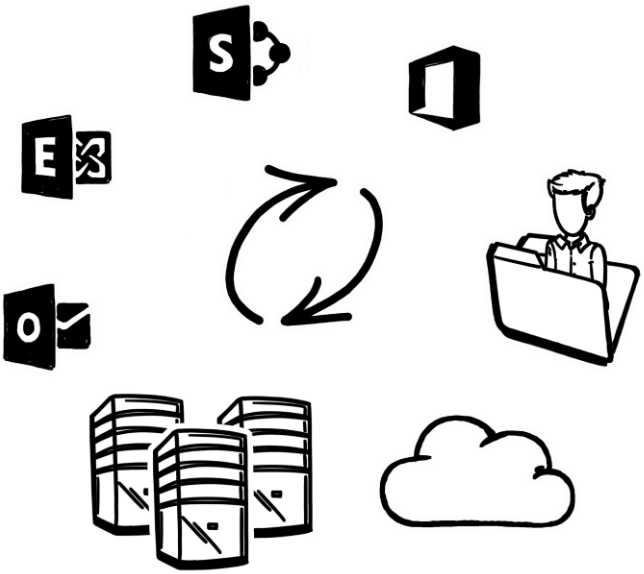
messageconcept

PeopleSync

Directory Connector for Mobile Devices



messageconcept PeopleSync 26.04

Setup and Configuration Guide

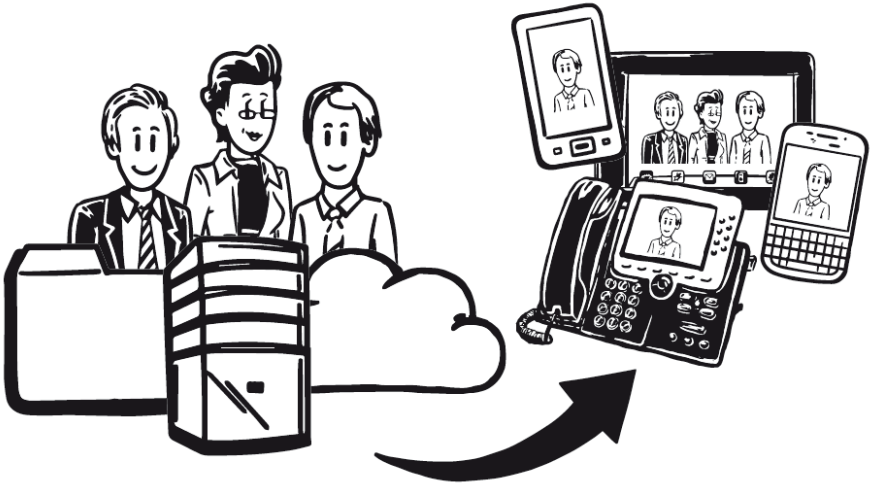
Contents

Hint: The **blue hint boxes** will save you time and are very helpful for the understanding of the software functionality.

Last Update: 2026-04-27

1 Introduction and Overview

Keeping all your contact data up-to-date and in sync and making it available everywhere can be a tedious task. Especially for enterprises which want to provide a global address book, this poses a challenge. If you have a wide variety of clients wanting to access this information, you need a solution which works on all platforms, including mobile ones. You also want tight control over which user has access to your data and you need powerful management tools.



PeopleSync was designed with all that in mind. It builds on industry standards such as CardDAV and LDAP and utilizes your existing LDAP directory service, such as Microsoft Active Directory, AD LDS, or NetIQ eDirectory to manage access control.

2 How does PeopleSync work?

PeopleSync consists of several components which work together to provide contact data to mobile devices. In this chapter, an overview will be given about how these components work together in PeopleSync.

2.1 Architecture

PeopleSync consists of several components which work together to provide contact data to devices and applications. In this section, an overview will be given about how these components work together in PeopleSync.

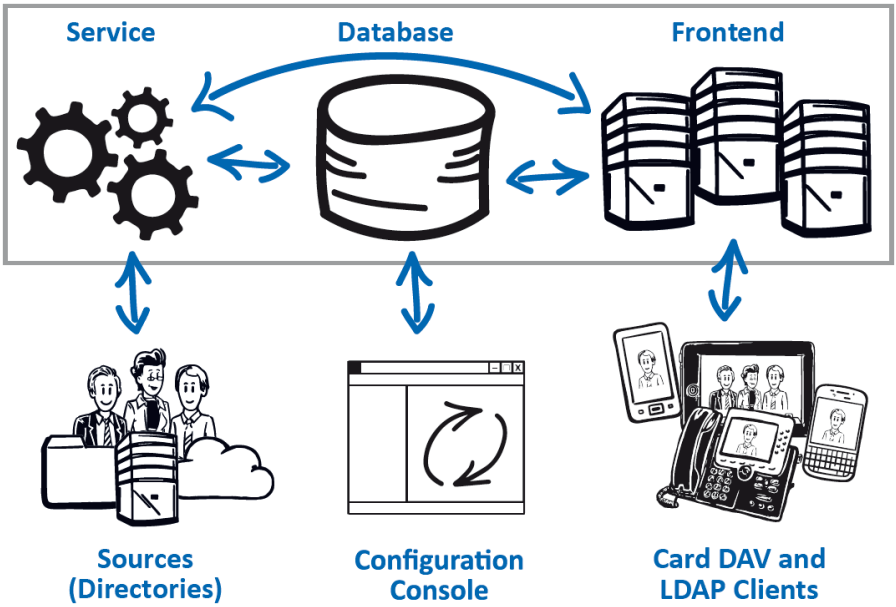


Figure 1: PeopleSync Architecture

Viewed from the client perspective, the devices and applications connect to the PeopleSync Frontend Server. The Frontend Server is a combination of two components. The CardDAV server runs on top of the Microsoft Internet Information Services (IIS). The LDAP service is based on Microsoft Active Directory Lightweight Directory Services (AD LDS).

The Frontend Server connects to an LDAP directory service to authenticate the user. The user's group memberships are used to determine which address list the user has access to. Address lists and their content are parallel stored in the PeopleSync Database in Microsoft SQL Server and in the LDAP directory. Devices and applications connect to PeopleSync via the standard protocols CardDAV and LDAP.

The PeopleSync Service executes PeopleSync Agents, which extract contact data from various source systems, e.g., Active Directory, Exchange, or SharePoint, and imports these contacts into corresponding address lists.

All Agents are unidirectional – i.e., they mirror contacts from a source system, but do not write back changes made in PeopleSync. Therefore, address lists serviced by PeopleSync Agent should be read-only for users.

Finally, the PeopleSync Console is used to configure address lists, permissions, and data import.

2.2 Software Components

PeopleSync comes with a modular and scalable design. The following software modules can be installed altogether on one machine or on dedicated machines.

2.2.1 Server Components

The **PeopleSync Service** is the core component of PeopleSync. The service executes all workflows including license checks, address list synchronization agents and database content management.

The **PeopleSync Frontend Server** is the single point of connection for the clients. The server provides the address lists for client-side synchronization via CardDAV with the database. It is supported to add several web servers for scalability and availability reasons in PeopleSync Enterprise Edition.

The **PeopleSync Database** stores the address lists and all configuration information in Microsoft SQL Server.

2.2.2 Administrative Components

The **PeopleSync Console** is the administrative GUI for PeopleSync. The console stores the configuration in the database.

2.3 Configuration Objects

In this chapter, an overview about the different configuration objects in PeopleSync is given.

2.3.1 Address Lists and Service Accounts

A **PeopleSync Address List** is a collection of contact items that are stored in the PeopleSync database. Agents store their data in address lists. Clients synchronize address lists – e.g., to a phone's local address book. The access to an address list is controlled by an access control list, which uses groups from an enterprise directory service.

A **PeopleSync Service Account** is an account with permissions to write to an address list. It is for use by an agent.

Address lists should be modified either by a single agent job or by a client. To modify contact data in a shared PeopleSync address list on PeopleSync clients, assign **Modify** permissions to a user or group in the access control list.

2.3.2 Agents

A **PeopleSync Agent** is a software interface for a specific data source. Agents synchronize contact items from a data source to a PeopleSync address list. The following agents come with PeopleSync:

- The **Active Directory Agent** imports contact data including thumbnail photos from Active Directory user and contacts to PeopleSync. An LDAP-filter selects and filters the synchronized data. This agent can be used to retrieve the GAL for Exchange on premise installations.
- The **Exchange GAL Agent** imports users and contacts from the Microsoft Exchange Server global address list to PeopleSync. A filter can be set to include only selected objects. This agent is primarily used for Office 365 Exchange Online GALs.
- The **Exchange Folder Agent** imports contacts located in a contacts folder in an Exchange mailbox or public folder.
- The **SharePoint Agent** imports items from SharePoint lists to PeopleSync. Default contact lists and customized lists are supported. The mapping of fields can be customized in the agent configuration.
- The **Database Agent** imports contacts from a database table into PeopleSync using a custom field mapping. The agent can also import photos referenced by URL or folder path.

It is possible to create several agent jobs per agent type to synchronize e.g., two different Exchange contact folders to dedicated PeopleSync Address Lists.

2.3.3 Workflows

An agent is defined by a **PeopleSync Workflow**. The workflow contains a set of tasks that will be executed to import contacts from data sources. Currently, Workflows cannot be customized. The customizing of workflows is expected to be supported in PeopleSync Enterprise Edition in the future.

3 System Requirements

The following system requirements apply for the PeopleSync components. We distinguish between the different PeopleSync server roles and the console:

Requirements / Roles	Service	Frontend	Database	Console
x64 CPU Architecture	X	X	X	X
System Memory (RAM)	8 GB			4 GB
Free Hard Disk Space	10 GB *			
Microsoft Windows Server 2016 and higher	X	X	X	X
Microsoft Active Directory Lightweight Directory Services				
Microsoft SQL Server 2014 or higher			X	
Windows Management Framework 3.0	X			

Note: It is possible to install all roles on a single server or on dedicated systems. All-in-one systems need to fulfill all requirements of the different roles.

3.1 User Directory

When users access address lists from their devices, they need to authenticate at the PeopleSync Frontend Server. PeopleSync contains no user directory, but instead relies on existing enterprise LDAP directories.

Currently, the following user directories are supported:

- Microsoft Active Directory
- Microsoft Active Directory Lightweight Directory Services (AD LDS)
- NetIQ eDirectory

When using Active Directory as a user directory, nested group memberships are evaluated by PeopleSync.

3.1.1 Special Requirements for NetIQ eDirectory

PeopleSync uses the following attributes and object classes in NetIQ eDirectory:

User object:

- objectClass: inetOrgPerson
- attribute for user name: uid
- group membership: groupMembership

The attribute **groupMembership** is used by PeopleSync to calculate rights to address books. If a group membership is not listed here, PeopleSync cannot know about it. In PeopleSync, eDirectory users authenticate with their **uid**.

Group object:

- objectClass: groupOfNames
- RDN: cn

In eDirectory, only direct group membership will be evaluated. It is not possible to use nested groups.

3.1.2 Special Requirements for AD LDS

PeopleSync uses the following attributes and object classes in AD LDS:

User object:

- objectClass: user
- attribute for user name: userprincipalName
- group membership: memberOf

The attribute **memberOf** is used by PeopleSync to calculate rights to address books. If a group membership is not listed here, PeopleSync cannot know about it. In PeopleSync, AD LDS users authenticate with their **userPrincipalName**.

Group object:

- objectClass: group
- RDN: cn

In AD LDS, only direct group membership will be evaluated. It is not possible to use nested groups.

3.2 PeopleSync Service

3.2.1 Hardware

We recommend the following minimum hardware:

- x64 CPU architecture
- 8 GB RAM
- 10 GB free hard disk space

The requirements for the Microsoft software products apply for PeopleSync also. Depending on the number of address book entries and clients, extended hardware requirements might apply.

3.2.2 Microsoft Software

The following **Microsoft software components** are required:

- Microsoft Windows Server 2016 and higher
- Windows Management Framework 3.0[1]

[1] Only required in all releases of Windows Server 2008.

3.3 PeopleSync Frontend Server

3.3.1 Hardware

We recommend the following minimum hardware:

- x64 CPU architecture
- 8 GB RAM
- 10 GB free hard disk space

The requirements for the Microsoft software products apply for PeopleSync also. Depending on the number of address book entries and clients, extended hardware requirements might apply.

Note: To scale to many clients, it is possible to implement several load balanced PeopleSync Frontend Servers.

3.3.2 Network requirements

The Frontend Server needs access to the PeopleSync Database and an LDAP Server. If port restrictions are in place, the following ports need to be opened:

- LDAP Server (Depending on directory type):
  - Active Directory: 389 TCP, 636 TCP, 3268 TCP
  - AD LDS: 389 TCP, 636 TCP
  - eDirectory: 389 TCP, 636 TCP
- Microsoft SQL Server: Port 1433 TCP[2]

[2] See Microsoft KB Article 287932 (http://support.microsoft.com/kb/287932/en)

3.4 PeopleSync Database

Microsoft SQL Server 2014 or higher is required as a local database instance or on a dedicated database server. SQL Server must be configured for **SQL Server Mixed Mode Authentication**.

Microsoft SQL Server hardware requirements apply for this system. Depending on the number of address book entries and clients, extended hardware requirements might apply.

Note: All SQL Server Editions (Express, Standard, Enterprise…) are supported.

3.5 PeopleSync Console

3.5.1 Hardware

We recommend the following minimum hardware:

- x64 CPU architecture
- 8 GB RAM
- 10 GB free hard disk space

The requirements for the Microsoft software products also apply to PeopleSync.

3.5.2 Microsoft Software

The following **Microsoft software and components** are required:

- Windows Server 2016 and higher

3.6 PeopleSync Clients

PeopleSync uses the open standards CardDAV and LDAP on the client side. Therefore, PeopleSync works with all CardDAV and LDAP clients in the market.

- **CardDAV Clients**

  The PeopleSync Frontend Server provides vCards via the CardDAV protocol in Microsoft IIS. The protocol is supported on all major mobile device platforms. Apple iOS, BlackBerry OS10 and Windows Phone come with native support for CardDAV.

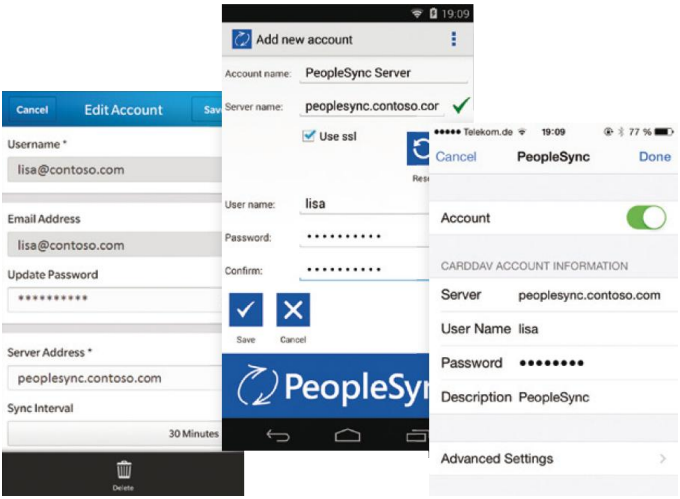


Figure 2: CardDAV clients in various smartphones

messageconcept provides a free CardDAV App for Android smartphones and tablets in the Google PlayStore and the Amazon Appstore. The app comes with AutoDiscover of the PeopleSync server settings via DNS.

- **PeopleSync-Clients**

  Beyond mobile devices, PeopleSync works with other CardDAV clients such as Apple's Address Book application on Mac OS X. Many email applications such as Microsoft Outlook or Mozilla Thunderbird support PeopleSync natively or via CardDAV plugins.

  The PeopleSync Frontend Server uses Microsoft AD LDS to provide directory services for LDAP clients. In contrast to CardDAV, the LDAP protocol supports no synchronization, but online access. The protocol is natively supported on most mobile platforms and in almost all email clients.

  Beyond computers and mobile devices, LDAP is supported by most desktop phones and telephone systems. This allows caller ID resolution on every office phone.

It is even possible to combine CardDAV and LDAP on a single device to synchronize via CardDAV a data subset, e.g., customer addresses of a dedicated sales district, and access other data via an LDAP online query. If you need to synchronize with further platforms, contact our support team to find a solution for your clients.

Please find more details on supported clients and devices in the PeopleSync Client Configuration Guide.

4 Setup

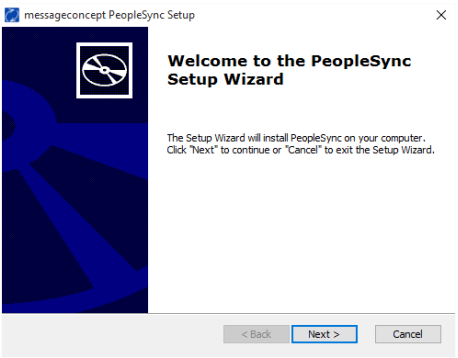
PeopleSync consists of a PeopleSync Agent, PeopleSync Console and PeopleSync Frontend Server. These components need to be installed in the following order:

1. PeopleSync Backend (Console, Agent)
2. PeopleSync Frontend Server
3. Initial Configuration
4. Optional: Further PeopleSync Consoles

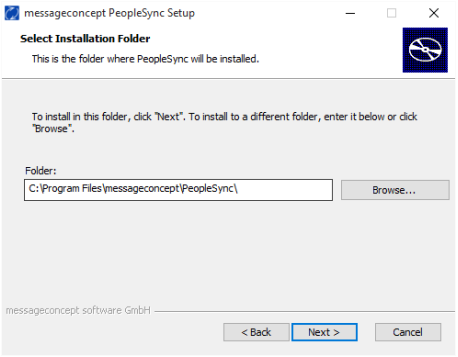
4.1 Backend Installation

The installer needs to be run with an account that is both a local administrator and an administrator of the SQL Server.

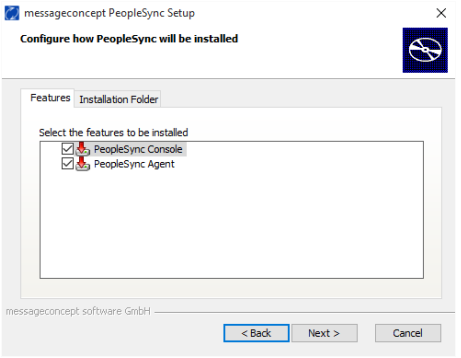
1. Start the PeopleSync Backend Installer.



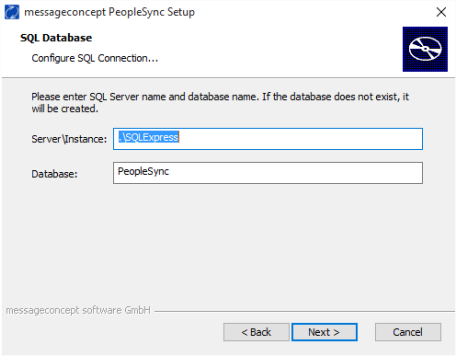
2. Accept the end user license agreement.
3. Select the installation folder.



4. Choose which components to install. If you choose to install the PeopleSync Agent, the console will automatically be selected.

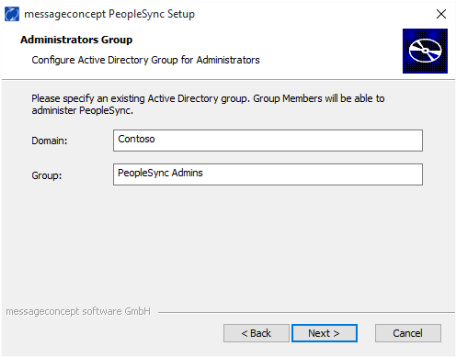


5. Enter the database connection. The database will be created by the installer. If you are connecting to the default instance of SQL Server, only the server's name needs to be entered.

