Device replacement for remote AD, non-AD, and SCIM users (IMD V2)

Overview

Device replace is an activity undertaken by most organizations to upgrade the user devices to the latest software versions. The user device may also require device replacement in events such as:

- Damage to the device
- Loss or theft of the device
- Upgrade to a new device

In such scenarios, the user should not find it challenging to restore the backed-up data from the old device onto the replacement device or new device.

To ensure that users find it convenient while migrating to the replacement device and there is no data loss during the device replacement activity, inSync features the capability through which administrators can remotely replace the user devices for the remote users who are working in an Active Directory (AD) and Non-AD environments.

Using this feature, the inSync administrators can restore the complete data onto the replacement device before it is shipped to the user. As a result, when the user activates the inSync Client on the replacement device, inSync tries to automatically map the restored data to the relevant destination paths and folders.

Option to add a new device

Administrators also get the option to add a new device for the user instead of replacing the old device to avoid any chances of losing data updates made on the older device while the new device is activated and shipped. The user will have two devices in inSync Client and can continue using both devices even after receiving the new device. As soon as the user activates the inSync Client on the new device inSync tries to automatically map the restored data to the relevant destination paths and folders, including the data that was backed up on the old device, while the new replacement device was in transit.

The capability to restore the most recent data from the old device onto the new device, while the new device is in transit is called Restore Delta Data. For more information see Add new device for Active Directory (AD) users and Add new device for Non-AD users.
Important: **Restore Delta Data** is an on-demand feature. Contact Support to enable this feature for your account.

Advantages of remote device replace

- The device is replaced remotely by the inSync administrator with minimal to no user efforts.
- The inSync administrator can restore the user's data on the new device, ensuring there is no loss of data while doing so.
- Restore failures due to poor connectivity or less available bandwidth issues are minimized considerably.
- The user gets a new device with data already restored on it.
- There is no loss of data, as even the restored data which cannot be mapped to its relevant path or folder stays in the temporary location unless inSync Client is uninstalled.

Limitations of remote device replace

- All User's data will always be restored and any other data if present will be overwritten. But if the other data is present and encrypted as well, then it will not be restored.
- As part of the device replace, share data will not be synced in the case of AD users. It will be synced only in the case of non-AD users.
- Device replace will not work if the user has enabled data privacy settings.
- Device replace is not supported for OpenLDAP users.

The inSync administrator can replace a device remotely by using Integrated Mass Deployment (IMD) for Active Directory (AD) or non-AD users.

**Device Replace workflow for AD users**

The device replace workflow for AD users is as follows:

**inSync Administrator actions:**

1. On the inSync Management Console, marks the device which needs to be replaced and start the device replace process.

**System Administrator actions:**

1. Using IMD, installs inSync Client on the user's new device and logs into the new device.
2. inSync Client restores all the data on the new device.
   After this step, the new device is ready to be shipped to the user.
Note:

- System settings and MAPI data are not scheduled for restore, by default.
- System settings and MAPI data are restored only after the user logs on to the device using their AD credentials.

User actions:

1. Using Active Directory credentials, logs in to the new device.
2. The inSync Client restores system settings and MAPI data. inSync Client then moves the restored data which is saved at the temporary location to relevant paths and folders as required.

The device is now ready to be used.

Device Replace process for AD Users

The following table describes the steps involved in replacing the user devices for remote users who are connected to the AD environment:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Mark the old device for replacement from the inSync Management Console.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Generate a mass deployment token.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select the IMD command parameters.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Run the IMD commands for AD users.</td>
</tr>
<tr>
<td>Step 5</td>
<td>inSync Client restores all the data on the new device. For more information, see Temporary location directories for restored data.</td>
</tr>
<tr>
<td>Step 6</td>
<td>The device is now ready to be shipped to the user. Users can complete further steps when they receive the replacement device. See User actions after the remote device replacement for AD users.</td>
</tr>
</tbody>
</table>

Device Replace workflow for non-AD users

The device replace workflow for non-AD users is as follows:

inSync Administrator actions:

1. On the inSync Management console, marks the device which needs to be replaced and start the device replace process.
System Administrator actions:

1. Login to the new device and create a local account.
2. Using IMD, install inSync Client on the user's new device.
3. Log in as the user on the new device.
4. inSync Client restores all the data including system settings and MAPI data on the new device.
5. inSync Client moves the restored data which is saved at the temporary location to relevant paths and folders as required.
   The device is ready to be shipped to the user.

User actions:

1. Login to the new device which is ready to be used.

Device Replace process for non-AD Users

The following table describes the multi-step process for the integrated mass deployment (IMD) device replace.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Mark the old device for replacement from the inSync Management Console.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Create a user account on the new device.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Generate a mass deployment token.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Select the IMD command parameters.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Log in as a user on the replacement device.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Run the IMD commands for the Non-AD users.</td>
</tr>
<tr>
<td>Step 7</td>
<td>inSync Client restores all the data on the replacement device including System Settings and MAPI data. For more information, see Temporary location directories for restored data.</td>
</tr>
<tr>
<td>Step 8</td>
<td>inSync Client moves the data from the temporary location to relevant folders and paths. For more information, see Device replace for Non-AD users.</td>
</tr>
<tr>
<td>Step 9</td>
<td>The device is now ready to be shipped to the user. Users can complete further steps when they receive the replacement device. See User actions after the remote device replacement for non-AD users.</td>
</tr>
</tbody>
</table>