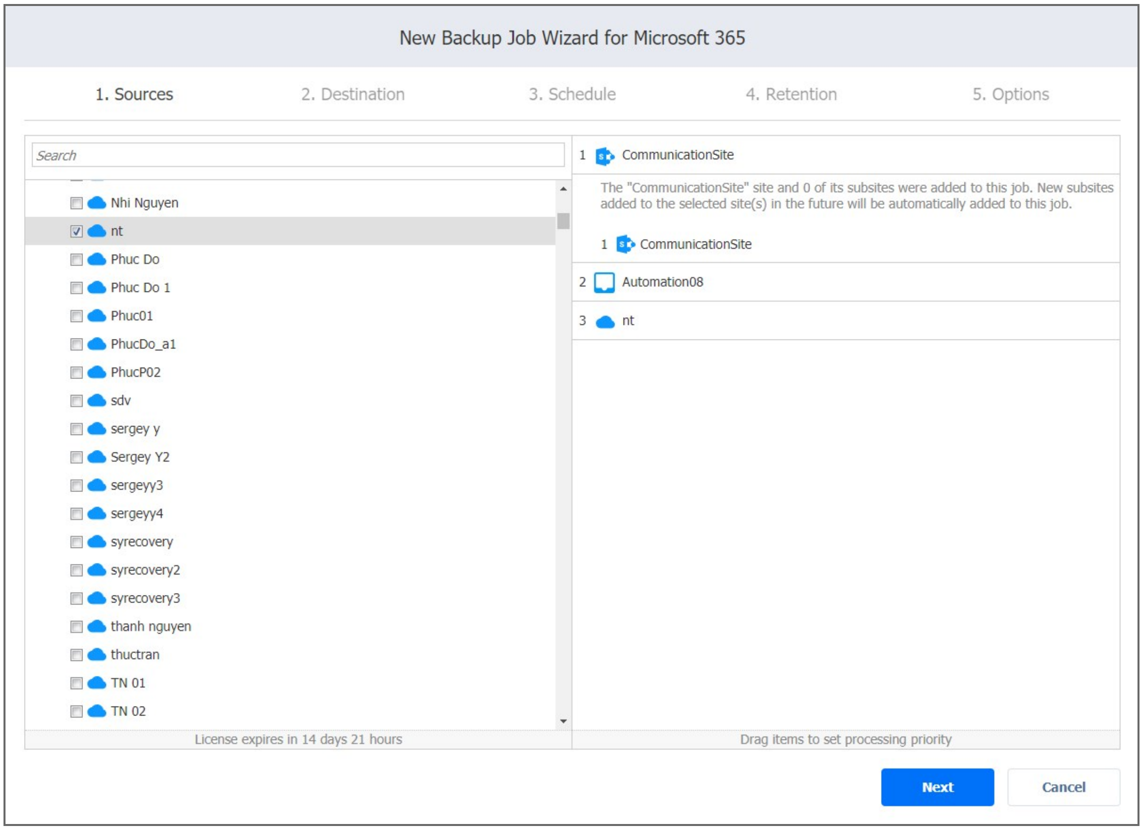
The **New Backup Job Wizard for Microsoft 365** opens. Complete the wizard as described in the sections below:

- “Backup Job Wizard for Microsoft 365: Source” on page 317
- “Backup Job Wizard for Microsoft 365: Destination” on page 318
- “Backup Job Wizard for Microsoft 365: Schedule” on page 320
- “Backup Job Wizard for Microsoft 365: Retention” on page 324
- “Backup Job Wizard for Microsoft 365: Options” on page 325

Backup Job Wizard for Microsoft 365: Source

On the **Source** page of the wizard, add the Microsoft 365 account(s) or separate OneDrives, SharePoint sites, and mailboxes hosted in Exchange Outline to your backup job. Proceed as follows:

1. In the left pane of the page, select the items you want to back up. If you select a Microsoft 365 account, all mailboxes, SharePoint sites, and OneDrive instances contained in that account are added to the backup job. To quickly find an item, use the **Search** functionality; you can enter a part of or the entire name of the item. Selected items are displayed in the right pane. You can remove items from the pane if necessary or change the priority of the item by dragging and dropping it in the required position. The priority determines the order in which the item will be processed during the job run.
2. Click **Next** to confirm the selection and go to the next page of the wizard.



- □ Nhi Nguyen
- ☑ nt
- □ Phuc Do
- □ Phuc Do 1
- □ Phuc01
- □ PhucDo_a1
- □ PhucP02
- □ sdv
- □ sergey y
- □ Sergey Y2
- □ sergeyy3
- □ sergeyy4
- □ syrecovery
- □ syrecovery2
- □ syrecovery3
- □ thanh nguyen
- □ thuctran
- □ TN 01
- □ TN 02

License expires in 14 days 21 hours

1 CommunicationSite

The "CommunicationSite" site and 0 of its subsites were added to this job. New subsites added to the selected site(s) in the future will be automatically added to this job.

1 CommunicationSite

2 Automation08

3 nt

Drag items to set processing priority

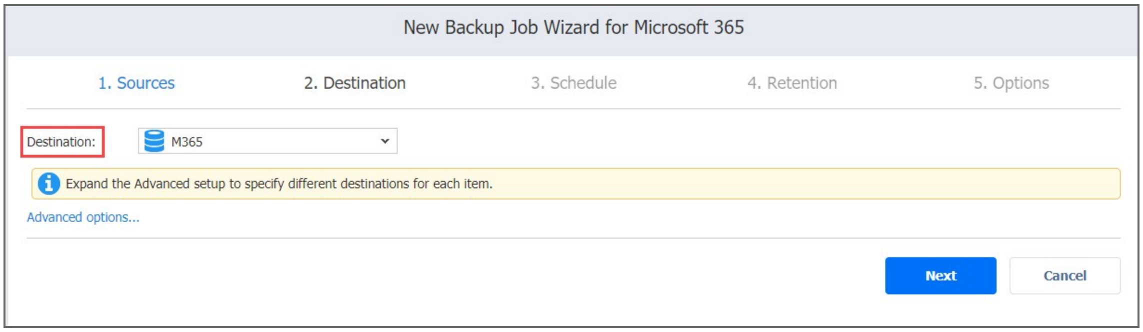
Backup Job Wizard for Microsoft 365: Destination

On the **Destination** page of the wizard, you can specify the storage location for the backup. You can specify a single location for all items in the backup or select different Backup Repositories for different items.

- Setting a Single Backup Repository for All Items
- Setting a Different Backup Repository for Each Item

Setting a Single Backup Repository for All Items

To back up all items selected on the **Sources** page to a single Backup Repository, choose a Backup Repository from the **Destination** drop-down list.


New Backup Job Wizard for Microsoft 365

Destination: M365

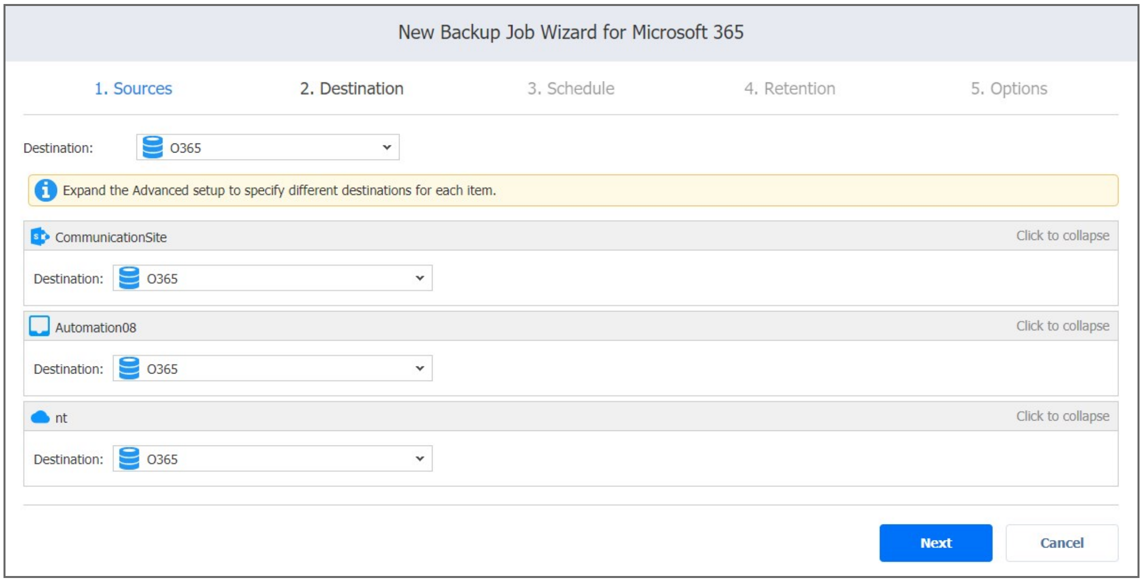
Expand the Advanced setup to specify different destinations for each item.

Setting a Different Backup Repository for Each Item

To back up the items to different Backup Repositories, follow the steps below:

1. Click **Advanced options** and do one of the following:
   - If you have selected a Microsoft 365 account(s) on the **Source** page, the account block is displayed.
     a. Click the Microsoft 365 name to expand it and view all of the mailboxes, OneDrive instances, and SharePoint sites.
     b. In the **Default Destination** drop-down list, select the Backup Repository for storing the backups of all services within the Microsoft account(s).
   - If you need a specific mailbox(es), OneDrive instance or SharePoint site to be stored in a different Backup Repository, click the name of the service and select a different location from the **Destination** drop-down list.

2. Click **Next** to go to the next page of the wizard.



New Backup Job Wizard for Microsoft 365

Destination: O365

Expand the Advanced setup to specify different destinations for each item.

CommunicationSite

Destination: O365

Automation08

Destination: O365

nt

Destination: O365

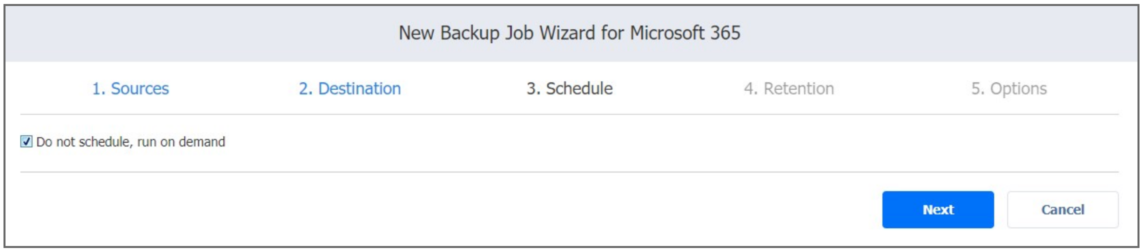
Backup Job Wizard for Microsoft 365: Schedule

On the **Schedule** page of the wizard, select to run the backup job manually or schedule the job to run on a regular basis.

- Disabling Scheduled Job Execution
- Daily of Weekly Backup
- Monthly or Yearly Backup
- Periodic Backup
- Chained Job
- Additional Schedule

Disabling Scheduled Job Execution

If you wish to start the job manually (without any schedule), select the **Do not schedule, run on demand** checkbox.



New Backup Job Wizard for Microsoft 365

1. Sources 2. Destination 3. Schedule 4. Retention 5. Options

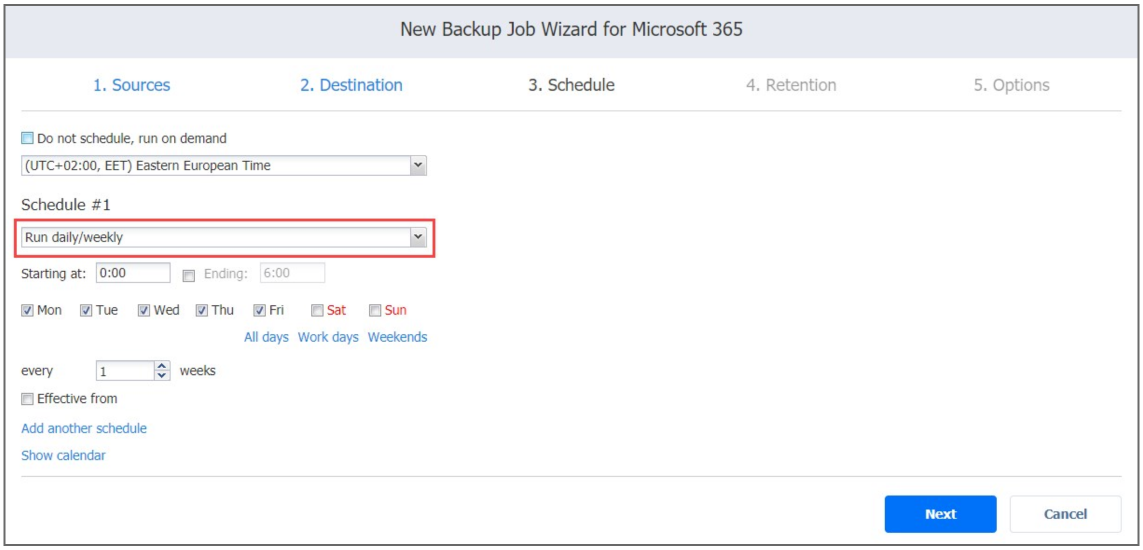
☑ Do not schedule, run on demand

Daily or Weekly Backup

To run the job once a day, choose **Run daily/weekly** from the schedule drop-down list and do the following:

- Choose a time zone that should be used for the job start and end times from the time zone drop-down list.
- Specify the time when the job should be started in the **Starting at** box.
- Specify the end time for the job in the **Ending** box. If the job has not completed by the time specified, the job will be stopped.
- Select the days of the week during which the job will be started.

