User Manual

Table of Contents

1. About IDrive® 360

1.1 Introduction to IDrive® 360

IDrive® 360 is a web-based backup and recovery management platform for intuitively managing your enterprise-scale cloud backup. You can secure all the computers of your organization to IDrive® 360 's encryption-protected cloud and manage their backups through a unified web console. IT can oversee data protection at the company-level and assign backup plans for units, groups, or individual devices.

With regular backups of your computers, you enable instant business recovery from accidental data loss, data theft, server failure, hardware crash, malware corruption, and more.

The dual centralized web console platform includes:

1.1.1.1 IDrive® 360 backup console

Manage all the backup requirements of your organization from a single centralized platform. The Backup Console enables you to run and supervise backups remotely, thereby ensuring continuous data protection for uninterrupted workflow.

1.1.1.2 IDrive® 360 management console

The enterprise-grade Management Console facilitates unified management by allowing admins to easily add multiple units and users within their account and manage as well as monitor them from one location. It also allows you to configure application settings, administer connected computers, monitor account activities, modify settings, and perform various administrative functions.

1.1.1.3 Company administrator has access to the following functions

- ✔ Manage devices and backups for the entire company
- ✔ Manage users and units of the organization (add, edit, disable and delete from the account)
- ✔ Managing user's computer
- ✔ View activity log reports

1.1.1.4 Users have access to the following functions

- ✔ Manage backup and recovery of the units
- ✔ Create and apply backup plans
- ✔ Manage groups and push settings
- ✔ View custom reports and alerts

1.2 About the manual

This manual describes the most important functions for working with the IDrive® 360 Backup and Management Consoles. It is intended to help you to better understand the functionalities of the dual centralized web consoles of IDrive® 360 cloud backup and provide you with initial support.

This manual provides step-by-step instructions for the following topics:

- How to get started with IDrive® 360
- Managing IDrive® 360 Backup Console
- Managing IDrive® 360 Management Console
- IDrive® 360 user account management

2. General

2.1 Installation

To configure and add computers to your account and schedule backup and restore operations, you need to first download and install the IDrive® 360 application on your computers.

Once the installation is performed, the application creates a tray option on your system tray, and runs silently in the background with minimal GUI.

You may read the step-by-step instructions for installing and adding computers to your IDrive® 360 account from the **Add Devices** section of this user manual.

2.2 System requirements

Following operating systems and their respective versions are supported by IDrive® 360 :

Windows

- ✔ Windows 10
- ✔ Windows 8.1
- ✔ Windows 8
- ✔ Windows 7
- ✔ Windows 2019 Server
- ✔ Windows 2016 Server
- ✔ Windows 2012 Server
- ✔ Windows 2008 Server
- ✔ Windows Home Server

Mac

- ✔ Mac OS X 10.10 Yosemite or greater

Linux

Debian-based:

- ✔ Ubuntu
- ✔ Linux Mint

RPM-based:

- ✔ CentOS
- ✔ Fedora
- ✔ OpenSUSE Leap

2.3 Graphical user interface

IDrive® 360 is a web based application. To start working with it, open https://www.idrive360.com/enterprise/login in a web browser and sign in with your account credentials.

Note:

- If you do not have an IDrive® 360 account, you can create a new account by clicking the **Sign up** button

After successfully logging in, you will be directed to the Backup Console by default.

Menu bar

The menu bar is used for navigation through the backup console. In the menu bar, the Device, Backup Plan as well as Settings and Reports tabs are displayed. Additional actions can be performed by choosing the respective tabs.

Title bar

View your plan type, add computers to your IDrive® 360 account and access your profile from the title bar menu.

2.3.1 Backup console

With access to the Backup Console, add and manage devices for backup, schedule logical backup plans for computer groups, and configure various backup settings according to requirements.

2.3.2 Management console

With access to the Management Console, configure organizational data backup structure, manage users and their access rights, monitor storage space utilization, and general reports as needed.

2.4 My account

Manage your account settings from the **My Accoun**t section.

To edit your IDrive® 360 account details, click **Name->My Account** on the top right corner of the title bar. Modify your profile details, manage password and account cancellation from this section.

2.4.1 Profile details

You can modify your account details such as display name, email address and phone number. After modifying the required details, click **Save Changes**.

2.4.2 Password change

Your existing IDrive® 360 password can be changed from the **My Account** section. Type the current password, new password, confirm it, and click **Save Changes** to apply the changes.

2.4.3 Account cancellation

If you do not wish to continue with IDrive® 360 , you can choose to cancel your IDrive® 360 account any time by clicking the **Cancel my account** link.

In the cancellation pop up, enter the details like password, phone number, email address, reason for opting account cancellation and comments, if any. Click **Cancel my account** to apply the changes.

3. Devices

3.1 Computers

In this section, admin of the IDrive® 360 account or a company / unit administrator can add new computers and also perform mass deployment for Windows and Mac. This can be achieved under the **Backup Console -> Devices** tab.

3.1.1 Add devices

To add computers to the IDrive® 360 account, you need to install and configure the IDrive® 360 application on your computer.

Follow the below steps to configure PCs and MAC

1. Click the **Add Devices** button.
2. From the **Add Devices** section, select the checkbox to set your own encryption method on app installation.
3. Select the operating system to download the corresponding setup file.
4. Run and install the application on your computer. On installation, the backup agent will run silently in the background and the computer will be added to your IDrive® 360 account.

Note:

- ❖ You can also add computers to your account by copying the app installation link and sharing it. Open the installation link in the computer you want to add, download and install the setup.
- ❖ All the added computers appear in the Devices tab.

Follow the below steps to configure Linux

1. Click the **Add Devices** button.
2. In the **Add Devices** screen, go to the 'Linux' tab.
3. Follow the steps appropriate for the Linux OS

CentOS / Fedora / openSUSE

1. Download the .rpm package.
2. Open the terminal.
3. Run rpm -ivh IDrive360_<Deployment Code>.rpm

Ubuntu / Linux Mint

1. Download the .deb package.
2. Open the terminal.

3. Run dpkg -i IDrive360_<Deployment Code>.deb

The Linux machine will appear in the 'Devices' tab.

3.1.2 Deployment through group policy on Windows OS

You can centrally install (or deploy) the application for Windows onto machines that are members of an Active Directory domain, by using Group Policy.

In this section, you will find out how to set up a Group Policy object to deploy IDrive® 360 onto machines in an entire domain or in its organizational unit.

Prerequisites

Before proceeding with deployment, ensure that

- You have logged in and downloaded the IDrive® 360 MSI installer package
- Configuration ID copied from the **Add Devices** section in the Backup Console
- Shared folder, accessible via all the domain users
- You have an Active directory environment running Microsoft Windows Server

Steps to create a Group Policy Object (GPO) under active directory environment:

1. From the **Start** menu, go to **Administrative Tools** and open **Group Policy Management**.
2. In the **Group Policy Management** console, navigate to **Forest**, the folder for creating group policy.
3. Double-click **Domains** and navigate to **Group Policy Object**.
4. Right-click **Group Policy Object** and select **New** from the drop-down menu.
5. Assign a name to the GPO group and click **OK**.

Steps to assign and install the IDrive® 360 application on domain computers:

1. Right-click the new group policy and select **Edit** from the drop-down menu. This will launch the **Group Policy Management Editor**.
2. Navigate to **Computer Configuration ->Policies ->Software Settings ->Software installation**.
3. Right-click **Software installation** and navigate to **New ->Package**.
4. Locate the shared network folder with the IDrive® 360 MSI installer package.
5. Select the package and click **Open** to add to the software installation container.
6. Select **Assigned** and click **OK**. This process may take a while depending on the size of the software.
7. Right-click on the MSI package and select **Properties**. The **IDrive® 360 Properties** window appears.
8. Go to the **Deployment** tab. Under **Deployment type**, select **Assigned** and under **Deployment options**, select **Install this application at logon**, and click **OK**.
9. Right-click the domain and select **Link an Existing GPO**. **The Select GPO** screen appears.
10. Select the newly created Group Policy and click **OK**.

The IDrive® 360 application will be assigned to the domain users on the next sign in and to the domain computers on the next reboot.

Steps to register a set of computers under a particular group via GPO:

1. Copy the configuration ID from the **Add Devices** section in the Backup Console.
2. Create a batch file with (Example: IDrive360_Register_Group.bat) the following command:

```
msiexec /i "D:\IDrive360<token>.msi"
WRAPPED_ARGUMENTS="/GROUP_NAME=Group_Name
/CONFIG_ID=Copied_Configuration ID"

Example:
msiexec /i
"\\ws08r2\Share\Org\IDrive360_iRBftnA4XfMLkF7z1NRF2157.msi"
WRAPPED_ARGUMENTS="/GROUP_NAME=Managers
/CONFIG_ID=iRBftnA4XfMLkF7z1NRF2157"
```

Where:

- IDrive360_iRBftnA4XfMLkF7z1NRF2157.msi: The setup downloaded from the **Add Devices** page. Make sure the file is placed in share and the same is accessible across domain users.
- WRAPPED_ARGUMENTS="/GROUP_NAME=Managers /CONFIG_ID=iRBftnA4XfMLkF7z1NRF2157": The group name is 'Managers' and CONFIG_ID is the configuration ID copied from the **Add Devices** section in the Backup Console.

3. In the group policy, instead of IDrive® 360 installer, use the above batch file.
4. Deploy the batch file via GPO to add the computers to respective groups.
5. Upon successful deployment, the computers will be listed under the specified group name.