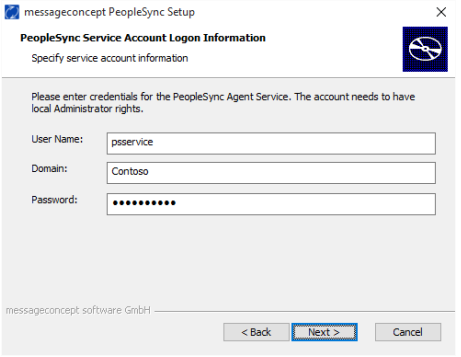


6. Enter the name of an existing Active Directory or local security group whose members will be allowed to use the PeopleSync Console. It is recommended to create a new group in Active Directory or locally. Please create the group

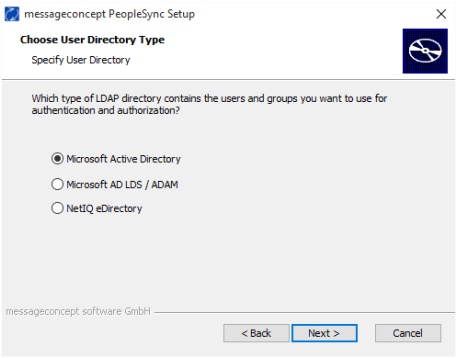
before proceeding; otherwise PeopleSync will not work properly.



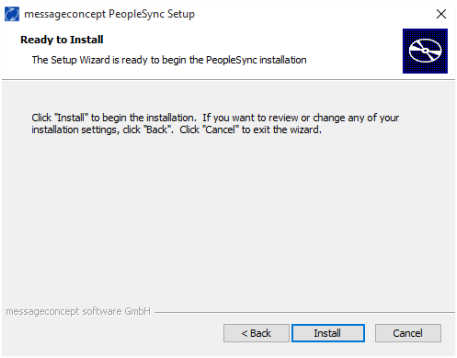
7. Enter credentials for PeopleSync Agent's service account. The service account must be a domain account that is a member of the server's local administrators group. Note that the account shouldn't have domain administrator rights.



8. Choose the type of LDAP directory you would like to use.



9. Start the installation.

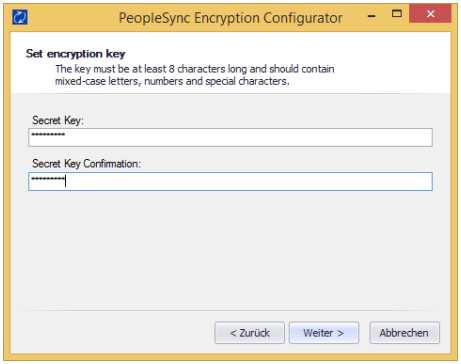


10. After installation has finished, a password must be set which will be used by PeopleSync to encrypt and decrypt sensitive configuration data. Please note the password you chose and enter the same password on all systems where you install either PeopleSync Console or Agent.

    The password is set with **PeopleSync Encryption Configurator**, which will be

automatically launched by the setup.

11. Enter an encryption key. It must be at least 8 characters long and should contain mixed-case letters, numbers and special characters.



12. In this step, the PeopleSync Encryption Configurator will check if the encryption key can be used to encrypt and decrypt data on the system. The

Output should be as shown below.

After setup has finished, please proceed with frontend server installation.

Attention: Please check, if the encryption key generation has been successful! In case of a failure run the PeopleSync Encryption Configurator again with elevated admin permissions.

4.2 Frontend Server Installation

This section will give detailed instructions on how to install and setup the PeopleSync Frontend Server on Windows Server. All screenshots and examples show Windows Server 2012 using Internet Information Server (IIS) 8.0. Other releases of Windows Server and IIS should be almost identical to these detailed instructions.

4.2.1 Preparing the database

The PeopleSync Frontend Server needs a SQL Server login to connect to the PeopleSync database. The following steps will guide you through the process of creating the login and granting the necessary permissions.

Please write down the login and password you created in the following steps, as those will be needed during further setup.

Configure SQL Server for mixed authentication mode:

1. Open SQL Server Management Studio.
2. In SQL Server Management Studio Object Explorer, right-click the server, and then click **Properties**.
3. On the **Security** page, under **Server authentication**, select **SQL Server and Windows authentication mode**, and then click **OK**.
4. In the SQL Server Management Studio dialog box, click **OK** to acknowledge the requirement to restart SQL Server.
5. In Object Explorer, right-click your server, and then click **Restart**. If SQL Server Agent is running, it must also be restarted.

Create a SQL Server login:

1. Open SQL Server Management Studio.
2. Open a new query window.
3. Type in the following command, set a password and hit Enter:

```
CREATE LOGIN psweb
WITH PASSWORD = '<enterStrongPasswordHere>',
 CHECK_POLICY = OFF;
GO
```

Grant permission to access the PeopleSync Database:

1. Open SQL Server Management Studio.
2. In Object Explorer, expand the **Databases** folder.
3. Expand the **PeopleSync** database.
4. Right-click the **Security** folder, point to **New**, and select **User…**.
5. In the **Database User – New** dialog box, on the **General** page, select **SQL user with login**.
6. In the **User name** box, enter the name **psweb**.
7. In the **Login name** box, enter the name **psweb**.
8. In the **Default schema** box, enter **dbo**.
9. In the **Membership** tab, select **db_datareader** and **db_datawriter**.
10. Click OK.

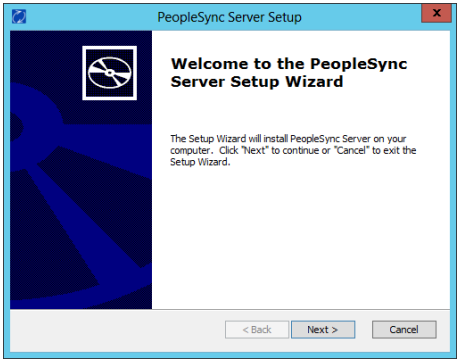
4.2.2 Installation

PeopleSync Server will automatically configure IIS and PHP for PeopleSync. It will add the necessary Windows Features to run IIS and will install its own PHP, as well as PHP Manager.

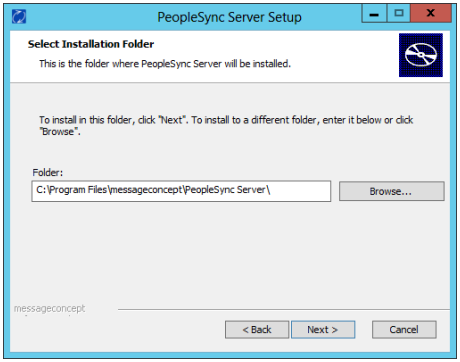
The automatic installation process can be run on a blank Microsoft Windows Server. No further preparation is necessary. Although no Windows features are removed, it is not recommended to use this process on a server where other IIS applications are already in use.

To perform the installation, complete the following steps:

1. Start PeopleSync Frontend Setup.

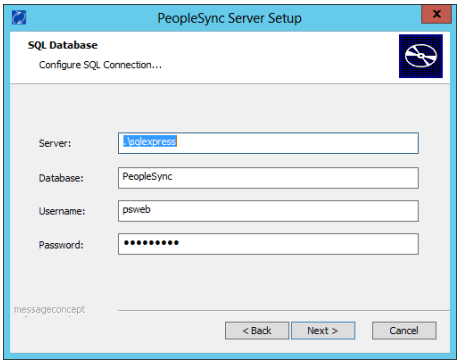


2. Select the installation folder.

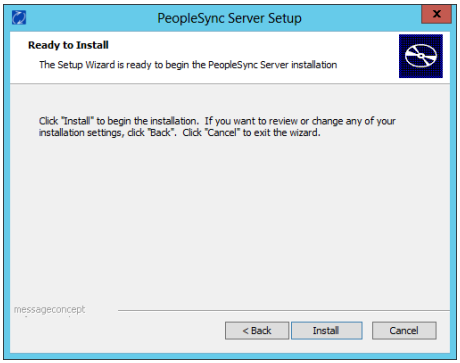


3. Enter the SQL Server computer and instance name, database name, as well as the SQL Server login **psweb** and corresponding password you created in

section 4.2.1



4. Start the PeopleSync Server installation.



After installation has finished, please proceed to **4.2.3 Configuring Hostname and SSL** to configure the hostname and SSL encryption in IIS.

4.2.3 Configuring Hostname and SSL

The recommended practice for the website's URL is to use a dedicated hostname like https://peoplesync.example.com. Alternatively, a dedicated port as in https://example.com:9443 can be used.

For security reasons, you must configure HTTPS on the PeopleSync Frontend's IIS website. Starting with iOS 12, it is also no longer possible to authenticate over an unencrypted connection.

To make it easier for you to evaluate PeopleSync, the PeopleSync Frontend Installer creates a self-signed certificate on your server. It is named:

`"PeopleSync on <HostName> - Replace Me with a valid cert"`

PeopleSync will then be available via HTTPS on ports 443 and 8843. These ports are the default ports for Android and iOS.

Attention: For production use, it is imperative to replace the self-signed certificate with a certificate issued by a trusted CA.

The following is unsafe and unsupported:
- To use self-signed certificates in production.
- To let CardDAV clients connect via HTTP.

For information on how to install a certificate, please see:
https://docs.microsoft.com/en-us/iis/manage/configuring-security/how-to-set-up-ssl-on-iis.

4.3 Setting up the PeopleSync LDAP Directory (optional)

PeopleSync uses a Microsoft Active Directory Lightweight Directory Services (AD LDS) instance to provide contacts via LDAP. Messageconcept provides an MSI installer that will install and configure a PeopleSync AD LDS instance. In case an existing instance or an Active Directory shall be used, please contact messageconcept support for guidance.

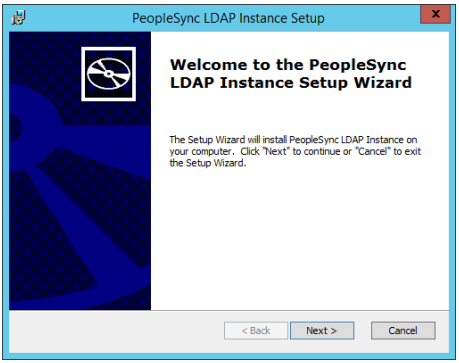
The PeopleSync LDAP directory will use the default LDAP/LDAPS ports 389 and 636. Please make sure that these ports are not in use by any other LDAP directory on the same server (e.g. Active Directory domain controller role). The LDAP directory can be installed on a server running one of the PeopleSync components or on a server of its own.

The PeopleSync LDAP directory will have two built-in accounts, an administrative account and an account with read-only permissions. The admin account psLDAP@PeopleSync.local is to be used by the PeopleSync service. The read-only account psRead@PeopleSync.local can be used by clients to search the directory.

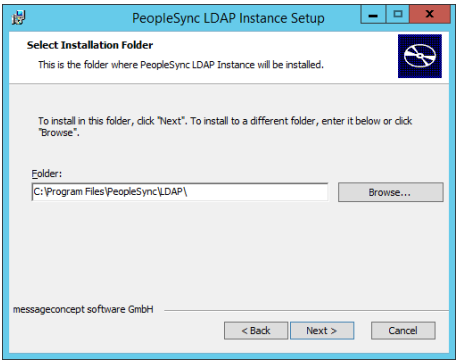
To set up the LDAP directory, please follow these steps.

1. Log in to the server where the LDAP directory shall be installed with an account having administrator rights.

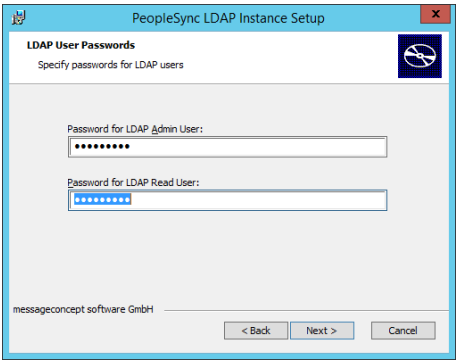
2. Run the PeopleSync LDAP Instance Setup MSI.



3. Please select an installation directory. This is the location where AD LDS data files will reside:



4. Please set passwords for the built-in PeopleSync LDAP accounts:



5. Please wait for the installation to finish.

To use the LDAP directory with PeopleSync, additional configuration in the PeopleSync Console is required. Please see section **4.4.2 LDAP Settings in PeopleSync Console (optional)**.

4.4 Initial System Configuration

To finish the initial setup of PeopleSync, PeopleSync system settings, as well as licensing information need to be configured. Finally, the PeopleSync Service can be started.

4.4.1 System Settings in PeopleSync Console

1. Run PeopleSync Console.
2. Log in with the user **Administrator** and an empty password. You will then be required to set a new password for the user **Administrator**.
3. In the console, click on **System Settings** in the navigation window.
4. Fill in the mandatory settings for Hostname, Domain Name, Base DN and Internal URL and click on the **Save** button.

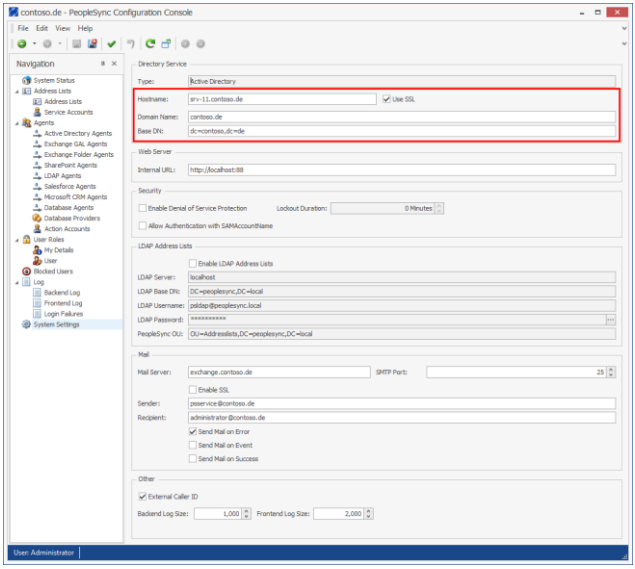


Figure 3: System Settings

Mandatory Settings

- **Hostname**: The IP address or DNS name of an LDAP Server. When using Active Directory, it must be a Global Catalog. Note that the PeopleSync Frontend server will also access this server.
- **Domain Name**: The Active Directory Domain's DNS name (e.g. contoso.de). Only needs to be filled when using Active Directory.
- **Base DN**: LDAP Directory's distinguished Name
  (e.g. dc=contoso,dc=de).
  To determine your DN, please see Appendix 9.1.
  Must be empty when using NetIQ eDirectory.
- **Internal URL**: The URL PeopleSync Agent should use to connect to the PeopleSync Frontend Server via the internal network
  (default: http://<Frontend-Server-Name>:88).
  Can be the same as the external URL. If possible, SSL should be used.

Optional settings:

In addition to the mandatory settings listed above, it is possible to configure email alerting to notify administrators in case errors occur in PeopleSync.

- **Use SSL**: Activate if you are connecting to your domain controller via SSL.

For email alerting, the following settings need to be configured:

- **Mail Server**: The DNS name or IP address of an SMTP server.
- **SMTP Port**: The SMTP server's TCP Port (e.g. 25).
- **Send Mail on Error**: Send mail only when an error occurs (recommended)

- **Send Mail on Event**: Send an email for every event logged to the PeopleSync database (only for debugging).
- **Send Mail on Success**: Send an email every time an agent successfully runs.

4.4.2 LDAP Settings in PeopleSync Console (optional)

If you want PeopleSync to provide contacts via LDAP, you need to configure the connection to the LDAP directory first. Please proceed as follows:

1. Run PeopleSync Console.
2. Log in with the user **Administrator**.
3. In the console, click on **System Settings** in the navigation window.
4. Enable the **Enable LDAP Address Lists** option.
5. Fill in the mandatory settings for **LDAP Server**, **LDAP Base DN**, **LDAP Username**, **LDAP Password**, **PeopleSync OU**, and click on the **Save** button.

The parameters must be set as follows:

- **Enable LDAP Address Lists**: Check to enable LDAP functionality.
- **LDAP Server**: The LDAP server's DNS name or IP address
- **LDAP Base DN**: The LDAP directory's base DN.
  For the PeopleSync LDAP directory, please set to **DC=peoplesync,DC=local**.
- **LDAP Username**: A user with write access to the LDAP directory. This can either be a domain or LDAP user account. If you are using an LDAP account, enter either the distinguished name or – if configured – the user principal name (UPN).
  For the PeopleSync LDAP directory, please set to **psLDAP@peoplesync.local**.
- **LDAP Password**: The LDAP user's password. Please note that except for the PeopleSync LDAP directory, password policies may apply, and the user's password may expire at some time. Please make sure that the account's

password will not expire (AD LDS attribute: **msDSUserDontExpirePassword**). For the PeopleSync LDAP directory, please use the LDAP admin user password you set during installation of the PeopleSync LDAP directory.

- **PeopleSync OU**: The organizational unit where PeopleSync will create LDAP address lists and contacts. For the PeopleSync LDAP directory, please use **OU=Addresslists,DC=peoplesync,DC=local**.

4.4.3 License Key

Please copy the license keys you received into the following directory: **%ProgramFiles%\messageconcept GmbH\PeopleSync\Agent\Licensekeys**

If you chose a different installation directory, please copy the license key into the **Agent\Licensekeys** directory in your installation folder.

Note: If you received a ZIP-file from your vendor, please unzip the file before copying the license key files (XML) to the **Agent\Licensekeys** directory.

4.4.4 Start the PeopleSync Service

As a final step, the PeopleSync Service needs to be started.

1. In the Start Menu, run **Services**.
2. Select the service named **PeopleSync Agent**.
3. Click on **Start** button.

4.5 Updating an existing PeopleSync installation

Please follow the following procedure to apply an update or hotfix:

1. Set the startup type for the **PeopleSync Service** to **Disabled**.
2. Restart the system.
3. Run the installer and fill all fields like in the initial installation.
4. Click **OK** in the **Configuration Required** dialog. A new configuration is not needed.
5. Set the startup type for the **PeopleSync Service** back to **Automatic**.

5 Configuration

For the configuration of PeopleSync a dedicated console application is provided.

5.1 Object Management

The PeopleSync Configuration consists of different objects, such as Address Lists, Agents and User Accounts. All object types are managed in a similar way. Therefore, we describe the management of objects on a general basis in this chapter.

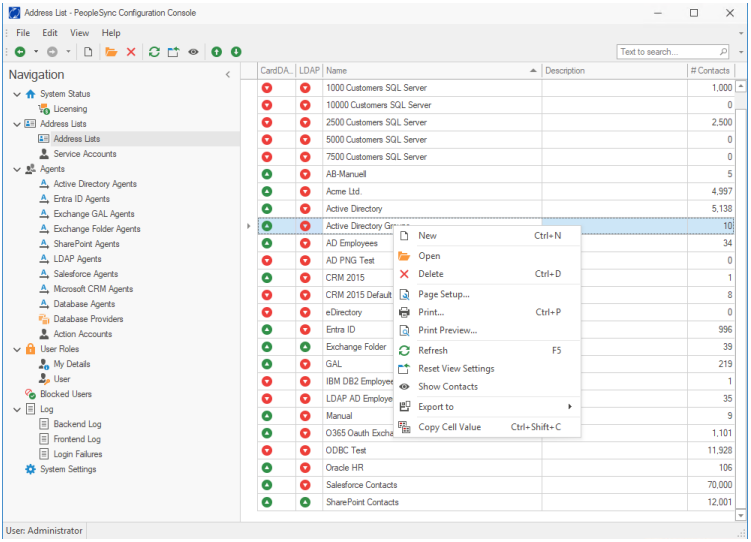


Figure 4: Object Management

All object management functions can be found in the menu, the symbol bar and the context menu. The console also offers shortcut keys for most functions.

5.1.1 Creation of new Objects

To create a new object (e.g. Address List) in the PeopleSync console, navigate to the corresponding menu item in the navigation bar. Use the **File New** command in the menu, the **New** symbol in the icon bar, the **New** command in the context menu or the keystroke **CTRL+N**.

5.1.2 Deletion of an Object

To delete an object in the PeopleSync console, highlight the object in the list. Use the **File Delete** command in the menu, the **Delete** symbol in the icon bar, the **Delete** command in the context menu or the keystroke **CTRL+D**.

