Create a profile

inSync Cloud Editions: ✓ Elite Plus ✓ Elite ✓ Enterprise ✓ Business

Overview

A profile is a set of configurations that are applied to a set of user accounts. As an administrator, you may come across creating inSync accounts for users who work across different departments and functions within the organization and these users may have various types of data to be protected across different data sources.

A profile greatly helps you to define the generic backup configuration parameters that can be automatically applied to the users that belong to that profile. So the next time you create a user account, you can simply assign a profile to match the data protection requirements across different users within your organization.

You can create a profile based on the following factors:

- Type of data sources such as Laptops, Desktops, Mobile Devices, SaaS Apps, and Share
- Type of Operating Systems such as Windows, Mac, Linux, Android, and iOS
- Type of files and applications
- Inclusion or exclusion of file types
- Backup schedules
- Data retention
- Data loss prevention
- Enable users to modify backup settings

You can define separate policy settings for devices and SaaS Apps, independent of each other. Depending on the settings enabled, you can define policy settings for Devices and/or SaaS Apps. For example, if you have purchased only a SaaS Apps license, you can view the Devices page, but you will not see an option to enable and define the settings for Devices. Similarly, if you have a Devices only license, you can view the SaaS Apps page, but you will not see an option to enable and define the settings for SaaS Apps. But if you have purchased, both, license for SaaS Apps and Devices, then you will get options to enable and define settings in both the sections.

If you have purchased only SaaS Apps license and would like to try out devices as well, now have the option to enable or disable the device on their profiles.

https://docs.druva.com/Endpoints/030_Set_up_inSync_for_Endpoints/010_Initial_Configuration/030_Create_and_manage_pr…
Updated: Sat, 25 Sep 2021 00:39:24 GMT
Powered by
You can create a new profile or also simply choose to create a copy of an existing profile and later modify its properties. Profiles ensure easy management of users because you no longer need to manage individual users. Using profiles, you can manage the following properties:

<table>
<thead>
<tr>
<th>Administrator Abilities</th>
<th>User Abilities</th>
<th>Others</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Access user's data</td>
<td>• Edit privacy settings</td>
<td>• Define the maximum users that a profile can have</td>
</tr>
<tr>
<td>• Define access policies such as:</td>
<td>• Restore data through web</td>
<td>• Define the maximum number of devices per user</td>
</tr>
<tr>
<td>◦ Restore through web</td>
<td>• Modify backup settings</td>
<td>• User login through Active Directory</td>
</tr>
<tr>
<td>◦ Select login methods</td>
<td>• Add folders for backup</td>
<td>• inSync system tray icon and user notifications</td>
</tr>
<tr>
<td>◦ Allow access through mobile devices.</td>
<td>• Add devices</td>
<td>• Data share policies</td>
</tr>
<tr>
<td>• Select data sources - Devices and SaaS Apps</td>
<td>• Modify the bandwidth consumed and CPU priority for backups</td>
<td>• Auto-delete inactive devices</td>
</tr>
<tr>
<td>• Select backup content - Include and exclude files</td>
<td>• Pause backups</td>
<td></td>
</tr>
<tr>
<td>• Define global exclusions</td>
<td>• Stop administrators from accessing user data</td>
<td></td>
</tr>
<tr>
<td>• Setup backup frequency</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Define data retention</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Bandwidth consumed and CPU utilized during backup</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Configure data loss prevention</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Set quota per user</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Allow users to modify backup settings</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

When you create a new profile, the new profile inherits all the settings of the Default profile. If you update the settings for the Default profile, any new profile that you create later inherits the updated settings, except the settings for the following:

• Backup folders
• Encrypted folders that administrators include for backup
• Mobile access and backup
• Enable device trace.

When you configure your inSync setup for the first time, you define the settings for the Default profile.
Note: We strongly recommend that an administrator creates a secondary administrator account as well. In the potential scenario where an administrator forgets the password to log on to the Druva Cloud Platform Console, only a secondary administrator can reset that password. Druva implements stringent password policies for inSync Cloud and is unable to reset administrator passwords.

To add a second administrator, click the link that is displayed on the inSync Management Console and follow the same procedure as Create a inSync Cloud administrator.

Procedure

To create a profile:

1. Login to the inSync Management Console.
2. On the inSync Management Console, click Profiles.
3. Click Create New Profile. The profile creation wizard appears.
4. Provide the appropriate information in each field as detailed in Step 1 through Step 4.
5. Click Finish.

