Quickstart to inSync user provisioning and integrated mass deployment

Overview

As an inSync administrator, you can configure the user devices in your organization for data protection. To start with, you need to import/provision the user-base from your organization directory into inSync. And as a next step, you can then bulk deploy inSync Client on the user devices by configuring one of the Integrated Mass Deployment (IMD) methods.

inSync supports bulk deployment of inSync Client on user devices across your organization during user on-boarding, as well as bulk replacement of user devices during the device replacement activities.

This quick reference guide helps you to choose the best strategy to manage user provisioning and inSync Client bulk deployment methods.

**Important**
inSync currently supports user and device management using Integrated Mass Deployment (IMD) for Mac and Windows devices.

The following illustration demonstrates the step by step workflow:
Step 1 - Select the user provision method

You can import the users from your organization using one of the following methods:

• **Directory services such as Microsoft Active Directory (AD) or Lightweight Directory Access Protocol (LDAP):**

  If your organization uses AD/LDAP to store user details, you can integrate the directories to provision users in inSync.
  To select this method, log on to the inSync Management Console and select

  > inSync Settings > Deployment.

• **Non-AD/LDAP:**

  If your organization maintains a non-AD/LDAP user base, you can import the users through a CSV file.
  To import a group of users in a non-AD/LDAP environment, see Add users through CSV file.

• **System for Cross-domain Identity Management (SCIM):**

  If your organization uses SCIM-compliant Identity Providers (IdPs) as a source directory to manage and authenticate users to provide access to different applications, you can integrate it with Druva inSync to provision users in inSync and across multiple SaaS applications.
  To select this method, log on to the inSync Management Console and select

  > inSync Settings > Deployment.

Step 2 - Integrate with inSync for user management

Based on the user provisioning method that you have opted in Step 1, you can select any of the following listed integration methods for user and device management in inSync.

• **AD/LDAP integration with inSync**

  AD/LDAP integration involves registering your AD/LDAP with inSync and helps you:
  ◦ Automatically import users at regular intervals
  ◦ Select user login mechanism
  ◦ Create AD mapping and define the filter parameters
  ◦ Automatic synchronization of user details
  ◦ Automatic update of user details

  To complete the AD/LDAP integration see, Integrate AD/LDAP with inSync.
• **Non-AD/LDAP integration with inSync**

Integration with a non-AD/LDAP environment involves mapping the group of users and their details using a device map CSV file in the inSync Management Console.

To complete the AD/LDAP integration see, [Import device map CSV](#).

• **SCIM integration with inSync**

SCIM integration involves configuring the SCIM app with inSync and helps you:
- Automatically import users
- Change SCIM mapping priority
- Define mapping sequence
- Define storage region
- Define storage quota

To complete the SCIM integration see, [Integrate SCIM with inSync](#).

**Step 3 - Mass Deployment of inSync Client**

Integrated mass deployment (IMD) is an automated process to bulk deploy and automatically activate inSync Client on Mac and Windows devices across your organization.

We have developed multiple versions of IMD to cater to the different scenarios, to help you perform user and device management in bulk. Based on the user provisioning method you have opted for, you can choose the associated inSync Client deployment method.

**Bulk deployment**

**AD/LDAP and SCIM managed users**  
Associated IMD version

- **Bulk deploy inSync Client on user devices**  
  IMD v2

- **Bulk deploy inSync Client for Azure AD users**  
  IMD v5

**Non-AD/LDAP managed users**  
Associated IMD version

- **Bulk deploy inSync Client on user devices**  
  IMD v3

**Device replacement**

Replacing user devices is a common activity across organizations that includes issuing new devices to their users as
part of device refresh scenarios or in the events like thefts or loss of the device. To address these scenarios, we have also developed various versions of IMD to cater to different use cases.

Using these methods, the inSync administrators can restore the 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.

<table>
<thead>
<tr>
<th>AD/LDAP and SCIM managed users</th>
<th>Associated IMD version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replace devices for remote users</td>
<td>IMD v2</td>
</tr>
<tr>
<td>Bulk replace of devices for users</td>
<td>IMD v4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Non-AD/LDAP managed users</th>
<th>Associated IMD version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replace devices for remote users</td>
<td>IMD v2</td>
</tr>
<tr>
<td>Bulk replace of devices for users</td>
<td>IMD v4</td>
</tr>
</tbody>
</table>