5.1.3 Documentation of your Configuration

You can print an object for documentation purposes. To print an object in the PeopleSync console, highlight the object in the list. Use the **File Print** command in the menu, the **Print** command in the context menu or the keystroke **CTRL+P**. You can change the **Page Setup** or to get a **Print Preview** in the menu and the context menu.

If you would like to export object information for documentation purpose on a file base, you are also able to use the **Export to** function in the menu or context menu.

5.2 System Status

In the **System Status** dashboard, the status of PeopleSync can be seen:

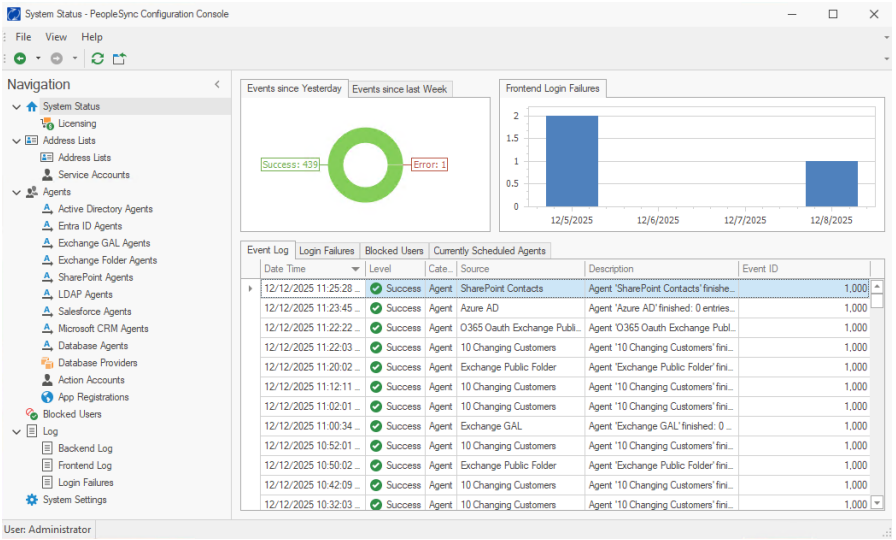


Figure 5: System Status

The dashboard in the PeopleSync console provides a centralized overview of system activity and health. It displays error messages generated by both the Backend and Frontend logs, offering immediate visibility into issues that may affect system performance or user experience. In addition to error reporting, the dashboard highlights login failures, making it easier to identify authentication problems and potential unauthorized access attempts.

An important feature of the dashboard is its ability to show the status of currently scheduled agents. This allows administrators to track which background processes are running, scheduled, or have encountered errors, enabling more effective management and troubleshooting.

5.3 Licensing Dashboard

In the licensing dashboard, the licenses configured for PeopleSync are shown:

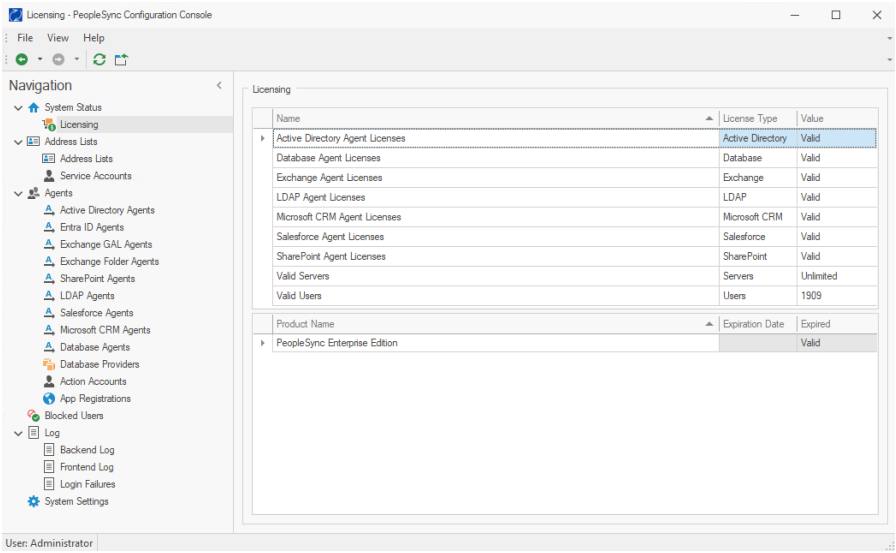


Figure 6: Licensing Dashboard

The licensing dashboard in PeopleSync provides a comprehensive view of all the licenses that have been configured for the system. It displays each license's status, type, and associated details, enabling administrators to monitor license usage and ensure compliance.

The dashboard includes visual indicators or summary statistics to help quickly assess whether any licenses are nearing expiration or require renewal

5.4 Address Lists

To manage Address Lists in the PeopleSync console, navigate to the **Address Lists** menu item in the navigation bar.

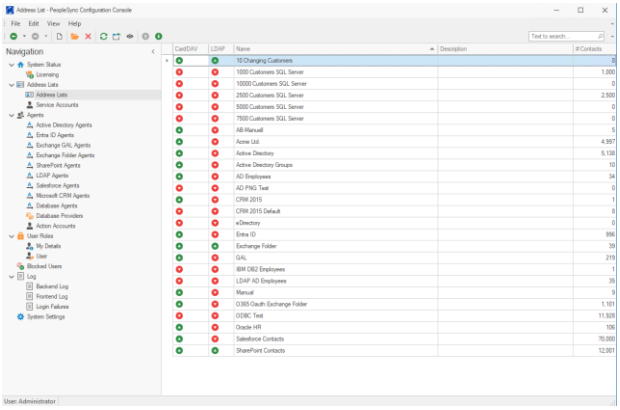


Figure 7: Address Lists

Address Lists in the PeopleSync console can be managed through the Address Lists menu item in the navigation bar. Administrators can create new Address Lists, provide meaningful names for display on users' mobile devices, and add descriptions for internal administrative purposes.

Each Address List requires the assignment of a Service Account, which is used by PeopleSync Agents to access and modify the list. Users can be granted modify permissions when an Agent is not assigned, allowing them to edit and share contacts directly.

Additionally, the Address Lists section displays the total number of contacts contained within each list. A preview feature is also available, allowing users to quickly view contact details in the main console.

5.4.1 Service Accounts

For the usage of an Address List in PeopleSync, you will need a Service Account first. The Service Account is used to read from and write to the Address List in the database.

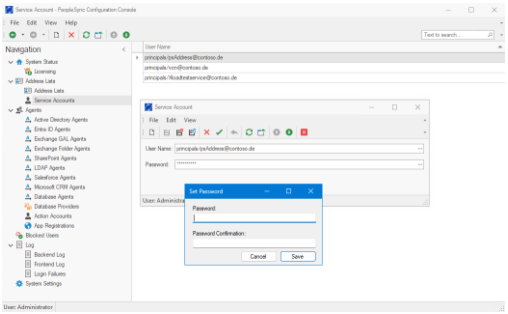


Figure 8: Service Accounts

The **User Name** can be chosen from a directory service with the **[…]** button. To enter the **Password**, click on the **[…]** button. The password will be encrypted before it is stored in the database.

5.4.2 Address Lists

An **Address List** is a logical container that holds contacts of a certain type. Every Agent needs a dedicated Address List to store its data. It is also possible to create an Address List that is not serviced by an agent. In this case, users can be given **modify** permissions so that they can edit and share contacts.

To create Address Lists in the PeopleSync console, navigate to the corresponding menu item in the navigation bar.

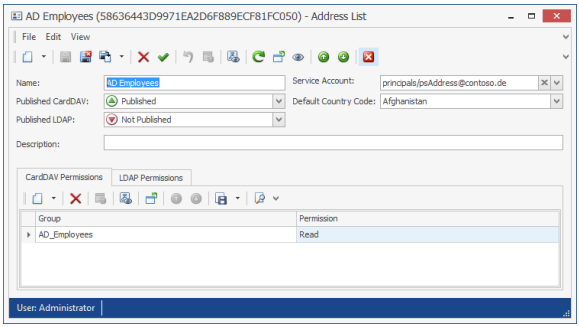


Figure 9: Address List

Each Address List has two text properties. The **Name** is the name of an Address List. The name will be shown on the mobile device. Therefore, it is recommended to choose a name that has meaning to users. The **Description** is used for administrative purposes only. Users will not see the description.

You need to set a **Service Account**. It is used by PeopleSync Agents to access the address list. The **Service Account** always has **Modify** permissions.

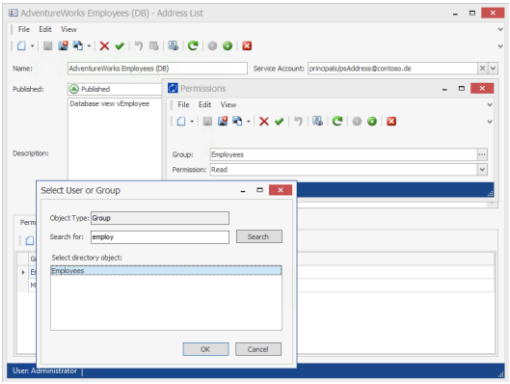


Figure 10: Selecting a Service Account from a directory service

Address Lists can be published to the PeopleSync CardDAV server, as well as to an LDAP directory. Using the **Published CardDAV** and **Published LDAP** properties, you can control if the Address List is visible by clients.

If **Published CardDAV** is set to “Not Published”, the address list will no longer be shown in the list of available address lists on the client. However, clients that already have subscribed to this address list will in general continue to see the address list.

In contrast, if **Published LDAP** is set to “Not Published”, the Address List does not exist in the LDAP directory. If the Address List was previously published in LDAP, it will be deleted from LDAP.

In the **CardDAV Permissions** and **LDAP Permissions** sections you can maintain the access control list for an Address List. You can grant permissions to one or several groups from your directory service. For LDAP, only read permission can be assigned, whereas for CardDAV, the following permission levels can be granted:

- **Read**

- **Write**
- **Modify**

Groups can be managed in Microsoft's Active Directory Users and Computers, PowerShell, LDAP administration or third-party identity management solutions.

To to view an address lists content, click on the "eye" icon in the toolbar.

5.5 Security

The PeopleSync Console has two layers of security. First, a user that needs to access the PeopleSync Console must be a member of the PeopleSync administrators group specified during setup.

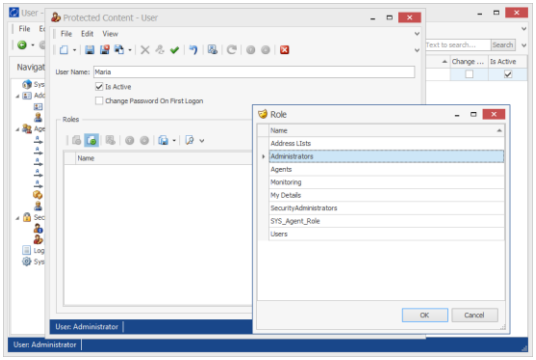


Figure 11: Adding a User Role

In addition to that, users with specific roles can be created in the PeopleSync Console. During installation, an administrative user named "administrator" with an empty password is created. This user can add further users with restricted permissions – e.g. the right to only manage address lists or agents.

Users can be managed in the application's **Security** section.

5.5.1 User Management

In **Security > Users** , the following actions can be performed:

- Create administrative user
- Manage administrative users
- Activate / deactivate administrative users
- Set user passwords
- Assign administrative roles

5.5.2 Roles

The following built-in roles can be assigned to administrative users in the **Security > Users** section:

- **Administrators**: Full permissions
- **Address Lists**: Create, delete, and manage address lists. Manage Address list permissions.
- **Agents**: Create, delete, and manage PeopleSync Agents
- **Monitoring**: View the PeopleSync log
- **My Details**: Use the My Details tab
- **Security Administrators**: Manage users and assign roles
- **Users**: Membership in all roles, except Administrators and Security Administrators.

5.5.3 My Details

The **Security > My Details** tab shows information about the currently logged-in user. Users can change their own password and see the roles they are a member of.

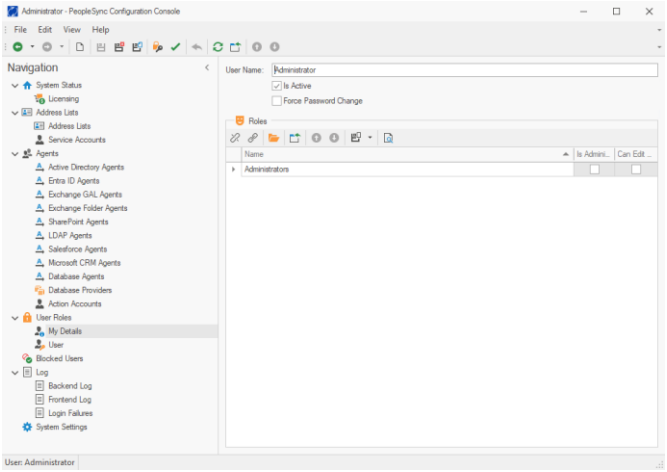


Figure 12: My Details

5.6 Denial of Service Protection

Denial of service protection (DoS protection) is a security feature of the PeopleSync Frontend Server. Upon detecting malicious activity, it blocks a combination of username and IP address for a set time and delays the response to the attacker.

If within 5 minutes a user tries logging in with a wrong password 5 times, the combination of username and IP address will be blocked for the time specified in System Settings.

DoS protection is not enabled by default and must be specifically enabled in System Settings. Blocked users can be unlocked in PeopleSync Console.

Example:

An attacker performs a brute-force attack and tries logging in with user “Alice” from IP A. After 5 unsuccessful login attempts within 5 minutes, PeopleSync blocks and delays further login attempts for user “Alice” from IP A for a set amount of time.

Meanwhile, the legitimate user “Alice” can still log in from IP B or IP C.

5.6.1 Configuring DoS Protection

Denial of service protection can be enabled and disabled in System Settings with the following parameters:

- **Enable Denial of Service Protection**: Enables denial of service protection.
- **Lockout Threshold**: The number of failed login attempts after which the combination of username and source IP will be blocked.
- **Lockout Duration**: The duration in minutes a user is locked out when denial of service protection is enabled.

- **Reset Block Counter After**: Number of minutes that must pass from the first failed login attempt until the failed login counter is reset.

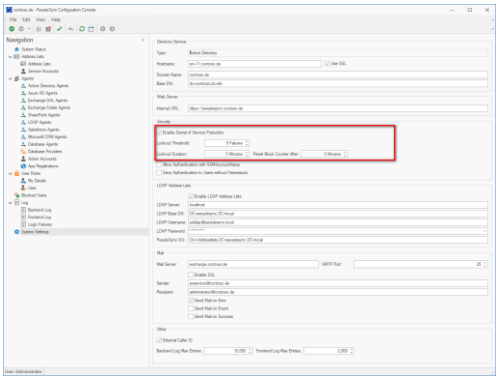


Figure 13: Configuring DoS protection

“Reset Block Counter After” cannot be less than “ Lockout Duration”.

5.6.2 Unlocking Users

Blocked users can be viewed and unlocked under “Blocked Users”.

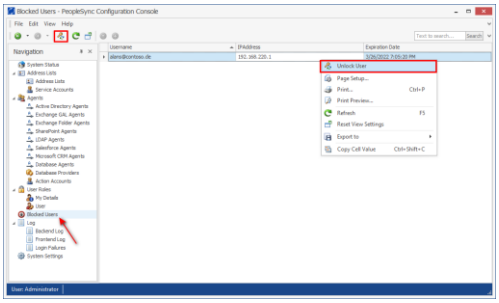


Figure 14: Unlocking Blocked Users

A combination of user and IP can be unlocked by selection “Unlock user” in the context menu or by clicking on the corresponding icon in the toolbar.

5.6.3 DoS Protection Logging

Denial of service protection events are logged in the PeopleSync Frontend Log and can be seen in the PeopleSync Console under Log > Frontend Log.

When a user is blocked the following event is logged with level “Warning”:

```
Too many authentication failures for user…
```

When the user tries logging in while being blocked, the following event is logged with level “Warning”:

```
Refusing access. User X (IP) has been blocked.
```

5.7 Log

Backend and Frontend events will be logged in the PeopleSync database and displayed in PeopleSync Console's **Log** section.

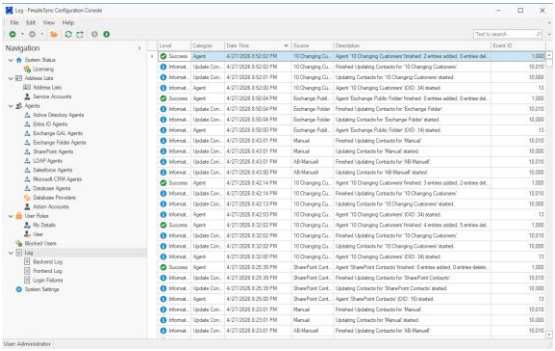


Figure 15: PeopleSync Log

The Log section is divided into three sections:

- Backend Log: Agent execution and licensing issues
- Frontend Log: All Frontend server events, such as login failures by mobile devices
- Login Failures: Failed logins at the Frontend. Username, IP address and the timestamp is shown.

Entries can have the following severity levels:

- Success: Agent has finished successfully
- Error: An error has occurred
- Warning: A warning, e.g. a login failure.
- Information: Informational events providing further detail for agent execution.

5.8 System Settings

In the System Settings dialog, essential settings for PeopleSync can be configured.

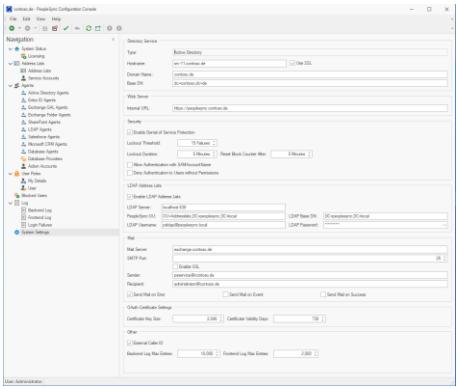


Figure 16: System Settings

5.8.1 Directory Service

- **Hostname**: The IP address or DNS name of an LDAP Server. When using Active Directory, it must be a Global Catalog. Note that the PeopleSync Frontend server will also access this server.
- **Domain Name**: The Active Directory Domain's DNS name (e.g. contoso.de). Only needs to be filled when using Active Directory.
- **Base DN:** The Active Directory Domain's distinguished Name (e.g. dc=contoso,dc=de). See Appendix 9.1 Determining an AD Domain's Distinguished Name.
  Must be empty when using NetIQ eDirectory
- **SSL Enabled:** If enabled, SSL will be used for all communications between PeopleSync components and LDAP directory service.

5.8.2 Web Server

- **Internal URL:** The URL PeopleSync Agent can use to connect to the PeopleSync Frontend Server via the internal network (e.g. https://srv01.contoso.local, http://srv01.contoso.de:88).

5.8.3 Security

- **Enable Denial of Service Protection**: Enables denial of service protection. See chapter “5.6 Denial of Service Protection”.
- **Lockout Duration**: The duration in minutes a user is locked out when denial of service protection is enabled.
- **Allow Authentication with SAMAccountName:** Allow users to logon from mobile devices with only their sAMAccountName. Option exists for compatibility reasons. For security reasons, keep disabled.
- **Deny Authentication to Users without Permissions:** When this option is enabled, the frontend will reject user logins with a 401 HTTP status code even when these users’ credentials are valid, but they have no permission to access a PeopleSync address list. This behavior will make it harder for attackers to guess user passwords via the PeopleSync Frontend as long as an account does not have permission to access an address list.

5.8.4 LDAP Address Lists (Optional)

If you want PeopleSync to publish Address Lists to an LDAP directory, you must configure the following parameters:

- **Enable LDAP Address Lists**: Check to enable LDAP functionality.
- **LDAP Server**: The LDAP server’s DNS name or IP address

- **LDAP Base DN**: The LDAP directory's base DN.
  For the PeopleSync LDAP directory, please set to **DC=peoplesync,DC=local**.
- **LDAP Username**: A user with write access to the LDAP directory. This can either be a domain or LDAP user account. If you are using an LDAP account, enter either the distinguished name or – if configured – the user principal name (UPN).
  For the PeopleSync LDAP directory, please set to **psLDAP@peoplesync.local**.
- **LDAP Password**: The LDAP user's password. Please note that except for the PeopleSync LDAP directory, password policies may apply, and the user's password may expire at some time. Please make sure that the account's password will not expire (AD LDS attribute: **msDSUserDontExpirePassword**).
  For the PeopleSync LDAP directory, please use LDAP admin user password you set during installation of the PeopleSync LDAP directory.
- **PeopleSync OU**: The organizational unit where PeopleSync will create LDAP address lists and contacts. For the PeopleSync LDAP directory, please use **OU=Addresslists,DC=peoplesync,DC=local**.