Steps:

- Step 1 of 4: General
- Step 2 of 4: Devices
- Step 3 of 4: SaaS Apps
- Step 4 of 4: Share

Step 1 of 4: General

The following table describes the fields in the Summary and User Privacy & Access area of the General page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile name</td>
<td>Type the name for the profile. The name of a profile enables you to quickly identify and assign the profile while creating users in inSync.</td>
</tr>
</tbody>
</table>

Tip: You can provide a name to the profile based on the name of the departments within your organization, type of devices (Laptops, Desktops, Mobile), or type of...
<table>
<thead>
<tr>
<th>Field</th>
<th>Action</th>
</tr>
</thead>
</table>
| **Example:** Engineering, QA Testing, Windows, Mobile devices. | **Max. # users** Type the maximum number of users that you want to assign to this profile. **Example:** 100  
*Note:* By providing a limit to the profile, you can achieve better control over license usage within your organization. **Note:** By providing a limit to the profile, you can achieve better control over license usage within your organization. Type 0 (zero) if you want to allocate the profile to unlimited inSync users. |
| **Description**        | Type a description that will help you and other administrators identify why this profile was created and other necessary details.                                                                                                                                                                                                                               |
| **Data Preservation**  | **Note:** By default, Data Preservation Settings are not inherited from the Default profile. You must specify Data Preservation Settings as per your preference.                                                                                                                                                                                                                                |
| **Auto delete preserved users** | You can mark users as preserved if you do not want inSync to back up the data for these users anymore. **Auto delete after** Specify the duration, in the number of days, when inSync should automatically delete preserved users. You can specify from 1 day to 365 days.  
*Note:*  
• Once the user is auto-deleted, data of that user is also deleted from inSync. You cannot recover this deleted data.  
• User data is retained or deleted based on the backup retention policy you have defined through profiles.  
• If a preserved user is under Legal Hold, the user will not be deleted.                                                                                                                                                                                                 |
| **Backup Inactivity Alert** | You can configure the profile to automatically trigger User Backup Inactivity alert if the user’s data sources are not connected to the inSync Cloud for a certain period. Specify the number of days after which you want inSync to raise the User Backup Inactivity alert. You can specify from 1 day to 365 days.                                                                 |

https://docs.druva.com/Endpoints/030_Set_up_inSync_for_Endpoints/010_Initial_Configuration/030_Create_and_manage_pr…

Updated: Sat, 25 Sep 2021 00:39:24 GMT
Powered by
<table>
<thead>
<tr>
<th>Field</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>backed up for</td>
<td></td>
</tr>
</tbody>
</table>

**User Privacy & Access: Backup Data Privacy Settings**

<table>
<thead>
<tr>
<th>Allow admin access to user backup data</th>
<th>As an administrator, you can access the user's data and perform data restore activities. If you do not want administrators to access and restore the user's data, clear this checkbox.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Important</strong> You cannot enable administrator access to the user data, once you save the profile by disabling this checkbox.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Allow users to edit data privacy settings</th>
<th>Select this checkbox if you want to allow users to edit the data privacy settings. If you allow users to edit data privacy settings, users can prevent administrators from:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Viewing or downloading user data.</td>
</tr>
<tr>
<td></td>
<td>• Performing data restores.</td>
</tr>
<tr>
<td></td>
<td>• Performing a search for users' data.</td>
</tr>
<tr>
<td></td>
<td>• Viewing user audit trail activities such as files and folder names that users have restored or downloaded. Click the relevant link to see the list of files and folders that users have restored or downloaded.</td>
</tr>
<tr>
<td></td>
<td>• Downloading data that users share with others. However, administrators can view the share activities for the users irrespective of the privacy settings.</td>
</tr>
</tbody>
</table>

**Note:** If you do not want the users to disable administrators to view/download their backup and share data through inSync Client, clear the 'Allow users to edit data privacy settings' check box.

**User Privacy & Access: Logs Privacy Settings**

<table>
<thead>
<tr>
<th>Allow admin access to logs</th>
<th>As an administrator, you can access the inSync Client logs from user devices to analyze and troubleshoot the issues, especially for remote users. If you do not want administrators to access inSync Client logs, clear this checkbox.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Allow users to edit logs privacy settings</th>
<th>Select this checkbox if you want to allow users to edit the logs privacy settings. If you allow users to edit the logs privacy settings, users can prevent administrators from downloading log files pertaining to the user's inSync activities.</th>
</tr>
</thead>
</table>

**Access Policy**

---

https://docs.druva.com/Endpoints/030_Set_up_inSync_for_Endpoints/010_Initial_Configuration/030_Create_and_manage_pr…

Updated: Sat, 25 Sep 2021 00:39:24 GMT
Powered by
<table>
<thead>
<tr>
<th>Field</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow restore from web browser</td>
<td>inSync Web allows users to log into their account remotely from a web browser, while they are away from their devices. Select this checkbox if you want to enable inSync Web access for users. See to About inSync Web to learn more.</td>
</tr>
<tr>
<td>Login using</td>
<td>Select a method from the drop-down list that you want users to use to activate inSync and log on to inSync Client.</td>
</tr>
<tr>
<td></td>
<td>• inSync Password: If you want users to login with a password.</td>
</tr>
<tr>
<td></td>
<td>• AD/LDAP Account: If you want users to use their AD/LDAP username and password.</td>
</tr>
<tr>
<td></td>
<td>◦ When you select AD/LDAP Account, the Select AD/LDAP Server field appears. Select the IP address or the fully qualified domain name (FQDN) that contains the AD or LDAP server.</td>
</tr>
<tr>
<td></td>
<td>• Single Sign-On: If you want users to login using Single Sign-On.</td>
</tr>
<tr>
<td></td>
<td>Important Single Sign-On (SSO) option is available only if SSO is configured in inSync. To configure SSO, see Enable backup from mobile devices.</td>
</tr>
<tr>
<td>Allow access from mobile devices</td>
<td>Select this checkbox to allow users the convenience of accessing inSync data from their mobile devices. For more information on how you can update this permission, see Enable backup from mobile devices.</td>
</tr>
<tr>
<td>Allow users to log on only through the MDM managed app</td>
<td>Select this checkbox if you want to allow users to log in to inSync Mobile App by using the MDM mobile app. This option is displayed only if you select the Enforce PIN for mobile access.</td>
</tr>
</tbody>
</table>
**Step 2 of 4: Devices**