Steps to register a set of computers under a particular group with Private Key encryption method via GPO:

1. Sign in to your IDrive® 360 account.
2. Click the **Add Devices** button and select the **Set your own encryption method** check-box. Copy the configuration ID, and click **Download MSI** to download the IDrive® 360 MSI setup with private key encryption option.
3. Create a batch file with (Example: IDrive360_Private_Key.bat) with the following command:

```
msiexec /i "D:\IDrive360_PrivateKey.msi"
WRAPPED_ARGUMENTS="/GROUP_NAME=Group_Name /PVT_KEY=Pvt_Key
/CONFIG_ID=Copied_Configuration ID"

Example:
msiexec /i "
\\ws08r2\Share\Org\IDrive360_iRBftnA4XfMLkF7z1NRF2157_Private.msi
" WRAPPED_ARGUMENTS="/GROUP_NAME=Managers  /PVT_KEY=123456
/CONFIG_ID=iRBftnA4XfMLkF7z1NRF2157"
```

Where:

- IDrive360_iRBftnA4XfMLkF7z1NRF2157_Private.msi: The setup with encryption key option downloaded from the **Add Devices** page. Make sure the file is placed in share and the same is accessible across domain users.
- WRAPPED_ARGUMENTS="/GROUP_NAME=Managers /PVT_KEY=123456 /CONFIG_ID=iRBftnA4XfMLkF7z1NRF2157": The group name is 'Managers', the private key is '123456' and the Configuration ID obtained from **Add Devices** section in the Backup Console.

Note:

- ❖ The encryption key must contain minimum of 6 characters and maximum up to 250 characters.

1. In the group policy, use the created batch file to deploy the setup.
2. Deploy the batch file via GPO to add the computers to respective groups with the private encryption option.
3. Upon successful deployment, the computers will be listed under the specified group name with the specified private encryption key.

Note:

- ❖ Always make sure to use the same private encryption key during any re-installation as used during the original installation.
- ❖ IDrive® 360 does not store your private encryption key on its servers. It is recommended that you archive it safely to backup and restore your data. However, if you choose the default encryption key, you need not remember it.

3.1.3 Mass deployment via Apple remote desktop On Mac OS

You can remotely deploy the IDrive® 360 application on multiple Mac computers or groups in the same network using Apple Remote Desktop software installed on administrator's computer, with IDrive® 360 group deployment package.

To use Apple Remote Desktop, you need Apple Remote Desktop Admin and Apple Remote Desktop client installed on your administrator Mac and client Macs respectively. Apple Remote Desktop client will be installed automatically during the standard macOS installation. However, the Apple Remote Desktop Admin is not a part of the standard installation. You will have to obtain the software from the Apple store and install it on the Mac from which you are deploying the IDrive® 360 application.

Read the detailed steps below to know more about how to deploy the IDrive® 360 package with Apple Remote Desktop.

Prerequisites

Before proceeding with deployment, ensure that:

- You have signed in and downloaded the IDrive® 360 mass deployment package
- Apple Remote Desktop Admin software installed on administrator Mac

Configure remote management services on target Macs

For a remote management tool like Apple Remote Desktop to work, the remote management services have to be configured in Mac OS on each individual Mac. In order to do so, you need to log in to each Mac and perform the following steps:

1. In Mac OS, open **System Preferences**>**Sharing** and select **Remote Management** under the service list.
2. Click **Options** and select the following options:
    a. Observe
    b. Control
    c. Open and quit applications
    d. Change settings
    e. Delete and replace items
    f. Copy items
3. Click **OK** and close the **System Preferences** window.

Set up task server in the administrator Mac

To set up a Task Server,

1. Open the Apple Remote Desktop Admin software installed on your administrator Mac, and navigate to **Remote Desktop**>**Preferences**.
2. Click on the **Task Server** tab and select **Allow remote connections to this server**.
3. Go to the **Scanner** tab and select **Local Network** from the drop-down.
4. From the computer list that appears, double-click on the computer which you wish to add to the Apple Remote Desktop.
5. Enter a valid system credential and click **Add**.

Steps to register a set of computers under a particular group or with a Private Key encryption method:

Admin may choose to register a set of computers under a particular group or with a private key encryption method during the mass deployment.

The installation requires configuring a **.plist** file and installing it along with the IDrive® 360 mass deployment package.

The **com.idrive360.packageinstaller.plist** file can contain the following keys:

Key	Value	Description	Default
groupName	String	Machine registers under this particular group	No group
encryptionKey	String	Machine registers with this private encryption key	No encryption key
configurationID	String	You can find this parameter in your IDrive® 360 account	No configuration ID
trayHidden	Number	1 - Enabling this option will prevent users from accessing the tray options on their computers 0 - Unhide tray and allow users to access tray options	0

Click com.idrive360.packageinstaller.plist to download a sample **.plist** file.

Note:

- The encryption key can contain a minimum of 6 characters and maximum upto 250 characters.
- Always make sure to use the same private encryption key during any re-installation as used during the original installation.
- IDrive® 360 does not store your private encryption key on its servers. It is recommended that you archive it safely to backup and restore your data. However, if you choose the default encryption key, you need not remember it.

To copy the **com.idrive360.packageinstaller.plis**t file to Mac machines,

1. Open the Apple Remote Desktop Admin software installed on your administrator Mac, and click the **All Computers** tab.
2. Select the desired destination Macs, and click the **Copy** button in the Apple Remote Desktop toolbar.
3. In the **Copy Items** window that appears, add the **com.idrive360.packageinstaller.plist** file to the Items to copy list either by dragging it there with the mouse or by locating the file using + button.

4. Under the **Place items in** drop-down, select **Specify full path** and enter the path as **/Library/Application Support/**.
5. Under the **If an item already exists** drop-down, select **Replace the item**.
6. Click **Copy**.

Admin may skip the above steps, if they do not wish to configure a **.plist** file. The IDrive® 360 application will then be deployed with the default configuration.

Deploy IDrive® 360 package

To deploy the IDrive® 360 package to Mac,

1. Sign in to your IDrive® 360 account.
2. Click the **Add Devices** button and click **Download Package** under the **Mass deployment for Mac** section to download the IDrive® 360 mass deployment package.

> **Note:**
> If the **com.idrive360.packageinstaller.plist** file is configured with a private encryption key, then make sure to select the **Set your own encryption method** check-box in the **Add Devices** page, and then click the **Download Package** button.

3. Open the Apple Remote Desktop Admin software installed on your administrator Mac, and click the **All Computers** tab.
4. Select the destination Macs in which you wish to install the IDrive® 360 application, and click the **Install** button in the Apple Remote Desktop toolbar.
5. In the **Install Packages** window that appears, add the IDrive® 360 package file to the **Packages List** either by dragging it there with the mouse or by locating the package using + button.
6. Click **Install**.

Once the package is distributed to online Macs, it executes and installs the IDrive360 application on client Macs

Mac OS Mojave or later requires user consent for applications to access privacy sensitive data. Hence the user needs to grant full disk access permission to **IDriveDaemon** after successful installation in the client Mac machines, in order to backup privacy sensitive data. Click here to read more.

3.1.4 Mass deployment via Jamf Pro on Mac OS

You can remotely deploy the IDrive® 360 application on multiple Mac computers or groups using Jamf Pro.

Read the detailed steps below to know more about how to deploy the IDrive® 360 package with Jamf Pro.

Prerequisites

Before proceeding with deployment, ensure that:

- You have signed in and downloaded the IDrive® 360 mass deployment package
- Jamf Pro software installed

Prepare the customized IDrive® 360 deployable PKG

The default IDrive® 360 folder must be packaged into a format that is deployable by Jamf Pro. This can be done using the Jamf Composer tool.

Steps to register a set of computers under a particular group or with a Private Key encryption method:

Admin may choose to register a set of computers under a particular group or with a Private Key encryption method during the mass deployment.

The installation requires configuring a **.plist** file and installing it along with the IDrive® 360 mass deployment package.

The **com.idrive360.packageinstaller.plist** file can contain the following keys

Key	Value	Description	Default
groupName	String	Machine registers under this particular group	No group
encryptionKey	String	Machine registers with this private encryption key	No encryption key
configurationID	String	You can find this parameter in your IDrive® 360 account	No configuration ID
trayHidden	Number	1 - Enabling this option will prevent users from accessing the tray options on their computers 0 - Unhide tray and allow users to access tray options	0

Click **com.idrive360.packageinstaller.plist** to download a sample **.plist** file.

Note:

- The encryption key can contain a minimum of 6 characters and maximum upto 250 characters.
- Always make sure to use the same private encryption key during any re-installation as used during the original installation.
- IDrive® 360 does not store your private encryption key on its servers. It is recommended that you archive it safely to backup and restore your data. However, if you choose the default encryption key, you need not remember it.

Perform the following steps:

1. Go to **/tmp** directory and create one folder called IDrive360, place the **com.idrive360.packageinstaller.plist** and IDrive® 360 package (**IDrive360_<token>.pkg**) into it.
2. Open Jamf Composer on your machine and log in if prompted (If you receive a prompt to choose the method for creating your package, click **Cancel**).
3. Drag and drop the IDrive360 folder from **/tmp** directory into the sidebar of the Composer under **Sources** and it should appear as one source.
4. Next, adjust the ownership and permissions of IDrive® 360 to match the private folder by selecting the Private folder in the center window, and using the gear icon select **Apply Permissions to Private and All Enclosed Items**.
5. Click **Build as PKG** and choose **Desktop** to save the **IDrive360.pkg** on the desktop.

Upload the PKG to Jamf Pro dashboard

To upload the PKG to Jamf Pro dashboard,

1. Login to Jamf Pro in the browser.
2. Add the target computers to Jamf Pro by installing Jamf Profile in all the target computers using the provided Jamf Pro enroll link.
3. In the top-right corner of the web page, **click Settings**.
4. In the **Computer Management** section, click **Packages**.
5. Click **New**.
6. Under the **General** pane, in the **Filename** section click **Choose File** and select the **IDrive360.pkg** from the desktop, which was created earlier using Jamf Composer.
7. Click **Save** to upload the package.