5.8.5 Mail

- **Mail Server:** The DNS name or IP address of an SMTP server.
- **SMTP Port:** The SMTP server's TCP Port (e.g., 25).
- **Send Mail on Error:** Send mail only when an error occurs (recommended)
- **Send Mail on Event:** Send an email for every event logged to the PeopleSync database (only for debugging).
- **Send Mail on Success:** Send an email every time an agent successfully runs.

5.8.6 OAuth Certificate Settings

- **Certificate Key Size**: Specifies the length of the cryptographic key used for the certificate, typically in bits (e.g., 2048 or 4096). A larger key size increases security but may require more computational resources.
- **Certificate Validity Days**: Determines how long the certificate is valid before it expires. Setting an appropriate validity period helps maintain security by ensuring certificates are renewed regularly.

5.8.7 Other Settings

- **Enable external caller ID**: Enables “Default Country Code” setting on address lists. This lets the user set a default country for the formatting of all phone numbers where a country cannot be deduced from address or phone data.
- **Backend Log Size**: Configure the number of events to be kept in the Backend Log.
- **Frontend Log Size**: Configure the number of events to be kept in the **Frontend** Log.

5.9 Frontend Server Configuration

During the installation, the installer will create a **server.ini** configuration file in the PeopleSync website root directory. This file is used to configure the database access and looks like this:

```
[server]
db_type = sqlsrv
db_host = 127.0.0.1
db_name = peoplesync
db_login = peoplesync
```

Optionally, the following keys can be set:

```
[server]
encrypt = true|false
trust_server_certificate = true|false
cache_driver = devnull
```

They keys **encrypt** and **trust_server_certificate** control the encryption of the database connection. If unset, the ODBC driver defaults are used. More detailed information about those configuration settings can be found at https://learn.microsoft.com/en-us/sql/connect/jdbc/understanding-ssl-support

For debugging purposes, it can be helpful to turn off caching of database and LDAP accesses. To achieve that, you can set **cache_driver** to devnull . In general, it is recommended though to not change this setting.

All further settings are stored in the database itself. This includes ACLs, user account information and the actual data for the contacts. To manage those settings in the database, please use PeopleSync Console.

Note: The hosting of the database on a dedicated server is supported. The server name or IP address can be altered in the file **server.ini**.

6 Agents

Agents are one-way connectors that can be scheduled to import contacts from a variety of source systems, such as Active Directory, SharePoint, Exchange and others into a PeopleSync address list. An address list will always reflect the state of the source system. There is no way to transfer data back to the source system. Changes made to an address list by parties other than the agent will be overwritten during the agent's next run.

Agents always import data from a single source system to a single address list. An agent cannot import data into an address list that is already served by another agent.

The PeopleSync Service runs the agents at the times defined in their schedules. Only enabled agents targeting an enabled address list are executed.

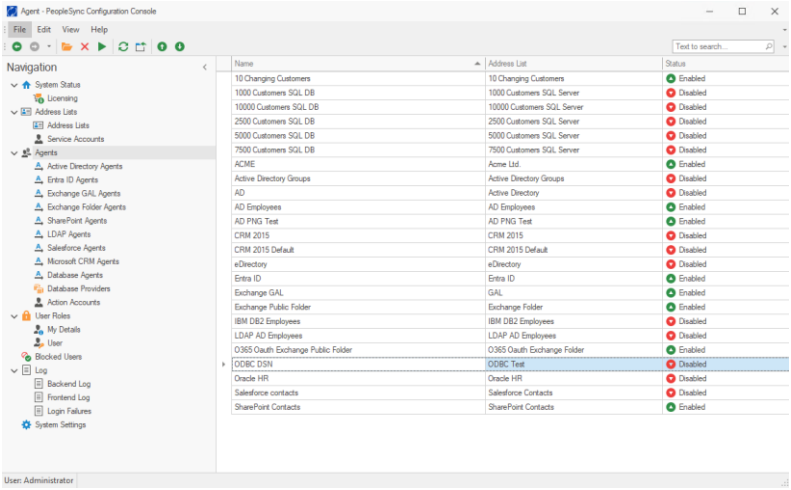


Figure 17: List of Agents

6.1 Agent Control and Sync Schedules

All Agents share a set of generic properties to control and schedule each Agent.

6.1.1 Agent Control

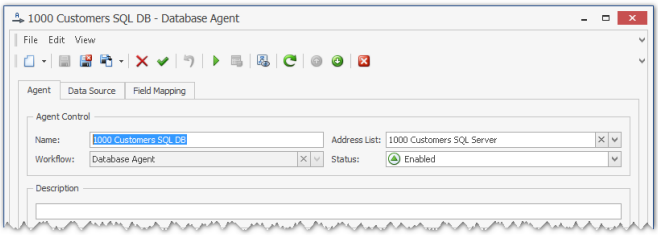


Figure 18: Agent Control

All Agents have the following four properties for agent control:

- The **Name** of an Agent describes the purpose of the agent.
- You need to select an existing **Address List** for each Agent. The Address List will be used to store the contact data, retrieved by the Agent.
- You can select a **Workflow** for the Agent. In most cases, only one workflow will be available.
- The **Status** of each Agent can be set to **Enabled** or **Disabled**. Only enabled Agents will retrieve data according to the schedule.

6.1.2 Sync Schedules

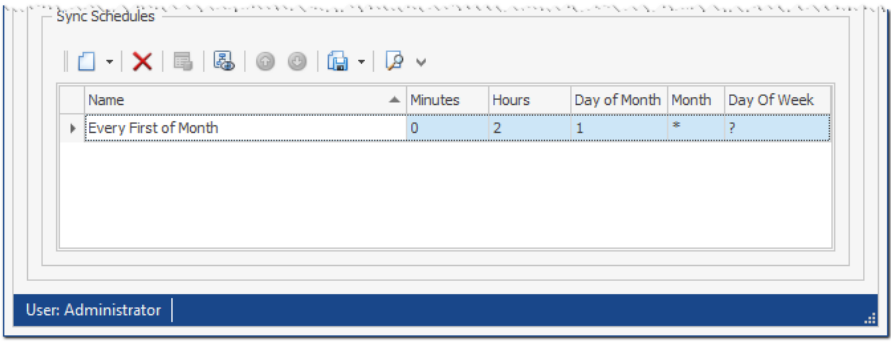


Figure 19: Sync Schedules Overview

You can configure one or more individual **Sync Schedules** for each Agent. A Sync Schedule in PeopleSync uses CRON-style syntax:

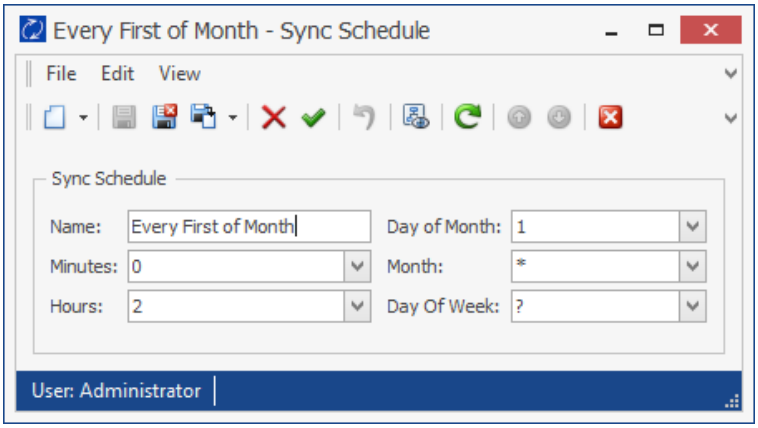


Figure 20: Sync Schedule Configuration

Each **Sync Schedule** has a unique **Name** for documentation purposes.

The **Sync Schedule** must be defined using the following CRON expressions:

Field name	Allowed Values	Allowed Special Characters
Minutes	0-59	,
Hours	0-23	, *
Month	1-12	, *
Day of Month	1-31	, * ?
Day of Week	0-6	, * ?

The following special characters are used as values:

Character	Description
,	Commas are used to separate items of a list. For example, using **8,12,16** in the field **hour** means hours 8, 12 and 16 of a day.
*	The asterisk indicates that the expression matches for all values of the field. E.g., using an asterisk in the field **month** indicates every month.
?	The **question mark** is used instead of ***** for leaving either **day-of-month** or **day-of-week** blank.

CRON expressions beyond the tables above are not supported.

6.2 Action Account

Action accounts store credentials for use in multiple agents. For example, if multiple Active Directory agents exist and both can run with the same credentials, they can use a single action account. Should the credentials change, they can be edited at a single point.

There are multiple types of action accounts in PeopleSync. These are explained in the following sections.

When creating an account, you can choose the type in the New command's drop-down.

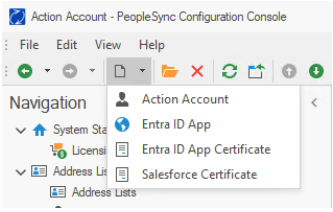


Figure 21: Creating an action account

6.2.1 Action Account (Username and Password)

Classic action accounts can be used in agents that use username and password authentication, such as Active Directory and LDAP.

If possible, the user name in the action account should be specified as a user principal name (UPN).

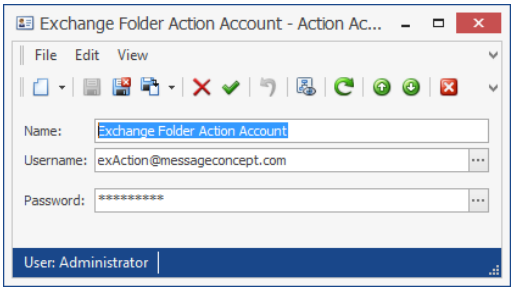


Figure 22: Action Account

6.2.2 Entra ID App

Entra ID App registrations are credentials used by PeopleSync agents to authenticate against Microsoft Azure or Office 365 services using modern authentication (OAuth).

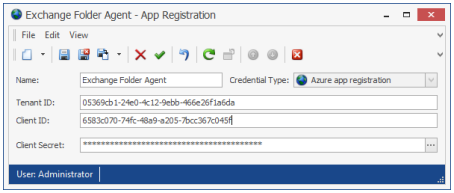


Figure 23: Entra ID App

Entra ID Apps are always tied to one tenant. They must first be created in Microsoft Azure Portal and then saved in PeopleSync Console.

Entra ID Apps contain the following information:

Tenant ID: A GUID that uniquely identifies the tenant. An agent using this Entra ID App will always use the app registration's tenant.

Client ID: A GUID that uniquely identifies the app registration.

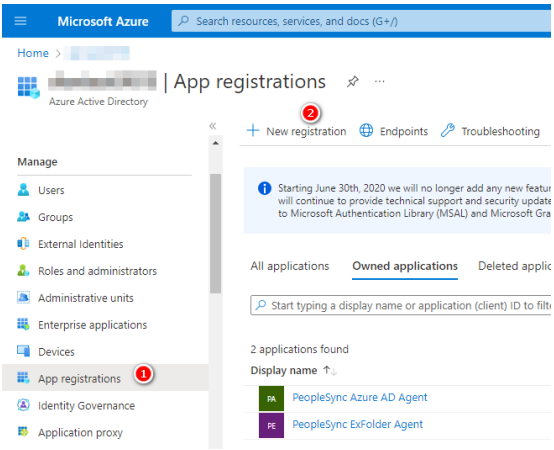
Client Secret: A string that is used together with tenant ID and client ID to authenticate against Entra ID using OAuth.

Note: Please note that the client secret has an expiration date in Entra ID. Before its expiration date, you must create a new client secret in Entra ID and update it in PeopleSync Console.

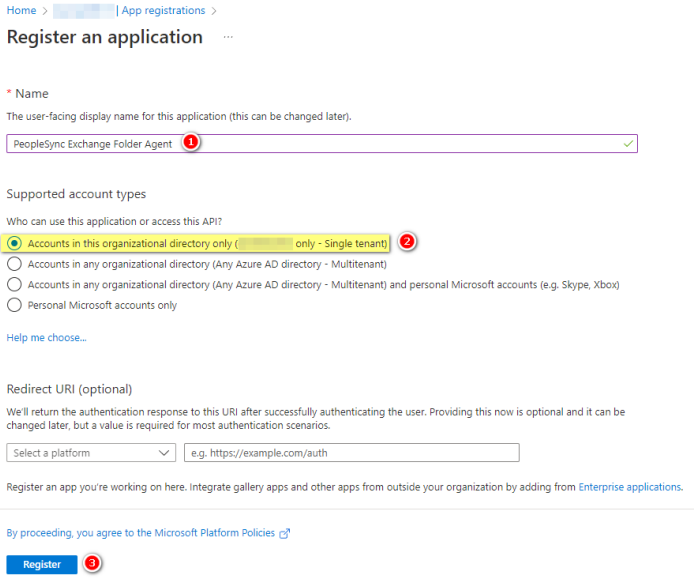
6.2.2.1 Creating an app registration in Azure Portal

To create an app registration in Microsoft Azure Portal, do the following:

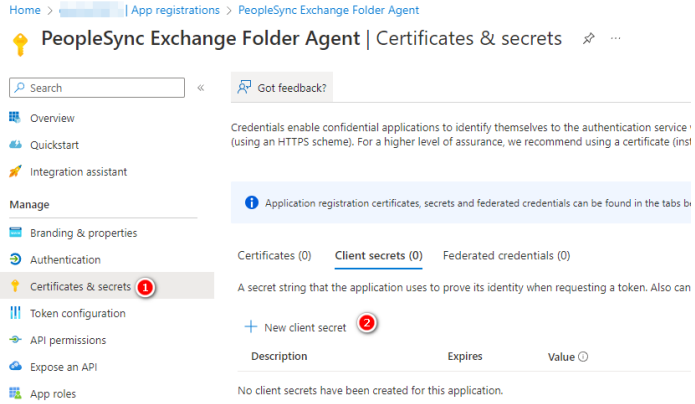
1. In a browser, navigate to https://portal.azure.com, then go to **Entra ID**.
2. On the left-hand side, select **App registrations,** then **New registration.**



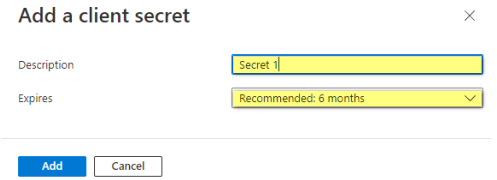
3. Enter a name for the app registration. As **account type**, select **Accounts in this organizational directory only**. Then click on **Register**.



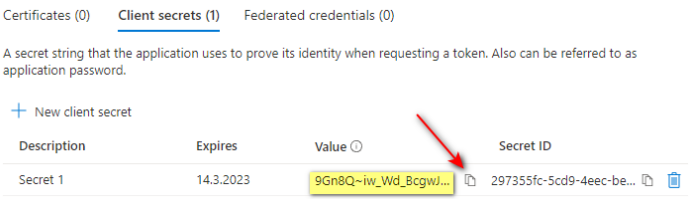
4. Inside the new app registration, go to **Certificates & Secrets** and select **New client secret** to create a new secret.



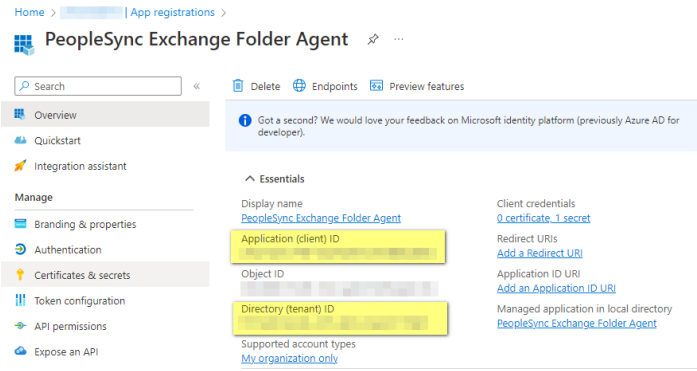
5. In the **Add a client secret** dialog, enter a description and validity period for the secret. Then click **add**.



6. The client secret will now be shown in the **client secrets** list. Click on the copy icon to copy the client secret's value and keep it for reference. This will be needed for PeopleSync.



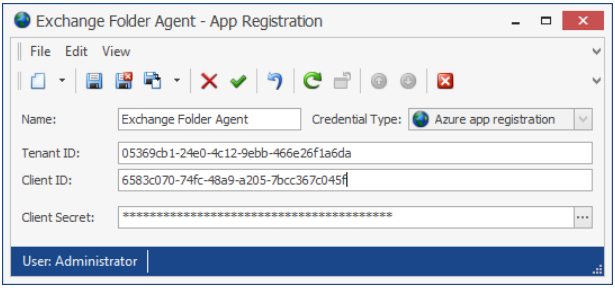
7. Return to the app registration's overview screen. Copy Application (client) ID and Directory (tenant) ID, and keep them for reference.



6.2.2.2 Saving an app registration in PeopleSync

To save an app registration in PeopleSync, do the following:

1. In PeopleSync Console, navigate to **Agents > Action Accounts**.
2. Click on the arrow next to the **New** icon and select **Entra ID App**.
3. In the dialog, enter the tenant ID, client ID and client secret values from the app registration you created in azure Portal.



6.2.3 Entra ID App Certificate

An Entra ID app certificate functions similarly to an Entra ID app that uses a client secret, but instead of relying on a client secret for authentication, it utilizes a certificate generated by PeopleSync. This certificate is then uploaded to the app registration in Azure. Using a certificate enhances security and is required for certain data sources, such as SharePoint Online.

PeopleSync will alert administrators about certificates that are set to expire in less than 30 days. These notifications appear in the backend log to ensure timely awareness. Additionally, if mail notifications are configured, PeopleSync will send email alerts, helping prevent service interruptions due to certificate expiration.

Entra ID Apps contain the following information:

Tenant ID: A GUID that uniquely identifies the tenant. An agent using this Entra ID App will always use the app registration's tenant.

Client ID: A GUID that uniquely identifies the app registration.

Certificate: A certificate created by PeopleSync.

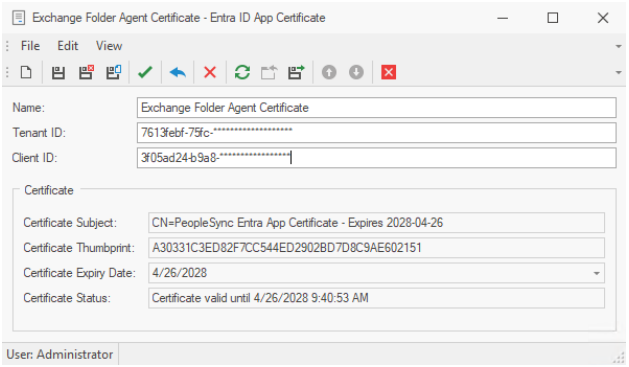


Figure 24: Entra ID App Certificate

The certificate is generated when a new Entra ID App Certificate object is created in PeopleSync. The public key can be exported by clicking on the **Download Public Key PEM)** icon in the toolbar.

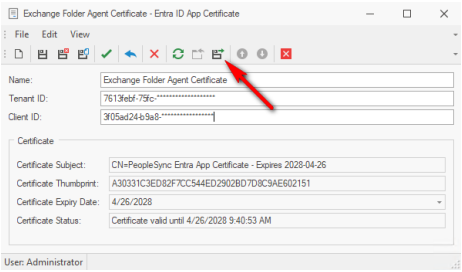
You can switch agents using PeopleSync Entra ID Apps to Entra ID App Certificates by creating an Entra ID App Certificate in PeopleSync and adding the certificate to the existing Entra ID app registration.