**Important:** You can enable and define the settings for Devices only if you have purchased a license for Devices. If you have not subscribed for the Devices license but would like to purchase one, contact Sales.

To enable the settings for devices, select **Enable Device Backup**. The setting options on the **Devices** page are displayed.

The following table describes the fields in the **Select Backup Content** area of the **Devices** page. Enter the required fields and click **Next**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Laptops & Desktops**       | You can configure the profile based on the operating systems. inSync provides data protection across Windows, Mac, and Linux operating systems. As applicable, click on the Windows, Mac, and Linux platform for which you want to configure the folders for backup. **Important:** If you are configuring files and folders for backup on macOS Mojave (version 10.14), see [Configuration guidelines on macOS Mojave](#). Select the folders that you want to back up. You can select the folders for each operating system. **Important:**
  - If you configure inSync to backup All Drives on Windows devices, inSync, by default, does not back up the drives which use the non-NTFS file system. To back up the drives which use the non-NTFS file system, you must configure the drives individually in the profile.
  - Select **All Drives** for backup when you are not sure about the location of the files that you want to backup on user devices.
  - If you configure **OneDrive** folder for backup, inSync backs up only the files that are available locally on the user's device. The On-Demand Files are excluded from backup if the **To configure specific folders for backup on user devices, see [Configure folders for backup](#).**
| **Folder to be backed up**   | **Important:**
  - If you configure inSync to backup All Drives on Windows devices, inSync, by default, does not back up the drives which use the non-NTFS file system. To back up the drives which use the non-NTFS file system, you must configure the drives individually in the profile.
  - Select **All Drives** for backup when you are not sure about the location of the files that you want to backup on user devices.
  - If you configure **OneDrive** folder for backup, inSync backs up only the files that are available locally on the user's device. The On-Demand Files are excluded from backup if the **To configure specific folders for backup on user devices, see [Configure folders for backup](#).**
| **Exclude from Automated Restore** | **Important:** This feature is available on request. Contact Support to enable this feature for your account. Select this checkbox for the folders that you want to exclude from auto-restore triggered during a device replacement. This accelerates the device replacement process and helps users quickly get started. |
inSync provides you an option to backup data based on the file extensions or file MIME types.

Selecting file MIME types over file extensions ensures that any inadvertent or malicious changes to the file extensions by end-users will not exclude business-critical files from being backed.

As applicable, select **Using File Extension** if you want inSync to backup data using the file extensions.

Alternatively, select **Using MIME Type** if you want inSync to backup data using the MIME types.

**Important:**
- Global exclusions are applicable only to file extensions and not applicable to file MIME types.
- This feature is available on request. Contact Support to enable this feature for your account.

For more information on defining file inclusions, see Define file inclusions for backup.

### Include Files
Enter the file types that you want to backup. If you are looking for a specific file type and if it does not appear in the standard list, type the file extension in the adjacent box.

For the list of file types that are by default included for backup, see Defined file types for backup.

### Enter file MIME types to include in backup
Enter the file MIME types that you want to backup. If you are looking for a specific MIME type and if it does not appear in the standard list, type the MIME type in the adjacent box.

**Important**: Global exclusions are applicable only to file extensions and not applicable to file MIME types.

### Exclude Files
If you do not want inSync to back up certain file types, enter the file types. If you are looking for a specific file type and if it does not appear in the standard list, type the file extension in the adjacent box.

**Note**: If you have the same file type in the Include Files and Exclude Files box, that file type is excluded from backups.

For the list of file types that are by default excluded from backup, see Defined file types for backup.

### Exclude Paths
Type the path to the files and folders that you want to exclude from backups.

**Example**: C:\Program Files\Microsoft Office\Data

In addition to the folders listed by default, you can choose to configure additional folders for backup.

**Add Folder**
To add a custom folder for backup, refer Add custom folder for backup.

**Example**: D:\Program Files\Projects
**Folder display name**

Type a name for the custom folder that you want to add for backup. This name is used as an identifier for the custom folder in inSync.

*Displayed only when you add a custom folder for backup using + Add Folder option*

**Important** Once defined, **Folder display name** cannot be edited.

**Tip:** In a few scenarios, inSync ignores the name defined in this field. For more information, see Naming convention for global variables.

inSync excludes the files types that you specify in the global exclude list irrespective of the filters set at the folder level by the administrator or the user.