Note:

- ❖ It is recommended to use the unique package name to avoid any error while uploading.

Add installer script

To add installer script,

1. In the **Computer Management** section, click **Scripts**.
2. Click **New**.
3. Enter Display Name **IDrive360InstallerScript** under **General** pane.
4. Go to the **Script** tab and paste the below code:

```
#!/bin/bash
PACKAGE_NAME=$4
PACKAGEPATH=/tmp/IDrive360/$PACKAGE_NAME
if [[ "$PACKAGE_NAME" == "" ]]; then
echo echo "Enter the complete package path"
fi
sudo installer -pkg $PACKAGEPATH -target /
if [ -d "/tmp/IDrive360" ] ; then
rm -rf "/tmp/IDrive360"
echo "Deleted IDrive360 from tmp folder"
fi
exit 0
```

5. Go to the **Options** tab and put **IDrive360 Package Name** as a label in **Parameter 4**.
6. Click **Save**.

Enable full disk access and Apple events via Jamf configuration profile

Follow the steps below to enable full disk access for IDrive® 360 and apple event from the Jamf Pro Dashboard:

1. Login to Jamf Pro and Navigate to **Configuration Profiles** under the **Computers** tab.
2. Click the **+ New** button and enter a profile name (e.g. IDrive360Profile).
3. Go to the **Privacy Preferences Policy Control** tab, and click **Configure**.
4. In the **App Access** section, add the below values:

    - **Identifier:** com.prosoftnet.IDriveDaemon
    - **Identifier Type:** Bundle ID
    - **Code Requirement:** identifier "com.prosoftnet.IDriveDaemon" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = JWDCNYZ922

5. Click the **+ Add** button and select **SystemPolicyAllFiles** from the drop-down list.
6. Click **Save**.
7. Click the **+** button on the top right corner to add new App Access.
8. In the **App Access** section, add the below values:

    - **Identifier:** com.prosoftnet.IDrive360
    - **Identifier Type:** Bundle ID
    - **Code Requirement:** identifier "com.prosoftnet.IDrive360" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = JWDCNYZ922

9. Click the **+ Add** button and select **AppleEvents** from the drop-down list. Add below values:

- **Receiver Identifier:** com.apple.systemevents
- **Receiver Identifier Type:** Bundle ID
- **Receiver Code Requirement:** identifier "com.apple.systemevents" and anchor apple

10. Click **Save**.
11. Navigate to the **Scope** tab. From the **Target Computers** and **Target Users** drop-downs, select **All Computers** and **All Users** respectively.
12. Click **Save**.
13. Click the **Logs** button to view the configuration profile installation status on all computers.

Create a computer policy

To create computer policy,

1. Click **Computers** at the top-left of the page.
2. Click **Policies**.
3. Click **New**.
4. Use the **General Payload** to configure basic settings for the policy, including the trigger and execution frequency.
5. Automatically re-run the policy on failure.
6. Click the **Packages** tab and select the deployable **IDrive360.pkg** uploaded earlier.
7. Click **Configure**.
8. Find your **IDrive360.pkg** and click **Add**.
9. Select **Cloud Distribution Point** option under **Distribution Point** drop-down.
10. Ensure that **Install** is selected.
11. Click **Save**.
12. Click the **Scripts** tab and select the script that is uploaded earlier.
13. Click **Configure**.
14. Find your **IDrive360InstallerScript** and click **Add**.
15. Enter parameter value under **IDrive360 Package Name** (e.g. IDrive360_JPwmv149Wi1u2DGcRE7P1726.pkg).
16. Click **Save**.
17. Click the **Scope** tab and configure the scope of the policy to choose computers this should be installed on. If you intend to install this on all computers, you can choose **All Computers** from the drop-down. Jamf admins should understand their own scope standards.
18. Click **Save**.
19. Under the **Computers** section, click on **Policies** and select **IDrive360_Deploy** Policy.
20. Click on **Logs** to see the deployment status of each machine.

3.1.5 Encryption key

Encryption is the process of encoding messages or information in such a way that it cannot be accessed without the key used to encode it. IDrive® 360 encrypts the files included in your backup set before the data is sent to your destination and it stores the data in encrypted format on your servers.

IDrive® 360 backups are encoded with Advanced Encryption Standard (AES) 256-bit encryption algorithm on transfer and storage.

By default, an encryption key is securely generated for your account and this key will be automatically used to encrypt all your data on transfer and storage.

If you do not wish to proceed with the default encryption option, you can set your own encryption option by following the below steps:

1. Click the **Add Devices** button.
2. Check the **Set your own encryption method** option and select the operating system to download the corresponding setup file.
3. On installation, you will be asked to set an encryption method for your computer. You can choose default or private encryption.
4. Choose **Default encryption key** to continue with default encryption method or select **Private encryption key** to set an encryption key of your choice, and click **Continue**.

Warning:

IDrive® 360 does not store your private encryption key on its servers. It is recommended that you archive it safely to backup and restore your data. However, if you choose the default encryption key, you need not remember it.

3.1.6 Stop backup

Follow the below steps to stop all ongoing backup of the devices present in a unit

1. In the **Devices** tab, click the company name drop-down to see the entire list of units.
2. Select the unit in which you wish to stop the ongoing backup operation.
3. Click the **Stop all current backups** button.
4. In the confirmation popup that appears, Click **Ok**.

Follow the below steps to stop ongoing backup of individual computer

1. Sign in to your IDrive 360 account
2. In the 'Backup Console' -> 'Devices' tab, click on the computer you wish to stop the backup. The remote management console appears.
3. Click ‘Stop’ beside the backup progress bar.
4. In the confirmation pop-up window, click ‘Yes’.

Note:

- All ongoing backups will stop and will resume at the next schedule. This operation may take some time.

3.1.7 Remove computer

Follow the below steps for removing computers from the IDrive® 360 account

1. Firstly, select the computers you wish to remove from the account and click **Delete**.
2. In the **Delete Computers** popup that appears, click **Delete**.
3. A confirmation popup to confirm the deletion appears. Click **Delete**.

Note:

- On removing, all the ongoing backups of the computer will stop and the computer will be removed from your account.

3.2 Groups

A group is a collection of computers organized together under the parent company. Users can create unlimited groups and organize computers according to the company or unit requirements. Users can perform group actions like adding computers to the group, and removing computers from the groups.

3.2.1 Create group

Follow the below steps to create a new group

1. In the **Devices** tab, click **Create new group.**
2. Enter the desired group name in the popup that appears and click **Create**.
3. You can now add computers to the newly created group.

3.2.2 Create group and add computers

Follow the below steps to create a new group and add computers to it

1. Select the computers you wish to add to the new group from the **Devices** tab and click **Add to Group**.
2. In the screen that appears, click **New Group**. Enter the desired group name in the popup that appears.
3. Click **Create**.
4. The selected computers will be added to the new group.

3.2.3 Add computers to an existing group

Follow the below steps for adding computers to an already existing group

1. Select the computers you wish to add to the new group from the **Devices** tab and click **Add to Group**.
2. From the list that appears, select the group to which you wish to add the computers, and click **Add**.
3. The computers will be added to the selected group.

3.2.4 Remove computers from group

Follow the below steps to remove computers from a group

1. In the **Devices** tab, click a group name and all the computers in the group will appear.

2. Select the computers you wish to remove, and click **Remove from Group**.
3. In the popup that appears, click **Remove**.

3.2.5 Move computers

Moving computers between groups can also be performed under the parent company. To do this, first remove the computers from the existing group and then add it to the desired group under the organization. Refer the **Add** and **Remove** steps mentioned above for detailed instructions.

3.2.6 Rename group

Follow the below steps to rename a group

1. In the **Devices** tab, hover over the group you wish to rename and click  .
2. Click **Rename** and enter a new name in the popup that appears.
3. Click **Save**.

3.2.7 Delete group

Follow the below steps to delete a group

1. In the **Devices** tab, hover over the group you wish to delete and click  .
2. Click **Delete**.
3. In the popup that appears, click **Delete**.

3.3 Backup plan

A backup plan is a set of rules that specify how the given data will be protected on a given machine.

With a backup plan, you can define backup policies with a set of instructions and parameters, at a predefined time schedule. Backup plans can be executed to multiple devices / groups simultaneously at the time of its creation, or later.

On creating your IDrive® 360 account, a backup plan is created by default with predefined folders and applied to the added computer. The same can be viewed from the Backup Plan tab. You can modify the backup rules, rename the plan name, disable the same, but you cannot delete the default backup plan.

A backup plan specifies:

- Devices / groups to include in backup
- Source with policy rules
- Destination to choose from cloud or local storage
- Backup schedule
- Files / folders to exclude from backup

3.3.1 Create backup plan

Following steps are involved in creating and executing a backup plan

1. In the **Backup Console**, click **Create Plan** from the **Backup Plan** tab.

2. Hover over the default plan name and click  . The Rename Backup Plan popup appears.
3. Enter the desired backup plan name and click **Save**.
4. Modify the menu options as given in the table below, and click **Create**.