6.2.3.1 Creating an Entra ID App Certificate

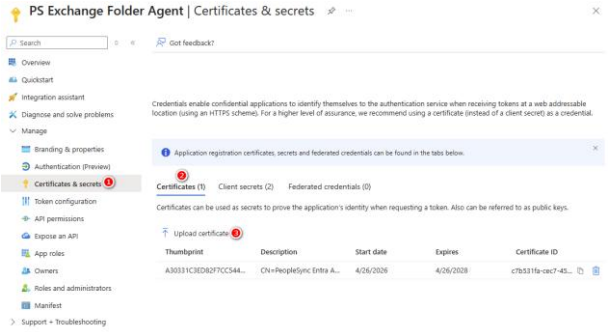
To create an Entra ID App Certificate, follow these steps:

1. Create an app registration in Entra ID by following steps 1-3 shown in "6.2.2.1 Creating an app registration in Azure Portal"
2. In PeopleSync Console, navigate to **Agents > Action Accounts**.
3. Click on the arrow next to the **New** icon and select **Entra ID App Certificate**.

4. Enter **client id** and **tenant id** from the newly created Entra ID app registration.
5. Click on the **Download Public Key PEM)** icon to download the certificate's public key:



6. In your Entra ID app registration, go to to **Certificates & Secrets > Certificates** and click on **Upload Certificate**. Upload the certificate you downloaded from PeopleSync in the previous step:



7. Your Entra ID App Certificate is now ready for use in PeopleSync.

6.2.3.2 Replacing an expiring Entra ID App Certificate

When a certificate is about to expire, follow these stepes:

1. Create a new Entra ID App Certificate in PeopleSync Console with the same settings as the expiring one.

2. Upload the certificate from the new Entra ID App Certificate into the Entra ID app registration.
3. In the agent using the old Entra ID App Certificate, switch to the new one.
4. Delete the obsolete Entra ID App Certificate in PeopleSync.

6.2.4 Salesforce Certificate

Salesforce supports OAuth certificate authentication, allowing secure, certificate-based access to its APIs and services. The PeopleSync Salesforce Certificate is designed to work seamlessly with this authentication method.

As with the Entra ID App Certificate, the PeopleSync Salesforce Certificate's public key needs to be uploaded to Salesforce.

When using Salesforce Certificate, PeopleSync will use the Salesforce OAuth 2.0 JWT Bearer Flow for Server-to-Server Integration.

PeopleSync will alert administrators about certificates that are set to expire in less than 30 days. These notifications appear in the backend log to ensure timely awareness. Additionally, if mail notifications are configured, PeopleSync will send email alerts, helping prevent service interruptions due to certificate expiration.

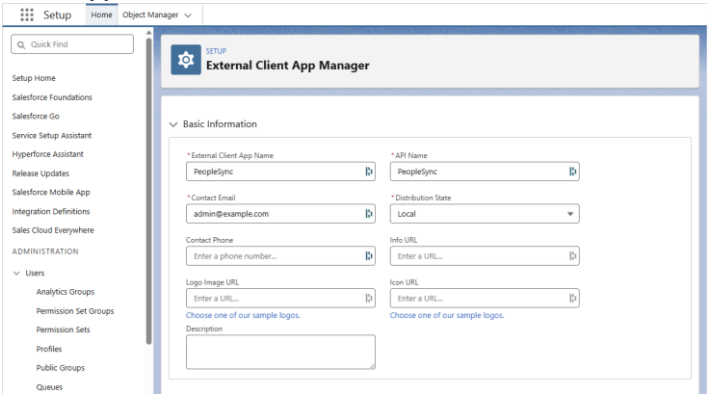
Salesforce Certificates contain the following information:

Consumer Key : The Salesforce Consumer Key is a unique identifier assigned to each app registration within Salesforce. It is similar to the client id in Entra ID.

Username: The Salesforce user whose permissions, sharing, and limits the issued access token will obey.

6.2.4.1 Creating an OAuth Application in Salesforce

1. In Salesforce Setup, go to **Apps > External Client Apps > Settings > External Client App Manager**.
2. Click **New Connected App**. In the **Basic Information** section fill **External Client App Name** and **Contact Email**.

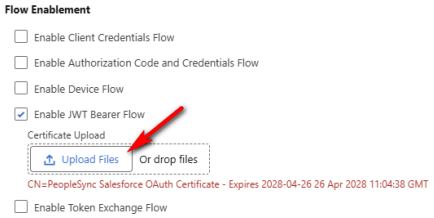


3. In the **API (Enable OAuth Settings)** section click **Enable OAuth Settings**.
4. Fill in the following OAuth settings:
    - **Callback URL**: http://localhost:33333
    - **Available OAuth Scopes** : Perform requests at any time (refreshtoken, offline_access), Manage user data via APIs (api)
    - Enable **JWT Bearer Flow**.
    - Disable **Require Proof Key for Code Exchange (PKCE) extension for Supported Authorization Flows**
5. Click the **Create** button at the bottom of the page.
6. Under **Settings > OAuth Settings**, click the **Consumer Key and Secret** button. Make a note of the consumer key.

6.2.5 Creating a Salesforce Certificate

After you have created the OAuth Application in Salesforce, you can create the corresponding Salesforce Certificate in PeopleSync.

1. In PeopleSync Console, navigate to **Agents > Action Accounts**.
2. Click on the arrow next to the **New** icon and select **Salesforce Certificate**.
3. Enter the consumer key from your Salesforce OAuth application.
4. Enter the salesforce username that is being impersonated.
5. Click on the **Download Public Key PEM)** icon to download the certificate's public key
6. Now go back to your Salesforce OAuth application.
7. In the **Settings** tab, click on **Edit**.
8. Below Enable JWT Bearer Flow, upload the Certificate from PeopleSync.



9. Save the OAuth Application.

6.3 Phone Number Mapping

On mobile devices, contact phone numbers are mapped to specific vCard phone fields. This default mapping is not always satisfactory, as for example a second phone number (other Phone) will be shown as “Voice” on the devices.

This default mapping can be changed in most agents, if the address book concerned does not have “Published LDAP” enabled.

Agents supporting a custom phone number mapping will have a tab “Phone Mapping”, where the vCard target field can be changed to a more appropriate field. For example, both “Phone” and “Other Phone” can be mapped to the “Phone” attribute in a vCard.

You can also set custom labels, such as “Office Phone”, by entering the label as text.

The number originating from the attribute “Phone” will always be shown first, whereas other numbers also mapped to the “Phone” attribute will be shown subsequently.

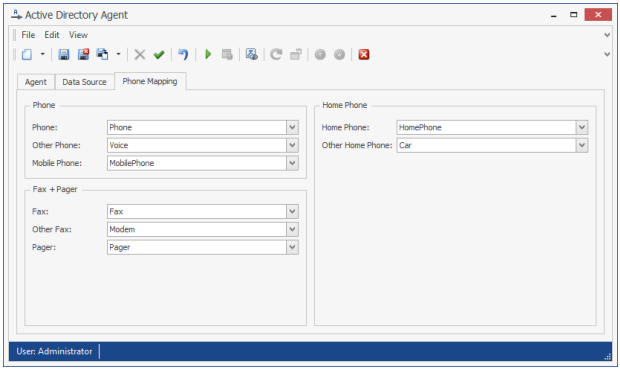


Figure 25: Phone Number Mapping Configuration

The above figure shows the default mapping. For greater ease of use, we suggest to also map “Other Phone” to “Phone”, “Other Fax” to “Fax” and “Other Home Phone” to “Home Phone”.

6.4 Active Directory Agent

The **Active Directory Agent** imports contact data from Active Directory users and contacts. It has a fixed mapping of Active Directory to vCard fields and imports the photo contained in the user objects' **thumbnailPhoto** attribute. It always needs to connect to a domain controller that is a global catalog server.

The agent retrieves all contacts or users found in the subtree of a base DN (i.e. an organizational unit or the domain root), that match the criteria defined by an object filter. To connect to the directory, an account with **read** permission is needed.

Figure 26: Active Directory Agent Configuration shows an Active Directory Agent that imports all "Person" objects in and below the "Marketing" organizational unit. It does not import initials and uses an account named "Active Directory Action Account" to access the directory.

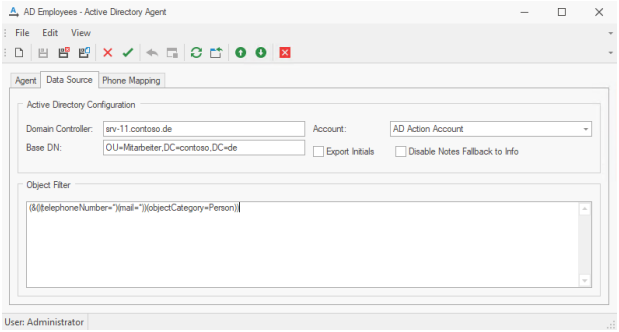


Figure 26: Active Directory Agent Configuration

6.4.1 Requirements

The following requirements must be met by the source system:

- Microsoft Active Directory based on Windows Server 2008 R2 and higher.

6.4.2 Configuration

The **Active Directory Agent** uses the following configuration parameters:

Global Catalog: The DNS name or IP address of an active Directory global catalog server.

Base DN: The distinguished name of a base container or organizational unit. Matching objects will be retrieved from this container and all child containers. For example, the organizational unit "Marketing" located directly below the root of the domain "ps.local" needs to be specified as "ou=Marketing,dc=ps,dc=local". Distinguished names can be copied from the "attribute editor" tab in Active Directory Users and Computers. This tab only shows when "Advanced Features" is enabled in the "View" menu.

Object Filter: The object filter defines which Active Directory objects shall be imported into PeopleSync. For example, the Filter " (objectCategory=Person)" makes sure that only objects of type "Person" – i.e. users and contacts are imported into PeopleSync.

The object filter supports the following classes:

- organizationalPerson
- contact
- user
- person (If object is also organizationalPerson)

The following object filters are provided for ease of use:

- **(objectCategory=Person)**
  All objects of type Person – i.e. users and contacts

- **(&(|(telephoneNumber=*)(mail=*))(objectCategory=Person))**
  All objects of type Person, such as users and contacts, provided they have a telephone number and email address.
- **(&(!(msExchHideFromAddressLists=TRUE))(|(telephoneNumber=*)(mail=*))(objectCategory=Person))**
  All objects of type Person, such as users and contacts, provided they have a telephone number and email address and are members of the Exchange Global Address List.

For an introduction on how to create LDAP filters, please refer to the documentation on Microsoft TechNet[3].

Account: An account that is used to read data from Active Directory and has at least read permission in Active Directory.

Export Initials: If checked, the "Initials" field will be imported.

Disable Notes Fallback to Info: This option determines whether information from the "Notes" field should be used as a backup (or "fallback") for the "Info" field if the "Info" field is empty or unavailable. When this setting is enabled (checked), the system will not use the "Notes" field as a substitute for missing "Info" data. When disabled (unchecked), if the "Info" field does not contain data, the system will automatically pull from the "Notes" field instead.

6.4.3 Field Mapping

The mapping of Active Directory properties to vCard fields can be found in Appendix 9.2 Active Diretory Agent – Field Mapping

[3] http://technet.microsoft.com/en-us/library/aa996205(v=exchg.65).aspx

6.4.4 Phone Number Mapping

Phone number mapping is supported by this agent. See chapter 6.3 Phone Number Mapping for details.

6.5 Entra ID Agent

The **Entra ID Agent** imports contact data from Entra ID to PeopleSync. It has a fixed mapping of Entra ID to vCard fields. It also imports the user's photo from Entra ID.

The agent uses an app registration to connect to Entra ID via Graph API. It will retrieve users and contacts that meet the criteria specified by a filter.

It can be used in scenarios where Exchange Online is used, but the users and contacts are not synched to Entra ID using Entra ID Connect. If users and contacts are synched from a local Active Directory to Entra ID, then you can use the Active Directory Agent instead.

Figure 27: Entra ID Agent Configuration shows an example configuration where contacts are loaded from Entra ID.

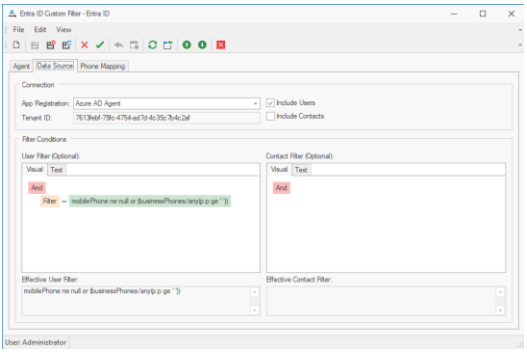


Figure 27: Entra ID Agent Configuration

6.5.1 Requirements

The following requirements must be met by the source system:

- Microsoft Entra ID

6.5.2 Configuration

The **Entra ID Agent** uses the following configuration parameters:

App Registration: An app registration in Entra ID with the following permissions:

- OrgContact.Read.All
- User.Read
- User.Read.All

Please see 6.2.2 Entra ID App or 6.2.3 Entra ID App Certificate for details on how to create one.

Tenant ID: Tenant from which users and contacts shall be loaded. Automatically filled from Entra ID App or Entra ID App Certificate.

Include Users: If checked, users are imported from Entra ID.

Include Contacts: If checked, contacts are imported from Entra ID.

User Filter: Optional filter to select specific user objects.

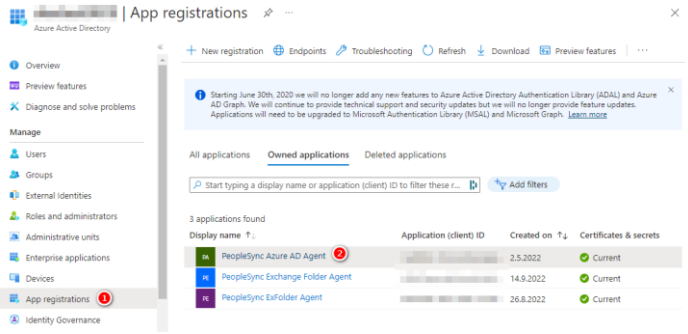
Include Contacts: Optional filter to select specific user objects

6.5.3 Creating an App Registration in Entra ID

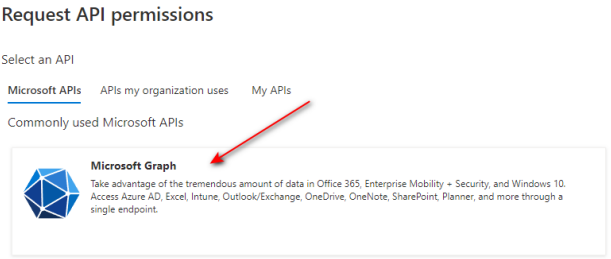
To configure the Entra ID Agent, proceed as follows:

1. Create an App registration with certificate or client secret authentication as explained in 6.2.2 Entra ID App or 6.2.3 Entra ID App Certificate.
2. In a browser, navigate to https://portal.azure.com, then go to **Entra ID**.

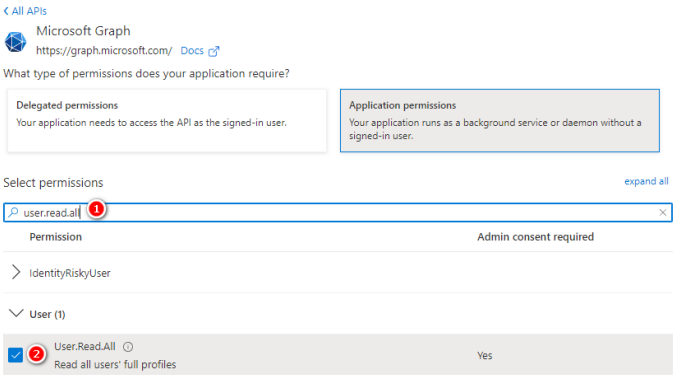
3. On the left-hand side, select **App registrations,** then select the relevant app registration in the list.



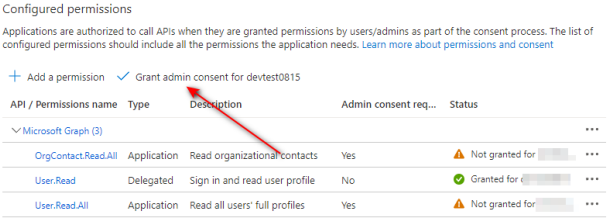
4. On the left-hand side, go to **API permissions**, then click on **Add a permission**.
5. Now select **Microsoft Graph**.



6. In the next step, select **application permissions**, then **User.Read.All** and **OrgContact.Read.All** permissions and click on **add permissions**.



7. On the API permissions tab, click on **Grant admin consent** and confirm to grant these permissions in your tenant.

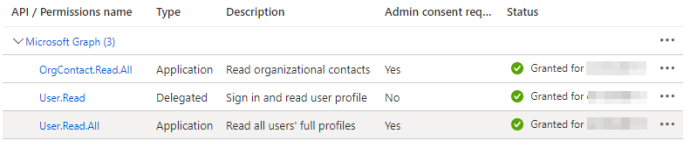


8. The following delegated permissions should now be set:

   Microsoft Graph:

   User.Read.All (Application),

   OrgContact.Read.All (Application)



6.5.4 Field Mapping

See Appendix 9.3 Entra ID Agent – Field Mapping.

6.5.5 Phone Number Mapping

Phone number mapping is supported by this agent. See chapter 6.3 Phone Number Mapping for details.

6.6 Exchange GAL Agent

The **Exchange GAL Agent** imports contact data from the Exchange Server global address list to PeopleSync. It has a fixed mapping of Active Directory to vCard fields. It also imports the photo associated with the user or contact if the source system is Exchange 2013 or higher.

Note: Microsoft is disabling basic authentication in Exchange Online from October 1st, 2022. For Exchange Online, use the Entra ID Agent instead.

The agent uses a remote PowerShell connection to an Exchange Server to retrieve users and contacts that meet the criteria specified by a filter. Furthermore, it downloads user and contact photos through the Exchange 2013 or Office 365 REST Web API.

It can be used in scenarios involving a hosted Microsoft Exchange solution, where Exchange Server can be queried by remote PowerShell, but the hosted Active Directory is inaccessible from client side.

Note: PowerShell 2.0 must be installed. Execution policy must be set to RemoteSigned4. This is configured during setup. The agent will malfunction in case the setting is changed to a level other than “RemoteSigned” or “Unrestricted”.

Figure 28: Exchange GAL Agent Configuration shows an example configuration where contacts are loaded from an Exchange Server. The PowerShell Server URL points to the Exchange Server and an account with permission to execute the "get-

[4] http://technet.microsoft.com/en-us/library/ee176961.aspx

user" and "get-contact" has been specified. In this case, basic authentication has been chosen as authentication method. The filters exclude users from the “ACME” corporation and the discovery mailbox.

Note: If you are using Exchange Server in an on-premise installation, we recommend using the Active Directory Agent to fetch the Exchange GAL.

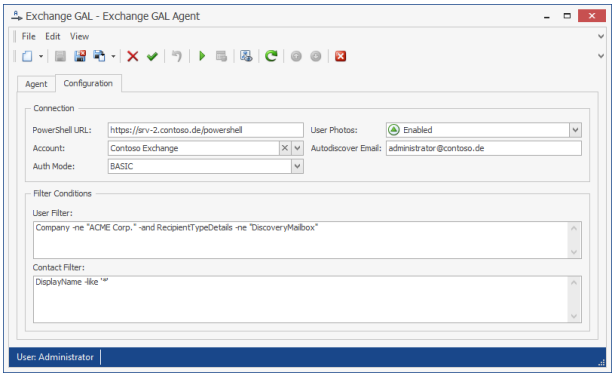


Figure 28: Exchange GAL Agent Configuration

6.6.1 Requirements

The following requirements must be met by the source system:

- Microsoft Office 365, Exchange Online, or
  Microsoft Exchange Server 2010 and higher
- For Photos: Microsoft Exchange 2013 and higher
- Remote Exchange Management Shell

6.6.2 Configuration

The **Exchange GAL Agent** uses the following configuration parameters:

PowerShell URL: The remote PowerShell connection URI to the Exchange Server (Office 365: https://ps.outlook.com/powershell).