For more information to configure the global exclude list for File Types, path and Folders, and Regular Expressions, see Global Exclusions.

**Smartphones and Tablets**

This checkbox appears only if you select the **Allow access from mobile devices** checkbox in General settings. Select this checkbox if you want to allow users to back up data from their mobile devices. As applicable, click backup.

**Important** Due to Android OS limitations, inSync no longer backs up the App Settings for Android devices.

For more information on how you can select mandatory folders for backup, see Select mandatory folders for backup.

**Schedule & Retention: Backup Schedule > Laptops & Desktops Schedule**

Select the frequency of scheduled backups on user devices. This is the time interval between two consecutive backups that are triggered automatically on user devices.

**Backup every**

The minimum duration can be 5 minutes and the maximum can be 1 week.

**Note:** The time in this list indicates the interval between two consecutive backups. For example, if the frequency for backups is 4 hours and a backup ends at 10:07 A.M., the next backup starts at 2:07 P.M.

To make sure the user data is backed up periodically, you can configure the profile to allow inSync to perform backup whenever the user attempts to log off from the device or shut down.

Select this checkbox if you want to trigger a backup every time users shut down or log off from their devices.
Note: This option is applicable only for Windows.

Select the preferred timeframe within which inSync can back up data from user devices for the selected backup frequency. Any backup triggered during this period will continue till the end time. **Example:** 12:00 AM - 12:00 AM.

**Note:**
- If Blackout window is configured for a profile, an ongoing scheduled backup will automatically pause if the ongoing backup enters into the Blackout window duration.
- The scheduled backup will automatically resume when the Blackout window duration is complete.
- Users can resume a paused backup if the backup has paused due to the Blackout window.
- inSync follows the time zone of the user device if **Use admin time zone** check box is not selected.

Select the preferred timeframe within which you do not want inSync to trigger any scheduled backups and automatically pause any ongoing backup.

If you do not want to apply this restriction, set the same start time and end time. **Example:** 12:00 AM - 12:00 AM.

**User devices are backed up based on the following criteria if you define the Blackout window duration:**
- An ongoing scheduled backup will automatically pause if the ongoing backup enters into the Blackout window.
- Users can resume a paused backup if the backup has paused due to the Blackout window.
- The scheduled backup will automatically resume when the Blackout window duration is complete.

**Note:** inSync follows the time zone of the user device if **Use admin time zone** field is not selected.

If you want to synchronize backups of all the devices to your time zone, select this checkbox.
Note:

- inSync backs up the devices associated to this profile as per the administrator time zone who updated the profile and selected the Use admin time zone option.
- If you select this check box, the configuration that you specify in the following
  Preferred backup window
  and
  Blackout window
  fields act accordingly to your time zone.

Example

If the administrator's time zone, who updated the profile, is New York (EDT) and the backup schedule time is at 08:00 A.M., backups will start from 05:00 AM for user devices in Los Angeles (PDT).

Schedule & Retention: Backup Schedule > Smartphones & Tablets

This field appears when you select the Enable mobile backup checkbox. Select the time interval between two consecutive backups that are triggered automatically on user mobile devices. The minimum duration can be every 5 minutes and the maximum can be every 1 week.

**Backup every**

By default, inSync performs a backup operation every 8 hours.

For more information about how you can update this permission, see Define the mobile backup interval.

**Use data network in absence of Wi-Fi**

Select this checkbox if you want backups to resume by using a cellular data connection when a wireless connection is not available.

Schedule & Retention: Data Retention for Devices

This is the duration for which you want to retain all the daily backups. At the end of the backup period, inSync will delete.

**Retain all backups for**

*Example:* If you specify that you want to retain all backups for 5 days and inSync completed the backup operation on January 6, 2019, it will delete the backups after the end of the backup period.

For more information about retention policy, see Configure the backup retention policy.

**Retain weekly backups for**

This is the duration for which you want to retain all the weekly backups. At the end of the backup period, inSync will delete.

Enter a value between 1 - 100 weeks as applicable.
Note: The weekly backup is the last backup in a calendar week. The calendar week starts on Sunday.

For more information about retention policy, see [Configure the backup retention policy](#).

Retain monthly backups for

This is the duration for which you want to retain all the monthly backups. At the end of the backup period, inSync will delete backups older than the specified number of months.

Enter a value between 1 - 100 months as applicable.

Note: The monthly backup is the last backup in a calendar month.

For more information about retention policy, see [Configure the backup retention policy](#).

Schedule & Retention: Laptops & Desktops Resources

Max bandwidth [WAN]

Type the maximum network bandwidth that the user devices can consume while backing up data over WAN. You can indicate the bandwidth in bytes per second (Bps), kilobytes per second (Kbps), or megabytes per second (Mbps) or as a percentage of total available bandwidth. If you do not want to set any restriction on bandwidth consumption, type 0 (zero).

