AOMEI® Cyber Backup

User Manual

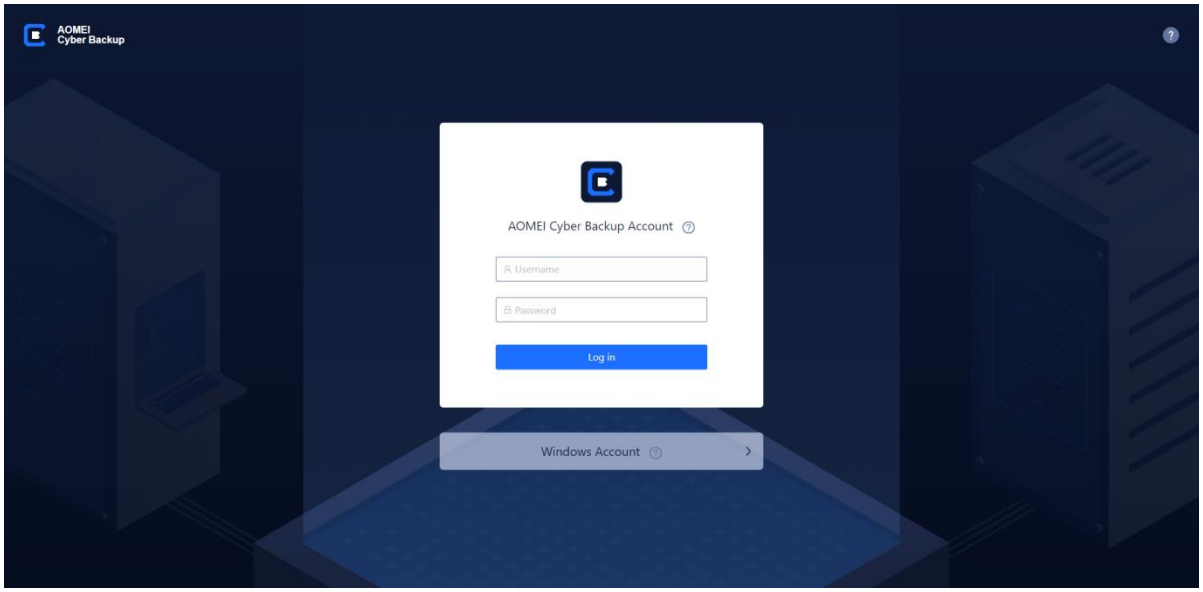

Table of Contents

1 Getting Started

This Chapter describes AOMEI Cyber Backup main features, the system requirements, supported file systems, operating systems and storage media.

Please take the time to become familiar with powerful and comprehensive features before using AOMEI Cyber Backup for the first time.

Additional assistance, including screenshots, can be viewed at: AOMEI Cyber Backup Help Guides

1.1 Overview of AOMEI Cyber Backup

AOMEI Cyber Backup provides a convenient and reliable solution for centralized backup management of multiple devices. It only needs to be deployed on one server, and then manage multiple devices via the web console.

- The most convenient centralized backup virtual machine software, no need to install any agent on the virtual host device.
- Monitor and manage the backup of the equipments via central control server.
- Back up all devices to a local or network location.

1.2 Software Requirements

1.2.1 Minimum Hardware requirements

- 1 Ghz x86 or compatible CPU
- 256MB RAM
- Mouse or another pointing device (recommended)
- 300 Mb of available disk space for installation

1.2.2 Supported Operating Systems

- Microsoft Windows 11
- Microsoft Windows 10
- Microsoft Windows 8/8.1
- Microsoft Windows 7 SP1
- Microsoft Windows Server 2022
- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 and 2012 R2
- Microsoft Windows Server 2008 R2 SP1

1.2.3 Supported Web Browsers

- Google Chrome 29 or advanced versions
- Mozilla Firefox 23 or advanced versions
- Microsoft Edge 25 or advanced versions

1.2.4 Supported Virtual Devices

1) Hyper-V environments：

- Microsoft Windows 11
- Microsoft Windows 10
- Microsoft Windows 8/8.1
- Microsoft Windows Server 2022
- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Windows Server 2012 R2
- Microsoft Hyper-V Server 2012 R2
- Microsoft Hyper-V Server 2016
- Microsoft Hyper-V Server 2019

2) VMware ESXi versions：

- ESXi 6.0 and above versions

1.2.5 Supported Storage Type

AOMEI Cyber Backup supports all storage devices recognized by Windows, such as IDE, SATA, SCSI hard disks, solid state disks, USB external disks, Redundant Array of Independent Disks (RAID) and Network Attached Storage (NAS) .
AOMEI Cyber Backup supports Master Boot Record (MBR, Master Boot Record) and GUID Partition Table (GPT, Globally unique identifier Partition Table) disk standards, which can effectively complete the boot process of Unified Extensible Firmware Interface (UEFI, Unified Extensible Firmware Interface).