Account: An account that has permission to connect via remote PowerShell and execute the "get-user" and "get-contact" commands.

Auth Mode: The authentication method used to authenticate the user's credentials. Supported methods are:

- **BASIC**: Basic authentication. Used for Office 365, among others.
- **KERBEROS**: Kerberos authentication is being used.
- **NEGOTIATE**: Either Kerberos or NT LAN Manager (NTLM) is used. Domain accounts are authenticated via Kerberos, while for local computer accounts, NTLM is used.

User Photos: Enables or disables the download of user and contact photos. Office 365 or Exchange 2013 and higher is required for this feature to work.

Autodiscover Email: The account's email address. This is used to automatically discover the Exchange Web Services URL. Optional when **User Photos** are deactivated.

User and Contact Filter: The filters define which users or contacts are loaded from the Exchange GAL. They use PowerShell-style Filter syntax. For a list of filterable properties, please refer to section 9.

The default user filter "RecipientTypeDetails -ne 'DiscoveryMailbox'" excludes the DiscoveryMailbox user, while the default contact filter "DisplayName -like '*'" excludes all contacts with an empty display name.

6.6.3 Field Mapping

The Exchange GAL Agent uses the same field mapping as the Active Directory Agent (see Appendix 9.2 Active Diretory Agent – Field Mapping).

6.6.4 Phone Number Mapping

Phone number mapping is supported by this agent. See chapter 6.3 Phone Number Mapping for details.

6.6.5 Choosing the right agent for hosted Microsoft Exchange

The Active Directory Agent, Entra ID Agent and Exchange GAL Agent are both able to fetch the GAL content from Active Directory.

On-Premises Exchange Server: In the case of an on-premises Exchange Server installation, we usually recommend the Active Directory Agent.

Hybrid environment: If you have Entra ID Connect in place, you can use the Active Directory Agent, as the source for the GAL is your on-premise Active Directory.

Exchange Online only: If you are not using Entra ID Connect or have users or contacts in your Exchange Online GAL that don’t exist in your on-premise AD, then use the Entra ID Agent.

Hosted Exchange Server: If you have outsource Exchange Server to a hosting provider and only have access to Exchange PowerShell, but not the underlying Active Directory, then use GAL Agent.

6.6.6 Tips for Implementing the Exchange GAL Agent

The GAL Agent runs the PowerShell cmdlets "get-user" and "get-contact" to get users and contacts from Exchange Server. Both cmdlets have a parameter "-filter"

which is configurable in the PeopleSync Console. To edit the filter, open the GAL Agent in the console and modify the "User Filter" and "Contact Filter".

The filters use PowerShell Syntax. For example, if you want to get all users that have email addresses in a specific domain (e.g. example.com), you can enter the following into the "User Filter" field:

```
WindowsEmailAddress -like '*@example.com'
```

You can use the following operators to build filters:

- -ne (not equal to)
- -lt (less than)
- -le (less than or equal to)
- -gt (greater than)
- -ge (greater than or equal to)
- -like (like—a wildcard comparison)
- -notlike (not like—a wildcard comparison)
- -contains (contains the specified value)
- -notcontains (doesn't contain the specified value)
- -and (add another condition)
- -or

You can develop and test the filters in PowerShell by opening a Remote PowerShell session to Exchange like this:

1. On the PeopleSync server, log in as the user the Agent runs under.
2. Open PowerShell with "Run as Administrator".
3. Run the following command and enter the credentials of the user you are using to connect to Office 365:

   ```
   $Cred = Get-credential
   ```

4. Run the following command. The ps.outlook.com URL is the Office 365 Remote Powershell URL:

```
$Session = New-PSSession -ConfigurationName Microsoft.Exchange -
ConnectionUri https://ps.outlook.com/powershell/ -Credential $Cred
-Authentication Basic –AllowRedirection
```

5. Run the following command. This should import the Remote PowerShell cmdlets needed to query Office 365:

```
Import-PSSession $Session
```

Then you can test the filter by entering one of the following:

```
get-user -Filter {<Here goes your filter>}

get-contact -Filter {<Here goes your filter>}
```

and check if the results are correct.

For example, to get all users with an email address in the example.com domain, you can try this filter:

```
WindowsEmailAddress -like '*@example.com’
```

To test this filter in PowerShell, you would run this command:

```
Get-User -Filter {WindowsEmailAddress -like '*@example.com'}
```

You can also use "-and" and "-or" to have multiple conditions, like the following:

```
WindowsEmailAddress -like '*@example.com' -and Department -eq 'IT'
```

The users matching this would need to have a primary email address in the example.com domain and be from the IT department, i.e. have "IT" set as the value in their "Department" attribute.

6.7 Exchange Folder Agent

The **Exchange Folder Agent** imports contact data from a Microsoft Exchange Server public folder or a folder inside a mailbox into an address list. It has a fixed mapping of contact to vCard fields. It can import the photo contained in the Exchange contact.

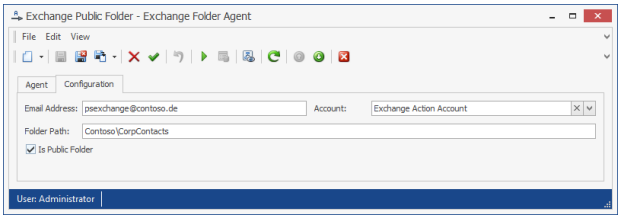


Figure 29: Exchange Folder Agent Configuration

The agent connects to Microsoft Exchange Server or Exchange Online via Exchange Web Services (EWS). As it uses Exchange Autodiscover, only an email address needs to be specified in the agent's configuration and the agent will determine the correct Exchange Server by itself.

Figure 29: Exchange Folder Agent Configuration shows a sample configuration. The **email address** "exchangeAction@messageconcept.com" is used to automatically determine the Exchange Server to connect to.

The **action account** named "Exchange Folder Action Account" is being used. The action account's user name would be the **windows login name** (more specifically: **user principal name**) associated with the mailbox, – i.e. "exchangeAction@messageconcept.com".

All contacts found in the public folder “Customers\TierA” are loaded into a PeopleSync address list. The checked **Is Public Folder** checkbox signals to the agent that the folder is in the public folder hierarchy and not the user’s mailbox.

6.7.1 Requirements

The following requirements must be met by the source system:

- Microsoft Office 365 Exchange Online OR
- Microsoft Exchange Server 2010 and higher
- Exchange Autodiscover
- Exchange Web Services

6.7.2 Configuration for On-Premises Exchange Server

When you are using an on-premises Exchange Server, please configure the agent as follows:

Email Address: The email address of an Exchange mailbox. This email address is used to automatically configure the connection to Exchange Server (Exchange Autodiscover). The folder specified in **Folder Path** must be in this mailbox, in case the **Is Public Folder** option is not selected.

Folder Path: The path to a contacts folder inside a mailbox or a public folder hierarchy. It uses Windows directory-style syntax. Subfolders are separated by “\”. Examples: Contacts, Sales\Contacts\VIP

Account: An action account with the credentials of the user account owning the mailbox specified in **Email Address** or permission to access the mailbox. The action account must have a mailbox.

Is Public Folder: If the folder specified in **Folder Path** is a public folder, this checkbox must be checked. If the folder is located inside the mailbox specified in **Email Address**, it must be unchecked.

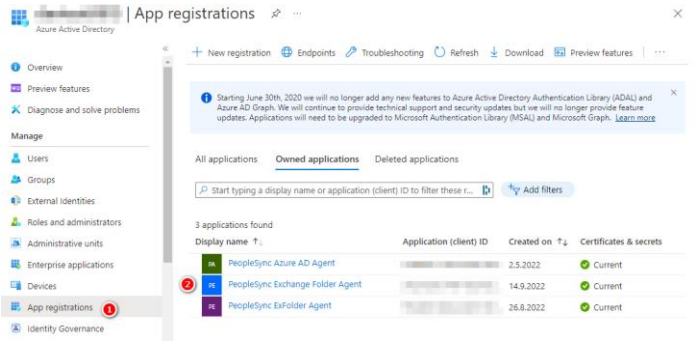
Exchange Web Services URL (Optional): If Exchange Autodiscover is not available, the Exchange Web Services (EWS) URL can be specified manually.

6.7.3 Configuration for Office 365 Exchange Online

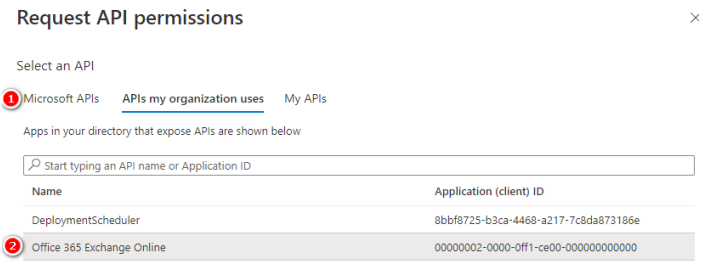
To access Exchange Online, the Exchange Folder Agent needs an app registration in Entra ID that has specific API permissions.

To configure Exchange Folder Agent for Office 365, proceed as follows:

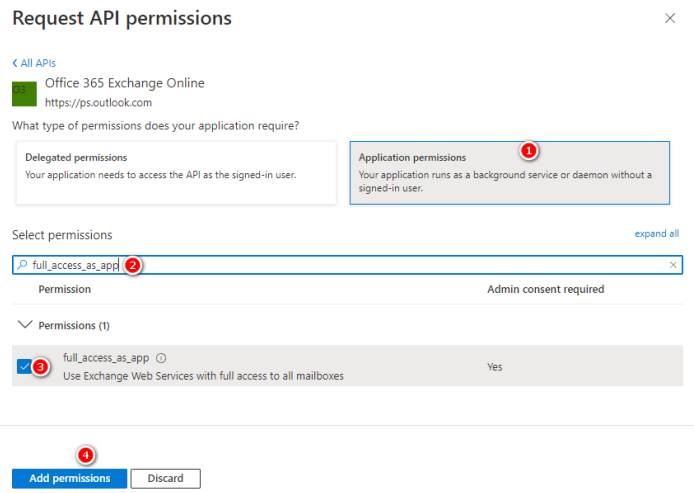
1. Create an App registration with certificate or client secret authentication as explained in 6.2.2 Entra ID App or 6.2.3 Entra ID App Certificate.
2. In a browser, navigate to https://portal.azure.com, then go to **Entra ID**.
3. On the left-hand side, select **App registrations,** then select the relevant app registration in the list.



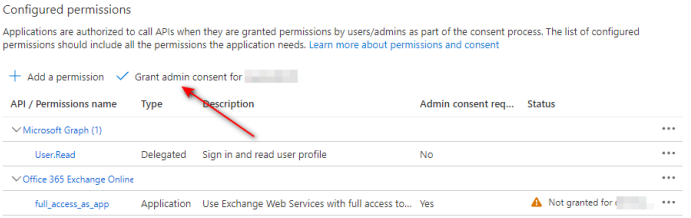
4. On the left-hand side, go to **API permissions**, then click on **Add a permission**.
5. Now select **APIs my organization uses** and select **Office 365 Exchange Online**.



6. In the next step, select **application permissions**, **full_access_as_app** permission and click on **add permissions**.



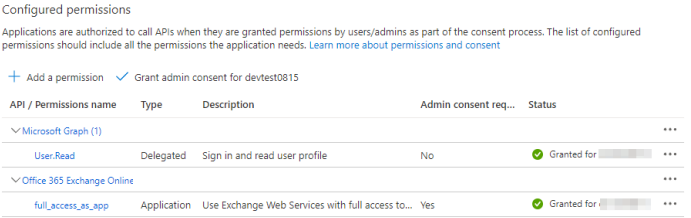
7. On the API permissions tab, click on **Grant admin consent** and confirm to grant these permissions in your tenant.



8. The following delegated permissions should now be set:

   Microsoft Graph: User Read

   Office 365 Exchange Online: full_access_as_app



9. Create an application access policy in Exchange Online to allow PeopleSync access to only those mailboxes PeopleSync should import contacts from. Please see https://docs.microsoft.com/en-us/graph/auth-limit-mailbox-access for guidance on how to do this.

> **Security Advice:** In Exchange Online, when granting "full_access_as_app" with type "Application" to an app registration, you are granting PeopleSync full access to all mailboxes in your tenant.
> For security reasons, create an application access policy to restrict the scope of PeopleSync's permissions to the mailboxes from which Peoplesync needs to import contacts.

In PeopleSync Console, you can now create an Exchange Folder agent and set the following properties:

Email Address: The email address of an Exchange Online mailbox. This email address is used to automatically configure the connection to Exchange Server (Exchange Autodiscover). The folder specified in **Folder Path** must be in this mailbox, in case the **Is Public Folder** option is not selected. The Exchange folder agent will impersonate as this mailbox to access public folders.

Folder Path: The path to a contacts folder inside a mailbox or a public folder hierarchy. It uses Windows directory-style syntax. Subfolders are separated by "\". Examples: Contacts, Sales\Contacts\VIP

Account: The app registration used to access the mailbox specified in **Email Address**.

Is Public Folder: If the folder specified in **Folder Path** is a public folder, this checkbox must be checked. If the folder is located inside the mailbox specified in **Email Address**, it must be unchecked.

Exchange Web Services URL (Optional): If Exchange Autodiscover is not available, the Exchange Web Services (EWS) URL can be manually specified.

For Office 365, use https://outlook.office365.com/EWS/Exchange.asmx.

6.7.4 Field mapping

The **Exchange Folder Agent** uses the field mapping described in Appendix 9.5 Exchange Folders Agent – Field Mapping.

6.7.5 Phone Number Mapping

Phone number mapping is supported by this agent. See chapter 6.3 Phone Number Mapping for details.

6.8 SharePoint Agent

The **SharePoint Agent** imports contacts from a list located on a SharePoint Server into an address list. The agent uses a default mapping of list fields to vCard fields, but a custom mapping can also be configured.

Figure 30: SharePoint Agent Configuration shows a sample configuration of the SharePoint agent. The agent will connect to the SharePoint web site http://intranet.messageconcept.com and fetch all contacts from the list named “Suppliers”. No custom field mapping is defined; instead, the default mapping is being used. The credentials used for the connection are stored in the action account named “SharePoint Action Account”.

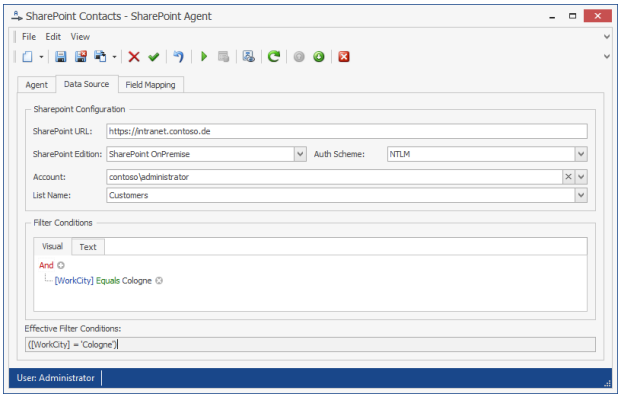


Figure 30: SharePoint Agent Configuration

6.8.1 Requirements

The following requirements must be met by the source system:

- Microsoft Office 365 SharePoint Online OR
- Microsoft SharePoint 2010 and higher

6.8.2 Configuration

The **SharePoint Agent** uses the following configuration parameters:

SharePoint URL: The SharePoint Site's base URL, not the URL to the list directly. Example: http://intranet.msio.de, https://extranet.msio.de

SharePoint Edition: SharePoint on premise or SharePoint Online**.**

Auth Scheme: The authentication mechanism for connecting to SharePoint. Default is NTLM. For SharePoint Online, AzureServicePrincipalCert must be used.

Account: An account that has the right to view the content of the list.

List Name: The name of the List. Example: "Clients"

Filter Conditions: A list of filter conditions. Blank, if no conditions are specified. The following operators may be used:

- And
- Or
- Equals / Does not equal
- Is less than / Is less than or equal to
- Is greater than / Is greater than or equal to
- Contains / Not Contains (Use Wildcard Operator '%')
- IN / NOT IN
- Begins With / Ends With

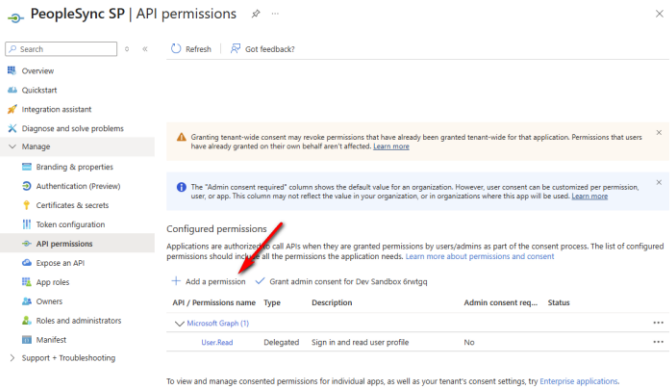
6.8.3 SharePoint Online

To connect PeopleSync to SharePoint Online, an app registration that utilizes certificate-based authentication must be used. PeopleSync facilitates this process by providing an Entra ID App Certificate.

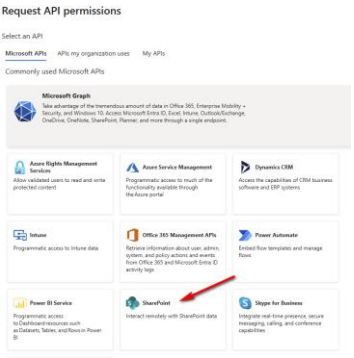
Starting from 05/01/2026, IDCRL authentication is disabled and will no longer be supported for SharePoint Online connections. To ensure continued access, you must use an Entra ID App Certificate for authentication from this date forward.

To connect to SharePoint Online, complete the following steps:

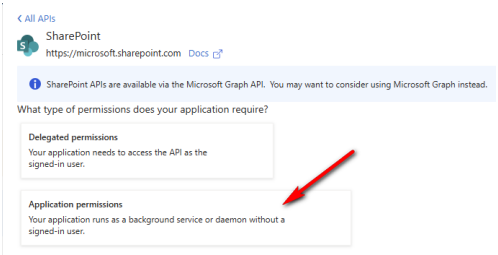
1. Create an App registration with certificate authentication as explained in 6.2.3 Entra ID App Certificate.
2. In a browser, navigate to https://portal.azure.com, then go to **Entra ID**.
3. On the left-hand side, select **App registrations,** then open the relevant app registration in the list.
4. In API Permissions, click on “Add a permission”.



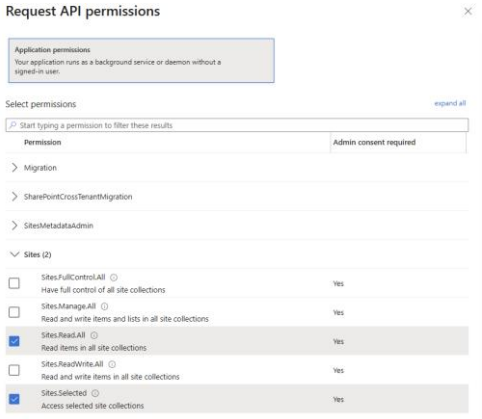
5. Select **SharePoint** API:



6. Choose **Application permissions**.

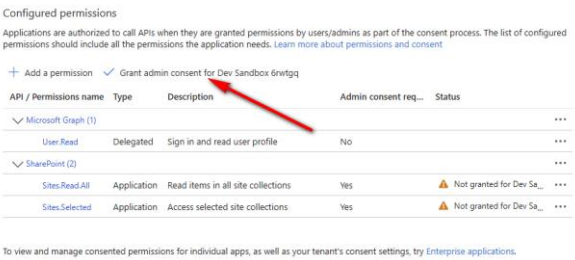


7. Choose Sites.Read.All and Sites.Selected permissions.



8. Click on “Add permissions”.

9. Grant admin consent for the permissions.



10. Use the Entra ID App Certificate in your SharePoint Agent.

    Make sure Auth Scheme is set to **AzureServicePrincipalCert**.

6.8.4 Field Mapping

All SharePoint fields may be freely mapped to contact fields. A default mapping is provided for contact lists.