Note: inSync requires a minimum bandwidth of 128 Kbps for backups over WAN. If you set the bandwidth as a percentage value, ensure that the maximum WAN bandwidth is not less than 128 Kbps.

CPU Priority

Select the priority that you want to assign to inSync, on the user devices. We recommend that you set CPU priority to an optimal value.

Data Loss Prevention: DLP for Laptops and Desktops

Device trace

Select this checkbox if you want to enable device tracking in case the user's device is lost or stolen. The location of the user

Note: When you select the Device trace check box, an advisory requesting your consent is displayed. Ensure that you read the advisory carefully and accept it to enable this feature.

Auto delete

If you want inSync to automatically delete data from the backup folders on devices if those devices do not connect with inSync. Example: 25.

Alert if device does not connect for

Specify the number of days after which you want inSync to alert you if the user's device does not connect to inSync. This box appears only after you select the Auto delete checkbox.

Delete folders/data if device

Specify the number of days after which inSync must automatically delete data from the backup folders on the device. This box appears only after you select the Auto delete checkbox.
does not connect for

This box appears only after you select the **Auto delete** checkbox.

Select the encryption as applicable:

- **All Folders**: If you want to encrypt all the backup folders.
- **Admin Configured Folder**: If you want to encrypt folders that administrators include in the backup.
- **Disabled**: If you do not want to disable encryption.

**Encrypt**

This box appears only after you select **Admin Configured Folder** in the **Encryption for Windows Laptops and Desktops** field.

Select mandatory backup folders for encryption

Select this checkbox if you want to encrypt files in the inSync Share folder for the users.

For more information, see the inSync Share folder for the users. For more information, see [Encrypt inSync Share folder for Windows laptops](https://docs.druva.com/Endpoints/030_Set_up_inSync_for_Endpoints/010_Initial_Configuration/030_Create_and_manage_pr…)

**Data Loss Prevention: DLP for Smartphone and Tablets**

Select this checkbox if you want to enable device tracking in case the user mobile device is lost or stolen. The location of the user's device appears on the world map in the **Note**: When you select the Device trace check box, an advisory requesting your consent is displayed. Ensure that you read the advisory carefully and accept it to enable this feature.

**Device trace**

Select remote device deactivation option from the list as applicable:

- **Optional**: If you want users to decide if they want to enable device deactivation.
- **Mandatory**: If you want to make it mandatory for users to enable device deactivation.
- **Disabled**: If you want to disable device deactivation.

**Remote device deactivation**

Select this checkbox if you want to allow users to access their favorite files while they are in offline mode.

**Allow offline access to files (Favorites in share)**
Allow other iOS apps to access inSync content

Select this checkbox if you want users to back up data by using other apps on an iOS device.

Encryption for android

Select this checkbox if you want to encrypt the data in the backup folders of the user's Android device.

User Settings: Allow Users to Change Settings > Backup Settings

Change backup schedule

Select this checkbox if you want users to modify and override the pre-defined backup schedule that you have set.

Note: Backup schedules modified by users override administrator backup schedules.

Change blackout window

Select this checkbox if you want to allow users to modify the blackout window period as per their preference.

Pause backup

Select this checkbox if you want to allow users to pause a scheduled backup that is in progress.

This will enable the users to conserve internet bandwidth or CPU usage that is required for a priority task that the user is performing.

Cancel backup

Select this checkbox if you want to allow users to cancel an ongoing backup that is in progress.

This will allow the user to cancel the ongoing scheduled/unscheduled backup operation that is in progress. inSync

User Settings: Allow Users to Change Settings > Backup Content

Add backup folders (laptops & desktops)

Select this checkbox if you want to allow users to add additional folders for backup.

Add content & edit settings (smartphones & tablets)

Select this checkbox, if you want users to modify content for backup, backup schedule or resource settings for mobile devices.

User Settings: Allow Users to Change Settings > Backup Resources

Modify backup resources

Select this checkbox if you want to allow users to modify the Max Bandwidth and CPU Priority values.
Note: After a user configures these settings, you cannot change these settings.

Opt out of networks for backup

Select this checkbox if you want to allow users to block specific networks from backing up data.

Example: Allow users to block backups on data card, personal mobile hotspots, or Mi-Fi devices during traveling to minimize the personal hotspot or Mi-Fi usage.

Note: Users will be able to opt out of networks with subnet mask of 24 bit or more only.

Edit proxy settings

Select this checkbox if you want to allow users to update proxy settings.

This will enable the users to connect to inSync Server directly in case the user relocates to a different business unit.

User Settings: Allow Users to Change Settings > User Notification Settings

Select this checkbox if you want to allow the users to select or deselect the type of notifications they prefer to see on their devices.

inSync notifications are classified as follows:

- Critical
- High
- Warning
- Informative

To learn more about the notifications, refer Notifications Shown on Devices.

User Settings: Device Settings for Users > Notification Shown on Devices

Critical

inSync notifications help users to get alerts and notifications about the activities performed by the inSync Client.