1.3 Install and Uninstall AOMEI Cyber Backup

Install

1. Run AOMEI Cyber Backup setup program XXXX.exe.

2. Click “I have read and agree to the license agreement”, and can browse the license agreement content.

3. Click “Advanced” to set HTTP port (default 9072), which is used to web communication. The installer will automatically open this port, please make sure that the port can pass through the firewall to receive or send requests.

4. Follow the next wizard installation guide to complete the installation.

Tips: When the system lacks the corressponding configuration file, it will install failed. Please download and install the configuration file manually according to the prompt information. After the configuration file is installed successfully, you need to restart the system to apply the corresponding system configuration and then install software again.

Uninstall

The software can be uninstalled using one of the following two methods.

1. Go to the Start Menu -> AOMEI Cyber Backup -> Uninstall AOMEI Cyber Backup.

Or

2. Go to the Windows Control Panel -> Uninstall Program, right-click AOMEI Cyber Backup and uninstall it.

Tips: If you don't want to keep any software usage information on the current device, you can check the "Delete software settings" option, which can delete all custom settings in the software. But if you want to upgrade the software, please don’t select this option.

2 Access Web Console

After install AOMEI Cyber Backup, you can click and run the software to open web console on this computer. Or, open the login address on web browser of other computers to access.

2.1 Native Access

After install AOMEI Cyber Backup, you can click and run the software on this computer. Then, it will open web login page of console. After that, you can use AOMEI Cyber Backup account or Windows account to log in it.

- AOMEI Cyber Backup account

  It is the default admin account of AOMEI Cyber Backup. The account can create sub-accounts for other users and assign corresponding permission.

  Tips: if the sub-accounts miss password, only the admin account can help to reset the password.

- Windows account

  It is sup-administrator account of this computer that installed AOMEI Cyber Backup. Other windows accounts temporarily can’t be supported.

2.2 Universal Access

You can remote access the web console on other computers that don’t install AOMEI Cyber Backup software. But, other computers and the computer that installed AOMEI Cyber Backup must be under the same LAN.

Type into the login address on the address bar of a browser to open web console. Then log in the web console via AOMEI Cyber Backup account (admin account or sub-account).

The login address is composed of the IP address of this computer that installed AOMEI Cyber Backup and the HTTP port (default 9072, also can custom port). Such as: https://192.168.0.1:9072/

3 Devices Management

Before creating backup task, you need to add the devices that you want to back up.

AOMEI Cyber Backup currently supports VMware ESXi and Hyper-V only. In the future, databases, PCs, and servers will be supported.

3.1 Add Devices

You don't need to install the agent program of devices on the computer. Only need the device information and account to add.

1. After log into the web console, click "Devices" on the left menu bar, then select device type you want to add. (VMware ESXi as the example).

2. Click "Add VMware ESXi", then type into the device's IP address or name, then fill in the account that log in the device.

3. Click "Confirm" to add the device.

Tips: If the adding time of a device is too long, you can click "Add in background", then it will exit the adding page and continue to add this device in the background. Then you can perform other operations on other pages, even exit the web console.

3.2 Bind Devices

After adding the device, you need to authorize license for the device. That's to say, you need to bind a license with the device so that you can create backup for it.

When the authorized devices have reached the upper limit of the devices that can be supported by the license, it can no longer continue to authorize new devices unless upgrading licenses.

1. Click "•••" on the added device, select "Bind Device".

2. Check the prompt information and click "Confirm" to bind the device.

Tips: After the device is successfully bound, it cannot be unbound and transfer the license to a new device.

3.3 Manage Devices

Device Details

Click "•••" on the added device, select "Details" to check the device information.

Delete Device

Click "•••" on the added device, select "Delete". When the device is deleted, it will be unable to continue to backup for the device.