The field mapping shows the names of the vCard fields as field names. The corresponding name of the source field must be entered into the text box next to the vCard field.

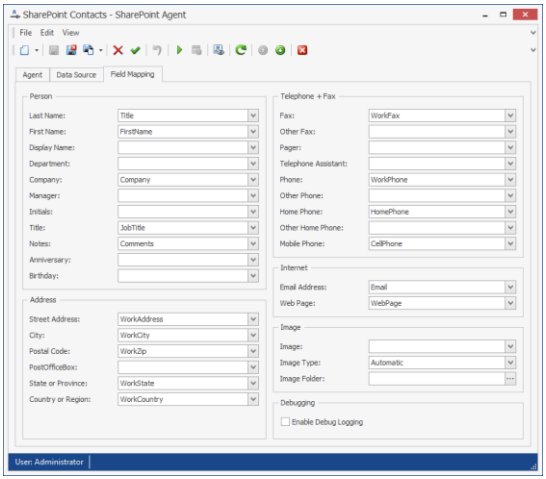


Figure 31: SharePoint Agent Field Mapping

In the field mapping, the following special parameters can be configured:

Image: The source field for the image data

Image Type: The image's type. One of the following:

- Automatic: The Agent automatically determines the type of the field.
- File Name: The source field contains a file name. If it is a relative path, the **Image Folder** parameter must be set to the base directory.
- Binary Data: The source field contains binary data.
- Base64 Data: The source field contains base64-encoded data.

Image Folder: The image file's base directory. When importing images of type File Name and the attribute value is a relative path, this must be set to the image's base directory.

Debugging: Enables debug logging to a file in the service account's temp folder. Enable only if requested by messageconcept support.

6.8.5 Phone Number Mapping

Phone number mapping is supported by this agent. See chapter 6.3 Phone Number Mapping for details.

6.9 LDAP Agent ■

The **LDAP Agent** imports contact data from LDAP directories. LDAP fields can be mapped freely to vCard fields. Importing an image field, such as the **thumbnailPhoto** attribute is also possible.

The agent retrieves all contacts or users found in the subtree of a base DN (i.e. an organizational unit or the domain root) that match the criteria defined by a filter condition. To connect to the directory, an account with **read** permission is needed.

Figure 32: LDAP Agent Configuration shows an LDAP Agent that imports all "OrganizationalPerson" objects in and below the "Baden-Württemberg" organizational unit. It imports all users and contacts with the title “Manager” from the departments of Finance, Controlling, Organization and HR. It uses an account named "AD Action Account" to access the directory.

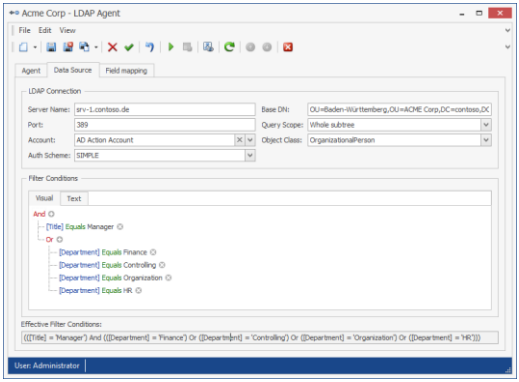


Figure 32: LDAP Agent Configuration

6.9.1 Requirements

The following requirements must be met by the source system:

- LDAP v2 or LDAP v3 Protocol

6.9.2 Configuration

The **LDAP Agent** uses the following configuration parameters:

Server Name: The DNS name or IP address of an LDAP server.

Port: The LDAP server's port. Default is 389.

Base DN: The distinguished name of a base container or organizational unit. Matching objects will be retrieved from this container and all child containers. For example, the organizational unit "Marketing" located directly below the root of the domain "ps.local" needs to be specified as "ou=Marketing,dc=ps,dc=local". Distinguished names can be copied from the "attribute editor" tab in Active Directory Users and Computers. This tab only shows when "Advanced Features" is enabled in the "View" menu.

Account: An account that is used to read data from Active Directory and has at least read permission in Active Directory.

Auth Scheme: Mechanism to be used for authenticating with the LDAP server.

- SIMPLE: Plaintext authentication (Default)
- DIGESTMD5: Digest-MD5 authentication
- NEGOTIATE: NTLM/Negotiate authentication

Query Scope: Defines the depth of the search.

- **Whole Subtree:** BaseDN and All objects on all levels below the BaseDN.
- **Single Level:** BaseDN and all direct descendants.
- **Base Object:** Only the BaseDN

Object Class: The type of object to be queried. Typical object classes include:

- **User**: A user
- **Contact**: A contact
- **OrganizationalPerson**: Superclass of User and Contact, excludes some mail and security attributes from the SecurityPrincipal and MailRecipient auxiliary classes.
- Group: A group

Filter Conditions: A list of filter conditions. Blank, if no conditions are specified.

For the LDAP Agent, the following operators may be used:

- And
- Or
- Equals
- Does not equal
- Is less than / Is less than or equal to
- Is greater than / Is greater than or equal to
- Contains (Use Wildcard Operator '%')

Object Filter: An LDAP object filter can be used instead of the SQL-Style filter. Do use an object filter, in filter conditions, switch to text mode and then enter the object filter using the following syntax: Filter = '<objectFilter>'.

Example: Filter = '(&(telephoneNumber=*)(objectCategory=Person))'

6.9.3 Field Mapping

All LDAP fields may be freely mapped to contact fields. A default mapping is provided for the **OrganizationalPerson** object class, which can also be used for the **User** and **Contact** object classes.

Note: When importing binary-encoded images from LDAP fields, i.e. the **ThumbnailPhoto** attribute, the image type field must be set to **Automatic** or **Base64 data**.

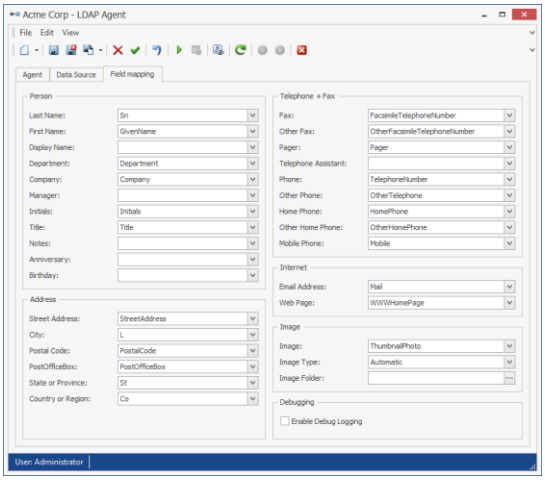


Figure 33: LDAP Agent field mapping

The field mapping shows the names of the vCard fields as field names. The corresponding name of the source field must be entered into the text box next to the vCard field.

In the field mapping, the following special parameters can be configured:

Image: The source field for the image data

Image Type: The image's type. One of the following:

- Automatic: The Agent automatically determines the type of the field.
- File Name: The source field contains a file name. If it is a relative path, the **Image Folder** parameter must be set to the base directory.

- Binary Data: The source field contains binary data.
- Base64 Data: The source field contains base64-encoded data. This must be set when importing data from the **ThumbnailPhoto** attribute.

Image Folder: The image file's base directory. When importing images of type File Name and the attribute value is a relative path, this must be set to the image's base directory.

Debugging: Enables debug logging to a file in the service account's temp folder. Enable only if requested by messageconcept support.

6.9.4 Phone Mapping

Phone number mapping is supported by this agent. See chapter 6.3 Phone Number Mapping for details.

6.10 Database Agent

The **Database Agent** imports contacts from a database table. The agent can connect to any relational database, provided the ADO.NET database provider is installed on the system running the agent, an appropriate connection string can be specified, and the database can be queried with a SQL SELECT command. The agent does not have a fixed field mapping. It can import a photo, provided it is specified as a file name having an absolute or relative path, or as a URL.

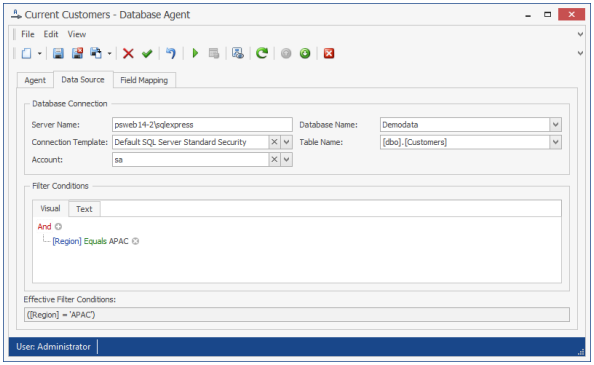


Figure 34: Database Agent Configuration

Figure 34: Database Agent Configuration shows a sample Database Agent configuration. Here, contacts are loaded from the table "[HumanResources].[vJobCandidate]" located in the SQL Server Database "AdventureWorks2012". The connection string template "Default SQL Server Integrated Authentication" is being used, which means that no action account needs to be entered, as the account running the People Sync service is used to connect to the database. In this case, all rows of the "vJobCandidate" Table are loaded, as no filter has been defined.

6.10.1 Requirements

The following databases are officially supported:

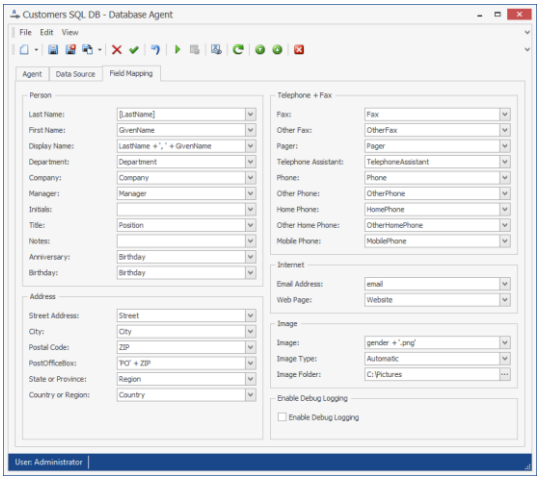
- SQL Server 2008 R2 and newer
- Oracle 11g and newer
- MySQL 5.6 and newer

Other database providers can be used but are not officially supported.

6.10.2 Configuration

The **Database Agent** uses the following configuration parameters:

Connection Template: Select an appropriate connection template for the type of connection that is being configured. The connection template contains a connection string and a corresponding database provider. PeopleSync ships with several pre-defined connection templates. To define custom connection templates, please refer to section 0 All Database fields may be freely mapped to contact fields.



The field mapping shows the names of the vCard fields as field names. The corresponding name of the source field must be entered into the text box next to the vCard field.

In the field mapping, the following special parameters can be configured:

Image: The source field for the image data

Image Type: The image's type. One of the following:

- Automatic: The Agent automatically determines the type of the field.
- File Name: The source field contains a file name. If it is a relative path, the **Image Folder** parameter must be set to the base directory.
- Binary Data: The source field contains binary data.
- Base64 Data: The source field contains base64-encoded data.

Image Folder: The image file's base directory. When importing images of type File Name and the attribute value is a relative path, this must be set to the image's base directory.

Debugging: Enables debug logging to a file in the service account's temp folder. Enable only if requested by messageconcept support.

Custom

Server Name: The server's DNS name or IP address. In case of SQL Server, if an instance other than the default instance is being used, the server name needs to be specified as {Server Name}\{Instance Name}.

Account: The account used to log on to the database, if credentials other than those of the account running the PeopleSync Service are needed.

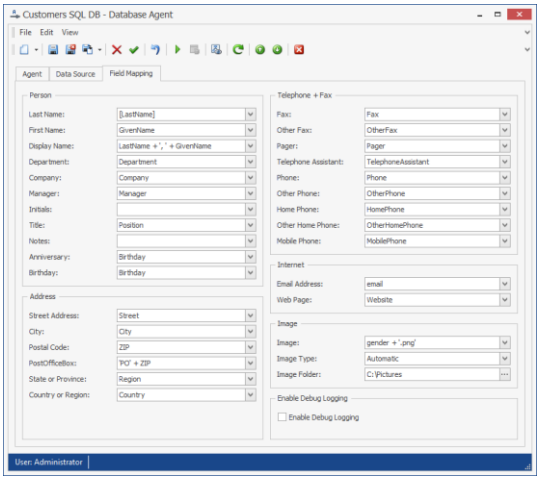
Database Name: The name of the database.

Table Name: The name of the table or view.

Filter Conditions: A list of filter conditions. Blank, if no conditions are specified.

6.10.3 Field Mapping

All Database fields may be freely mapped to contact fields.



The field mapping shows the names of the vCard fields as field names. The corresponding name of the source field must be entered into the text box next to the vCard field.

In the field mapping, the following special parameters can be configured:

Image: The source field for the image data

Image Type: The image's type. One of the following:

- Automatic: The Agent automatically determines the type of the field.
- File Name: The source field contains a file name. If it is a relative path, the **Image Folder** parameter must be set to the base directory.
- Binary Data: The source field contains binary data.
- Base64 Data: The source field contains base64-encoded data.

Image Folder: The image file's base directory. When importing images of type File Name and the attribute value is a relative path, this must be set to the image's base directory.

Debugging: Enables debug logging to a file in the service account's temp folder. Enable only if requested by messageconcept support.

6.10.4 Custom Database Providers

Custom database providers can be defined in the **Database Providers** section. They can be used to create a connection with a database provider that is not officially supported or to accommodate for a special connection string.

A custom database provider consists of a Display Name, Provider Factory Type Name, Provider Assembly Full Path and a Connection String Template.

PeopleSync uses .net 7.0+ compatible database drivers that implement System.Data.Common.DbProviderFactory.

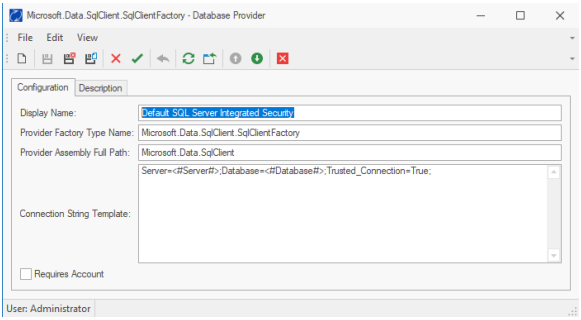


Figure 35: Custom Database Provider

Provider Factory Type Name: The class name, including namespace, of the DbProviderFactory, e.g. "Microsoft.Data.SqlClient.SqlClientFactory".

Provider Assembly Full Path: The name or full path of the assembly containing the DBProviderFactory, e.g. "Microsoft.Data.SqlClient".

Connection String Template: The connection string template contains a connection string with placeholders that will be filled when the template is used in an agent. The following placeholders may be used in a connection template:

- **#Server#** The DNS name or IP address of the database server.
- **#Database#** The database name
- **#User#** The username required to connect to the database
- **#Password#** The password required to connect to the database.

An example of a connection string template can be seen in Figure 35: Custom Database Provider.

Requires Account: This setting should be checked if the **#User#** and **#Password#** placeholders have been used in the connection string. This activates a validity check during agent configuration and prevents users from inadvertently forgetting to configure an action account. Do not check if the connection string template uses integrated authentication – i.e., authenticates with the credentials of the PeopleSync Service.

6.10.5 Phone Mapping

Phone number mapping is supported by this agent. See chapter 6.3 Phone Number Mapping for details.

6.11 Salesforce Agent ■

The **Salesforce Agent** imports contacts from the **contacts** list in Salesforce. The agent uses a default mapping of list fields to vCard fields, but a custom mapping can also be configured.

Figure 36: Salesforce Agent Configuration shows a sample configuration of the Salesforce agent. The agent will connect to Salesforce and fetch all contacts available to the configured service account.

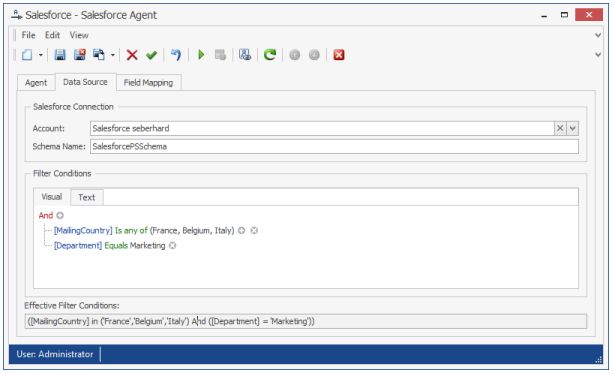


Figure 36: Salesforce Agent Configuration

Note: The Schema Name “SalesforcePSSchema” should not be changed. If you need a custom schema, please contact messageconcept support.

6.11.1 Requirements

API access must be enabled for the organization. As described in Salesforce knowledge article 000005140, the organization must be on one of the following editions:

- Enterprise Edition
- Unlimited Edition
- Developer Edition
- Performance Edition

6.11.2 Configuration

The **Salesforce Agent** uses the following configuration parameters:

Service Account: An account that has the right to view the organization's contacts. Please add the Salesforce user's security token at the end of the password when saving the Salesforce Service Account in PeopleSync. For example, if the Password is Password1 and the security token is XXXXXXXXXX, the Service Account's password must be saved as Password1XXXXXXXXXX.

OAuth can also be used for authentication. Please see 6.2.4 Salesforce Certificate for information on how to configure OAuth with the JWT Bearer Flow.

Filter Conditions: A list of filter conditions. Blank, if no conditions are specified. The following operators may be used:

- And
- Or
- Equals / Does not equal
- Is less than / Is less than or equal to
- Is greater than / Is greater than or equal to

- Contains / Not Contains (Use Wildcard Operator '%')
- IN / NOT IN

6.11.3 Field Mapping

Field Mapping (Tab): In the **Field Mapping** tab (see Figure 37: Salesforce Agent Field Mapping), a custom mapping of SharePoint list fields to vCard fields can be specified. The field mapping shows the names of the vCard fields as field names. The corresponding name of the Salesforce field must be entered into the text box next to the field. For example, to map the Salesforce field "Description" to the "Notes" field in the vCard, it needs to be entered into the text box next to the "Notes" caption.

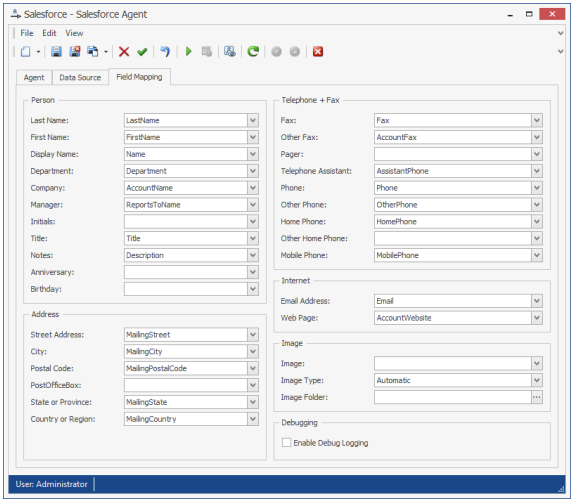


Figure 37: Salesforce Agent Field Mapping

In the field mapping, the following special parameters can be configured:

Image: The source field for the image data

Image Type: The image's type. One of the following:

- Automatic: The Agent automatically determines the type of the field.
- File Name: The source field contains a file name. If it is a relative path, the **Image Folder** parameter must be set to the base directory.
- Binary Data: The source field contains binary data.
- Base64 Data: The source field contains base64-encoded data.

Image Folder: The image file's base directory. When importing images of type File Name and the attribute value is a relative path, this must be set to the image's base directory.

Debugging: Enables debug logging to a file in the service account's temp folder. Enable only if requested by messageconcept support.

6.11.4 Phone Mapping

Phone number mapping is supported by this agent. See chapter 6.3 Phone Number Mapping for details.

6.12 Microsoft CRM Agent ■

The **Microsoft CRM Agent** imports contacts from the **contacts** list in Microsoft Dynamics CRM. The agent uses a default mapping of list fields to vCard fields, but a custom mapping can also be configured.

Figure 38: Microsoft CRM Agent Configuration shows a sample configuration of the Microsoft CRM agent. The agent will connect to a Microsoft Dynamics CRM instance and fetch all contacts available to the service account. The credentials used for the connection are stored in the action account named “contoso\administrator”.