- If necessary, select the **Effective from** checkbox and pick the date when the schedule comes into effect.



New Backup Job Wizard for Microsoft 365

1. Sources 2. Destination 3. Schedule 4. Retention 5. Options

□ Do not schedule, run on demand

(UTC+02:00, EET) Eastern European Time

Schedule #1

Run daily/weekly

Starting at: 0:00 □ Ending: 6:00

☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri □ Sat □ Sun

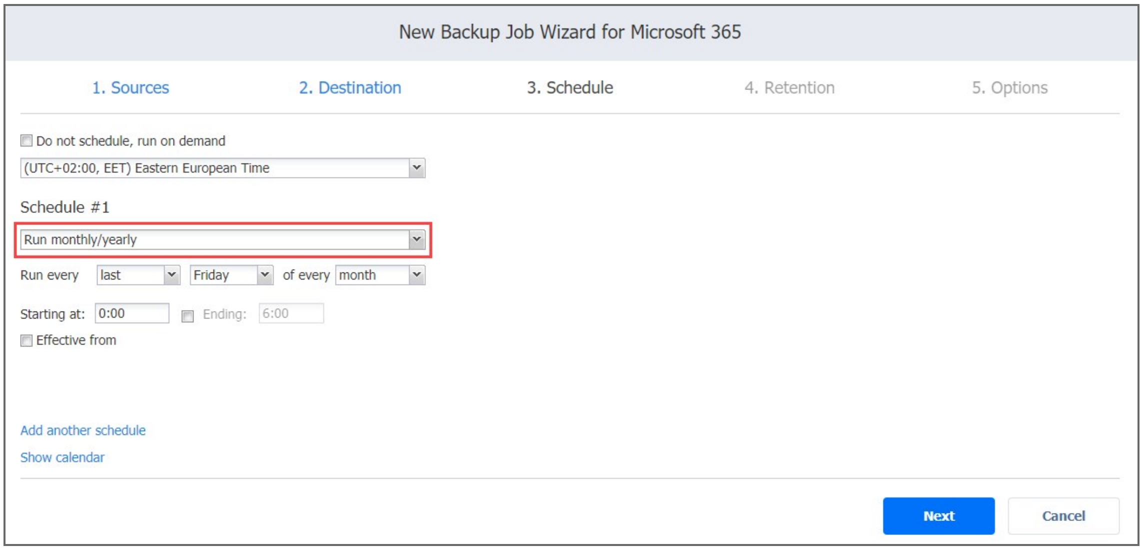
every 1 weeks

□ Effective from

Monthly or Yearly Backup

To run the job monthly or yearly, choose **Run monthly/yearly** from the schedule drop-down list and do the following:

- Specify the job start schedule in the appropriate boxes.
- Specify the day and month when the job should be started in the **Run every** boxes.
- Specify the time when the job should be started in the **Starting at** box.
- Specify the end time for the job in the **Ending** box. If the job has not completed by the time specified, the job will be stopped.
- If necessary, select the **Effective from** checkbox and pick the date when the schedule comes into effect.



New Backup Job Wizard for Microsoft 365

1. Sources 2. Destination 3. Schedule 4. Retention 5. Options

□ Do not schedule, run on demand

(UTC+02:00, EET) Eastern European Time

Schedule #1

Run monthly/yearly

Run every last Friday of every month

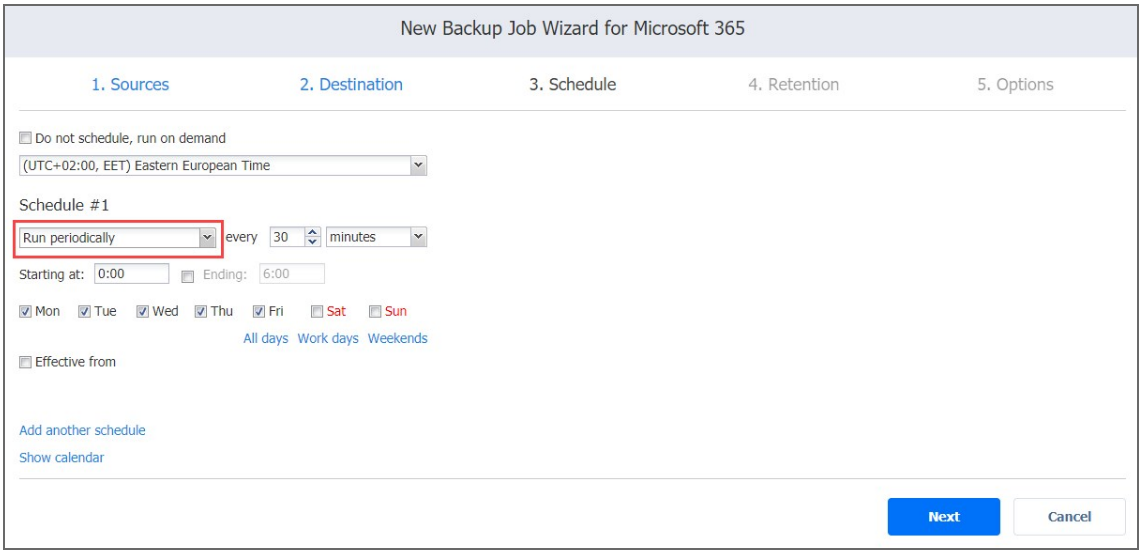
Starting at: 0:00 □ Ending: 6:00

□ Effective from

Periodic Backup

To run the job multiple times per day, choose **Run periodically** from the schedule drop-down list and then choose a time period from the appropriate boxes:

- Specify the time when the job should be started in the **Starting at** box.
- Specify the end time for the job in the **Ending** box. If the job has not completed by the time specified, the job will be stopped.
- Select the days of the week during which the job will be started.
- If necessary, select the **Effective from** checkbox and pick the date when the schedule comes into effect.



New Backup Job Wizard for Microsoft 365

1. Sources 2. Destination 3. Schedule 4. Retention 5. Options

□ Do not schedule, run on demand

(UTC+02:00, EET) Eastern European Time

Schedule #1

Run periodically every 30 minutes

Starting at: 0:00 □ Ending: 6:00

☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri □ Sat □ Sun

All days Work days Weekends

□ Effective from

Add another schedule

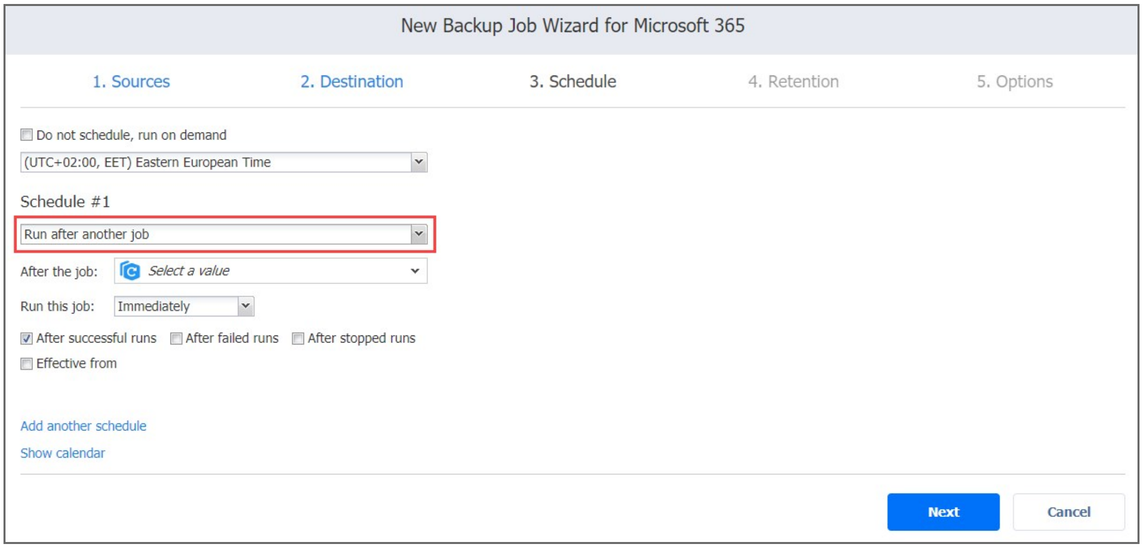
Show calendar

Chained Job

To run the job after a previous one has completed, choose **Run after another job** from the schedule drop-down list and set the options as follows:

- **After the job**: Select a job after which the current job will be started.
- **Run this job**: Choose whether to run the current job immediately after the previous one has completed or within a delay.
- **After successful runs**: If selected, the job will run if the previous one has completed successfully.
- **After failed runs**: If selected, the job will run if the previous one has failed.
- **After stopped runs**: If selected, the job will run if the previous one has been stopped.

- **Effective from**: If selected, the schedule will come into effect on the date picked.



□ Do not schedule, run on demand

(UTC+02:00, EET) Eastern European Time

Schedule #1

Run after another job

After the job: Select a value

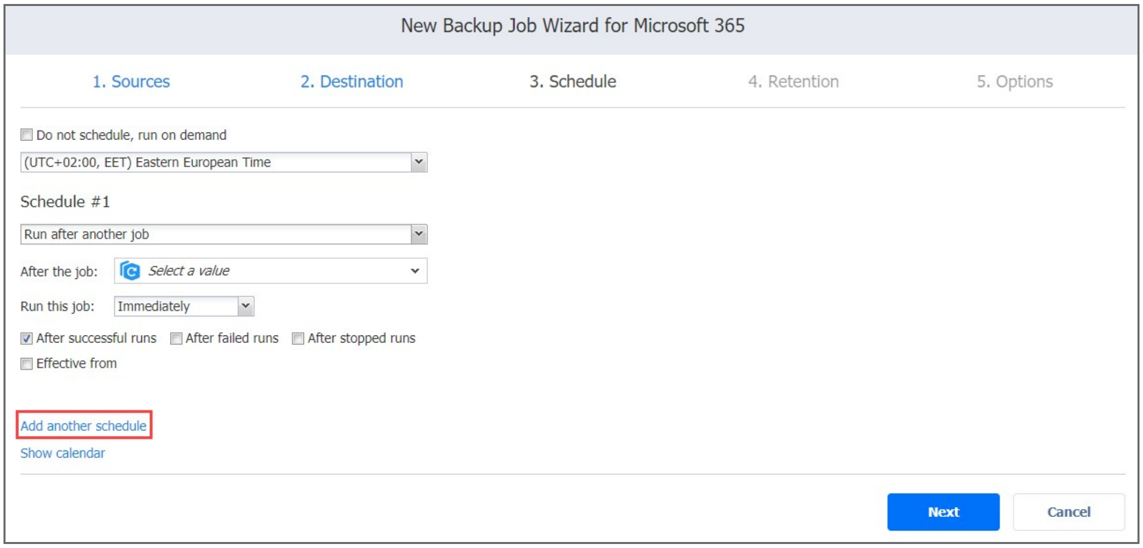
Run this job: Immediately

☑ After successful runs □ After failed runs □ After stopped runs

□ Effective from

Additional Schedule

If you want to have more than one schedule for your job, click **Add another schedule** and set it up as has been described above.



□ Do not schedule, run on demand

(UTC+02:00, EET) Eastern European Time

Schedule #1

Run after another job

After the job: Select a value

Run this job: Immediately

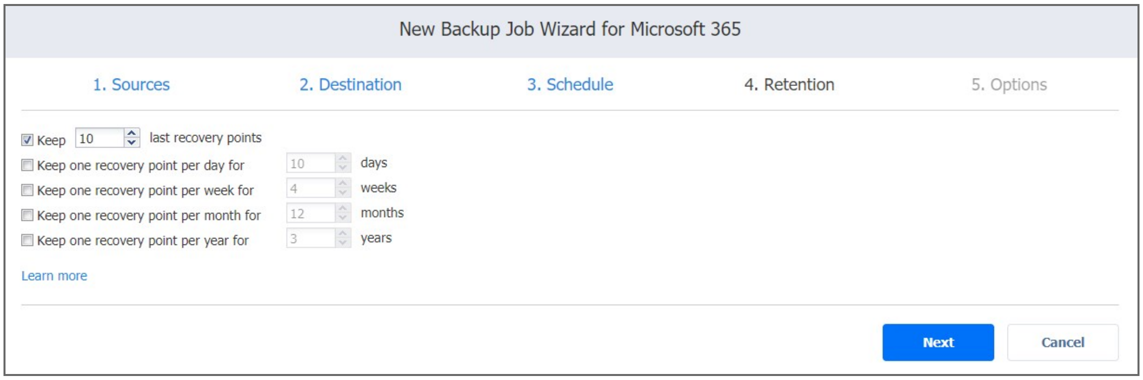
☑ After successful runs □ After failed runs □ After stopped runs

□ Effective from

Backup Job Wizard for Microsoft 365: Retention

After each job run, NAKIVO Backup & Replication creates a recovery point for each item in the Backup Repository. A recovery point represents the backed up Microsoft 365 account or mailboxes as of a particular moment in time and allows you to recover individual objects or the entire account from the Backup Repository. You can specify how many recovery points should be preserved in the Backup Repository using the Grandfather-Father-Son (GFS) backup rotation scheme. Use the following options:

- **Keep X last recovery points**: Keeps the specified number of last recovery points for each item in the job.
- **Keep one recovery point per day for X days**: Keeps one last recovery point per day for the specified number of days.
- **Keep one recovery point per week for X weeks**: Keeps the last available backup of every week for the specified number of weeks.
- **Keep one recovery point per month for X months**: Keeps the last available backup of every month for the specified number of months.
- **Keep one recovery point per year for X years**: Keeps the last available backup of every year for the specified number of years.