And, if there are related tasks for the device, you need to first delete the corresponding task, then delete the device.

Tips: Delete Device can't de-authorize the device.

Edit Device

If the login certificate of the device is changed, Click "•••" on the added device, select "Edit", then type into the new certificate.

Refresh Device

Click "..." on the added device, select "Refresh" to refresh virtual machines of the device.

Note:

- When adding a Hyper-V device, to ensure the smooth running of the Hyper-V task, you need to manually download the configuration file and run it on the Hyper-V device to be added.

4 Backup

When you add and bind devices, you can continue to create backup tasks for them.

4.1 Create Task

1. Click "Backup Task" on the left menu bar.

2. Click "Create New Task" to open the task creating page.

3. Set a "Task Name". It will have a default name.

4. Select "Backup Type": VMware ESXi Backup and Hyper-V Backup are supported currently.

5. Select "Device Name", and then check one or multiple virtual machines under the device.

Tips:

- Only added and bound devices can be selected to backup. If you don't add any devices, you first need to add and bind devices. Please refer to Chapter 3.
- When a virtual machine has already been backed up in an existing backup task, you can't select the virtual machine again to create a new task. If you want to re-create backup task for it, please delete the virtual machine from the existing backup task first.

6. Select "Backup Target" to save backups. You can select a local or network path.

  - Create a new locate path: it will list the local directory of this computer that installed AOMEI Cyber Backup, then you can select a location as backup target.
  - Create a new network path: you can type into a network path (such as: 192.168.1.1\data), then fill in username and password of the network path to add. After that, you can continue to select a folder of the network path as backup target.
  - Favorite Storage: it will list all added backup target. So, you can select the favorite backup target without adding it again.

As for backup target management, please refer to Chapter 6.

7. Set Schedule Backup and Backup Scheme. Generally, the schedule and scheme are enabled by default. You can change the schedule and scheme based on your needs, or disable them. For more details, please refer to the following 4.2 and 4.3 parts.

8. Click “Start Backup” to create the backup task and perform backup now. And, when you enable schedule, you can select “Add the backup and start backup now” or “Add the schedule only”.

4.2 Schedule Backup

Schedule Backup help you back up your devices automatically and regularly, which can enhance data security to a large extent.

When you create a new backup task, it enables a schedule by default.

Default Schedule:

Full backup: at 17:24 of every Monday.

Incremental backup: at 17:24 of every Tuesday, Wednesday, Thursday, Friday.

You can click the “default schedule content” into schedule setting page. Then, you can modify the schedule or disable it.

4.2.1 Backup Way

AOMEI Cyber Backup supports Full Backup, Incremental Backup and Differential Backup. Incremental Backup is recommended.

Full Backup: Back up all data of the machines you selected in the backup task. The first backup must be full backup. And, full backup is the basic of Incremental and differential backup.

Incremental Backup: Back up changed or added data based on the previous related backup, either a full or incremental backup depending on what was last done.

Data that have not changed will not be backed up. Thus, the backup time and storage space required for incremental backups are both less than a full backup.

A Full Backup must exist as the start point of a series of incremental backups.

A typical Incremental in time sequence backup:

progression would be as follows.

Full Backup, as basis

Incremental Backup 1

Incremental Backup 2

…

Incremental Backup n.

All the backup versions in an incremental backup series share a sequential relationship so if any one of the incremental backup version in the sequence is damaged or missing, then subsequent backup versions will be invalid.

When you do the restore, only need to select an incremental backup version to restore, then data can be recovered to the state when the selected incremental backup was done.

Differential Backup: Back up changed or added data based on the last full backup was performed. Differential backup is always based on the related full backup.

Therefore, compared to a full backup, the backup time and storage

space required are both normally much less.

If one differential backup becomes damaged or lost, it will not affect the subsequent

differential backup. But, if the related full backup is damaged or lost, all differential backups are invalid.

When restore, only need to select a differential backup file to restore, then data

can be recovered to the state when the selected differential backup was performed.

If data is added or changed significantly then each differential backup will

become progressively larger, because each one will contain more changes

made since the last full backup was performed. Compared to an incremental

backup, differential backup takes more time and requires more disk space. So Incremental Backup is recommended.

4.2.2 Schedule Type

AOMEI Cyber Backup supports Everyday, Every Week, Every Month (by week or date) schedules.

Everyday

Set a future time point to perform the backup task once each day.

