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:

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.

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.

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

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 Computers** section of this user manual.

2.1.1 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

2.2 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.

2.2.1 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.

2.2.2 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.

2.3 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.

2.3.1 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**.

2.3.2 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.

2.3.3 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 group deployment via MSI. This can be achieved under the **Backup Console -> Devices** tab.

3.1.1 Add Computers

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 and add your computer:

1. Click the **Add Computers** button.
2. From the **Add Computers** 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.

3.1.2 Deployment through group policy

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 downloaded the IDrive 360 MSI installer package
- Shared folder, accessible via all the domain users
- You have an Active directory environment running Microsoft Windows Server

Step 1: 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**.

Step 2: 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.

Step 3: Register a set of computers under a particular group via GPO

1. 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"

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

Where:

- IDrive360_iRBftnA4XfMLkF7z1NRF2157.msi : The setup downloaded from the **Add Computers** page. Make sure the file is placed in share and the same is accessible across domain users.
- WRAPPED_ARGUMENTS="/GROUP_NAME=Managers" : The group name is 'Managers'

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

3.1.3 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 Computers** 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 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.

3.1.4 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 pre-defined 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	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.

Option	Description
• **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
o **Notify always**	Select this option to get notifications always
o **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 **Add** and filter hidden files or system files from the backup set or add full or partial file / folder names to exclude them from being backed up, and 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 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**.

3.3.4 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.

3.3.5 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  . 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 View Excluded Files

With this feature, you can exclude files / folders present on your computer from being backed up. Selection can be done based on full path, file name or partial name of the files / folders.

Follow the below steps to exclude files / folders:

1. In the **Backup** tab, click **View excluded files**.
2. Enter the file name, partial file name or the path of the files / folders that you want to exclude. You also can exclude system files / folders and hidden files / folders by selecting the appropriate checkbox.
3. Click **Save Changes**.

3.4.3 Restore

You can restore your backed up files / folders from your IDrive 360 cloud account or from 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.

3.4.4 Snapshots

Snapshots are historical view 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.

3.4.5 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.

3.4.6 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
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

Option	Description
• **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.

4 Units and Users

4.1 Units

Administrators can create unlimited units and sub-units, which typically correspond to business units or departments of the organization.

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

4.1.1 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	As an admin, the user will have access to both Management and Backup consoles. Admin can manage users and backup operations for the entire unit and sub-units
Backup User	The access will be limited to only the Backup console. Users can add computers and manage the backup and recovery operations

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.

4.1.2 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.

4.1.3 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**.

4.1.4 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.

4.2 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.

4.2.1 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	As an admin, the user will have access to both Management and Backup consoles. Admin can manage users and backup operations for the entire unit and sub-units
Backup User	The access will be limited to only the Backup console. Users can add computers and manage the backup and recovery operations

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.

4.2.2 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
5. In the popup that appears, click **Add Users.**

Note:

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

4.2.3 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**.

4.2.4 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.

4.2.5 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**.

4.2.6 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.

4.2.7 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**.

5 Settings

5.1 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.**

5.1.1 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.

5.1.2 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

Option	Description
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.

5.1.3 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.

5.1.4 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

Option	Description
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.

5.1.5 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.

6 Security

6.1 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.**

6.1.1 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.

6.2 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 sent to your registered email address or phone number, while signing in to IDrive 360.

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

6.2.1 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.

Follow the below steps to enable 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 click **Enable 2FA**.

6.2.2 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.

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 you wish to disable 2FA, click  and click **Disable 2FA**.

6.2.3 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 in addition to your account password, on all the subsequent logins.

Follow the below steps to sign in 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** as your preferred method of receiving the one-time verification code and click **Confirm**. If you have chosen a Phone Number, enter the same and click **Send Code**.
3. You will be prompted to enter a verification code sent to your email address or phone number.
4. Enter the code and click **Verify**.

6.3 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.

6.3.1 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.

6.3.2 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**.

6.3.3 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.

6.3.4 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.

7 Logs and Reports

7.1 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**.

7.1.1 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**.

7.1.2 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**.

7.1.3 Download

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

7.2 Reports

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

7.2.1 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.

7.2.2 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**.

7.2.3 Download

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