Option	Description
Devices/Groups	Select devices or groups from the All Devices or Groups tab respectively, which you wish to backup and click Done. Read more.
What to backup	Select **Files/Folders** if you wish to backup certain files. For the entire machine backup, Select **Entire Machine**.
Items to backup	Click **Specify** and choose policy rules for backup from the drop-down list or select **Customize** and add items manually which you wish to include in the backup set by entering the path location, and click **Done**. Read more.
Where to backup	Choose between **Cloud Storage** or **Local Storage** as backup destination. Read more.
Schedule	You can set your backup schedule here, and click **Done**. Read more.
• **Daily schedule**	Select this option to run your backup jobs daily
• **Weekday(s)**	Select the days of the week on which you wish to run your backup jobs
• **Backup start time**	Set the time at which your scheduled backup should start
• **Start backup immediately**	Select this option to run a backup job immediately.
• **Cut off time**	Set the time at which your scheduled backup should stop
• **Email notification**	Select this option to receive email notifications on the status of the scheduled backup job. Enter the email address on which you want to receive the notifications

○ **Notify always**	Select this option to get notifications always
○ **Notify on failure**	Select this option to get the notifications only when there are failures
● **Start the missed scheduled backup when the computer is turned on**	Select this option to resume a missed scheduled backup job due to the computer being turned off
Exclude files / folders	Click **Modify** and add the full path, file name, or partial name of the files you want to exclude from backup. You can also exclude system and hidden files from backup by selecting respective checkboxes. Click **Done**. Read more.

Once created, the backup plan will be applied automatically to selected devices / groups and the backup will start immediately or at the scheduled time, as per the chosen option.

A conflict may occur when you try to create a backup plan for a device that is already part of another backup plan. In such cases, you can view the details of the conflict and choose to remove the existing backup plan for the device and apply the new plan for the same. The already applied plans will then be disabled for the devices.

3.3.2 Define backup rule

You can define a backup rule for selecting files / folders in all your backup plans.

There are two methods for selecting files / folders, either by using policy rules or by customized selection method.

Method 1: Select files / folders using policy rules

1. In the **Backup Console**, click **Create Plan** from the **Backup Plan** tab.
2. Under **What to backup?** option, click **Specify** and select **Using policy rules**.
3. Click  and select any of the predefined rules.
4. Click **Done**.

The policy rules will be applied to all of the machines included in the backup plan. If no data meeting at least one of the rules is found on a machine when the backup starts, the backup will fail on that machine.

Selection rules for Windows

- **[All Files]:** Select all files from all local drives of a machine.
- **[All Profiles Folder]:** Selects the folder where all user profiles are located (usually, **C:\Users**).

- **[PROFILEDEFAULTFOLDERS]:** Selects the default user profile folder (for example, **C:\Users\Anna\Desktop**, **C:\Users\Anna\Documents**, **C:\Users\Anna\Music**, **C:\Users\Anna\Pictures** and **C:\Users\Anna\Videos**).
- **%ALLUSERSPROFILE%:** Selects the folder where the common data of all user profiles is located (usually, **C:\ProgramData**).
- **%PROGRAMFILES%:** Select the Program Files folders (for example, **C:\Program Files**).
- **%WINDIR%:** Selects the folder where Windows is located (for example, **C:\Windows**).

Selection rules for Mac

- **[All Files]:** Selects root volume of the machine.
- **[All Profiles Folder]:** Selects **/Users**. This is the folder where all user profiles are located by default.
- **[PROFILEDEFAULTFOLDERS]:** Select the default user profile folders (for example, **/Users/Anna/Desktop**, **/Users/Anna/Documents**, **/Users/Anna/Pictures** and **/Users/Anna/Music**).

Method 2: Customize and select files / folders

1. In the **Backup Console**, click **Create Plan** from the **Backup Plan** tab.
2. Under **What to backup?** option, click **Specify** and select **Customize**.
3. In the text box, enter the file / folder name, partial name or path of the items to include in the backup set (Examples: **C:\Data*.log**, **C:\Data\Finance\, C:\Data\Finance\F.log, /Users/JOHN/Desktop/*.txt, /User/JOHN/Desktop/F.txt** etc.).
4. Click **Done**.

3.3.3 Propagate backup plan

Follow the below steps to manually push backup plans to devices and groups

1. From the **Backup Plan** tab, hover on the backup plan name you wish to push, and click  .
2. Select the Devices or Groups to which you want to push the backup plan from the **All Devices** or **Groups** tab, respectively.
3. Click **Propagate**.

3.3.4 Edit backup plan

Follow the below steps to modify an existing backup plan

1. From the **Backup Plan** tab, hover on the backup plan name you wish to modify and click  .
2. In the **Update Plan** screen that appears, modify your backup plan details and click **Update**.

3.3.5 Disable / Enable backup plan

Follow the below steps to disable a backup plan

1. From the **Backup Plan** tab, select the backup plan you wish to disable.
2. Click the **Disable** button.
3. In the popup that appears, click **Disable**.

You can also enable a disabled backup plan. To do so, select the same and click **Enable** and click **Yes** in the popup that appears.

3.3.6 Delete backup plan

Follow the below steps to delete a backup plan

1. From the **Backup Plan** tab, select the backup plan you wish to delete.
2. Click the **Delete** button.
3. In the popup that appears, select the confirmation checkbox and click **Delete**.

Note:

- On deleting a backup plan, all the backups with the configured settings will be discontinued for the associated devices.

3.4 Remote manage

Admin of the IDrive® 360 account or a company / unit administrator can remotely manage data backups, restore files / folders to the corresponding computers, modify application settings, set specific settings for mapped drives, select file / folder from USB / network drives for backups, view activity logs for users, and do much more on each of the connected computers, with the Remote Manage feature.

Manage a user's computer remotely by hovering on the same from the **Devices** tab, and click  and select **Remote Manage**. The remote management interface appears, with various tabs like Backup, Restore, Scheduler, and Settings.

3.4.1 Backup

You can manage your computer's backup operation from the **Backup** tab. Once backup is initiated, IDrive®360 creates a unique folder in your account with your computer name to backup data.

Follow the below steps to perform backup

1. In the **Backup** tab, files already selected for backup appear in the backup set.
2. By default, the **Backup files to my IDrive® 360 account** option is selected. Alternatively, to perform a local backup, select **Backup files to my local device**.
3. To remove or add files to the backup set, click **Change**.
4. Click **Backup Now** to initiate the backup.

To automate data protection, you can also schedule your backups. In the **Backup** screen, click **Schedule** and configure the scheduling parameters like backup date, time, frequency, and notification type, and click **Save Changes**.

You can view the detailed backup progress status during a backup process. Once the backup operation is complete, a popup will display the backup summary.

3.4.2 Restore

You can restore your backed up files / folders from your IDrive® 360 cloud account or from a local device, to any location on your computer or a different computer, from the **Restore** tab.

Follow the below steps to perform restore

1. In the **Restore** tab, select the desired files / folders.
2. Choose the restore location on your computer using the **Restore location** field.
3. Click **Restore To (your computer name)** to restore the files / folders to your computer.

During restore, the restore progress status appears on the bottom of the application interface. Once the restore operation is complete, a popup will display the summary.

3.4.3 Snapshots

Snapshots are historical views of your data stored in your IDrive®360 account, which allow you to perform point-in-time recovery.

Follow the steps below to perform snapshot based restore

1. From the **Restore** tab, click **Snapshots**.
2. Select the date and time and click **Submit**. A list of all the data backed up on or before the selected date appears.
3. Select the required files / folders and click **Restore to (your computer name)** to restore the files / folders to your computer.

Note:

- The additional storage requirements for Snapshots have no impact on your IDrive® 360 account storage space.

3.4.4 Scheduler

Schedule automated backups; set the day, time and notification options for your backup operations. You can set the following options under the **Scheduler** tab to schedule automated backups:

Option	Description
Backup start time	Set the time at which your scheduled backup should start.
Backup start days	Select the days when you want to schedule the backup.
Start backup immediately	Select this option to run a backup job immediately.

Hourly Schedule	Select this option to configure hourly backup operations.
Cut-off Time	Set the time at which your scheduled backup should stop. This is helpful if you want to hard stop the backup progress at a specific time.
Email notification	Enter your email address to receive backup status notifications. **Notify always** and **Notify on failure** are the two notification options that you can select.
Start the missed scheduled backup when the computer is turned on	Your missed scheduled backups will start automatically once you turn on your computer.

3.5 Entire machine backup

Entire Machine Backup helps you to backup your entire computer securing data from any disasters. The entire computer (excluding image files) - system files, programs, boot files, operating systems, etc., is backed up under Entire Machine Backup.

Note:

- This feature is available only for Windows computers.

3.5.1 Perform entire machine backup

The entire machine backup is done only over the cloud.

Here are the steps to perform entire computer backup for the existing machines:

1. Sign in to your IDrive 360 account.
2. Go to **Devices > Computers**.
3. Click on the machine you wish to perform the entire machine backup. It will open the remote management console.

   Alternatively, you can click  and select Remote Manage.
4. Click 'Entire Machine Backup' and go to 'Backup'> 'Schedule'.
5. Create a schedule for performing regular entire machine backup and click 'Save Changes'.

The backup will start at the scheduled date and time.

Here are the steps to perform entire machine backup for new machines:

1. Sign in to the IDrive 360 account.
2. Click ‘Enable Backup’ on the device added.
3. Click ‘Create Plan’ to create the Entire Machine Backup plan.

a. Choose ‘Entire Machine’ under ‘What to Backup’. By default, the backup location is selected as ‘Cloud Storage’.
b. Under Schedule, choose backup time, days, cut-off time, and email notification option and click ‘Done’.
c. Click ‘Create & Apply Plan’.

If you already have existing backup plans, click ‘Apply’ beside the required.

4. The backup process will begin according to the schedule.

To update the entire machine backup schedule, go to the ‘Backup Plan’ tab and click on the required computer. Update the backup plan schedule and click ‘Update’.

3.5.2 Entire machine backup for groups

Entire Machine Backup is possible for multiple computers excluding Mac. Here are the steps for multiple machine backup:

1. Sign in to your IDrive 360 account.
2. Go to **Backup Plan** tab.
3. Click **Create Plan**.
4. After selecting the backup plan name and other details, click **Create**.