Set a time frame in a day first then choose the time interval between each

backup. It will perform the backup at intervals of 1, 2, 3, 4 or 6 hours

within the selected time frame each day.

Every Week

Choose the day(s) for the backup task. And then, set a time point. It will automatically perform the backup at a given time point on the chosen day(s) each week.

When selecting incremental or differential backup way, you can set full backup, incremental or differential backup at the same time. For example, you can set full backup on every Monday, incremental backup on every Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday.

Different backup types are distinguished by different colors, and you can switch the backup type or cancel the setting by clicking the mouse on the “day” box.

Every Month (By week)

Divide a month by week. Choose one day of the week to perform the backup task each month. Multiple days can also be selected. For example, perform the backup on the third Tuesday of each month.

When selecting incremental or differential backup way, you can set full backup, incremental or differential backup at the same time. For example, you can set full backup on the first Monday every month, incremental backup on the second, third and fourth Monday every month.

Different backup types are distinguished by different colors, and you can switch the backup type or cancel the setting by clicking the mouse on the “day” box.

Every Month (By date)

Choose one day from the calendar to perform the backup task each

month. Multiple days can also be selected on the calendar.

When selecting incremental or differential backup way, you can set full backup, incremental or differential backup at the same time. For example, you can set full backup on 1st every month, incremental backup on other days every month.

Different backup types are distinguished by different colors, and you can switch the backup type or cancel the setting by clicking the mouse on the “day” box.

4.3 Backup Cleanup

Backup Cleanup help you clear history backup versions based on rule to save storage space.

When you create a new backup task, it enables a cleanup rule by default.

Default cleanup rules:

Full backup retention period: 60 Day.

Incremental/Differential backup retention period: 7 Day.

Always retain: the first full backup.

You can click the “default clean content” into setting page. Then, you can modify the clean rule or disable it.

You can modify the retention time of Full/Incremental/Differential. So, old backup versions that meet the set time will be deleted automatically.

And, you can enable always retain the first full backup (every week/month/ quarter/year). So, the first full backup will not be deleted.

Full backup clean will delete single full backup when it meets the clean rule.

Incremental backup will delete all incremental backups of a whole incremental backup group when the last incremental backup of the group meets the clean rule (full backup of the group isn’t deleted until it meets the full backup clean rule).

Differential backup will delete differential backup when it meets the clean rule (the related full backup isn’t deleted until it meets the full backup clean rule).

Note:

- Backup scheme will be applied for all backups, include old backups created before enabling the backup scheme.
- Backup scheme will detect if backups meet the delete rule only when the backup task is performed successfully every time.

4.4 Backup Management

When backup tasks are created, they will be added to Task List. Then, you can easily check the status, destination, next backup time of all tasks here.

For the single task, you can check progress, details and logs of the task, and edit, run or delete the task.

1. Click “...” on the single task, click “Backup” under the drop-down menu, then you can manually run Full/Incremental/Differential Backup for the task.

2. Click “...” on the single task, click “Task Details” under the drop-down menu, then you can check details for the task, such as backup source, destination, related settings, and so on.

3. Click “...” on the single task, click “Edit” under the drop-down menu, then you can edit the task. For example, modify backup destination, schedule and clean settings.

4. Click “...” on the single task, click “Task Progress” under the drop-down menu, then you can check the detailed progress of the task when it is running.

5. Click “...” on the single task, click “Restore” under the drop-down menu, then you can select a backup version to restore. For more details about restore, please refer to Chapter 5.

6. Click "..." on the single task, click "Task Log" under the drop-down menu, then you can check the detailed log (backup result/reason, backup type, backup time) of the task.

7. Click "..." on the single task, click "Delete Task" under the drop-down menu, then you can delete the task only, or delete task and related backup files.

Note:

- It always performs full backup the first time.
- When the last backup status of the virtual machine has changed, it will do a full backup again. The changed backup status includes that the virtual machine is restored, or the last backup file is incomplete.
- When the device related to the task is not bound with a license, the task will suspend the schedule backup. When the device is successfully bound, it will start schedule backup automatically.

4.5 Backup Log

You can check the backup logs of all tasks under Task-->Backup Logs. It will record backup result, backup way, backup size and backup time of every task.

And, you can filter logs based on task, device, result and time so that you can quickly check needs logs.

5 Restore

When you create backups for your devices, you can restore them at any time.