☑ Keep 10 last recovery points
□ Keep one recovery point per day for 10 days
□ Keep one recovery point per week for 4 weeks
□ Keep one recovery point per month for 12 months
□ Keep one recovery point per year for 3 years

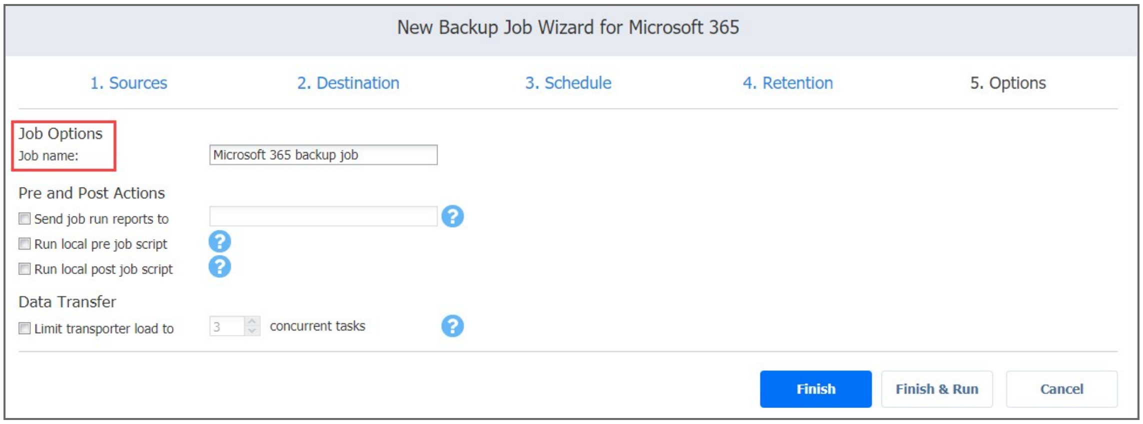
Backup Job Wizard for Microsoft 365: Options

On the **Options** page, you can specify the job’s name, define pre and post actions, and limit the Transporter load. Proceed as described in these sections:

- Job Options
- Pre and Post Job Actions
    - Email Notifications
    - Pre Job Script
    - Post Job Script
- Data Transfer
    - Transporter Load
- Completing the New Backup Job Wizard for Microsoft 365

Job Options

Enter a name for the job into the **Job name** box.



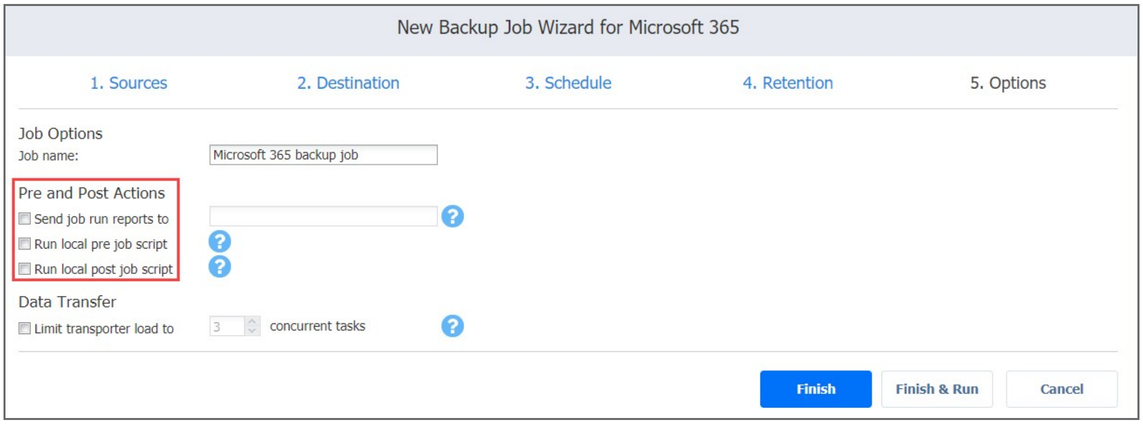
Job Options
Job name: Microsoft 365 backup job

Pre and Post Actions
□ Send job run reports to
□ Run local pre job script
□ Run local post job script

Data Transfer
□ Limit transporter load to 3 concurrent tasks

Pre and Post Job Actions

NAKIVO Backup & Replication provides you with the ability to enable certain actions before a backup job begins and after it has completed. You can choose to send job run reports and run local pre and post job scripts. For more information, refer to “Pre and Post Job Scripts” on page 10 .


New Backup Job Wizard for Microsoft 365

1. Sources 2. Destination 3. Schedule 4. Retention 5. Options

Job Options

Job name: Microsoft 365 backup job

Pre and Post Actions

□ Send job run reports to

□ Run local pre job script

□ Run local post job script

Data Transfer

□ Limit transporter load to 3 concurrent tasks

Email Notifications

NAKIVO Backup & Replication can send email notifications on job completion status to specified recipients. This feature complements global notification and provides you with the ability to configure notifications on a per-job level.

Note

To enable this option, configure your email settings. For details, refer to "Email Notifications" on page 195 .

To send email notifications, select **Send job run reports to** and specify one or more email addresses in the text box. The semi-colon character (;) should be used to separate multiple email addresses.

Pre Job Script

To run a script before the product begins backing up your items, do the following:

1. Place a script file on the machine where the Director is installed.
2. Select the **Run local pre job script** option.
3. Specify the following parameters in the dialog box that opens:
   - **Script path**: Specify a local path to the script on the machine where the Director is installed. The script interpreter should be specified.

     Example (Windows): *cmd.exe /c D:\script.bat*

     Example (Linux): *bash /root/script.sh*
   - **Job behavior**: Choose one of the following job behaviors in relation to script completion:
     - **Wait for the script to finish**: When selected, the backup is started only after the script is completed.
     - **Do not wait for the script to finish**: When selected, the product runs the script and starts backing up your items at the same time.
   - **Error handling**: Choose one of the following job behaviors in relation to script failure:
     - **Continue the job on script failure**: When selected, the product performs the backup job even if the script has failed.

- **Fail the job on script failure**: When this option is selected and the script fails, the job fails and the backup is not performed.

Post Job Script

To run a script after the product has finished backing up all items, do the following:

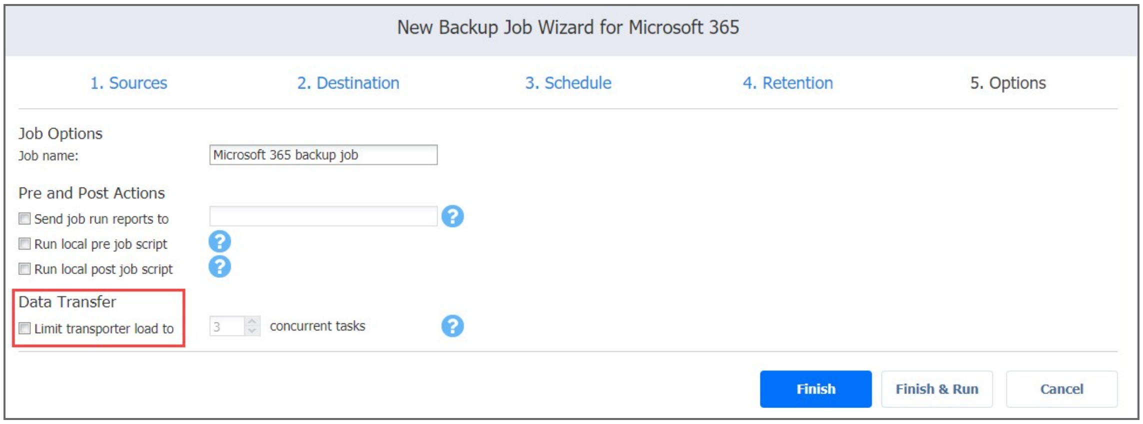
1. Place a script file on the machine where the Director is installed.
2. Select the **Run local post job script** option.
3. Specify the following parameters in the dialog box that opens:
   - **Script path**: Specify a local path to the script on the machine where the Director is installed. The script interpreter should be specified.
     Example (Windows): *cmd.exe /c D:\script.bat*
     Example (Linux): *bash /root/script.sh*
   - **Job behavior**: Choose one of the following job behaviors in relation to script completion:
     - **Wait for the script to finish**: When selected, the job remains in the “running” state until the script is completed.
     - **Do not wait for the script to finish**: When selected, the job is completed even if the script execution is still in progress.
   - **Error handling**: Choose one of the following job behaviors in relation to script failure:
     - **Continue the job on script failure**: When this option is selected, script failure does not influence the status of the job.
     - **Fail the job on script failure**: When this option is selected and the script fails, the job status is set to “failed” even if backup has been successful.

Note

Pre and post job scripts can be executed only on the machine on which the Director is installed.

Data Transfer

In the *Data Transfer* section, you can specify a Transporter load.



Job Options

Job name: Microsoft 365 backup job

Pre and Post Actions

□ Send job run reports to

□ Run local pre job script

□ Run local post job script

Data Transfer

□ Limit transporter load to 3 concurrent tasks

Transporter Load

You can limit the maximum number of Transporter tasks used by the job. By default, the number is set to 3 concurrent tasks. For a Microsoft 365 backup job, one task is equal to processing one mailbox or one OneDrive instance.

To change the default number of tasks, do the following:

1. In the *Data Transfer* section, select the **Limit transporter load to** checkbox.
2. Specify the number of concurrent tasks in the corresponding box.

Completing the New Backup Job Wizard for Microsoft 365

Click **Finish** or **Finish & Run** to complete the job creation.

Note

If you click **Finish & Run**, you will have to define the scope of your job.

Deleting Backups

With NAKIVO Backup & Replication, you can permanently delete a backup (including all of its recovery points) if it is available in a Backup Repository. Also, you can delete specific recovery points of a backup without affecting any of the others.

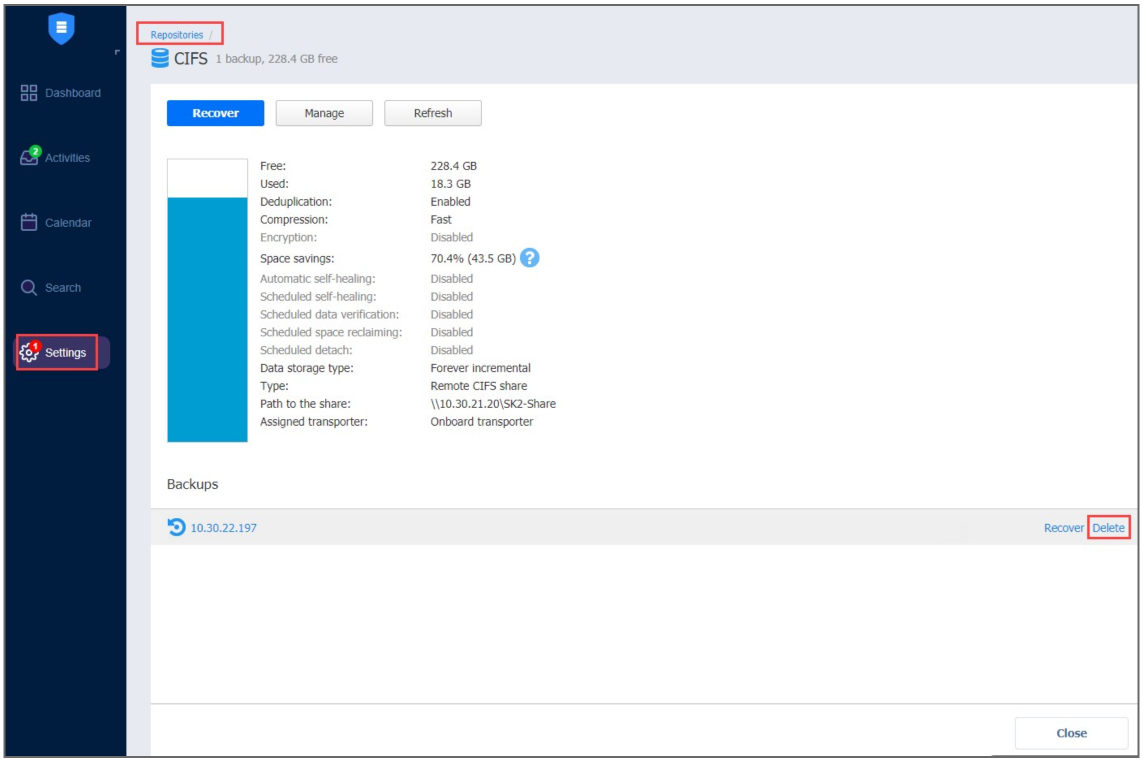
Refer to one of the following sections:

- Deleting a Single Backup
- Deleting Backups in Bulk
- Deleting Recovery Points
    - Deleting a Single Recovery Point
    - Bulk Recovery Points Deletion

Deleting a Single Backup

To delete a backup permanently, follow the steps below:

1. Click **Settings** in the main menu of the product.
2. Go to the **Repositories** tab and click a Backup Repository.
3. Click the backup you want to delete.
4. In the backup page, click **Delete**.
5. Click **Delete** in the dialog box that opens.



