

How to set up an LDAP Sync

Print Director can import and maintain user records by synchronising its database with LDAP (example: Active Directory or AD). This alleviates the administrative task of ensuring users have the correct up-to-date settings and information (e.g. full name, email address, telephone extension). Once the user has been placed in the correct Organisational Unit (OU), they will inherit all the settings that have been defined for the Department in Print Director (e.g. Rules and device access, account access and opening balance, popup billing requirements, etc.)

Create the LDAP Sync Scheduled Task

- Open Resource Manager.
- Navigate to **Scheduled Tasks > LDAP Sync**.
- On the right-hand side, click **Add**.
- In the **Scheduled Task Name** textbox, enter a descriptive name, e.g. Management user accounts.
- In the **Execute on PDServer** dropdown, choose the server on which you would like the task to execute.

Specify the schedule on which the task will execute

- Open your LDAP Sync scheduled task if it is not still open.
- Click the **Schedule** tab.
- In the **Schedule Range** frame, change to the desired **Execute time** if the task is **not** going to run **Hourly**. If it is going to run Hourly, the execute time has no effect.
- In the **Schedule Pattern** frame, choose the frequency of the execution. The default is **Daily**. AD Syncs are often required to run **Hourly** to ensure that user information stays current.

Sync Settings tab, Import settings

Here we will specify the general import settings for the sync.

Specify the import limits and containers

- Open your LDAP Sync scheduled task if it is not still open.
- On the **Import Settings** tab, ensure that the correct domain name appears in the **Server or domain name** textbox. This could be a domain name, server host name, or IP address.
- Ticking the **Don't import disabled users** checkbox will avoid importing disabled users.
- If the container from which we will import contains other nested OUs we might want to import the user objects from all these nested OUs. If this is the case, tick the **Import from all sub-OUs** checkbox. If you only want to import users that exist in the root of the container, untick this checkbox.
- In the **Import from the following containers** box, we will define one or more containers from which to import:
 - Click the **Add** button.
 - A **Browse** window will appear showing a tree structure of the domain. If you want to import from the entire domain, tick the root domain item. Otherwise, expand the domain and choose one or more OUs from which to import (Note: Do not tick OUs that are contained within other ticked OUs unless the **Import from all sub-OUs** checkbox is unticked).

- Click **OK**.
- If you want to limit the users imported based on their group membership:
 - Click the **Group Filters and Rules** tab.
 - Click the **Download all groups** button.
 - Select the group (or multi-select) for which a membership requirement will be set.
 - In the group form, set the desired requirement from the **Membership requirement** drop-down (if multi-editing, tick the checkbox to the left of the **Membership requirement** label). The following membership requirement options are available:
 - **no requirement**: This group will not be used to filter the users that will be imported.
 - **required membership**: The user must be a member of this group.
 - **exclude if member**: The user must not be a member of this group.
 - **require membership of at least one**: The user must be a member of at least one of the groups which are set to require membership of at least one.
 - Click **OK**.

Specify how users will be placed into groups (Departments)

- Open your LDAP Sync scheduled task if it is not still open.
- On the **LDAP Sync Settings** tab, click the **Department Mapping** tab.
- Normally users are placed into Departments based on the OU in which their account exists. This is why the **Map Department to** dropdown defaults to **Organisational Unit (OU)**. However, this is not always the case. Some sites would like the Department mapping to be based on an attribute (e.g. Department, Division or Company). It could even be mapped to a Custom attribute. Choose the mapping method from the **Map Department to** dropdown.
- If users are imported that cannot be placed into a pre-defined Department, they will be placed into the Department that appears in the **Add unmatched users to** dropdown.
- Tick the **Auto-create unmatched Departments** checkbox, if Departments must simply be auto-created based on the Department mapping settings.
- If the Department mapping is based on OU, then we can specify which parent OU must map to the Department. This can be the parent of a parent, or indeed the parent of a parent to any number of parent levels. If the user's immediate OU is called Staff, which is contained within an OU called CallCentre, we would want the Department to map to CallCentre and not Staff. In this case we would specify **Map Department to parent OU 2 levels from User side**. Otherwise if the user objects have immediate parents called CallCentre, HR, Marketing, etc. we would choose **1 level from User side**.

Specify user attribute mappings

- Open your AD Sync scheduled task if it is not still open.
- On the **LDAP Sync Settings** tab, click the **Map User Attributes** tab.
- **Map user name**: Tick this checkbox to specify the attribute that contains the user's full name. The default is **[cn]** but you could change this to specify two attributes: **[givenName] [sn]**. This will import the user's first name and surname with a space in between.
- **Map Controller ID (PIN)**: The PIN is used for the following:
 - Logging in to printers configured for PIN number authentication (as opposed to card-swipe or username+password, etc).
 - Logging in to PDAgent Client for those PDAgents configured for PIN login.
- **Map card number**: If you have card readers on the printers and the card numbers are recorded in the Active Directory tick this and specify the attribute.