5.1 New Restore

1. Click "Backup Management" on the left bar, select "Restore Records".
2. Click "New Restore" to open restore page.
3. Select source device, please refer to the next 5.1.1 part.
4. Select restore content (backup version), please refer to the next 5.1.2 part.
5. Select restore target location, please refer to the next 5.1.3 part.
6. Click "Start Restore" to perform the restore.

5.1.1 Select Source

1. On the restore page, click "Select" of Select Source, it will list all backup tasks on the open page.

2. Select a backup task you want to restore, it will list all backed up devices on the task.

3. Select a device that you want to restore.

4. Click “Ok”. It will list the selected device as source on the restore page.

5.1.2 Select Content

1. On the restore page, click “Select” of Select Content, it will list all backed up virtual machines of the selected device.

2. Select a virtual machine you want to restore, and then select a backup version of the virtual machine.

3. Click “Ok”. It will list the selected backup version as restore content on the restore page.

5.1.3 Select Target

Restore to original location

If you want to restore to original location, you don’t need to select target. “Restore to original location” is selected by default, you can directly start restore.

For VMware ESXi device, “Restore to original location” will restore system and data of the original virtual machine to the status that the restored backup version is created. But, if you create snapshots before restore, it will still retain these snapshots, you can recover these snapshots after when you need them.

For Hyper-V device, “Restore to original location” will overwrite the original virtual machine with the backup version. If there are new important data, please back up them before restore.

Restore to new location

You also can select “Restore to new location”, It will create/restore the virtual machine on a new location.

5.2 Restore from backup task

1. On Task page, locate the task you want to restore, click “...”--> “Restore”.

2. Select a backup version on the open page.

3. Select the target (original location or a new location) that you want to restore to, please refer to 5.1.3.

4. Click “Start Restore” to perform the restore.

5.3 Restore history version

1. Click “Backup Management” on the left bar, select “History Versions”.
2. Browse and select a history version that you want to restore.
3. Click “...” of the history version, select “Restore” on the drop-down menu.
4. Select the target (original location or a new location) that you want to restore to, please refer to 5.1.3.
5. Click “Start Restore” to perform the restore.

5.4 Restore Records

When click “Start Restore”, it will start to perform the restore and add the restore task to restore list under Restore Records.

You can check the restore source, target, status and time of every restore task.

When a restore task is running, you can click “...” on the restore task, select “Stop Restore” to stop the restore progress when you don’t want to continue to restore. But, the restore operation is irreversible, so the data overwritten or deleted can’t be recovered.

Note:

- Before the restoration starts, you need to shut down the virtual machine.
- “Restore to original location” must confirm the original location exist. Or else, you can only select “restore to new location”.

6 Destination Management

You can add the target locations first, then they will be listed under the Favorite Storage of creating task page, so you can easily select destination when you create a backup task. And, you can also easily manage destinations under Destination Management.

AOMEI Cyber Backup currently supports local and network location as destination.

6.1 Local Location

You can select the local locations of this computer that installed AOMEI Cyber Backup software as backup destination.

6.1.1 Add local location

1. Select “Target Storage” on the left bar, click “Local Storage”.

2. Click “Add Target”, it will list the local directories that installed AOMEI Cyber Backup software.

3. Browse and select a local location, click “OK” to add the destination.

6.1.2 Manage local destination

When adding local location successfully, it will be listed on the target list.

1. You can see the detailed path and free space of the local location.

2. Click “•••” on the added local destination, select “Associated Tasks” to check all backup tasks that back up to the location.

3. Click “•••” on the added local destination, select “Delete” to delete the location. If there are some backup tasks are using the location as destination, you need to first delete these tasks, then continue to delete the location.

4. Click “•••” on the added local destination, select “Refresh” to refresh space information of the location.

6.2 Network Location

You can add a Network/Share drive as backup destination. But, the network location and backup devices must be on the same LAN.

6.2.1 Add network location

1. Select “Target Storage” on the left bar, click “Network Storage”.

2. Click “Add Target”, then type into a network path (such as: 192.168.1.1\data) on the open page, then click “>”.

3. Fill in username and password of the network path, or use “Anonymous login” when you don’t set username and password for the network path, then click “Confirm” to verify login information.

4. When verify successfully, it will list all directories under the network path. Please browse and select a directory, click “OK” to add the network location.