CIFS 1 backup, 228.4 GB free

Free:	228.4 GB
Used:	18.3 GB
Deduplication:	Enabled
Compression:	Fast
Encryption:	Disabled
Space savings:	70.4% (43.5 GB)
Automatic self-healing:	Disabled
Scheduled self-healing:	Disabled
Scheduled data verification:	Disabled
Scheduled space reclaiming:	Disabled
Scheduled detach:	Disabled
Data storage type:	Forever incremental
Type:	Remote CIFS share
Path to the share:	\\10.30.21.20\SK2-Share
Assigned transporter:	Onboard transporter

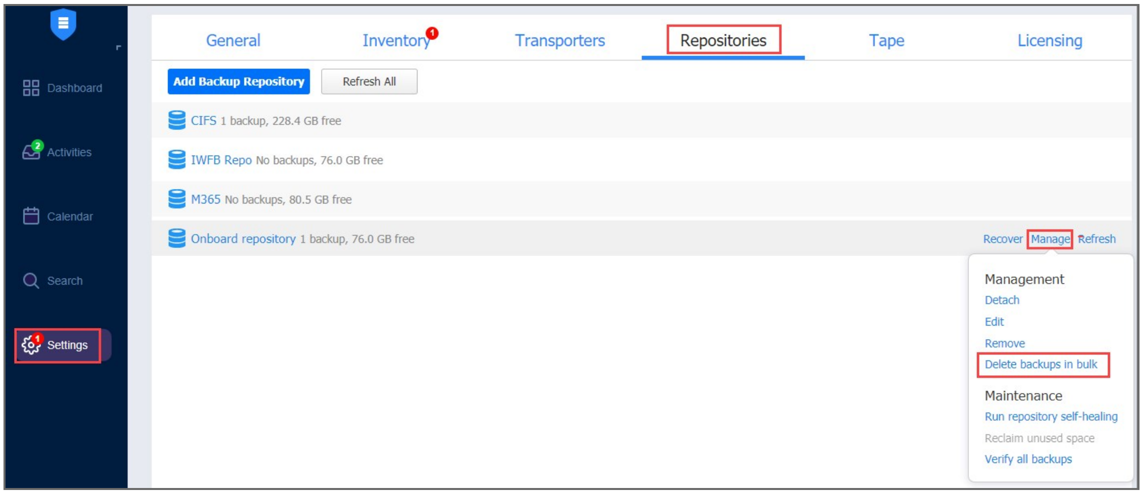
Backups

10.30.22.197 Recover Delete

Deleting Backups in Bulk

To permanently delete a number of backups that match particular criteria, follow the steps below:

1. Click **Settings** in the main menu.
2. Go to the **Repositories** tab and hover over a Backup Repository.
3. Click **Manage** and then click **Delete backups in bulk**.



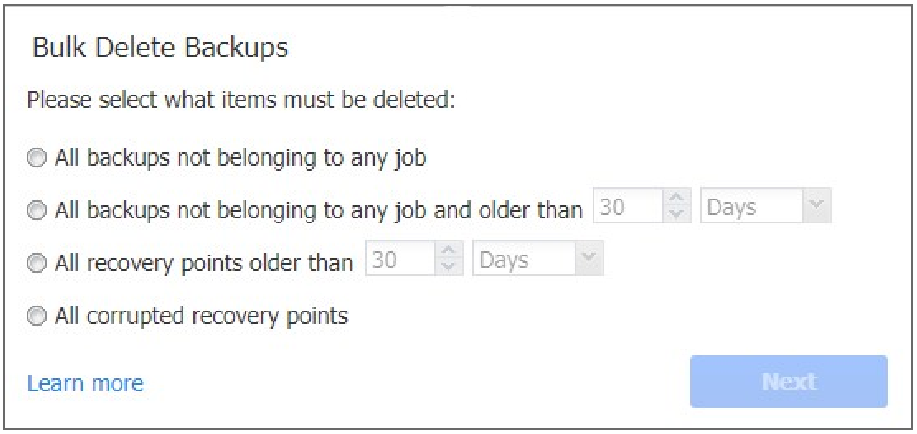
CIFS 1 backup, 228.4 GB free

IWFB Repo No backups, 76.0 GB free

M365 No backups, 80.5 GB free

Onboard repository 1 backup, 76.0 GB free

The **Bulk Delete Backups** dialog box opens.



Bulk Delete Backups

Please select what items must be deleted:

○ All backups not belonging to any job

○ All backups not belonging to any job and older than 30 Days

○ All recovery points older than 30 Days

○ All corrupted recovery points

4. Select one of the available options:
   - All backups not belonging to any job
   - All backups not belonging to any job and older than X <time_units>, where X is an integer and <time_units> is either Days, Weeks, or Months

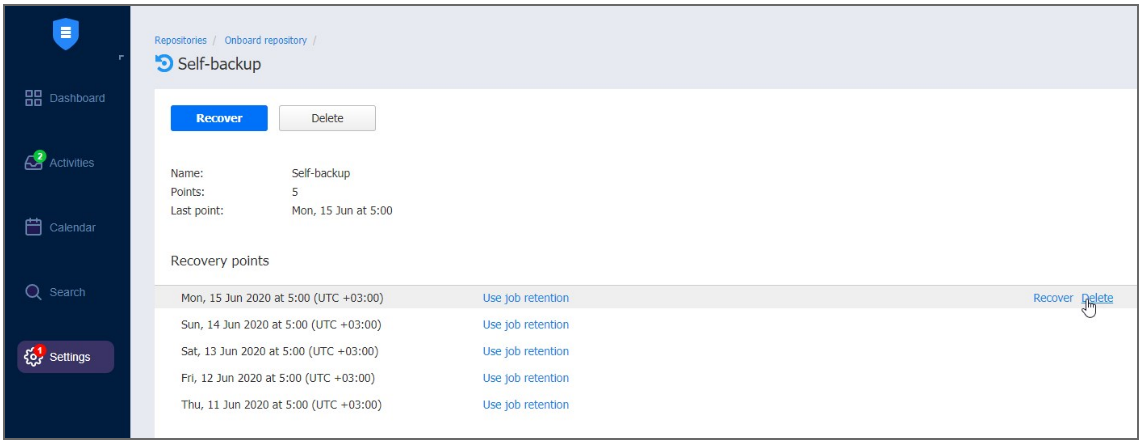
     The dialog shows the number of backups to be deleted.
5. Click **Next**.
6. A list of backups/recovery points to be deleted opens. Click **Delete**.

Deleting Recovery Points

You can delete either a single recovery point, all corrupted recovery points, or all recovery points older than the specified number of days.

Deleting a Single Recovery Point

1. Click **Settings** in the main menu.
2. Go to the **Repositories** tab.
3. Click a Backup Repository.
4. Click the backup where you want to delete a recovery point.
5. Hover over the recovery point you want to delete.
6. Click **Delete**.



Name: Self-backup
Points: 5
Last point: Mon, 15 Jun at 5:00

Recovery points

Mon, 15 Jun 2020 at 5:00 (UTC +03:00)	Use job retention	Recover Delete
Sun, 14 Jun 2020 at 5:00 (UTC +03:00)	Use job retention	
Sat, 13 Jun 2020 at 5:00 (UTC +03:00)	Use job retention	
Fri, 12 Jun 2020 at 5:00 (UTC +03:00)	Use job retention	
Thu, 11 Jun 2020 at 5:00 (UTC +03:00)	Use job retention	

7. Click **Delete Recovery Point** in the message box that opens.

Bulk Recovery Points Deletion

1. Click **Settings** in the main menu of the product.
2. Go to the **Repositories** tab.
3. Click a Backup Repository.
4. Click **Manage**.
5. Click **Delete backups in bulk**.
6. The **Bulk Delete Backups dialog** box opens. Select criteria for recovery points to be deleted:
   - **All recovery points older than** X <time_units>, where X is an integer and <time_units> is either Days, Weeks, or Months: When selected, the recovery points that are older than the specified time interval will be deleted.
   - **All corrupted recovery points**: If selected, all recovery points that are corrupted will be deleted.
7. The **Bulk Delete Recovery Points** dialog box opens displaying the list of recovery points to be deleted. Click **Delete** to confirm the deletion of recovery points.

Object Recovery for Microsoft 365

The Object Recovery for Microsoft 365 feature enables browsing, searching, and recovering Exchange Online mailboxes, OneDrive for Business instances, and SharePoint Online sites directly from backups. This feature is agentless, works right out of the box, and does not require creating a special lab or running a special backup type.

Important

- Refer to Microsoft 365 Platform Limitations of the latest Release Notes for the full list of Microsoft 365 items that are not supported.
- Refer to Required API Permissions for Microsoft 365 to see the list of required permissions for recovering Microsoft 365 objects.

Refer to the following topics for more information:

- “Starting Object Recovery for Microsoft 365” on page 333
- “Microsoft 365 Object Recovery Wizard: Backup” on page 335
- “Microsoft 365 Object Recovery Wizard: Recovery Account” on page 336
- “Microsoft 365 Object Recovery Wizard: Objects” on page 337
- “Microsoft 365 Object Recovery Wizard: Options” on page 340

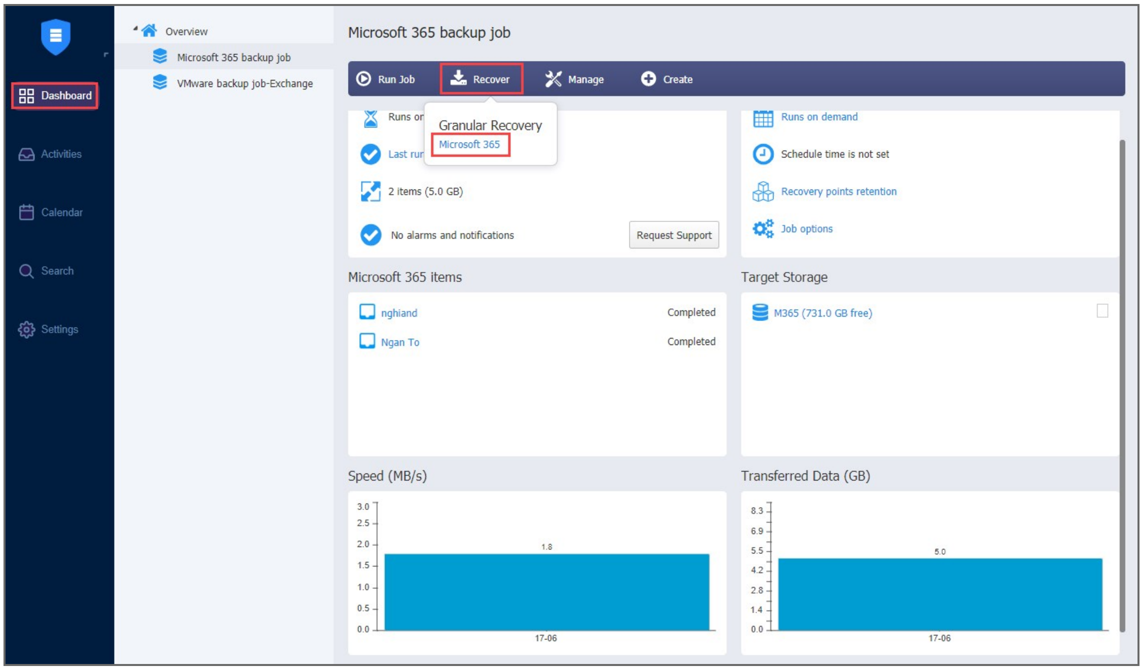
Starting Object Recovery for Microsoft 365

You can start the recovery process either from the **Dashboard**, or from the **Repositories** page in Settings (for example, if you no longer have a backup job, but still have the backup). Refer to the following sections for more details:

- Starting Object Recovery for Microsoft 365 from Dashboard
- Starting Object Recovery for Microsoft 365 from a Backup Repository

Starting Object Recovery for Microsoft 365 from Dashboard

To start object recovery for Microsoft 365 from the **Dashboard**, click **Recover** and then click **Microsoft 365**.

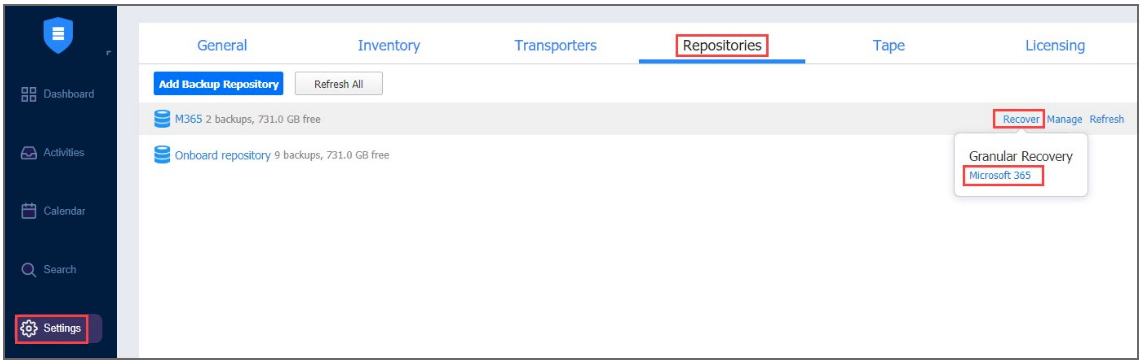


Starting Object Recovery for Microsoft 365 from a Backup Repository

To start object recovery for Microsoft 365 from a Backup Repository, do the following:

1. Go to the main menu of NAKIVO Backup & Replication and click **Settings**.
2. Go to the **Repositories** tab and hover the cursor over the Backup Repository containing the required backup.