3.5.3 Create plan for multiple machine backup

In order to backup multiple computers, you need to create a backup plan. Here are the steps:

1. Once you sign in to your IDrive 360 account, go to the Backup **Plan** tab and click **Create Plan**.
2. The Create Plan screen will appear. Choose the options below as required:
   - **Devices/Groups:** You can add all the computers except for Mac that you wish to backup.
   - **What to backup:** Select **Entire Machine** for entire machine backup. Note that Mac and Linux systems are not supported for entire machine backup.
   - **Where to backup:** The default backup storage location will be cloud.
   - **Schedule:** Select date, time, and notification options and click **Done**.

3.5.4 Entire machine backup schedule

To schedule the entire machine backup, here are the steps:

1. Sign in to your IDrive 360 account.
2. Go to **Devices > Computers**.
3. Click on the computer you wish to backup and the remote manage screen will appear.
4. Click on **Entire Machine Backup**.
5. In the backup screen, click **Schedule** and the **Scheduler** tab will appear.

To schedule entire machine backup for multiple computers,

1. Sign in to your IDrive 360 account.
2. Go to **Backup Plan** and click on **Create Plan**.
3. In the **Create Plan** screen, click on the option present beside **Schedule**.

The **Scheduler** tab has the following options:

- **Backup set name:** Choose the **Entire Machine BackupSet** for the entire machine backup.
- **Backup start time:** Set the time for the backup to begin.
- **Backup start days:** Choose the days for backup. You can choose daily/weekly backup.
- **Start backup immediately:** Backup starts immediately.
- **Hourly schedule:** Backup happens once every hour.
- **Cut-off time:** Set the cut-off time to hard stop the backup.
- **Email Notification:** You can choose to get notified regarding backup status.
- **Start the missed schedule backup when the computer is turned on:** Choose this to automatically resume backup once the system is on.

3.6 Entire machine restore

Restore your entire computer's files including program files, operating systems, etc., using Entire Machine Restore. There are two ways of restoring your computer.

1-step restore

Here are the steps to recover your entire machine using 1-step restore:

1. Ensure these prerequisites:

   USB bootable flash drive to boot your machine.

   Download WinRE ISO file and double-click to mount it.

   Copy all the data to the USB flash drive.

2. Plug-in the WinRE boot disk and launch the windows recovery environment by booting the machine via the USB.
3. In the Entire Machine Restore screen, sign in to the IDrive® 360 web application.
4. Select the device and in case your device is configured with private encryption, you will be prompted to enter the private key. Provide the private key to proceed. Choose the Entire Machine Backup folder (IDMachineBackup) to restore the data.
5. Select the hard disk to which you wish to restore the data and click on Restore Now.
6. In the pop-up window for confirmation to override the existing contents present in the device, click Yes if you wish to proceed.

7. Once the restore is complete, select your hard disk in BIOS and boot your machine to get the operating system.

2-step restore

Restore the entire computer along with the OS with 2-step restore. Here, files are restored to a local machine or external device and OS is also recovered in two steps. The data can be restored to a different computer with or without similar hardware.

1. Ensure these prerequisites:

   A USB bootable flash drive to boot your machine.

   Download and double-click the WinRE ISO bootable file to mount it. Copy the entire content to a USB bootable flash drive.

   The entire-machine-backup folder (IDMachineBackup), downloaded from your IDrive® 360 Cloud to an external drive using the IDrive® 360.

   A target hard drive with sufficient storage space for performing the restore operation.
2. Plug-in the WinRE boot disk and launch the windows recovery environment by booting the machine via the USB.
3. Choose 2-step restore.
4. Click  . Navigate and select the entire machine backup folder (IDMachineBackup), pre-downloaded from your IDrive® 360 cloud backup account for restore.
5. Select the hard disk to which you wish to restore the data and click on Restore Now.
6. In the pop-up window for confirmation to override the existing contents present in the device, click Yes if you wish to proceed.
7. Once the restore is complete, select your hard disk in BIOS and boot your machine to get the operating system.

3.6.1 Advanced settings

The **Advanced Settings** tab lets you change the cleanup and performance settings depending on your requirements. Set up automated cleanup and other performance parameters such as backup priority and network speed that ensure speedier backup.

3.6.1.1 Cleanup

The data in your account is cleaned up periodically based on the Cleanup settings defined by you in the web console.

Follow the below steps to define cleanup settings

1. Click  next to the computer you wish to update Cleanup settings.
2. In the **Backup Settings** window click **Advanced Settings**.
3. Set the following options in the **Cleanup** section:
4. Automatically perform cleanup after every '-' incremental backup
5. Delete versions that are older than '-' months
6. Click **Save Changes**.

3.6.1.2 Performance

You can enhance performance by setting Backup Priority and Network Speed as per your requirements.

Backup priority

Set the Backup Priority to Low, Medium, or High using the toggle slider under the **Performance** drop-down tab. Click **Save Changes**.

Note:

- High priority is recommended for ensuring fast backup.

Network speed

Select **Don't Limit** to obtain unrestricted network speed and access for faster backup. Alternatively, select **Limit To** and use the toggle slider to adjust the network speed. Click **Save Changes**.

3.6.2 Email notifications

Receive alerts and notifications about the backup status and other activities in your account on the email address specified at the time of registration for all the computers linked with your account.

To add other recipients for receiving email alerts related to a computer,

1. Click  next to the computer you wish to add recipients.
2. In the **Backup Settings** window click **Email Notification**.
   The registered email address is displayed by default.
3. Enter the email address of the intended recipient in the **Send email notification** field and click **Add**.
4. To enter custom SMTP details, click **Custom SMTP settings**. Enter your SMTP server name, port, username, and password.
5. In the **Backup Notifications** section, choose to receive notifications when the backup is complete or when the backup fails, or in both cases.
6. Click **Save Changes** to update the email notification settings.

3.7 Mobile backup

IDrive® 360 mobile backup feature lets you backup contacts, calendar events, photos, and video files from your phone. Additionally, backup call logs, SMS, and music and other files from your Android devices. This feature is available for all IDrive® 360 plans.

3.7.1 Token-based login & backup

Sign in to IDrive® 360 using the mobile token from your web account and add your device for backup.

To get the sign-in token for mobile,

1. Sign in to your IDrive® 360 web account.
2. Click **Add Devices**.
3. Select **Set your own encryption method** if you wish to set up private encryption. Skip this step to proceed with default encryption.
4. Make a note of the token in the **Mobile Devices** section. You can also enter the email addresses of recipients and share the token via email.

To add your device for backup,

1. Launch the IDrive® 360 Android app on your device.
2. Enter the token noted earlier.
3. Tap **Sign In**.
   Note: If you signed in with a private encryption token, you will be prompted to set up the encryption.

After signing in, you will have the option to backup all your device contacts, photos, videos, and calendar events from iOS and Android devices to your IDrive account by tapping on **Backup Now**. Additionally, you can backup SMS, call logs, music, and other files from Android devices.

You can also customize the selection based on your requirement and tap **Backup Now**.

3.7.2 Auto camera upload

Auto Camera Upload helps to automatically backup media files that include photos and videos.

To enable,

1. Go to IDrive® 360 home screen.
2. Tap **Backup** > Tap  > **Enable.**
3. Select **Only Image(s)** or **Include Video(s).**

Alternatively,

1. Go to IDrive® 360 home screen > **Backup**.
2. Enable **Auto Camera Upload**.
3. Tap **Include videos** to backup videos. If you wish to backup only images, tap **Only Images**.

3.7.3 Perform mobile backup

Backup contacts, calendar events, photos, and videos from mobile devices using the following steps. Additionally, you can secure SMS, call logs, music, and other files from Android devices.

I. Contacts

1. Backup Contacts

To backup contacts,

a. Go to IDrive® 360 home screen > **Backup**.

b. Select contacts.

c. Tap **Backup Now**.

View all the backed up contacts in **My Phone Backup/My Device Backup** screen.

2. Share Contacts

To share all contacts from your device,

a. Go to IDrive® 360 home screen > **Access and Restore**.

b. Tap **My Phone Backup** or **My Device Backup**.

c. Tap **Contacts**.

d. For Android, select multiple contacts to share by using  .

To share all contacts, tap  and tap **Select All**. Tap **Share** and select the app to share the contact with.

For iOS, tap  > Select the required contacts > **Share**. Alternatively, tap  > **Select All** > **Share**.

3. Restore Contacts

To restore all contacts,

a. Go to IDrive® 360 home screen.

b. Tap **Access and Restore**.

c. Tap  next to the contacts folder you want to restore.

To restore specific contacts,

a. Tap the contacts folder.

b. Tap  for android and  for iOS to select the contacts you wish to restore.

c. For iOS, tap **Restore** > Choose **Simply restore to Address Book** or **Delete Address Book & Restore**. To restore one contact, open the contact you wish to restore and tap **Restore**.

For Android, long-press a contact and select multiple contacts using  . Select all contacts to restore using  .

Note: To restore earlier versions, tap **Contacts** > **Version**, and select the desired version.

II. Calendar events

1. Backup Calendar events

To backup all calendar events,

a. Go to IDrive® 360 home screen.

b. Tap **Backup**.

c. Tap **Calendar** > **Backup Now**.

To select calendar events for backup in iOS,

a. Go to IDrive® 360 home screen > **Backup**.

b. Select **Calendar**.

c. Set **Start Date** and **End Date** and tap **Done**.

d. Tap **Backup Now**.

View all the backed up calendar events in **My Phone Backup/My Device Backup** screen.

2. Restore Calendar events

To restore all calendar events,

a. Go to IDrive® 360 home screen > **Access and Restore**. For Android, tap **My Device Backup**.

b. Tap  next to the calendar folder and tap **Yes**.