6.2.2 Manage network destination

When adding the network location successfully, it will be listed on the target list.

1. Click “•••” on the added local destination, select “View details” to check the detailed path and free/used space of the network location.

2. Click “•••” on the added local destination, select “Authentication” to edit and re-verify the login information of the network path.

3. Click “•••” on the added local destination, select “Associated Tasks” to check all backup tasks that back up to the location.

4. Click “•••” on the added local destination, select “Delete” to delete the location. If there are some backup tasks are using the location as destination, you need to first delete these tasks, then continue to delete the location.

5. Click “•••” on the added local destination, select “Refresh” to refresh space information of the location.

7 Settings

There are global settings for the software, including: system settings, operation logs, user management, and serial numbers.

7.1 System Settings

1. Security: Set Automatic Logout time after a given time of user inactivity.

2. About: Display software information (software name and current version), official website address, contact email. And, click "Check for Updates" to immediately check for an updateable version. When there is an updateable version, continue to click "Download New version" to jump to the update webpage to download the latest version.

7.2 Operation log

The operation log mainly records the operation behavior of each user, including: login, create task, add device/target, and so on.

You can filter the log via type and time to view specific operation logs.

7.3 Users Management

The admin account can create and manage users under Users Management.

7.3.1 Create user accounts

1. Click “Create account”, then type into user account name and password, and confirm the password.

2. Click “Next”, then set the role of the user account. Different role will match different permissions.

3. Click “OK” to add the user account.

Role Details:

Admin: Currently, there is only one administrator account, which has the highest management role. The role cannot be assigned to other users.

You can use the Windows super administrator account as admin to log in.

The highest administrative privileges of the admin account:

1) Only the admin account can create other users accounts.

2) Only the admin account can view the list of all users, and modify the role or reset passwords for other users. Other users can only view their own account information and modify their own passwords.

3) Only the admin account can manage serial numbers.

Viewer: Viewer can only view dashboards and abnormal events, and can view and operate system settings, and view their own account information under user management.

Monitor: Monitor can only view tasks, devices, targets, backup management, and can view and operate dashboards, abnormal events, system settings, and view their own account information under user management.

Backup Operator：Backup Operator can only view target, backup management, and can view and operate dashboards, abnormal events, tasks, devices, system settings, and view their own account information under user management.

Restore Operator：Restore Operator can view and operate dashboards, exceptions, tasks, devices, targets, backup management, system settings, and view their own account information under user management.

7.3.2 Manage accounts

Admin account can view the list of all users, and modify the role or reset passwords for other users.

Other role accounts can view own account information.

Modify Password: all users can change their own password, but need to enter the old password to verify first.

Reset Password: When the user account’s password is forgotten, you need to contact the admin user to reset the password.

1) Enter the admin password.

2) Enter new password and confirm password.

After the setting is successful, you can log in to the user account with the new password.

8 License Management

You can check the following information:

License type and period: when the license/subscription expired, it can't continue to back up for your devices until renewing the subscription.

Bound Devices: it is the number of devices that has been bound with the license.

Device upper limit: it is the number of devices in total that the license allows binding.

Virtual hosts and clusters: it shows all added devices' information(device name, IP address, and the number of virtual machines) and bound status. When the device is not bound, you can click the "bind" button on the right side of the list to bind it.

9 Overview

Overview is a global monitor, including dashboards and alerts.

9.1 Dashboard

Dashboard is the data monitor of multiple functional modules including tasks, devices, targets, and so on. You can add modules that you want to monitor.

9.1.1 Add views

1. Click "Add View", then check modules you needed.

2. Click "Confirm" to add these modules to dashboard (or uncheck modules to remove).

9.1.2 Manage views

1. Click "Manage View", all modules on the dashboard will be movable status.

2. Then, you can drag modules to resize their location.

3. Or, you can click "X" button on module to remove it.

4. Click "OK" to save the modification.

9.1.3 Views details

- Task

It counts the number of tasks that different execution status (Success, Failure and Partial Failure) each day of the last week.

- Schedule Tasks

It lists all schedule tasks and next run time of every schedule.

- Task Statistics

It counts the number of task that different execution result (Finish, Alerts and Error) of the last 7 days, 30 days, 90 days, year.

- Data backed up

It counts the amount of data backed up every day of the last week.