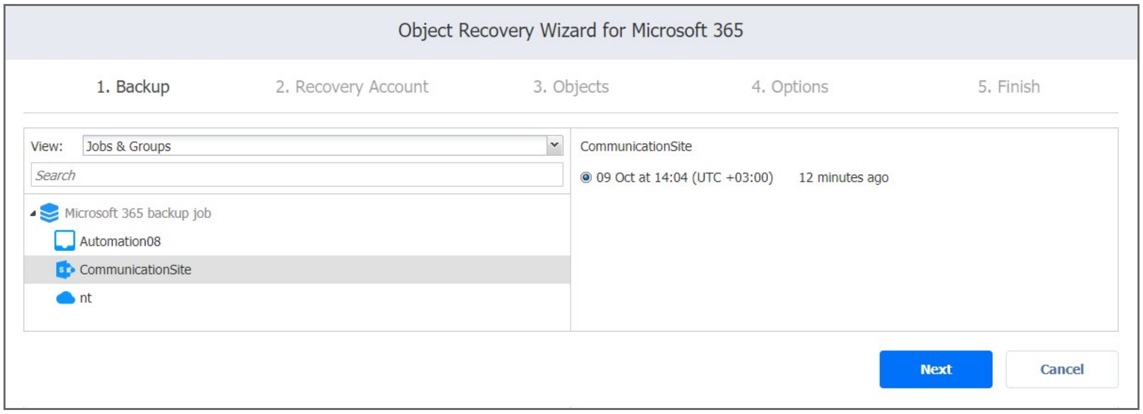
3. Click the **Recover** button and then click **Microsoft 365**.



The **Object Recovery Wizard for Microsoft 365** opens.

Microsoft 365 Object Recovery Wizard: Backup

On the **Backup** page of the Object Recovery Wizard for Microsoft 365, select a backed up Exchange Online mailbox, OneDirve for Business, or a SharePoint Online site using either a **Backup Repository** or **Jobs & Groups** view in the left pane. Then select a recovery point in the right pane. Note, that only one backup can be selected at a time.



Object Recovery Wizard for Microsoft 365

View: Jobs & Groups

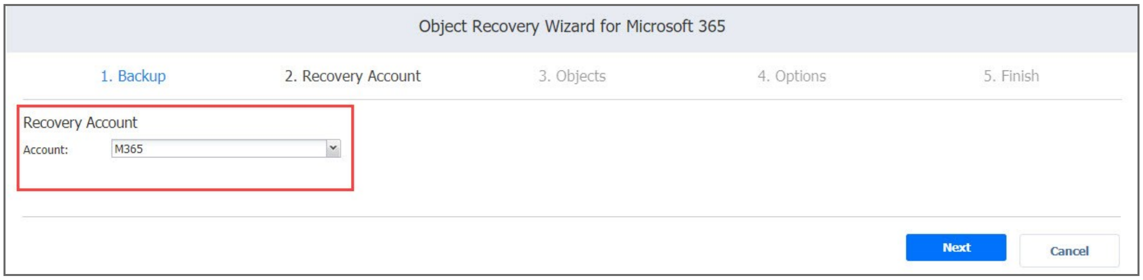
CommunicationSite

● 09 Oct at 14:04 (UTC +03:00) 12 minutes ago

Click **Next** to proceed to the next page of the wizard.

Microsoft 365 Object Recovery Wizard: Recovery Account

On the **Recovery Account** page, specify the Microsoft 365 account to which you want to recover your items. You can choose to recover to a specific Online Exchange mailbox, OneDrive for Business, or a SharePoint site later in the wizard. Select the required account from the **Account** drop-down list. The list contains all Microsoft 365 accounts added to the inventory. Refer to “Adding Microsoft 365 Accounts” on page 236 for details.



Object Recovery Wizard for Microsoft 365

1. Backup 2. Recovery Account 3. Objects 4. Options 5. Finish

Recovery Account

Account: M365

Click **Next** to proceed to the next page of the wizard.

Microsoft 365 Object Recovery Wizard: Objects

On the **Objects** page, the following items can be selected for recovery:

- Exchange Online emails, folders, contacts, and calendars
- OneDrive for Business folders and files
- SharePoint Online sites, subsites, document libraries, lists, list items, and individual files and folders.

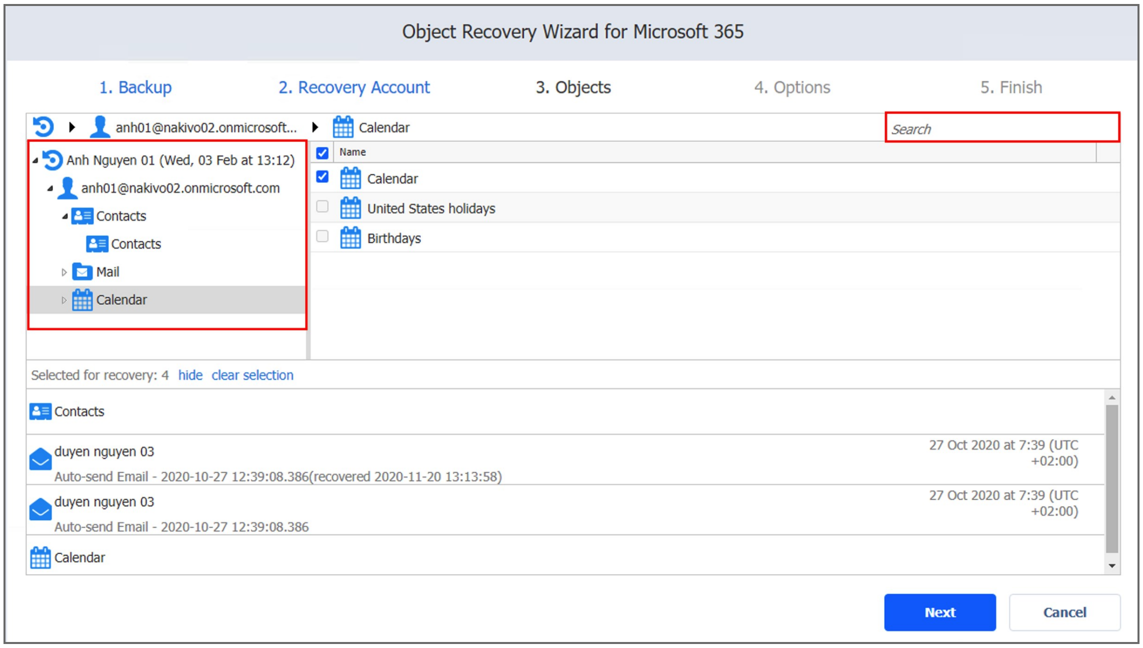
  Notes

  - Linked contacts are displayed as separate contact items.
  - The lookup data of SharePoint lists displayed in the recovery wizard is inaccurate, and it can't be recovered.
  - Read-only calendars and calendars added from the directory can't be recovered.
  - Refer to the Microsoft 365 Platform Limitations of the latest Release Notes for the full list of Microsoft 365 items that are not supported.

The **Objects** page contains:

- **Navigation**: Use the Navigation pane on the left to locate the items you need to restore. Selecting the container in the Navigation pane loads its contents in the right pane. If a container has sub-folders, they are also displayed in the right pane.
- **Search**: The search box allows you to search for objects you want to recover. The search is performed within:
  - Exchange Online mailbox, mailbox folders, individual emails, contacts, and calendars;
  - OneDrive, OneDrive folders, and individual files;
  - SharePoint site, document libraries, folders, files, lists, and list items.

Enter the word or a part of the word into the search box and hit Enter on the keyboard. All items matching the criteria will be displayed in the Contents pane on the right.



anh01@nakivo02.onmicrosoft... ▸ Calendar

- Anh Nguyen 01 (Wed, 03 Feb at 13:12)
  - anh01@nakivo02.onmicrosoft.com
    - Contacts
      - Contacts
    - Mail
    - Calendar

☑	Name
☑	Calendar
□	United States holidays
□	Birthdays

Selected for recovery: 4 hide clear selection

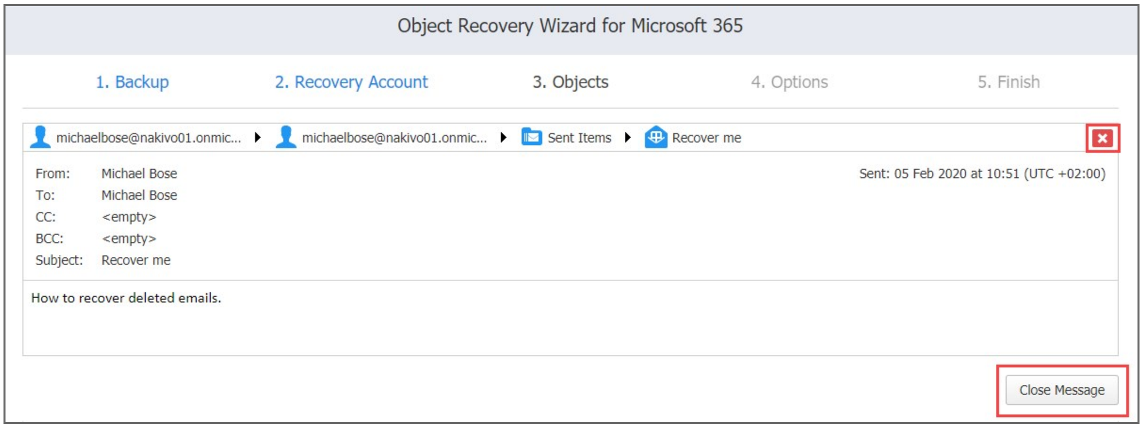
Contacts

duyen nguyen 03 — 27 Oct 2020 at 7:39 (UTC +02:00)
Auto-send Email - 2020-10-27 12:39:08.386(recovered 2020-11-20 13:13:58)

duyen nguyen 03 — 27 Oct 2020 at 7:39 (UTC +02:00)
Auto-send Email - 2020-10-27 12:39:08.386

Calendar

When recovering emails, you can also preview the contents of an email message by clicking its name in the right pane. To close the message preview, click the “Close” button at the bottom or click the ”X” button above the item body.



michaelbose@nakivo01.onmic... ▸ michaelbose@nakivo01.onmic... ▸ Sent Items ▸ Recover me

From: Michael Bose
To: Michael Bose
CC: <empty>
BCC: <empty>
Subject: Recover me

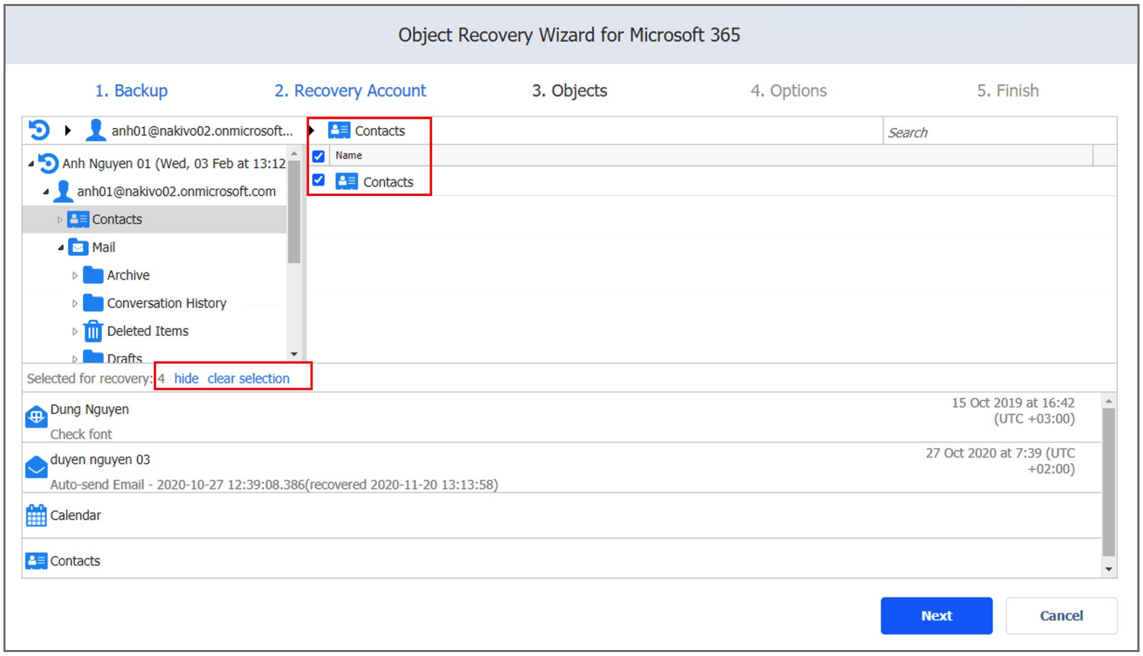
Sent: 05 Feb 2020 at 10:51 (UTC +02:00)

How to recover deleted emails.

After locating the items you need to recover, select the checkboxes next to their names. You can select different object types for recovery at the same time. The number of items selected for recovery is displayed at the bottom of the wizard page. You can also:

- Click **show** to view the list of all items selected for recovery.
- Click **clear selection** to clear the list of items selected for recovery.

- Click **hide** to hide the list of items selected for recovery.



Object Recovery Wizard for Microsoft 365

anh01@nakivo02.onmicrosoft...

- Anh Nguyen 01 (Wed, 03 Feb at 13:12
  - anh01@nakivo02.onmicrosoft.com
    - Contacts
    - Mail
      - Archive
      - Conversation History
      - Deleted Items
      - Drafts

Contacts

Search

☑	Name
☑	Contacts

Selected for recovery: 4 hide clear selection

Dung Nguyen Check font	15 Oct 2019 at 16:42 (UTC +03:00)
duyen nguyen 03 Auto-send Email - 2020-10-27 12:39:08.386(recovered 2020-11-20 13:13:58)	27 Oct 2020 at 7:39 (UTC +02:00)
Calendar	
Contacts	

Click **Next** to proceed to the next page of the wizard.