To restore specific calendar events,

a. Tap the calendar folder, tap  for android and  for iOS to select the calendar events you wish to restore.

b. For Android, tap  to restore and select 'Simply Restore to Calendar/Delete All Calendar Events & Restore'.
For iOS, tap **Restore** > Choose **Simply restore to Calendar** or **Delete Calendar & Restore**.

To restore one calendar event,

a. Tap the calendar folder.

b. Open the calendar event you wish to restore.

c. Tap **Restore**.

III. Photos/Videos

1. Backup photos/videos

To backup photos/videos,

a. Go to IDrive® 360 home screen.

b. Tap **Backup**.

c. Select Photos or Videos > **Backup Now**.

To select photos/videos for backup,

a. Go to IDrive® 360 home screen > **Backup**.

b. Tap the Photos or Videos folder.

c. Choose the photos or videos you wish to backup.

d. Tap **Done** > **Backup Now**.

View all the backed up photos and video files in the **My Phone Backup/My Device Backup** screen.

2. Share photos/videos

To share a photo/video,

a. Go to IDrive® 360 home screen > **Access and Restore**.

b. Tap **My Phone Backup/My Device Backup** > Open the photo/video you wish to share.

c. For Android, tap  and select the app to share the selected file with. For iOS, tap  > **Send mail**.

3. Restore photos/videos

To restore photos or videos,

a. Go to IDrive® 360 home screen > **Access and Restore** > **My Device Backup.**

b. Tap  next to the photos/videos folder you want to restore.

To restore specific photos/videos,

a. Tap the photos/videos folder > tap  .

b. Tap **Edit** and choose the photo/video > **Restore**.

IV. SMS

1. Backup SMS

To backup SMS files from your device,

a. Go to IDrive® 360 home screen > **Backup**.

b. Tap on the **SMS** folder > tap **Backup Now**.

All backed up SMS files will be available in **My Device Backup** folder.

2. Restore SMS

To restore all SMS files,

c. Go to IDrive® 360 home screen > **Access and Restore** > **My Device Backup.**

d. Tap  next to the **SMS** folder.

To restore specific SMS files from your device,

a. Go to IDrive® 360 home screen > **Access and Restore** > **My Device Backup.**
b. Tap on the **SMS** folder > Long press on any file > select the files you want to restore > Tap  .

V. Music files

1. Backup music

To backup music files from your device,

a. Go to IDrive® 360 home screen > **Backup**.
b. Tap on the **Music** folder > tap **Backup Now**.

All backed up music files will be available in **My Device Backup** folder.

2. Restore music

To restore all music files,

e. Go to IDrive® 360 home screen > **Access and Restore** > **My Device Backup.**
f. Tap  next to the music folder you want to restore.

To restore specific music files from your device,

a. Go to IDrive® 360 home screen > **Access and Restore** > **My Device Backup.**
b. Tap on the **Music** folder > find the files you wish to restore > tap  .

VI. Call logs

1. Backup call logs

To backup call logs from your device,

a. Go to IDrive® 360 home screen > **Backup**.
b. Tap **Call Logs** and tap **Backup Now**.

All backed up call logs will be available in **My Device Backup** folder.

2. Restore call logs

To restore all call logs,

a. Go to IDrive® 360 home screen > **Access and Restore** > **My Device Backup.**

b. Tap  next to the call logs folder you want to restore.

To restore specific call logs from your device,

a. Go to IDrive® 360 home screen > **Access and Restore** > **My Device Backup.**
b. Tap on the **Call Logs** folder > Long press on any log > select the logs you want to restore > Tap  .

VII. Other files

1. Backup other files

To backup other file types,

a. Go to IDrive® 360 home screen > **Backup**.
b. Tap **Other Files** and tap **Backup Now** to backup all the files from your internal and external storage.

To backup specific files,

a. Tap the **Other Files** folder and then navigate to the files.
b. Select the files using  .
c. Tap **Done** and then tap **Backup Now**.

All backed up files will be available in **My Device Backup** folder.

2. Restore other files

To restore all other files,

c. Go to IDrive® 360 home screen > **Access and Restore** > **My Device Backup.**
d. Tap  next to other files you want to restore.

To restore specific other files from your device,

c. Go to IDrive® 360 home screen > **Access and Restore** > **My Device Backup.**
d. Tap on **Other Files** > find the files you wish to restore > tap  .

3.7.4 Cancel backup upload

To cancel a folder upload in progress,

a. Go to the IDrive® 360 home screen > Backup.

b. Tap  next to the uploading folder.

To cancel a photo/video file upload in progress,

a. Go to the IDrive® 360 home screen > Backup.

b. Go to the photos/videos folder where the backup is in progress.

c. In the Upload screen > tap  next to the file you wish to cancel the upload.

To cancel Auto Camera Upload,

a. Go to the IDrive® 360 home screen > Backup screen >  .

b. Tap Disable.

3.7.5 Delete files

To delete a specific file for iOS,

1. Go to IDrive® 360 home screen > **Access and Restore**.
2. Select the folder that has the content to be deleted >  > Edit.
3. Open the file you want to delete > **Delete** > **Delete**.

To delete an entire folder content for iOS,

1. Go to IDrive® 360 home screen > **Access and Restore**.
2. Select the folder that has the content to be deleted >  > Edit.
3. Tap the folder you want to delete > **Delete** > **Delete**.

To delete specific files/folders (within Other Files, Music, Photos, and Videos folder) for Android,

1. Go to IDrive® 360 home screen > **Access and Restore** > **My Device Backup**.
2. Long-press the folder you wish to delete and tap  . Alternatively, you can tap  > **Edit**, select the folders you wish to delete, and tap  .

   Note: To view an image before deleting, tap on the image. You may tap  right from the full-view screen.

3. Tap **Yes** in the confirmation window.

Note:

- Root folders cannot be deleted.

3.8 Settings

You can configure account settings for individual computers under the Remote Manage -> Settings tab. Set the following options under the **Settings** tab:

Option	Description
Continuous Data Protection	IDrive® 360 automatically recognizes the changes made to the files (up to 500 MB) present in your backup set and backs them up in real-time. To enable, select the **Continuous data protection** checkbox, and set the frequency of your choice from the drop-down list. To verify the backup integrity, enter the required days of interval and desired time for verifying the backup set or click **Verify Now** to verify instantly.
Exclude Files	Exclude specific files in the backup set from being backed during **Online Backup**, **Local Backup,** and **Mapped Drive Backup.** Add the full path, file name, or partial name in the **Exclude items which match the following criteria** field. You can also exclude system and hidden files from backup by selecting respective checkboxes. Click **Done**.
General Settings:	
• **Update software automatically**	The software will get updated automatically
• **Notify as 'Failure' if the total files failed for backup is more than '-' % of the total files backed up**	The application will notify backup as 'Failure' if the number of files failed for backup is more than '-' % of the total files backed up
• **Notify as 'Failure' if the total files missing for backup is more than '-' % of the total files backed up**	On selecting this option, the application will notify backup as 'Failure' if the total files missing for backup is more than '-' % of the total files backed up
• **Automatic power off after the completion of the scheduled jobs#**	Your computer will be powered off automatically after the completion of the scheduled backup job

• **Wake up the computer from Hibernate / Sleep mode#**	IDrive® 360 will wake up the computer from Hibernate / Sleep mode and then perform the scheduled backup job
• **Upload multiple file chunks simultaneously**	IDrive® 360 will optimize the transfer speed by uploading multiple file chunks simultaneously
• **Show hidden files / folders**	You can choose this option to make IDrive® 360 show the hidden files and folders on your computers
• **Start IDrive Monitor on system startup**	IDrive® 360 application interface will launch immediately after you startup your computer
• **Use black and white menu bar icon**	You can enable this option to activate the black and white menu bar icon on the IDrive® 360 menu
• **Stop scheduled backup when battery fails to '-' percent#**	With this option, you can choose to stop ongoing scheduled backup whenever the laptop battery drops below a certain percent value. You can set the percentage
Bandwidth Throttle#	Set the Internet bandwidth to be used by the IDrive® 360 application for backups. You can also set **Auto-Pause** during backup operations to enable optimum desktop experience with **PC in use** and **PC not in use** option
CPU Throttle*#	CPU throttle lets you set the CPU usage for backups. You can change the CPU utilization to suit the workload of your computer. By default, the CPU throttle value is set at 100%.

Note:

- *Not applicable for Mac.
- #Not applicable for Linux.

3.9 Units

Administrators can create unlimited units and sub-units, which typically correspond to business segments, departments, subsidiaries etc. within the organization.

An administrator can manage units, sub-units, delegate unit administration to users, and remotely supervise all units and user accounts.

3.9.1 Add units

To add a unit, go to Management Console (click **Go to Management Console)** and follow the steps below

1. Go to the **Units** tab, and click **Add Unit**
2. Enter the **Unit Name**. Create an admin by entering **Email**, **First Name** and **Last Name** of the admin.
3. Click **Create**.

The newly created unit appears under the **Units** tab with details such as unit name, overall space used, total number of users and computers in the unit.

To further add sub-units within a unit, in the **Units** tab, click on a **Unit Name ->Add Unit**.

Note:

- You need to create a unit first, and then populate it with user accounts. Once created, existing accounts cannot be moved between units or between the company and units.

Follow the steps below to add users to a unit

1. Go to the **Units** tab, hover over the unit where you wish to add users to and click  .
2. Enter the email address. You can also add multiple users by entering email addresses, separated by commas. Click here to read the procedure for inviting users via a CSV template.
3. Select a sub-unit from the **Add user(s) to unit** dropdown, if you wish to add the user(s) under a sub-unit.
4. Set a role by selecting the required checkbox and click **Create.**

Role	Description
Unit Administrator	The admin with this role will be able to manage backup and restore operations along with other management operations for the entire unit.
Backup Administrator	This role allows the user to add devices, manage backup, restore and modify settings for devices added by them.
Backup User	Users with this role can perform backup and manage settings for the assigned devices.
Restore User	Users with this role can restore data from assigned devices.
Backup and Restore User	Perform backup and restore and manage settings for the assigned devices.