- Data Backed up Statistics

It lists the amount of data backed up, the number of backup versions and devices of all tasks since you using the software.

- Devices

It displays the number of all added devices, device type, and the number of virtual machines in every device.

- Target

It lists all added target locations, and displays the space usage of every location. When the free space of a target is insufficient, a red warning will be shown.

- Error Log

It displays all error logs of failed backup.

9.2 Alerts

It shows error logs of all failed tasks. And, it classifies error logs based on the abnormal type of device, target and other.

For single error log, you can click "..." to view details or remove it via ignoring the record.

10 Technical Support

Before seeking technical support, please first refer to our tutorials at https://www.ubackup.com/enterprise/help/

If further assistance is required, please send an email to support@aomeitech.com.

AOMEI Cyber Backup common FAQs:

Q: Why does the web console suddenly log out?

A: An account is allowed to log in a single device at the same time. If the administrator has logged into your account, you will be temporarily logged out.

In another case, if you have set automatic logout on the Settings-->System Settings-->Security page, it will also automatically logout when there is no operation at the set time.

Q: Why do I get "The network share/NAS username or password is wrong..." while backing up?

A: It may be that the username and password of the share/NAS you added have been changed. You can click the detailed error message to authenticate the network location. After the verification is successful, you can back up again.

Q: What versions of VMware ESXi does AOMEI Cyber Backup support?

A: VMware ESXi 6.0 and above versions are supported.

Q: Why is the backup size of an incremental or differential backup of a virtual machine the same size as a full backup?

A: It may be that the virtual machine has been restored, and the program will back up the virtual machine as a new virtual machine.

Q: Does AOMEI Cyber Backup now support backup of VMware vCenter Server?

A: Currently, backing up VMware vCenter Server is not supported.

Q: Which Hyper-V systems does AOMEI Cyber Backup support backing up?

A: Windows Server 2012 R2/2016/2019/2022 and Windows 8/8.1/10/11.

Q: What account do I need to use when adding a Hyper-V host?

A: You need to use the administrator account to add.

Q: Is it supported to backup virtual machines larger than 4G to FAT32 partition?

A: Not supported.

Q: What browsers does the web interface of AOMEI Cyber Backup support?

A: Google Chrome 29 or higher, Mozilla Firefox 23 or higher, Microsoft Edge 25 or higher.

Q: Why AOMEI Cyber Backup prompts 0x001084 error when backing up.

A: It may be caused by the previous situations:

The original virtual machine has been modified or deleted;

The uuid is changed after the virtual machine is restored to its original location;

And, we recommend that you create a new task to back up these virtual machines again.

11 Glossary

Term	Meaning

Backup	Backup is to store the selected data in a target, and the corresponding data file will be generated in the target. It can be used to restore to the original state when you need them.
History Versions	Each backup will generate a history version, which corresponds to point-in-time information. If data is lost, any history version can be used to restore its content to the corresponding point-in-time state.
Restore	Restore refers to restoring the content of the data files from the backup to the state of the backup point-in-time.
Full Backup	Back up all data of the machines you selected in the backup task. The first backup must be full backup. And, full backup is the basic of Incremental and differential backup.
Differential Backup	Back up changed or added data based on the last full backup was performed. Differential backup is always based on the related full backup. Therefore, compared to a full backup, the backup time and storage space required are both normally much less. If one differential backup becomes damaged or lost, it will not affect the subsequent differential backup. But, if the related full backup is damaged or lost, all differential backups are invalid. When restore, only need to select a differential backup file to restore, then data can be recovered to the state when the selected differential backup was performed.
Incremental Backup	Back up changed or added data based on the previous related backup, either a full or incremental backup depending on what was last done. Data that have not changed will not be backed up. Thus, the backup time and storage space required for incremental backups are both less than a full backup. A Full Backup must exist as the start point of a series of incremental backups. All backup versions in an incremental backup series share

	a sequential relationship so if any one of the incremental backup files in the sequence is damaged or missing, then subsequent backup versions will be invalid. When you do the restore, only need to select an incremental backup version to restore, then data can be recovered to the state when the selected incremental backup was done.
Network Path	A network drive is a storage device on a local access network (LAN) within a business or home. Within a business, the network drive is usually located on a server or a network-attached storage (NAS) device. A shared drive is a storage device on a local computer, which lets users quickly share files from computer-to-computer. The shared network most often operates on a Local Access Network (LAN).