Microsoft 365 Object Recovery Wizard: Options

On the **Options** page, specify the location to which the items will be restored and overwrite behavior for folders. Proceed as described in the sections below:

- Recovering to the Original Location
- Recovering to Mailbox
- Recovering to OneDrive
- Recovering to Site

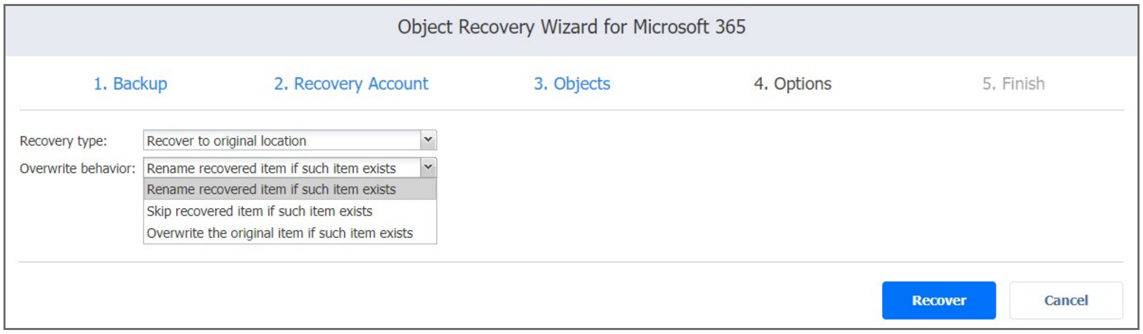
Recovering to the Original Location

To recover Microsoft 365 items to the original location, take the following steps:

Note

Contact and calendar items can only be recovered to the original location.

1. Select **Recover to original location** from the **Recovery type** drop-down list. All selected items will be recovered to their original places within the Microsoft 365 account. This option is disabled if a mailbox, OneDrive or site no longer exists (deleted from the product, for example) or if you have selected a recovery account on the **Recovery Account** page of the wizard that is different from the original account.
2. Choose the naming convention for the recovered items by selecting one of the following **Overwrite behavior** options:
   - **Rename recovered item if such item exists**
   - **Skip recovered item if such item exists**
   - **Overwrite the original item if such item exists**
3. Click **Recover**.



Object Recovery Wizard for Microsoft 365

1. Backup
2. Recovery Account
3. Objects
4. Options
5. Finish

Recovery type: Recover to original location

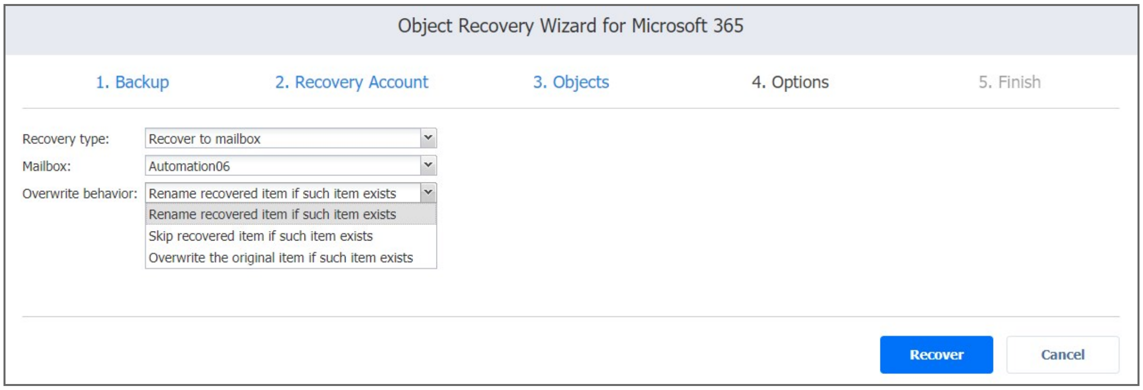
Overwrite behavior: Rename recovered item if such item exists

Rename recovered item if such item exists
Skip recovered item if such item exists
Overwrite the original item if such item exists
Recover
Cancel

Recovering to Mailbox

If you want to recover items to a specific mailbox, take the following steps:

1. Select **Recover to mailbox** from the **Recovery type** drop-down list.
2. Select the required mailbox from the **Mailbox** drop-down list.
3. Choose the naming convention for the recovered items by selecting one of the following **Overwrite behavior** options:
   - **Rename recovered item if such item exists**
   - **Skip recovered item if such item exists**
   - **Overwrite the original item if such item exists**
4. Click **Recover**.


Object Recovery Wizard for Microsoft 365

Recovery type: Recover to mailbox

Mailbox: Automation06

Overwrite behavior: Rename recovered item if such item exists

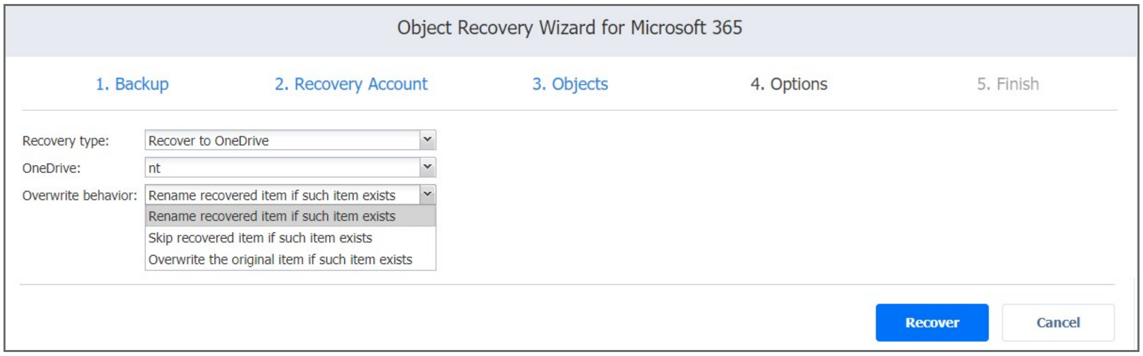
1. Backup
2. Recovery Account
3. Objects
4. Options
5. Finish
Rename recovered item if such item exists
Skip recovered item if such item exists
Overwrite the original item if such item exists
Recover
Cancel

Recovering to OneDrive

To recover OneDrive items to a specific OneDrive account, take the following steps:

1. Select **Recover to OneDrive** from the **Recovery type** drop-down list.
2. Select the required OneDrive from the **OneDrive** drop-down list.
3. Choose the naming convention for the recovered items by selecting one of the following **Overwrite behavior** options:
   - **Rename recovered item if such item exists**
   - **Skip recovered item if such item exists**
   - **Overwrite the original item if such item exists**

4. Click **Recover**.


Object Recovery Wizard for Microsoft 365
1. Backup
2. Recovery Account
3. Objects
4. Options
5. Finish

Recovery type: Recover to OneDrive

OneDrive: nt

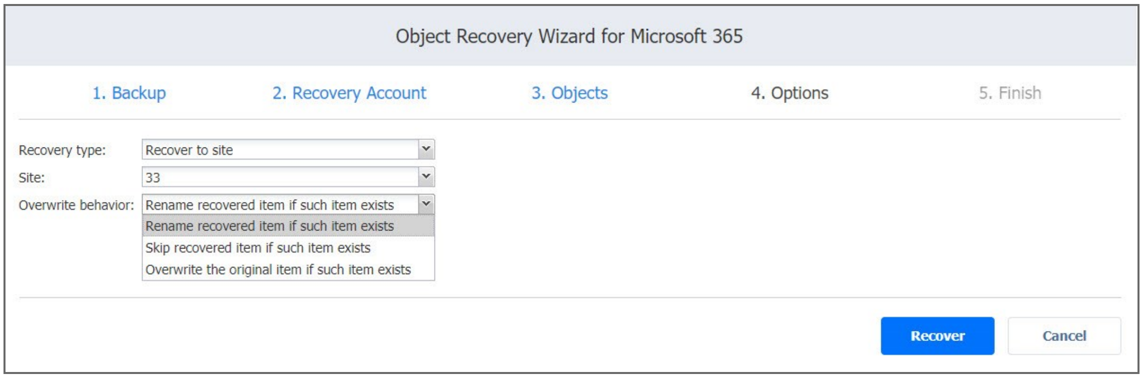
Overwrite behavior: Rename recovered item if such item exists

Rename recovered item if such item exists
Skip recovered item if such item exists
Overwrite the original item if such item exists
Recover
Cancel

Recovering to Site

To recover SharePoint objects to a specific site, take the following steps:

1. Select **Recover to site** from the **Recovery type** drop-down list.
2. Select the required site from the **Site** drop-down list.
3. Choose the naming convention for the recovered items by selecting one of the following **Overwrite behavior** options:
    - **Rename recovered item if such item exists**
    - **Skip recovered item if such item exists**
    - **Overwrite the original item if such item exists**
4. Click **Recover**.


Object Recovery Wizard for Microsoft 365
1. Backup
2. Recovery Account
3. Objects
4. Options
5. Finish

Recovery type: Recover to site

Site: 33

Overwrite behavior: Rename recovered item if such item exists

Rename recovered item if such item exists
Skip recovered item if such item exists
Overwrite the original item if such item exists
Recover
Cancel

When the recovery process is completed, the **Finish** page is displayed. You cannot return to the previous pages at this point, however, you can check the progress of the job by clicking the **Activities** link.

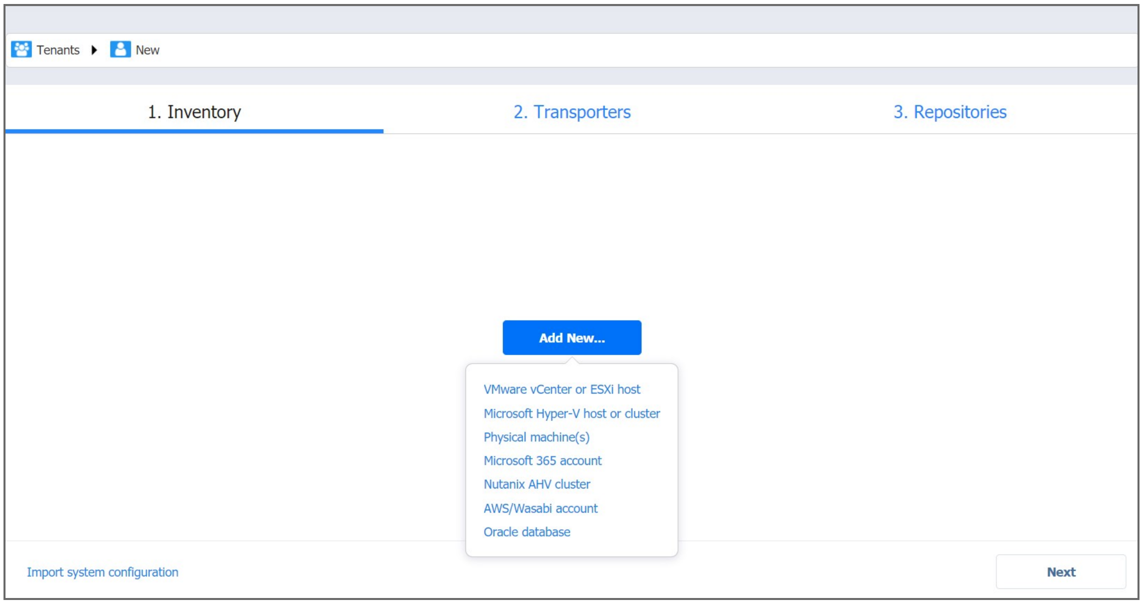
Multi-Tenant Mode

This section covers the following topics:

- “Tenant Creation” on page 345
- “Tenant Configuration” on page 344
- “Tenant Management” on page 347
- “Granting Self-Service Access” on page 358

Tenant Configuration

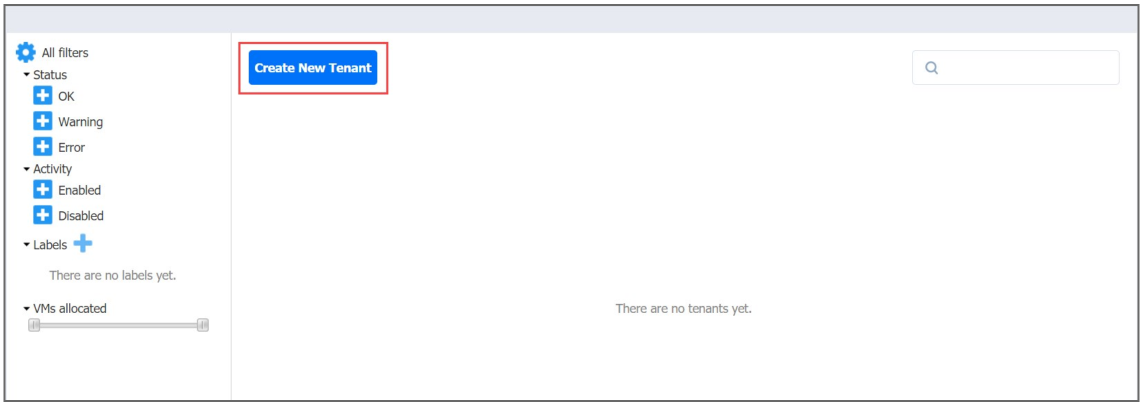
After creating a new tenant, click the tenant to open the initial Tenant Configuration Wizard which will guide you through the tenant setup process. Refer to "First Steps with NAKIVO Backup & Replication" on page 28 for a description of the initial configuration wizard.