As an administrator, you can choose the type of inSync notifications you want to display on the user devices.

For more information about the types of notifications and their nature, refer Enable inSync notifications.

High

Warning

Informative

As applicable, select the checkbox for Critical, High, Warning, and/or Informative notifications.

User Settings: Device Settings for Users
Allocate the amount of data that each user assigned to this profile can backup and share on their devices.

**Example:** If you set this to 1000 GB, inSync will back up and share the user data for up to 1000 GB.

If you do not want to set any restriction on the data size, type 0 (zero).

**Note:** If the size of the files in the backup and share folders exceed the assigned quota, the backup and share from user devices will fail.

If you want users to activate inSync on their devices, select this checkbox.

If you do not select this checkbox, you must activate inSync for all users.

**Note:** This setting is not applicable for mobile device activation.

This box appears only when you select **Allow users to add devices** checkbox.

**Example:** If you enter 2, the user will be able to activate inSync on a maximum of 2 devices.

Select this checkbox if you want the inSync icon to appear in the system tray of the user’s devices.

If this is enabled, the users can view the various statuses of inSync on system tray such as connection, backup, restore, etc.

**User settings:** Device Settings for Users > Manage Inactive Devices

Specify the number of days after which inSync must mark the device as inactive in the absence of any connection between the user device and inSync.

**Example:** If you set the period as 5 days and if a user device did not connect for 5 consecutive days, inSync flags the device as inactive. You can specify any value from 1 to 365.

Enables auto-delete of inactive devices setting for the profile. inSync automatically deletes inactive devices associated with the profile after the number of days specified.

**Warning:** Once the device is deleted, snapshots of that device will not be available for download or restore.

Specify the number of days after which inSync must delete the inactive devices. The default value is 180 days.
Click **Disable Device Backup** to disable the backup on the devices associated to this profile at anytime.

---

**Configuration guidelines on macOS Mojave**

**Locations that display a prompt**

*Important:* The macOS Mojave (version 10.14) has a User Data Protection feature, which displays an authorization prompt when inSync Client tries to access the following locations if configured for backup:

- Location Services
- Contacts `~/Library/Application Support/Address Book`
- Calendars `~/Library/Calendars`
- Reminders `~/Library/Calendars`
- Photos `~/Pictures/Photos Library,photoslibrary`

If you want inSync to back up the locations but do not want the macOS Mojave to display the permission prompts to the users, you can pre-configure the authorization to inSync via MDM (Mobile Device Management) which is used in your organization. Druva also recommends educating the inSync Client users of your organization to pre-approve inSync by adding it to **Full Disk Access** in **System Preferences > Security and Privacy** pane for a seamless backup experience.

If you do not want inSync to backup the mentioned locations, you must configure these locations in the Global Exclude list, defined at Profile level. inSync skips the locations mentioned in the Global Exclude list while backing up user data. For more information, see [Configure the global exclude list](https://docs.druva.com/Endpoints/030_Set_up_inSync_for_Endpoints/010_Initial_Configuration/030_Create_andManageProfiles#Enable the global exclude list).

**inSync Client v6.1.1**

inSync Client v6.1.1 supports macOS Mojave (version 10.14).

*Important:*  
- *Druva recommends that you upgrade the inSync Client to v6.1.1 before upgrading user devices to macOS Mojave.*
- *If inSync Client users do not take any action on the prompts, inSync will pause the ongoing backup and it will remain in that state until the user takes an action.*

**For inSync Client v6.1.0 and earlier:**

inSync Client v6.1.0 and earlier, running on macOS Mojave will skip the backup of the mentioned locations, even if they
are configured for backup. Administrators must upgrade user devices running on macOS Mojave to inSync Client v6.1.1 or later to successfully backup the mentioned locations.

**Locations that do not display a prompt**

**For inSync Client v6.1.1:**

inSync Client will skip the following configured locations by default while performing the backup if it does not have the required access permissions:

- Mail
- Messages
- Safari Browsing History
- HTTP Cookies
- Call History
- iTunes Backups
- Time Machine Backups

Druva recommends educating the inSync Client users of your organization to pre-approve inSync access to the configured locations. To learn more, refer to [inSync Client changes for macOS Mojave (version 10.14)](https://docs.druva.com/Endpoints/030_Set_up_inSync_for_Endpoints/010_Initial_Configuration/030_Create_and_manage_pr...).

**For inSync Client v6.1.0 and earlier:**

inSync Client v6.1.0 and earlier, running on macOS Mojave will skip the backup of the mentioned locations, even if they are configured for backup. Administrators must upgrade user devices running on macOS Mojave to inSync Client v6.1.1 or later to successfully backup the mentioned locations.

**Step 3 of 4: SaaS Apps**

You can enable and define the settings for SaaS Apps only if you have purchased a license for SaaS Apps. If you have not subscribed for the SaaS Apps license but would like to purchase one, contact Sales.

To enable the settings for SaaS Apps, click **Enable SaaS Apps Backup**. The setting options on the SaaS Apps page are displayed.

