Profile Details page

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

About Profile Details page

This page displays the total number of users associated with the profile, backup status, and users with highest storage consumption. This page also displays the configuration settings that you had defined in the policy creation wizard.

Access path

1. On the inSync Management Console, click Profiles. The Manage Profiles page appears.
2. Click the desired Profile Name to view the details of the profile.

Summary

The following table describes the fields in the Summary area.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users</td>
<td>The number of users and the maximum number of users that can be associated with a profile. For example, 1 [5] indicates that 1 user is associated with the profile to which a maximum of 5 users can be associated.</td>
</tr>
<tr>
<td>Devices Enabled</td>
<td>The number of devices belonging to users associated with a profile.</td>
</tr>
<tr>
<td>Total Data</td>
<td></td>
</tr>
<tr>
<td>Cloud Apps Enabled</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Total Data</td>
<td>The amount of data backed up by users associated with a profile.</td>
</tr>
<tr>
<td></td>
<td>Note: The count includes data backed up from SaaS Apps.</td>
</tr>
<tr>
<td>Cloud Apps Enabled</td>
<td>Number of SaaS Apps enabled for backup out of the number of SaaS Apps</td>
</tr>
<tr>
<td></td>
<td>configured for backup.</td>
</tr>
</tbody>
</table>

**Backup Statistics**

![Backup Statistics Chart]

The following table describes the fields in the Backup Statistics area:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backed Up</td>
<td>The number of Devices/SaaS Apps from which the last backup was successful.</td>
</tr>
<tr>
<td>Successfully</td>
<td></td>
</tr>
<tr>
<td>Backed up with errors</td>
<td></td>
</tr>
<tr>
<td>Failed backups</td>
<td></td>
</tr>
<tr>
<td>Inactive</td>
<td></td>
</tr>
<tr>
<td>Never Backed Up</td>
<td></td>
</tr>
</tbody>
</table>

The number of SaaS Apps for which the last backup stopped due to throttling errors such as HTTP 429.

Note: You can see this error message when you select SaaS Apps.
### Inactive
The number of Devices/SaaS Apps that did not communicate with the inSync Master for a specific number of days.

| Never Backed Up | The number of Devices/SaaS Apps that were never backed up. |

### Top users by storage consumption

![Top Users By Storage Consumption](image)

As a graphical representation, the **Top users by storage consumption** displays the top five users of a profile that backed up the most data.

### Profile details

#### Profile Summary

The following table lists the fields in the **Profile Summary** area of the **Summary** page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile name</td>
<td>The name for the profile.</td>
</tr>
<tr>
<td>Max. number of users</td>
<td>The maximum users that you want to assign to this profile.</td>
</tr>
<tr>
<td></td>
<td>0 (zero) indicates that you do not want to set any restriction on the number of users.</td>
</tr>
<tr>
<td>Profile description</td>
<td>A short description of the profile.</td>
</tr>
</tbody>
</table>
## User Privacy & Access

The following table lists the fields in the **User Privacy & Access** area.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto delete preserved users</td>
<td>Indicates that you want to allow users to prevent inSync administrators to restore data from their devices on a server. <strong>Note:</strong> Once a user selects preventing administrators from accessing data, administrators will not be able to restore data to the inSync Master for that user even if you change the profile settings or move the user to a different profile.</td>
</tr>
<tr>
<td>Allow admin access to user data</td>
<td>Indicates that you want to allow users to edit the privacy settings. If selected, users can disallow administrators to view or download their data. <strong>Note:</strong> Once a user selects preventing administrators from accessing data, administrators will not be able to restore data to the inSync Master for that user even if you change the Profile settings or move the user to a different Profile.</td>
</tr>
<tr>
<td>Allow restore from a Web browser</td>
<td>Indicates that users can restore data by accessing their inSync account through a Web browser.</td>
</tr>
<tr>
<td>Log-in using</td>
<td>Indicates whether an inSync Password, Active Directory, or single sign-on will be used to authenticate access to inSync.</td>
</tr>
<tr>
<td>Allow access from mobile devices</td>
<td>Indicates that you want users to access data from the inSync Mobile App.</td>
</tr>
<tr>
<td>Allow users to log on only through the inSync MDM app</td>
<td>This option is displayed only if you check <strong>Allow access from mobile devices.</strong> Select this check box if you want to allow users to log on by using only the inSync for MobileIron app from iOS devices.inSync for MobileIron app from iOS devices.</td>
</tr>
<tr>
<td>Enforce PIN for mobile access</td>
<td>Indicates that the four-digit security code is mandatory for accessing inSync mobile app.</td>
</tr>
</tbody>
</table>
General tab

The following fields are displayed in the Profile Summary area of the General tab.

Summary

• Profile name
• Max. # users
• Description

Data Preservation

• Auto delete preserved users after a set duration
• Delete preserved users after
• User Privacy & Access
• Allow admin access to user data
• Allow users to edit privacy settings
• Allow restore from a Web browser
• Log-in using
• Allow access from mobile devices
• Allow users to log on only through the inSync MDM app
• Enforce PIN for mobile access

Devices tab

The following fields are displayed under the Devices tab.

Laptops & Desktops

• Windows/Mac/Linux
• Global Exclusions
• Exclude Files
• Exclude Paths
• Smartphones and Tablets
• Enable mobile backup

Schedule & Retention: Backup Schedule > Laptops & Desktops Schedule

• Backup every
• Backup at logoff/shutdown
• Preferred backup window
• Blackout window
• Use admin time zone
Schedule & Retention: Backup Schedule > Smartphones & Tablets

- Backup every
- Use data network in absence of Wi-Fi
- Schedule & Retention: Data Retention for Devices
  - Retain all backups for
  - Retain weekly backups for
  - Retain monthly backups for

Schedule & Retention: Laptops & Desktops Resources

- Max bandwidth [WAN]
- CPU Priority

DLP for Laptops and Desktops

- Device trace
- Auto delete
  - Auto delete folders if device does not connect for
  - Delete folders/data if device does not connect for
- Encrypt
  - Select mandatory backup folders for encryption
  - Encrypt inSync Share folder
  - Geofencing

DLP for Smartphone and Tablets

- Device trace
- Remote device deactivation
  - Allow offline access to files (Favorites)
  - Allow other iOS apps to access inSync content
- Encryption for android

User Settings: Allow Users to Change Settings > Backup Settings

- Change backup schedule
- Change blackout window
- Pause backup

User Settings: Allow Users to Change Settings > Backup Content

- Add backup folders (laptops & desktops)
- Add content & edit settings (smartphones & tablets)
User Settings: Allow Users to Change Settings > Backup Resources

- Modify backup resources
- Opt out of networks for backup
- Edit proxy settings

User Settings: Device Settings for Users

- Quota per user
- Allow users to add devices
- Max. devices per user
- Mark device inactive if not backed up for
- Show inSync icon in system tray
- Show desktop notifications

Cloud Apps tab

The following fields are displayed under the SaaS Apps tab.

- Microsoft 365
- OneDrive
- Exchange Online
- Box
- Google Workspace
- Global Exclusions

Schedule & Retention: Backup Schedule

- Backup every

Schedule & Retention: Data Retention for Cloud Apps

- Retain all backups for
- Retain weekly backups for
- Retain monthly backups for

Share tab

The following fields are displayed under the Share tab.

- # versions of a file to be retained
- Allow sharing with profiles
- Allow sharing with guests
• Allow adding guest users
• Enable link sharing
• Mandatory password for links
• Link expires in