The invited users will get an email with the link to register to IDrive® 360 . Once the users register, their accounts will be added to your account and will appear in the **Users** tab.

3.9.2 View units

To view the computer quota allocated for your unit, go to Management Console (click **Go to Management Console)** and follow the steps below:

1. Go to the **Units** tab, hover over the unit you wish to view and click  .
2. Computer allowed for the unit will be displayed in the **Devices** section.
3. Click  to edit the profile name, if you wish to do.

3.9.3 Delete unit

By deleting a unit, all the associated users also get deleted. However, the configured computers can still be accessed by the admin.

To delete a unit, go to Management Console (click **Go to Management Console)** and follow the steps below:

1. Go to the **Units** tab and navigate to the unit you wish to delete. Hover over the unit and click 

2. In the popup that appears, agree to the terms by clicking the checkbox.

3. Click **Delete**.

3.9.4 User list

User List populates the list of users under a unit.

To view the list of users under a unit, go to Management Console (click **Go to Management Console)** and follow the steps below:

1. Go to the **Units** tab and navigate to the unit for which you wish to view the user list. Hover over the unit and click  .
2. The list of users under the selected units will be populated.

3.10 Users

Each newly created user account belongs to the organizational unit or sub-unit under the Management Console. Administrator can set the preferred role for each user account.

3.10.1 Add user

To create a new user account, go to Management Console (click **Go to Management Console)** and follow the steps below:

1. Go to the **Users** tab, and click **Add User**.
2. Enter the email address. You can also add multiple users by entering email addresses, separated by commas. Click here to read the procedure for inviting users via a CSV template.
3. Add the user to any existing unit or sub-units, by selecting from the **Add user(s) to unit** dropdown list.
4. Set a role by selecting the required checkbox and click **Create**.

Role	Description

Unit Administrator	The admin with this role will be able to manage backup and restore operations along with other management operations for the entire unit.
Backup Administrator	This role allows the user to add devices, manage backup, restore and modify settings for devices added by them.
Backup User	Users with this role can perform backup and manage settings for the assigned devices.
Restore User	Users with this role can restore data from assigned devices.
Backup and Restore User	Perform backup and restore and manage settings for the assigned devices.

The invited users will get an email with the link to register to IDrive® 360 . Once the users register, their accounts will be added to your account and will appear in the **Users** tab.

Note:

- To view the list of users added under a unit or sub-unit, click  and select the respective unit or sub-unit from the drop down.

3.10.2 Invite users via CSV file

Admin can add a group of users to the account by importing information from a CSV file.

The CSV template file can be downloaded under the **Create User** option. Open the downloaded template file in a spreadsheet application, replace the sample entries and then upload the modified file.

Follow the below procedure to invite users via CSV file

1. Go to the **Users** tab, and click **Add User**.
2. Click the **Download CSV** button.
3. Once the file is downloaded, open the file, delete the sample entry and add the information of your users. Save the modified file.
4. Drag and drop your saved CSV file onto the **Upload or Drag and drop your CSV file** area. Alternatively, click the area to browse for your CSV file and upload in the popup that appears, click **Add Users.**

Note:

- You can add up to 500 users at a time using the CSV file.

3.10.3 Resend invitation email

When you invite and add a user to your account, they appear listed in the **Users** tab. However, the status against the name will show as inactive till the user accepts the invite and registers for an IDrive® 360 account.

To resend the invitation, click  against the name of the inactive user.

Once the user has registered for an account, the status will change to **Active**.

3.10.4 Reset password

Follow the below steps to reset user's password

1. In the Management Console, go to **Users** tab.
2. Select the user whose password you want to reset, and then click  .
3. Confirm your action by clicking **Reset** in the popup that appears.

The user can now complete the password resetting process by following the instructions in the email received.

3.10.5 Edit user

You can view as well as edit the user settings, or specify roles and permissions for the user. To edit and modify user settings,

1. In the Management Console, go to **Users** tab.
2. Hover over the user profile you wish to modify the settings and click  .
3. In the popup that appears, click  and modify the required changes.
4. Click **Save Changes**.

3.10.6 Disable user

You can disable an active user account profile from your IDrive® 360 account. Once disabled, the user will not be able to sign in to their account. To do so,

1. In the Management Console, go to **Users** tab.
2. Hover over an active user's name and click  .
3. Confirm your action by clicking **Yes** in the popup that appears.

To enable the account, click  against the disabled user's name and confirm your action by clicking **Yes** in the popup that appears.

3.10.7 Delete user

Admin can delete user profiles from the IDrive® 360 account. Once deleted, the user will not be able to sign in to their account. However, the configured computers can still be accessed by the admin. To do so,

1. In the Management Console, go to **Users** tab.
2. Hover over the user you wish to delete and click  .
3. In the popup that appears, agree to the terms by clicking the checkbox and click **Delete**.

4. Settings

4.1 Backup console settings

Configure and manage the Backup Console settings, and push them across units or groups. Settings can be accessed from **Backup Console ->Settings.**

4.1.1 Alerts / Notification

Under the Alerts / Notification section, the following options can be set:

Option	Description
Update software automatically	The software will get updated automatically
Notify as 'Failure' if the total files failed for backup is more than '-' % of the total files backed up	The application will notify backup as 'Failure' if the number of files failed for backup is more than '-' % of the total files backed up
Notify as 'Failure' if the total files missing for backup is more than '-' % of the total files backed up	On selecting this option, the application will notify backup as 'Failure' if the total files missing for backup is more than '-' % of the total files backed up.
Start IDrive Monitor on system startup	IDrive® 360 application interface will launch immediately after you startup your computer
Use black and white menu bar icon	You can enable this option to activate the black and white menu bar icon on the IDrive® 360 interface
Show hidden files / folders	You can choose this option to make IDrive® 360 show up the hidden files and folders on your computers
Stop scheduled backup when battery fails to '-' percent	With this option, you can choose to stop ongoing scheduled backup whenever the laptop battery drops below a certain percent value. You can set the percentage
Stop the email notifications from IDrive desktop application:	Select this option to stop from receiving email notifications from the IDrive® 360 desktop application

Follow the below steps to apply the settings

1. From the **Alerts / Notification** tab, click  against the particular settings you wish to push.
2. Select your company name or select **Specific Group** to push the settings respectively.
3. Click **Push** and select **Yes** in the popup that appears.

4.1.2 Backup settings

IDrive® 360 automatically recognizes the changes made to files (limited to 500 MB in size) present in your backup set and backs them up in almost real-time using the **Continuous Data Protection (CDP)** method. The temporary files, system files, network / mapped / external drives are excluded from the operation.

Follow the below steps to enable continuous data protection

1. From the **Backup Settings** tab, Check the **Enable continuous data protection** option and set the frequency from the drop-down list.
2. Click  and select your company name or select **Specific Group** to push the settings respectively.
3. Click **Push** and select **Yes** in the popup that appears.

Under the Backup Settings section, the following options can also be set:

Option	Description
Backup set verification	You can verify the backup set integrity by entering the required days of interval and desired time
Ignore file / folder level access rights / permission errors	IDrive® 360 does not backup any file / folder in your backup set which has insufficient access rights / permissions. Hence in such a case, by default, your backup will be considered as 'Failure'. You can enable this option to ignore file / folder level access rights / permission errors. IDrive® 360 will not consider this as an error and status of your backup will be displayed as Success
Automatic power off after the completion of the scheduled jobs	Your computer will be powered off automatically after the completion of the scheduled backup job
Wake up the computer from Hibernate / Sleep mode	IDrive® 360 will wake up the computer from Hibernate / Sleep mode and then perform the scheduled backup job
Upload multiple file chunks simultaneously	IDrive® 360 will optimize the transfer speed by uploading multiple file chunks simultaneously
Open file Backup	You can backup open files like Outlook files (.pst), QuickBooks, Quicken, ACT, MS Word, MS Excel, MS Money, MS Access, and MS FoxPro

Follow the below steps to apply the settings

1. From the **Backup Settings** tab, click  against the particular settings you wish to push.
2. Select your company name or select **Specific Group** to push the settings respectively.

3. Click **Push** and select **Yes** in the popup that appears.

4.1.3 Update / Reinstall application

Perform the following steps to initiate the update / reinstallation of IDrive® 360 application for all users or particular groups.

1. From the **Update / Reinstall Application** tab, click  against the option **Update / Reinstall IDrive® 360 application for all users or particular groups**.
2. Select your company name or select **Specific Group** to push the settings respectively.
3. Click **Push** and select **Yes** in the popup that appears.

4.1.4 Bandwidth throttle

The **Bandwidth Throttle** feature lets you set the Internet bandwidth to be used by the IDrive® 360 application for backups. By default, the bandwidth throttle value is set to 100%.

You can set the **Auto-Pause** option during backup operations to enable optimum desktop experience with the following options:

Option	Description
PC in use	This option lets you set the bandwidth to be used by IDrive® 360 for backups, when it is in use. By default, it is set to 25%. This allows other applications to run without hindrance
PC not in use	This option lets you set the bandwidth to be used by IDrive® 360 for backups when it is not in use. By default, it is set to 100%

To enable Auto-Pause and change the bandwidth settings

1. From the **Bandwidth Throttle** tab, enable **Auto-Pause** to set the **PC in use** and **PC not in use** options.
2. Use the sliders to set the bandwidth to be used, and click  .
3. Select your company name or select **Specific Group** to push the settings respectively.
4. Click **Push** and select **Yes** in the popup that appears.