The following table describes the fields in the Select Backup Content area of the SaaS Apps page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Important</strong> Only the SaaS Apps which are configured with inSync is displayed for backup.</td>
</tr>
</tbody>
</table>

https://docs.druva.com/Endpoints/030_Set_up_inSync_for_Endpoints/010_Initial_Configuration/030_Create_and_manage_pr...
Important:
- The Global Exclusion for the Exclude Paths option is supported for Exchange Online, Gmail.
- For Gmail and Exchange Online, only folder name or relative paths are supported for Exclude Paths.
- For Google Drive and OneDrive, folder or file name or relative paths are supported for Exclude Paths.

In the Exclude File Types box, type the file types that you want to exclude from the backup. The file extension is automatically added to the adjacent field. If you want to remove a file type, click the file type.

Note: Exclusions of file types are supported for OneDrive and Google Drive only.

In the Exclude Paths box, type the file or folder name or relative path to the files and folders that you want to exclude from backups. Entries using a semicolon (;) and there is no white space between two entries.

For more information on how you can configure the global exclude list, see,
- Configure a global exclusion list for files for SaaS Apps
- Configure a global exclusion list for folders for SaaS Apps

Microsoft 365
If you want to choose all Microsoft 365 applications for backup, then select this checkbox.

To backup only OneDrive data, select this checkbox.

You can exclude specific files and specific file and folder paths from backup.

- Exclude File Types: If you do not want inSync to back up certain file types, enter the file types. If you are looking for a specific list, type the file extension in the adjacent box.
- Exclude Paths: Type the file or folder name or relative path to the files and folders that you want to exclude from backups. Entries using a semicolon (;) and there is no white space between two entries.

Example: Let’s assume you have the following folders in your OneDrive:
- /Druva/Templates/Paths.txt
- Druva/Paths.txt

You specify Paths.txt in the Exclude Paths field. Now, during the backup operation, inSync excludes Paths.txt from backing up ‘/Druva/Paths.txt’ from getting backed up.
To backup only Exchange Online data, select this checkbox. In-Place Archive for Exchange Online is also backed up if Exchange Online is selected.

- **Backup Recoverable Items**: Optionally, if you want inSync to backup the Exchange Online ‘Recoverable Items’ folder, which keeps the deleted emails, items in the Deletions and Purges items, select the **Backup Recoverable Items** checkbox. This enables administrators and accidental or malicious deletion.

- **Exclude Paths**: Type the folder name or relative path to the folders that you want to exclude from backups. Ensure that you separate consecutive entries using a semicolon (;) and there is no white space between two entries.

  **Example**: Let’s assume you have the following folder in your Exchange Online:
  - Inbox/Mails
  - /Templates

  You specify *Inbox/Mails ;Templates* in the **Exclude Paths** field. Now, during the backup operation, inSync excludes.

  **Note**: Avoid using ‘:&’ when specifying the path for exclusion.

---

To backup only Google Workspace data, click the tab. Under **Google Workspace** tab, you can select the following:

- **Gmail**: To backup only Gmail data, select this checkbox. You can exclude specific folder names from the backup.
  - **Exclude Paths**: Type the folder name or relative path to the folders that you want to exclude from backups. Ensure that you separate consecutive entries using a semicolon (;) and there is no white space between two entries.

  **Example**: Let’s assume you have the following folder in your Gmail:
  - Inbox/Mails
  - /Templates

  You specify *Inbox/Mails ;Templates* in the **Exclude Paths** field. Now, during the backup operation, inSync excludes.

  **Note**: Avoid using ‘:&’ when specifying the path for exclusion.

---

- **Google Drive**: To backup only Google Drive data, select this checkbox. You can exclude specific file types and shared data owned by other users.
  - **Exclude File Types**: If you do not want inSync to back up certain file types, enter the file types. If you are looking for a specific standard list, type the file extension in the adjacent box.
  - **Backup shared data owned by other users**: Select this checkbox if you want to backup all the Google Drive data.
  - **Exclude Paths**: Type the file or folder name or relative path to the files and folders that you want to exclude from the backup. Ensure that you separate consecutive entries using a semicolon (;) and there is no white space between two entries.

  **Example**: Let’s assume you have the following folders in your Google Drive:

  `/Druva/Templates/Paths.txt`
You specify Paths.txt in the **Exclude Paths** field. Now, during the backup operation, inSync excludes Paths.txt from getting backed up.

**Note:** Selecting the **Backup shared data owned by other users** checkbox might slower your incremental backups. For faster backup and restore, it is recommended to deselect this checkbox. For existing administrators, this checkbox is selected by default. You have to manually deselect this option.

### Schedule & Retention: Backup Schedule

**Backup every**

Select how frequently you want inSync to back up SaaS Apps data. By default, inSync performs the backup operation once a day. For more information, see [interval for SaaS Apps](https://docs.druva.com/Endpoints/030_Set_up_inSync_for_Endpoints/010_Initial_Configuration/030_Create_and_manage_pr…).