Tenant Creation

To create a new tenant, follow the steps below:

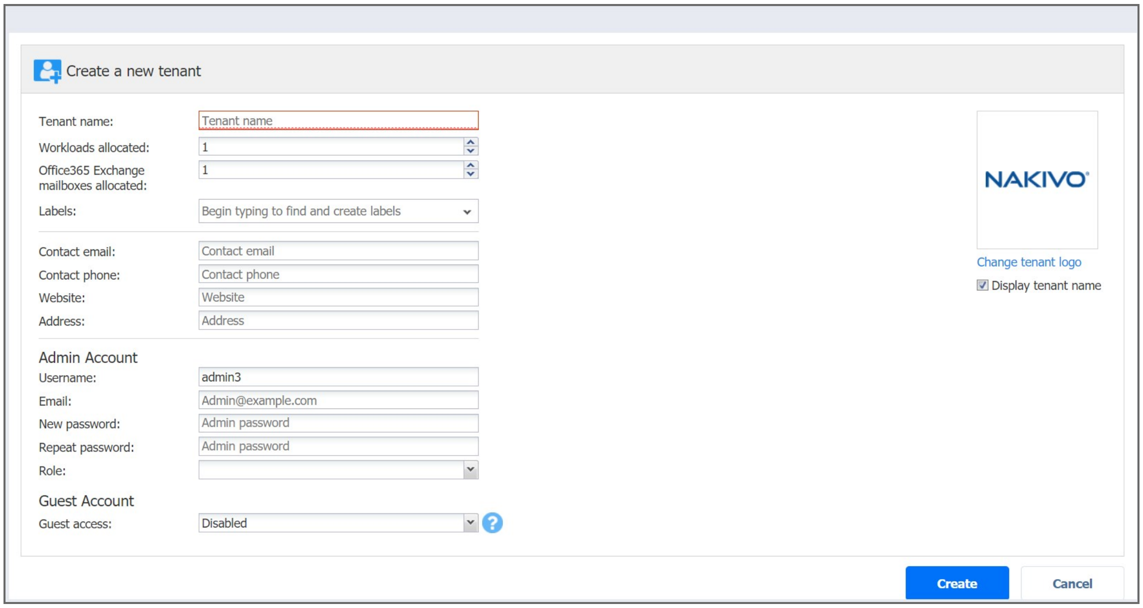
1. Log in to NAKIVO Backup & Replication as a Master Admin.
2. Click **Create New Tenant.**



3. In the **Create a new tenant** dialog, do the following:
   - **Tenant logo**: To add a tenant logo, click **Change tenant logo**, navigate to a new image, select it, and click **Open**.
   - **Tenant name**: Specify a name for the tenant. By default, the tenant name will be displayed under the tenant logo. If you do not want the tenant name to be displayed, deselect the **Display tenant name** check box.
   - **Workloads allocated:** Specify the number of workloads that you would like to allocate to the tenant.
   - **Office365 Exchange mailboxes allocated**: Specify the number of Office365 Exchange mailboxes that you would like to allocate to the tenant.
   - **Labels**: Assigning a label to a tenant allows you to quickly sort existing tenants into different categories, such as location, SLA level, and so on. You can do the following:
     - To create a new label and assign it to the tenant, enter the new label name in the **Labels.**
     - To assign an existing label to the tenant, choose the label name from the **Labels** drop-down list.
   - **Contact email**: Enter the tenant's contact email.
   - **Contact phone**: Enter the tenant's phone number.
   - **Website**: Enter the tenant's website address.
   - **Address**: Enter the tenant's physical address.
   - **Admin Account**: The admin account has access to the product features inside the tenant dashboard (such as edit and update tenant inventory, Transporters, and Backup Repositories, as well as creating and managing jobs and groups). Specify the credentials for the admin account:
     - **Username**: A unique login for accessing the tenant self-service interface.
     - **Email**: An email address of the tenant admin that will be used for sending email notifications to the tenant.

    - **New password**: Create a password for accessing the tenant self-service interface.
    - **Repeat password**: Repeat the password you've just created.
    - **Role**: Choose a role for the admin account. Refer to “Managing User Roles” on page 227 for more details on managing user roles.
- **Guest Account**: If **Guest access** is selected, the guest user will be able to view Dashboards, generate reports, and recover files (optional). Guests will not be able to run, edit, or delete jobs or access Configuration. To complete creating a guest account, enter the options as follows:
    - **Username**: A unique login for accessing the tenant self-service interface.
    - **Email**: An email address of the tenant guest that will be used for sending email notifications to the tenant.
    - **New password**: Create a password for accessing the tenant self-service interface.
    - **Repeat password**: Repeat the password you've just created for accessing the tenant-self-service interface.
    - **Role**: Choose a role for the guest account. Refer to “Managing User Roles” on page 227 for more details on managing user roles.

4. Click **Create**. The tenant appears on the **Tenants** dashboard.



Create a new tenant

Tenant name:	Tenant name
Workloads allocated:	1
Office365 Exchange mailboxes allocated:	1
Labels:	Begin typing to find and create labels
Contact email:	Contact email
Contact phone:	Contact phone
Website:	Website
Address:	Address

Admin Account

Username:	admin3
Email:	Admin@example.com
New password:	Admin password
Repeat password:	Admin password
Role:	

Guest Account

Guest access:	Disabled

Tenant Management

This section covers the following topics:

Using Filters

- About Filters
- Applying Filters
- Dismissing Filters

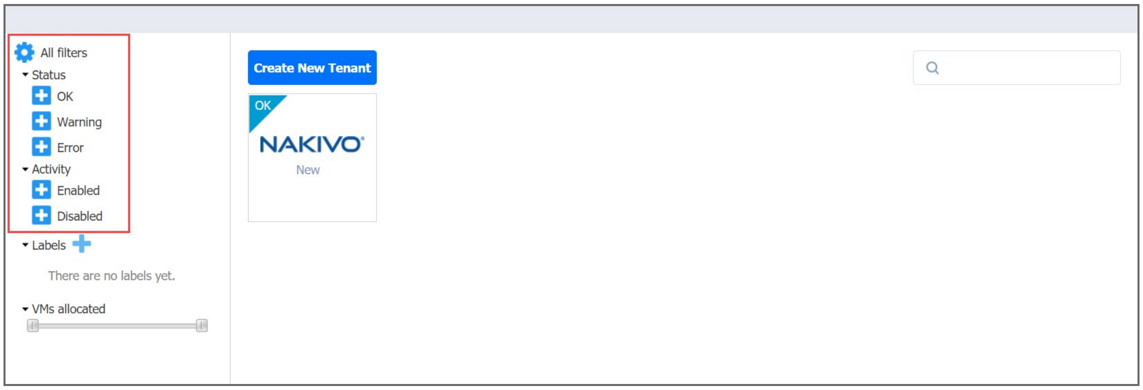
About Filters

NAKIVO Backup & Replication comes with four built-in filters that allow you to quickly display tenants according to their state. The following filters are available:

- **OK**: Displays tenants that have no errors and notifications.
- **Warning**: Displays only tenants that have notifications.
- **Error**: Displays only tenants that have errors.
- **Enabled**: Displays only enabled tenants.
- **Disabled**: Displays only disabled tenants.

Applying Filters

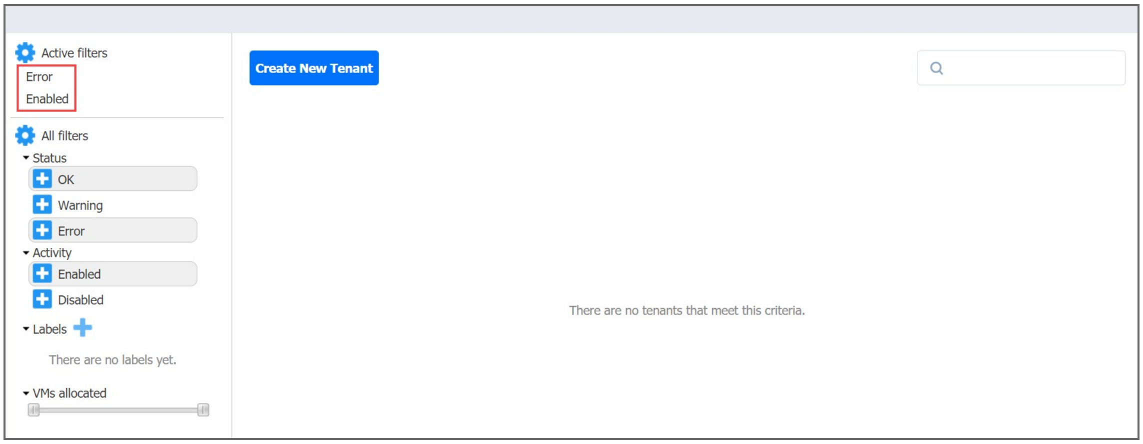
To apply a filter, click on the filter name.



The filters that are currently applied are displayed under the **Active Filters**.

Dismissing Filters

To dismiss a filter, click the filter name under **Active filters**.



There are no labels yet.

There are no tenants that meet this criteria.

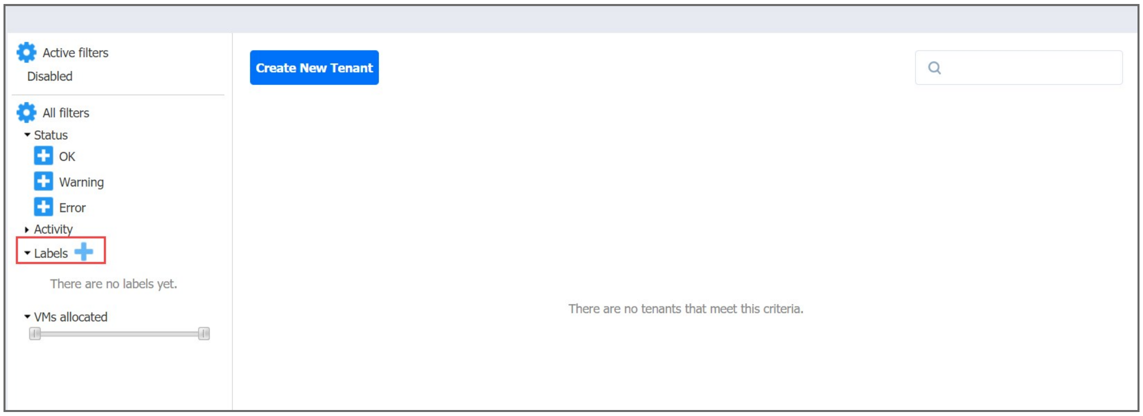
Using Labels

About Labels

With NAKIVO Backup & Replication, you can create custom labels and assign them to tenants. Assigning a label to a tenant allows you to quickly sort existing tenants into different categories, such as location, SLA level, etc.

Creating Labels

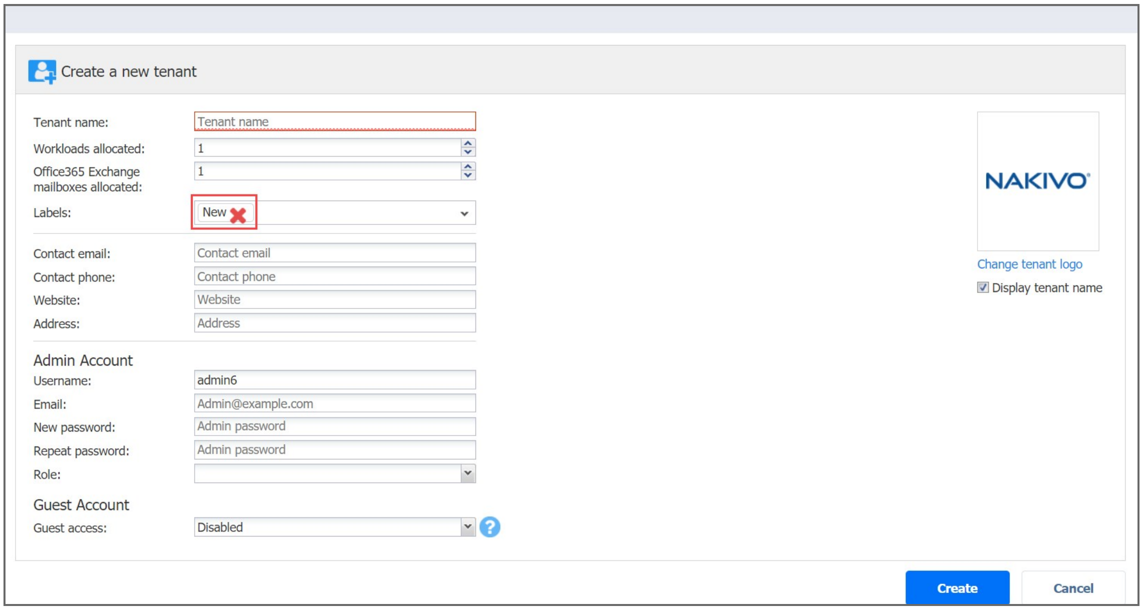
To create a new label, click the **Plus** icon next to **Labels** and enter a name for the new label, and press the **Enter** key.



You can also create a new label when creating a new tenant.

Assigning Labels to Tenants

You can assign a label to a tenant either during the tenant creation or by editing the tenant.