4.1.5 Periodic cleanup

This feature lets you make a one-to-one match of the local data in the backup set, with the same in your cloud account. If data is deleted from your computer that has already been backed up, the corresponding data in your IDrive® 360 account would be permanently deleted.

Follow the below steps to push periodic cleanup

1. From the **Periodic Cleanup** tab, set up periodic automated cleanup by enabling **Periodic Cleanup** check box. Set the number of days and percentage of files to be considered for cleanup.
2. Click  and Select your company name or select **Specific Group** to push the settings respectively.
3. Click **Push** and select **Yes** in the popup confirmation that appears.

Note:

- Periodic Cleanup permanently deletes data which no longer exists on your computer to free up space in your account. Users will need to delete empty folders manually in order to remove them from the account.
- Periodic Cleanup may result in automatic deletion of data from your IDrive® 360 account. So use / set this option carefully.

5. Security

5.1 IP based login

Enabling IP based login control secures your IDrive® 360 data by restricting users based on their IP address.

You can control and enable access from a specific IP address, range of addresses or subnets and also deny access to IPs that are not authorized.

Admin can enable IP based login under **Management Console ->Settings ->Security.**

5.1.1 Enable IP based login

To enable IP based login, go to Management Console (click **Go to Management Console)** and follow the steps below:

1. Go to the **Settings** tab and select **Security**.
2. In the **IP based login control** section, click **Enable**.
3. Enter the IP addresses, range of IP addresses or subnets from which the members of a unit can sign in to the backup management or user management console.
4. Click **Submit**.

> **Note:**
> - You can enter multiple IP addresses separated by commas, specify a range of IP addresses, or enter a subnet.

5.2 Two-step verification

Two-step verification is a type of multi-factor authentication that checks a user identity by using a combination of two different factors:

- Account Password
- One-time verification code

The two-step verification process enhances the security of your account and prevents access by unauthorized parties.

Once enabled, in addition to your password, you will need to enter a one-time verification code received on your registered email address or phone number or Time-based OTP authenticator app, while signing in to IDrive® 360 .

Two-step verification can be enabled under **Management Console -> Settings -> Security.**

5.2.1 Enable two-step verification

Follow the below steps to enable two-step verification for all the users in your account

1. In the **Management Console**, go to **Settings ->Security**.
2. Click **Enable** in the **Two-step Verification** section.
3. In the popup that appears, click **Enable**.

Note:

- Once enabled, all users as well as the admin must configure two-step verification in order to sign in. If you do not wish to configure for all users, you can select and disable it for particular users. Read more.

5.2.2 Use cases

Once two-step verification is enabled for your IDrive® 360 account, you need to enter a one-time verification code received on your mobile number or email address or Time-based OTP authenticator app in addition to your account password, on all the subsequent sign ins.

Follow the below steps to set OTP preferences after two-step verification is enabled

1. On the sign in screen, enter your username and password and click **Sign In**.
2. Select **Email Address** or **Phone Number** or **Time-based OTP authentication** as your preferred method of receiving the one-time verification code and click **Confirm**.

a. Verification via email address or phone number

i) You will be prompted to enter the verification code sent to your email address or phone number.

Note:

- If you have chosen Phone Number as the preferred method of receiving one-time verification code, you need to first enter your phone number, and click **Send Code.**

ii) Enter the code and click **Verify & Enable**.

b. Verification via time-based OTP authentication

i) Install and launch any Time-based OTP authenticator app on your mobile device (See supported TOTP apps) and scan the QR code displayed on your computer screen. Alternatively, you can also view the key by clicking on **enter key manually** and type it manually on your mobile device, and click **Next**.

ii) Copy and save the recovery code displayed on your computer screen securely or click **Download** to download and save as a **.txt** file. Click **Continue**.

Note:

- You will require the recovery code to deactivate two-step verification for your account, in case you lose access to your mobile device where the Time-based OTP Authenticator app is installed.

iii) Enter the one-time code generated by the Time-based OTP Authenticator app in your mobile device, and click **Activate**.

5.2.3 Disable two-step verification

Follow the below steps to disable two-step verification for all the users in your account

1. In the **Management Console**, go to **Settings ->Security**.
2. Click **Disable** in the **Two-step Verification** section.
3. In the confirmation popup that appears, click **Disable**.

Follow the below steps to disable two-step verification for a particular user in your account

1. In the **Management Console**, navigate to the **Users** tab.
2. Hover over a user's name, click  and select **Disable 2FA**.

5.3 Single sign-On

Single Sign-On (SSO) is a one-step user authentication process. Admin of IDrive® 360 account or a company or unit administrator can allow their users to access IDrive® 360 by signing in to a central identity provider.

With single sign-on, you can put the identity provider you already trust in charge of authentication, and your users can access IDrive® 360 without another password to manage.

5.3.1 Configure Identity Provider (IdP)

Standard Assertion Markup Language (SAML) 2.0 is one of the standards used to configure SSO between IDrive® 360 and IdP. For implementing SAML authentication, SAML URLs and Certificate are needed, which can be obtained from any supported IdP.

Once an admin registers with an IdP of their choice, they will receive the following parameters

Parameter	Description
IdP Issuer URL	This URL uniquely identifies the application for which single sign-on is being configured.

Single Sign-On URL	This URL processes an authentication request from the user's browser and returns an authentication response to verify the user.
X.509 certificate (Base64)	An X.509 certificate is a security certificate that you receive from your identity provider to verify your identity. It comes in different formats, but IDrive® 360 only accepts .pem or .cer format.

5.3.2 Configure single sign-on

Admin needs to provide the received SAML 2.0 URLs and Certificate in the Single Sign-On section of IDrive® 360.

Follow the below steps to configure SSO in IDrive® 360

1. In the **Management Console**, go to **Settings ->Single Sign-On (SSO)**.
2. Upload the X.509 (Base64) certificate received from your IdP.
3. Click **Configure Single Sign-On**.

5.3.3 Create IdP profiles

IDrive® 360 allows you to create your own SAML 2.0 identity providers like Okta, Azure, OneLogin, AD FS, etc., and configure for SSO.

Parameters required to implement your own IdP are,

- IDrive® 360 uses SAML 2.0 with the HTTP Redirect for binding IDrive® 360 to IdP and expects the HTTP Post binding for IdP to IDrive® 360 .

Parameter	URL
Single sign-on URL	https://www.idrive360.com/sso/process
Audience URL (SP Entity ID)	https://www.idrive360.com/sso/metadata

- While configuring with SAML, use the following URLs and save the changes:
- Your identity provider may ask whether you want to sign the SAML assertion, the SAML response, or both. IDrive® 360 requires the SAML response to be signed.
- You can choose signed or unsigned SAML assertion.

5.3.4 Disable and delete single sign-on

Follow the below steps to disable and delete a single sign-on profile

1. In the **Management Console**, go to **Settings ->Single Sign-On (SSO)**.
2. Click  corresponding to the SSO profile you wish to disable.
3. Click **Disable** in the confirmation popup to disable the SSO profile.

4. Once disabled, click  corresponding to the disabled SSO profile.
5. In the popup that appears, agree to the terms by clicking the checkbox and click **Delete** to delete the SSO profile.

6. Logs and Reports

6.1 Logs

The **Activity Log** provides a chronological record of the activities performed by the users in IDrive® 360 account.

The activity logs are generated based on:

- **Event**
  Short description of the event. For example, backup plan name has been added, backup plan has been updated.
- **Date**
  The date and time when the event occurred.
- **IP Address**
  The IP address of the machine from which the event was initiated.

To view activity logs, click **Management Console ->Activity Logs**.

6.1.1 View

You can generate and view the custom activity log report of your IDrive® 360 account. To view the activities during a particular date range, select **Start Date** and **End Date** and click **View Report**.

6.1.2 Filters

You can filter the events by description, or event type. To filter, click  and select the event type from the drop-down list, and click **Apply**.

6.1.3 Download

To download a PDF copy of the generated log report, click  .

6.2 Reports

View and download reports of your backup / restore operations from the **Backup Console ->Reports** tab**.**

6.2.1 Alerts

View alerts and reports corresponding to the backup / restore operations performed. The reports generated are based on:

- **Alert time**
  The date and time when the event occurred.

- **Alert severity**
  Shows the priority of the occurred event.
- **Device name**
  Name of the device in which the operation was performed.
- **Alert message**
  Shows the alert description.

Alerts can also be filtered based on duration

- **Daily Activities**
  View the daily account activities.
- **Weekly Activities**
  View the account activities, based on per week.
- **Summary**
- Choose the Summary tab to view the overall activity summary.

6.2.2 Email report

The generated backup / restore operation reports can be send through email.

Follow the below steps to send an email report

1. In the **Backup Console**, go to **Reports ->Email Report**.
2. In the window that appears, enter the name and email addresses of the recipient(s).
3. Select the file format for the report and click **Send**.

   You can also schedule and send the reports of your backup / restore operation on a daily or weekly basis.

To schedule and send the report

1. In the **Email Report** window, enable the **Schedule** button to select the day and time to schedule the reports.
2. Click **Schedule**.

6.2.3 View scheduled reports

You can view all the scheduled reports, and even edit and delete the same under the **View Scheduled Reports** section.

To view and modify a scheduled report

1. Click **View Scheduled Reports**. All the scheduled reports will be listed.
2. Hover on the report name you wish to edit and click  . Make the required changes and click **Save** to save the changes.
3. To delete a particular report, hover on the same and click  . Click **Delete** in the confirmation pop that appears.

6.2.4 Download

You can download reports, click **Download** and select PDF or Excel format to save the file.