### Schedule & Retention: Data Retention for Files

**Retain daily data backups for**

Type the number of days that you want to retain all the backups. At the end of the backup period, inSync will retain all the backups set.

For example, if you specify that you want to retain all backups for 5 days and inSync completed the backup operation on January 6, 2017, inSync will retain storage till January 11, 2017.

For more information about retention policy, see [Configure the backup retention policy](https://docs.druva.com/Endpoints/030_Set_up_inSync_for_Endpoints/010_Initial_Configuration/030_Create_and_manage_pr…).

**Retain weekly data backups for**

Type the number of weeks that you want to retain all the weekly backups.

At the end of the weekly backup period, inSync will retain the data /snapshots within the storage based on the retention period set.

For example: If you type 5, inSync will automatically retain all the weekly snapshots for 5 weeks.

For more information about retention policy, see [Configure the backup retention policy](https://docs.druva.com/Endpoints/030_Set_up_inSync_for_Endpoints/010_Initial_Configuration/030_Create_and_manage_pr…).

**Note:** The weekly backup is the last backup in a calendar week. The calendar week starts on Sunday.

**Retain monthly data backups for**

Type the number of months that you want to retain all the monthly backups.

At the end of the monthly backup period, inSync will retain the data/snapshots within the storage based on the retention period set.

Example: If you type 3, inSync will automatically retain all the monthly snapshots for 3 months.

For more information about retention policy, see [Configure the backup retention policy](https://docs.druva.com/Endpoints/030_Set_up_inSync_for_Endpoints/010_Initial_Configuration/030_Create_and_manage_pr…).
Note: The monthly backup is the last backup in a calendar month.

Schedule & Retention: Data Retention for Emails

Select this option if you wish to apply the files' data retention settings for Microsoft 365 Exchange Online and Gmail snapshots.

inSync retains the email backed-up snapshots within the storage as per the configured daily, weekly, and monthly retention period settings for files.

For example, if you specify that you want to retain all backups for 5 days and inSync completed the backup operation on January 6, 2019, inSync retains the email backed-up snapshots till January 11, 2019.

For more information about retention policy, see Configure the backup retention policy.

Important:
- If you have selected this option, then the Retention Period assigned to the files is not applicable for Microsoft 365 Exchange Online and Gmail snapshots.
- Delete Emails older than option is applicable for Microsoft 365 Exchange Online and Gmail only.

Select and type the number of months up to which you want inSync to retain all backed up emails within Exchange Online and Gmail snapshots.

For example, if you type 6, inSync will retain all emails across all snapshots whose sent or received timestamp is less than 6 months old.

By default, inSync retains emails for 84 months.

Emails are retained based on the email’s event date and timestamp. The maximum retention period that you can specify is 250 months and the minimum is 1 month. Type zero (0) for unlimited retention of emails.

For more information about retention policy, see Configure the backup retention policy.

Note: Data retention settings for files and emails do not apply in the following scenarios:

- If the users associated with the SaaS Apps profile are put on Legal Hold.
- If the retention settings for Files for the SaaS Apps profile has unlimited retention settings for daily, weekly, and monthly frequencies. i.e. The Retention Settings for Files for the SaaS Apps profile is set to Zero.
**Step 4 of 4: Share**

If you want the users associated with the profile to use the inSync Share functionality, click **Enable Share**. inSync creates the inSync Share folder on all their devices.

The following table describes the fields in the **Share Settings** area of the **Share** page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td># versions of a file to be retained</td>
<td>This box appears only after you select the <strong>Enable Sharing</strong> checkbox. Type the number of versions that you want inSync to maintain for any file that is within the inSync Share folder of a user's devices.</td>
</tr>
<tr>
<td>Allow sharing with profiles</td>
<td>This box appears only after you select the <strong>Enable Sharing</strong> checkbox. Type or select the profiles with which you want to allow the users of this profile to share files. Users of this profile can share files only with the users of the profiles that you select.</td>
</tr>
<tr>
<td>Allow sharing with guests</td>
<td>This box appears only after you select the <strong>Enable Sharing</strong> checkbox. If you want to allow users to share files with existing guest users, select this check box.</td>
</tr>
<tr>
<td>Allow adding guest users</td>
<td>This box appears only after you select the <strong>Allow sharing with guests</strong> check box. If you want to allow users to add guest users, select this check box.</td>
</tr>
<tr>
<td>Enable link sharing</td>
<td>This box appears only after you select the <strong>Enable Sharing</strong> checkbox. If you want the users of this profile to create download links for files in the inSync Share folder, select this check box.</td>
</tr>
<tr>
<td>Mandatory password for links</td>
<td>Select this checkbox if you want users to password-protect their shared links.</td>
</tr>
<tr>
<td>Link expires in</td>
<td>This box appears only after you select the <strong>Enable link sharing</strong> checkbox. Type a number between 1 and 365 to specify the number of days that you want the download link to remain active. When this link expires, anyone with whom your users shared their content cannot download the shared content.</td>
</tr>
</tbody>
</table>
Note: Click Disable inSync Share to disable sharing associated to this profile at anytime.