Create a new tenant

Tenant name: Tenant name

Workloads allocated: 1

Office365 Exchange mailboxes allocated: 1

Labels: New

Contact email: Contact email

Contact phone: Contact phone

Website: Website

Address: Address

Admin Account

Username: admin6

Email: Admin@example.com

New password: Admin password

Repeat password: Admin password

Role:

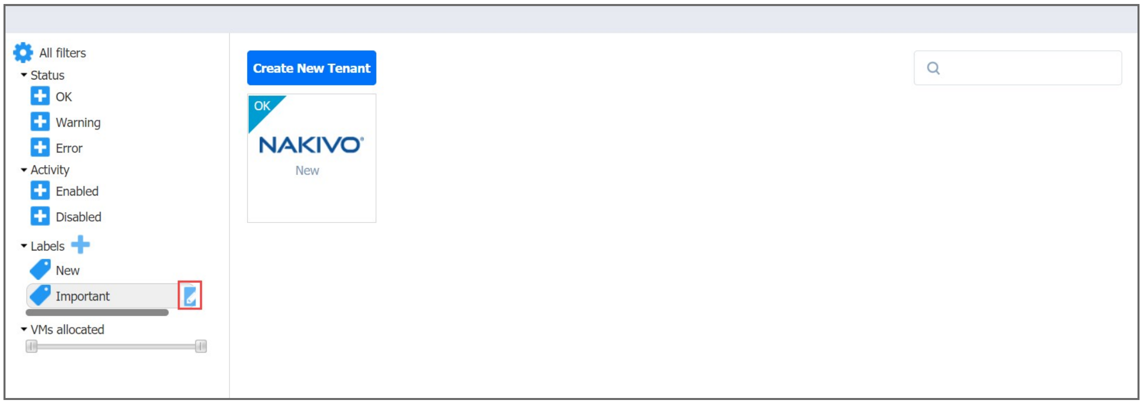
Guest Account

Guest access: Disabled

Editing Label Names

To change a label name, do the following:

1. Hover over the label.
2. Click the **Edit** icon.



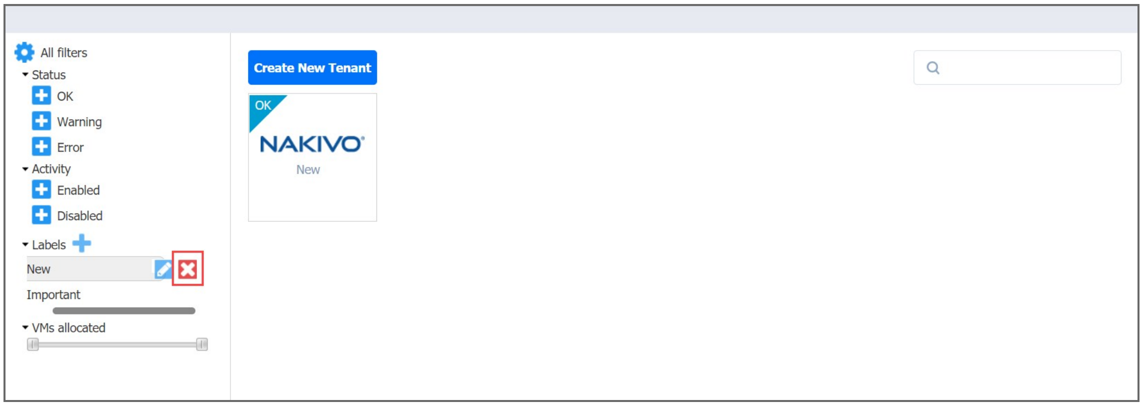
3. Enter the new label name and press the **Enter** key.

Deleting Labels

To permanently delete a label, do the following:

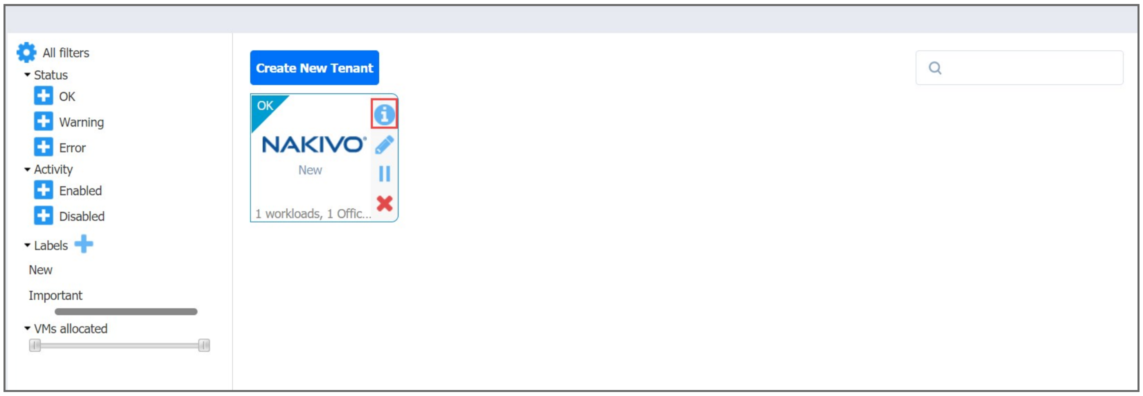
1. Hover the mouse pointer over a label.
2. Click the **Delete** icon.

3. In the dialog box that opens, click **Delete** to confirm that you wish to permanently delete the label



Viewing Tenant Information

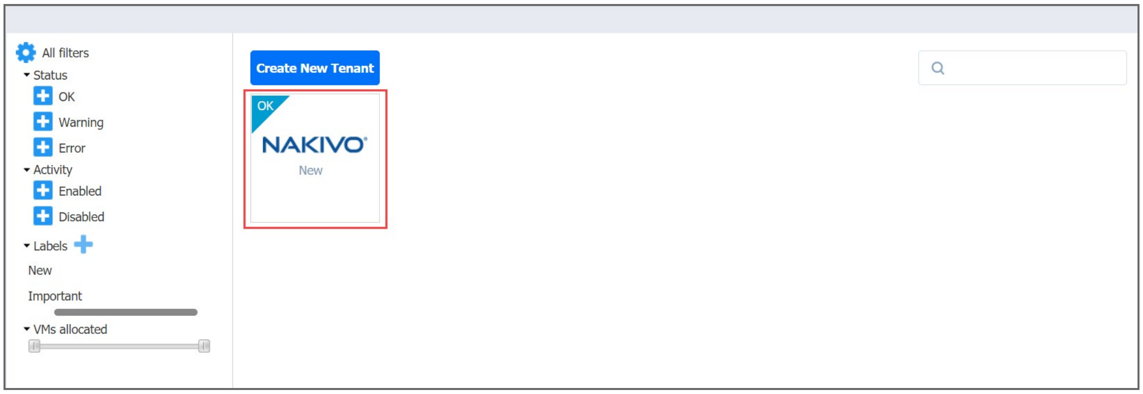
To view tenant information, hover over the tenant and click on the **Info** button.



The tenant information is displayed.

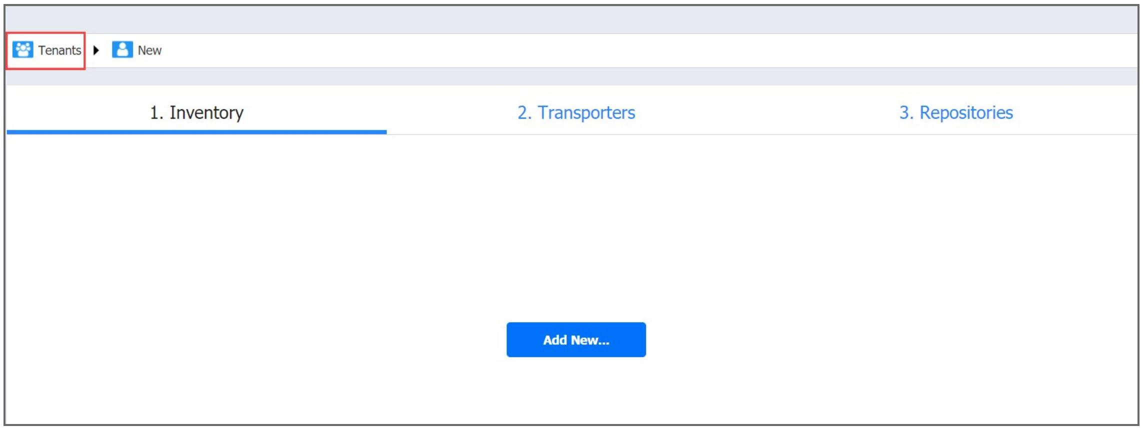
Opening Tenant Dashboard

In the multi-tenant mode, you need to open the tenant dashboard to perform tenant configuration, create jobs and groups for the tenant, and recover files and emails. To open a tenant dashboard, simply click the tenant.



Returning Master Admin Dashboard

To return to the **Master Admin** dashboard, click **Tenants** in the navigation bar.

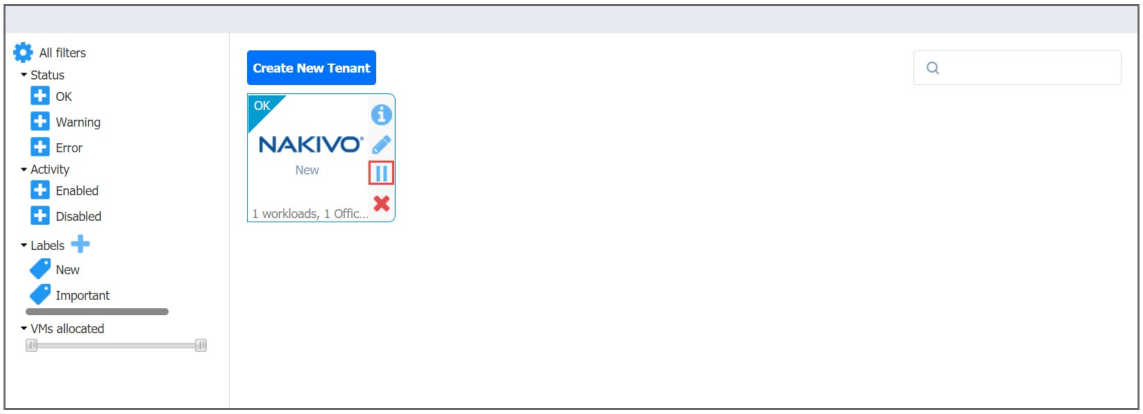


Disabling Tenants

In multi-tenant mode, you can disable a tenant to temporarily stop delivering backup, replication, and recovery services for that tenant. After disabling a tenant:

- Tenant admin and tenant guest will not be able to log in to the self-service interface. A message saying that the service has been disabled will be displayed after login attempts.
- Existing jobs will not be run on schedule.
- All currently running jobs will be allowed to complete.

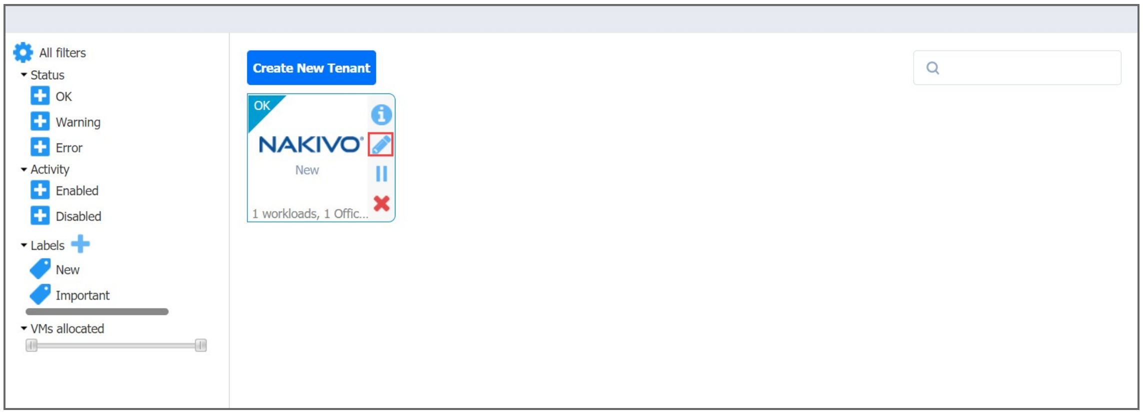
To disable a tenant, hover over the tenant and click the **Disable** button.



Editing Tenants

To edit a tenant, do the following:

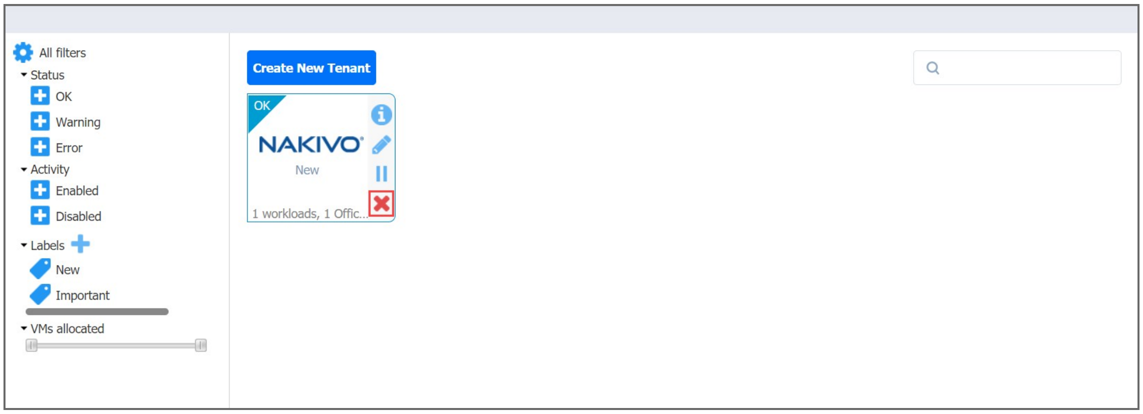
1. Hover over a tenant box and click the **Edit** icon.



2. In the **Edit** dialog that opens, make the required changes and click **Save**.

Deleting Tenants

To permanently delete a tenant from the product, hover over a tenant and click the **Delete** icon.



The tenant will be permanently deleted from NAKIVO Backup & Replication.

Tenant Transporters are not uninstalled and the Tenant Backup Repositories are not removed.

Granting Self-Service Access

In the multi-tenant mode, you can provide tenants with access to their dashboards. By default, a tenant admin account is automatically created when you create a new tenant. The tenant admin has full control over the product features inside the tenant dashboard (such as edit and update tenant inventory, Transporters, and Backup Repositories, and create and manage jobs and groups). For each tenant, one guest account can also be created. The tenant guest has limited permissions inside the tenant and can only generate job and group reports by default. To provide a tenant with access to the self-service interface, send the following information to the tenant:

- Link to NAKIVO Backup & Replication Director
- Tenant login
- Tenant password