- **Map User Account Code:** Mapping the User Account Code is only necessary if you have users with popup account billing and their User Account Code is different from their windows account name. If left unticked, it will default to their windows account name.
- **Map email address:** Mapping the email address is especially useful. Email addresses are used for the following:
 - Scan-to-me functionality on printers using the embedded module.
 - Auto-emailing directly from Resource Manager (useful for sending PIN numbers).
 - Rule violation notifications.
 - User resetting the printer PIN numbers from the PDAgent Client app.
 - User resetting their login password via the PDAgent Client app.
 - Sending the Welcome email after a user is created in PD.
- **Map secondary email:** Currently, the secondary email address is only used for Google Cloud Print authentication. When documents arrive at the print server from Google Cloud, they contain the users' Gmail address. Print Director then authenticates the user by matching the Gmail address to the secondary email address (Note Google Cloud Print has been discontinued by Google and support will be removed from PD).
- **Map home folder:** Konica Minolta printers will add a **Home** button to the scan destination favourites if the 'scan to home' settings have been configured on the printer, and a home folder path has been imported for the logged in user.
- **Map PBX PIN:** If telephone PIN numbers are stored in the Active Directory, specify the attribute by ticking this checkbox. This allows calls to be assigned to users based on their telephone PIN number (and not just the extension number).
- **Map Extension:** Allocating users to telephone extension numbers assists in producing more meaningful reports as calls are assigned to users. This is critical for users who make use of popup account billing. The system must be able to assign calls to users in order for the popup to appear at the correct workstation.
 - **Create Ext on PBX:** The pre-defined PBX record on which the Extension exists can be chosen here or:
 - **Map PBX to attribute:** If the PBX name exists in an attribute for each user it can be specified.

After user created actions

If a user is created during a sync, we can perform some actions so the user can immediately log in to printers:

- **Auto create PIN:** This will automatically create a PIN number if the Controller User ID (PIN) user field is not mapped, or the mapped attribute value is empty. The number of characters is specified in the System Configuration. See Menu bar > **Tools** > **System Configuration** > **General** tab > **Auto setting user PINs** frame > **Auto PIN length** box.
- **Send welcome email:** If this is enabled, the new user will receive an email based on the template specified in the drop-down. This email could contain their new PIN number and instructions on how to log in to a printer to release jobs.

Test the LDAP Sync settings to ensure correct attribute mapping and Department placement

Once all the settings have been defined, click the **Test Settings** button. This will not make any changes to the database; it will just show a list of imported users for the purposes of confirming that all the attributes specified are correct.

Note that this test will query the Active Directory using the credentials for the user account under which Resource Manager is running. This is normally a domain user account so it should work. If however, you are logged in with a local user account, an 'access denied' error may be encountered. Please run Resource Manager under a domain account and try again.

Note that this test does not confirm that the actual scheduled task will succeed. This is because the task is run on the PDServer which runs under the SYSTEM account. This must be tested separately.


Ensure the PDServer service is running under an account that can query the Active Directory

The PDServer service has the job of executing scheduled tasks. By default, the PDServer runs under the SYSTEM account. This user account has local administrative rights to the server. This is sufficient for operational tasks such as communicating with the embedded modules on printers and emailing reports. However, the SYSTEM account may not have sufficient rights to query the AD. If the server on which the PDServer is running is a domain controller, it will most likely be able to query the AD. If it is a different server, then it may not. In this case, it may be necessary to change the account under which the PDServer service runs to a domain account.

Test whether the PDServer can execute the scheduled task

If you know that the SYSTEM account will not be able to query the Active Directory, skip to the next heading (Create domain user account). Otherwise, the quickest way to confirm is to test it:

- Open Resource Manager.
- Navigate to **Scheduled Tasks > LDAP Sync**.
- In the right-hand pane, right click the AD Sync and choose **Execute now**.

Now wait a minute or two and then click the refresh button: 

In the **Last Status** column, you might see an error, or it will tell you how many users were imported. If you see an error (e.g. **The server is not operational**), it is most likely because the SYSTEM account cannot query the AD. In this case move on to the next section to change the user account under which the PDServer Windows service runs to a domain account.

Create a domain user account and add it to the local administrators user group

These steps are only necessary if the SYSTEM account cannot query the AD.

The user account that is created only needs to be a member of the Domain Users security group. It does not need any other domain access rights. However, it does have the following requirements:

- The password for the account must not expire. If the account's password changes, the service will not function.
- The user account must be added to the **local** Administrators user group on the server. Local administrative rights are required to perform its other tasks.

Change the Log On account for the PDServer service

- In the **Server Manager**, click **Tools > Services**.
- In the **Services** window, scroll down to **PDServer** and double click the item.
- Click the **Log On** tab.
- Change the **Log on as** option to **This account**.
- Click the **Browse** button.
- Enter the user account name and click **Check Names**.
- If the account matches, click **OK**. If not, ensure the **From this location** is showing the domain or **Entire Directory** and try again.
- Enter the user account password and again in the confirmation field.
- Click **OK**.
- Restart the **PDServer** service.

Document revision date: 2025/01/23

Software version: 2.4.20.3

© 2025 Blue Swift Software CC