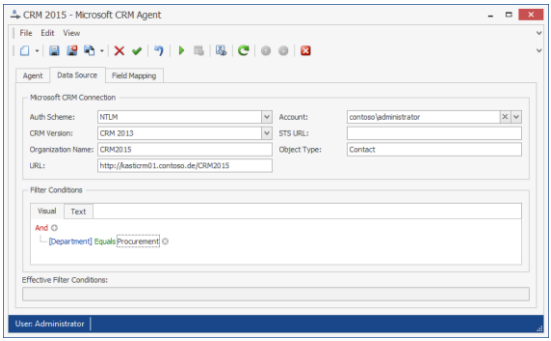


Figure 38: Microsoft CRM Agent Configuration

6.12.1 Requirements

The following Microsoft Dynamics CRM versions are supported:

- CRM Online WLID (Windows Live)
- CRM Online Office 365
- CRM 2013
- CRM 2011
- CRM 2011 IFD
- CRM 4.0

6.12.2 Configuration

The **Microsoft CRM Agent** uses the following configuration parameters:

CRM Version: The type of Dynamics CRM server to which you are connecting. In case of Dynamics CRM Online, use either “CRM Online WLID” or “CRM Online Office 365”. The “CRM Online WLID” setting is required to connect using the Windows Live security token service (STS), and “CRM Online Office 365” is required to connect using the Office 365 STS. For a CRM Online with local ADFS or an IFD instance of CRM, you must also specify the “STSURL” property.

Organization Name: The name of the organization, e.g. “TheOrganization”. This can be determined from the URL used to access Microsoft Dynamics CRM.

URL: The URL of the CRM organization, e.g. “http://mycrm/TheOrganization”.

Auth Scheme: The authentication method used. One of: NTLM, BASIC, DIGEST, NONE. Only used for connections to CRM 4.0.

Service Account: An account that has the right to view the organization’s contacts.

STS URL: The URL of the security token service (STS). Must only be set for IFD instances of CRM or CRM Online with local ADFS.

Filter Conditions: A list of filter conditions. Blank, if no conditions are specified.

For the LDAP Agent, the following operators may be used:

- And
- Or
- Equals
- Does not equal
- Is less than / Is less than or equal to
- Is greater than / Is greater than or equal to
- Contains (Use Wildcard Operator '%')

6.12.3 Field Mapping

In **Field Mapping** (see Figure 39: Microsoft CRM Agent Field Mapping), a custom mapping of CRM fields to vCard fields can be specified.

The field mapping shows the names of the vCard fields as field names. The corresponding name of the CRM field must be entered into the text box next to the field. For example, to map the CRM field "Description" to the "Notes" field in the vCard, it needs to be entered into the text box next to the "Notes" caption.

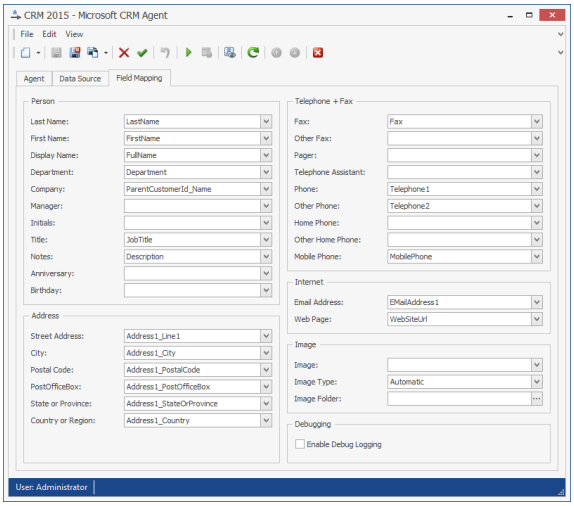


Figure 39: Microsoft CRM Agent Field Mapping

The default field mapping for the Microsoft CRM Agent is described in 9.8 Microsoft CRM Agent – Field Mapping.

In the field mapping, the following special parameters can be configured:

Image: The source field for the image data

Image Type: The image's type. One of the following:

- Automatic: The Agent automatically determines the type of the field.
- File Name: The source field contains a file name. If it is a relative path, the **Image Folder** parameter must be set to the base directory.
- Binary Data: The source field contains binary data.
- Base64 Data: The source field contains base64-encoded data.

Image Folder: The image file's base directory. When importing images of type File Name and the attribute value is a relative path, this must be set to the image's base directory.

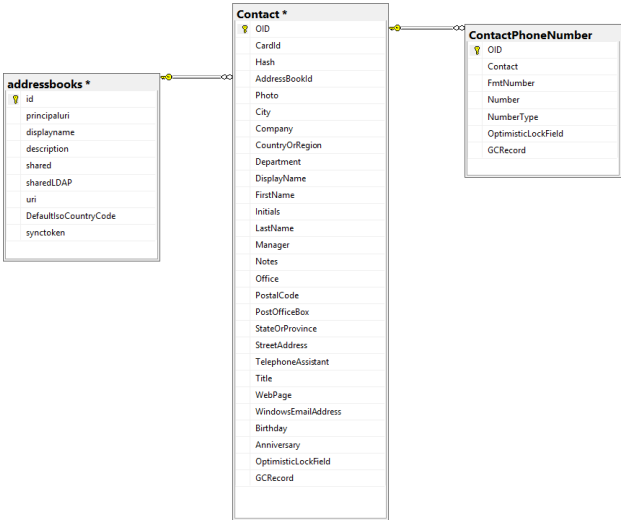
Debugging: Enables debug logging to a file in the service account's temp folder. Enable only if requested by messageconcept support.

6.12.4 Phone Mapping

Phone number mapping is supported by this agent. See chapter 6.3 Phone Number Mapping for details.

7 Access to Contact Data by Third-Party Systems

Third-Party systems can access PeopleSync contact data through a set of database tables. The schema is as follows:



Access to these tables is read-only. Any changes to the tables will be reverted once the respective Agent runs. Changes made in these tables will also not be propagated to devices.

The ContactPhoneNumber.FmtNumber is the telephone number formatted in E.164 format, i.e. +49123456789.

Please enable the “**Enable external caller ID**” setting in System Settings. Then set a default country code for each address list. This will improve formatting accuracy when the country can’t be deduced from the contact.

Note: Please be advised that this data is only available for address lists that are updated via a PeopleSync Agent.

8 Troubleshooting and Support

8.1 Troubleshooting PeopleSync Frontend Server

If your clients cannot successfully connect to the PeopleSync server or no address books and no contact data is shown on the clients. You can try the following steps to narrow down the problem.

First, switch the **PHP Error Reporting** to **Development machine**. For that, go to PHP Managers main view. Under **PHP Settings** click on **Configure error reporting**. This will open the following view.

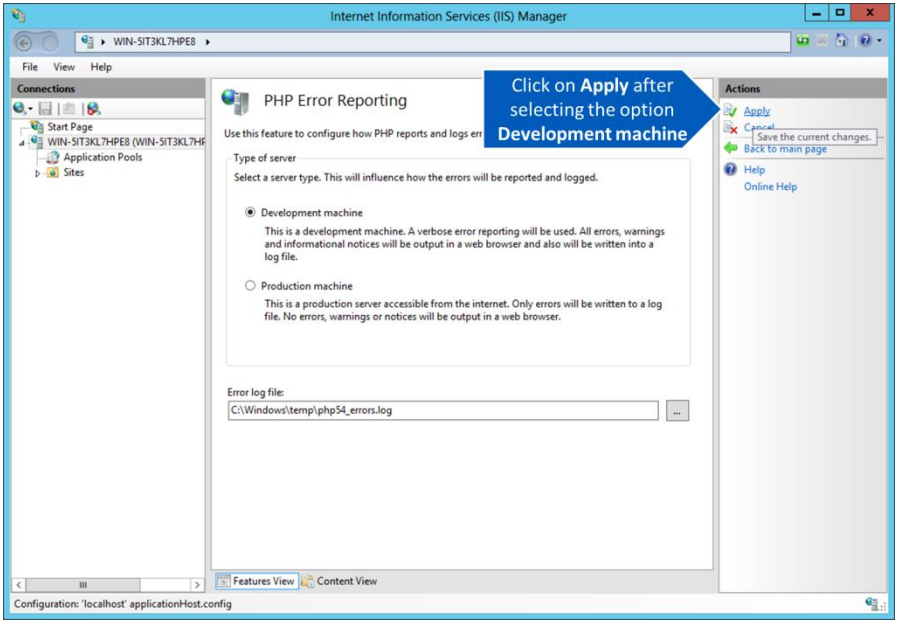


Figure 40: IIS Manager PHP Error Reporting

By switching the server type to **Development machine**, the PHP settings are changed to show errors in the browser instead of logging them to a file. Then open a web browser and enter the URL of your PeopleSync server, such as http://peoplesync.example.com/.

This will prompt you for a user name and password. If this succeeds, you can browse through the address books which have been made available for this given user. If this step fails, an error message from the server will be displayed in the web browser. Typical errors include:

- database server not reachable

  → check your **server.ini**
- database not correctly setup

  → use PeopleSync Console to correct this
- failure to authenticate the user

  → check with PeopleSync Console if the configured Active Directory server is correct.

Note: Don't forget to switch **PHP Error Reporting** back to **Production Machine** after solving problems and finishing troubleshooting. Not switching back to **Production Machine** poses a security risk as passwords can potentially be logged in the PHP error log.

8.2 Typical Problems in PeopleSync Agent

This chapter covers typical problems in PeopleSync Agent. Listed below are some of the reasons and solutions to common problems.

8.2.1 Login to PeopleSync Console fails

Symptoms:

- Error message “The application cannot connect to the specified database, because the latter doesn't exist, or its version is older than that of the application. (…)” after login.

Cause:

- The Windows domain user has no sufficient permissions.

Resolution:

- Check that the user is a member of the **PeopleSync Admins** group.
- Check that the **PeopleSync Admins** group has **Datareader** and **Datawriter** permissions in the PeopleSync Database.
- Check that the **PeopleSync Admins** group has Mbodify permissions for the file **<PeopleSync Directory>\Console\LogonParameters**.

8.2.2 PeopleSync is not licensed

Symptoms:

- The PeopleSync log shows “Error” events of category “Licensing”.
- The PeopleSync Service is stopped.

Cause:

- PeopleSync is not licensed, license keys have not been copied to the proper directory or license keys have expired.

Resolution:

- Make sure license keys have been copied to “Licensekeys” folder in the PeopleSync Agents’ installation directory (e.g. C:\Program Files\messageconcept GmbH\PeopleSync\Agent)
- Verify that license keys are still valid by opening the license file in a text editor or reading the PeopleSync log entries.
- Restart the PeopleSync Service.

8.2.3 PeopleSync Service stopped: Invalid user, insufficient rights

Symptoms:

- The PeopleSync Service is stopped.
- System event log shows errors with source “Service Control Manager” for service “PeopleSync Agent”

Cause:

- The service user account password is invalid
- The service user does not have sufficient privileges to run a service

Resolution:

- Check that the service user account password is correct.
- Make sure the service user account is an administrator on the local server.

8.2.4 PeopleSync Service fails to start: Database problem

Symptoms:

- The PeopleSync Service is stopped.
- Application event log shows errors with source “PeopleSync_Agent” and event text contains “System.Data.SqlClient.SqlException” and “DevExpress.ExpressApp.Updating.CompatibilityException”.

Cause:

- SQL Server is unreachable
- The database connection is wrong

Resolution:

- Make sure the database is running and the service account running PeopleSync Service has sufficient rights in the database.
- Search for “ConnectionString” in the agent.exe.config file located in the PeopleSync Agents’ installation directory (e.g. C:\Program Files\messageconcept GmbH\PeopleSync\Agent). Make sure the connection string is still correct.

8.2.5 Exchange GAL Agent fails to connect to WinRM server

Symptoms:

- Error message 20900 in the event log: “Connecting to remote server ps.outlook.com failed with the following error message: WinRM cannot complete the operation.”
- If you are using an Exchange Server on premise instead of Office 365, the server name might differ from ps.outlook.com.

Cause:

- Agent connection to the remote server has been blocked by a local firewall or network firewall.
- Problem with forwarding the traffic by a proxy server to the remote server.
- The agent caused too many requests and run in Throttling state.

Resolution:

- Check that the agent can communicate with the remote server.
- Check the Throttling configuration in Exchange Server or Office 365.

- Let the Exchange GAL Agent run less often.

8.2.6 Agent does not load data

Symptoms:

- A PeopleSync Agent does not load data or is not running.

Cause:

- Agent or address list may be disabled
- Schedule is invalid
- Agent configuration is invalid

Resolution:

- Check that the agent and the corresponding address book are both enabled.
- Check the validity of the Schedule. For example, a cron expression that contains the same number twice (e.g. 0,5,10,5) is invalid.
- Check the PeopleSync log for errors regarding this agent. Verify that the agent's configuration parameters are correct.

8.3 Typical Problems in PeopleSync Address lists

This chapter covers typical problems in PeopleSync address lists. The listed possible reasons for your problem might help you to troubleshoot the problem.

8.3.1 Address list not available on device

Symptoms:

- Address list is not visible on device

Cause:

- Device not synchronized
- Insufficient permissions
- Address book disabled

Resolution:

- Make sure that the address list is enabled in the PeopleSync Console.
- Verify that a group has been assigned with at least “Read” permissions and that the user in question is a member of the group.
- Try to force synchronization on the device. If the address list still does not appear, have the user open the PeopleSync Server URL in a web browser and log on with his credentials. Navigate to **addressbooks**, then click on the username and verify that the address list is shown.

8.3.2 Address list content changes continuously or changes are undone

Symptoms:

- Address list changes continuously, although the underlying data source does not.
- Changes made by users are undone after some time.

Cause:

- A user group can modify the address list's content and the address list has an agent configured.
- It is not recommended to allow users to modify an address list, and at the same time, have an agent import data into the same list.

Resolution:

- Revoke the "Modify" permission in the address list's permissions.
- As an alternative, disable the associated agent.

8.4 Contacting Support

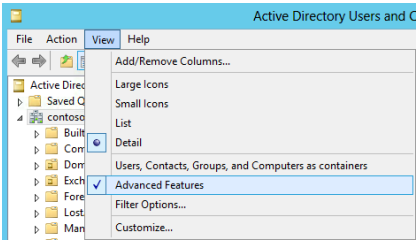
If this manual does not help solve your problem, please contact our support team. Our support staff will guide you through the troubleshooting process or will establish a remote session, if needed.

9 Appendix

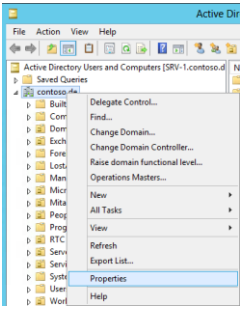
9.1 Determining an AD Domain's Distinguished Name

1. Open **Active Directory Users and Computers**.

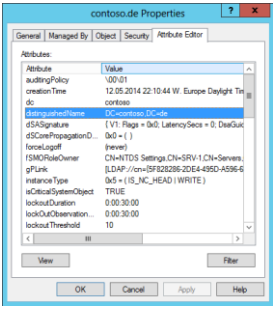
   In the **View** menu, enable **Advanced Features**.



2. Right-click on the Domain and select **Properties**.



3. Open the **Attribute Editor** tab.



4. Double-click on the **distinguishedName** attribute and copy its value.

9.2 Active Diretory Agent – Field Mapping

The **Active Directory Agent** uses the following field mapping:

Active Directory		**VCard**
Display Name EN	**LDAP Name**	**Field Name**
Initials	initials	Additional Names
Last Name	sn	Family Name
First Name	givenName	Given Name
Company	company	Organization Name
Department	department	Organizational Unit
Home Phone (Others)	otherHomePhone	Car
Mobile Number	mobile	Cell
Fax Number	facsimileTelephone Number	Fax
Home Phone	homePhone	Home
Fax Number (Others)	otherFacsimile TelephoneNumber	Modem
Pager Number	pager	Pager
Phone Number (Others)	otherTelephone	Voice
Telephone Number	telephoneNumber	Work
Country	co	Country Name

Active Directory		VCard
Display Name EN	**LDAP Name**	**Field Name**
City	l	Locality
Post Office Box	postOfficeBox	Post Office Box
ZIP/Postal Code	postalCode	Postal Code
State/Province	st	Region
Street Address	streetAddress	Street Address
E-Mail Address	mail	E-Mail
Display Name	displayName	Formatted Name
Description	description info (Fallback)	Note
Photo	thumbnailPhoto	Photo
Job Title	title	Title
	MD5 (distinguishedName)	UID
Web Page Address	wWWHomePage	URL
Assistant's telephone	telephoneAssistant	X-MS-ASSISTANT
Manager	manager	X-MS-MANAGER

Note: The Exchange GAL Agent uses the same field mapping as described in the table above.

9.3 Entra ID Agent – Field Mapping

The **Entra ID Agent** uses the following field mapping:

Entra ID	VCard		
Field Name	**Field Name**	**User**	**Contact**
Last Name	Family Name	x	X
First Name	Given Name	X	X
Company	Organization Name	X	X
Department	Organizational Unit	X	X
Mobile Number	Cell	X	X
Fax Number	Fax	X	X
Business Phone	Work	X	X
Home Phone	Home	-	X
Other Phone	Other	-	X
Pager	Pager	-	X
Country	Country Name	X	X
City	Locality	X	X
ZIP/Postal Code	Postal Code	X	X
State/Province	Region	X	X
Street Address	Street Address	X	X

Entra ID	VCard		
Field Name	**Field Name**	**User**	**Contact**
E-Mail Address	E-Mail	X	X
Display Name	Formatted Name	X	X
Photo	Photo	X	-
Job Title	Title	X	X
	UID		
Manager	X-MS-MANAGER	X	-

9.4 Exchange GAL Agent – Filterable Properties

Property Name	User	Contact
AllowUMCallsFromNonUsers	x	x
AssistantName	x	x
City	x	x
Company	x	x
CountryOrRegion	x	x
Department	x	x
DisplayName	x	x
DistinguishedName	x	x
ExchangeVersion	x	x
Fax	x	x
FirstName	x	x
Guid	x	x
HomePhone	x	x
Initials	x	x
LastName	x	x
Manager	x	x
MemberOfGroup	x	x

Property Name	User	Contact
MobilePhone	x	x
Name	x	x
Notes	x	x
Office	x	x
OtherFax	x	x
OtherHomePhone	x	x
OtherTelephone	x	x
Pager	x	x
Phone	x	x
PhoneticDisplayName	x	x
PostalCode	x	x
PostOfficeBox	x	x
RecipientType	x	x
RecipientTypeDetails	x	x
SamAccountName	x	
SimpleDisplayName	x	x
StateOrProvince	x	x
StreetAddress	x	x

Property Name	User	Contact
TelephoneAssistant	x	x
UMDtmfMap	x	x
UMRecipientDialPlanId	x	x
UserPrincipalName	x	
WhenChanged	x	x
WhenCreated	x	x
WindowsEmailAddress	x	x

9.5 Exchange Folders Agent – Field Mapping

The **Exchange Folder Agent** uses the following field mapping:

Exchange Contact	vCard
Initials	Additional Names
Last Name	Family Name
First Name	Given Name
Company	Organization Name
Department	Organizational Unit
Home Phone (Others)	Car
Mobile Number	Cell
Fax Number	Fax
Home Phone	Home
Fax Number (Others)	Modem
Pager Number	Pager
Phone Number (Others)	Voice
Telephone Number	Work
Business Address Country	Work Address Country Name
Business Address City	Work Address Locality
Business Address Post Office Box	Work Address Post Office Box

Exchange Contact	vCard
Business Address ZIP/Postal Code	Work Address Postal Code
Business Address State/Province	Work Address Region
Business Address Street Address	Work Address Street Address
E-Mail Address	E-Mail
Display Name	Formatted Name
Description	Note
Photo	Photo
Job Title	Title
Web Page Address	URL
Assistant's telephone	X-MS-ASSISTANT
Manager	X-MS-MANAGER

9.6 SharePoint Agent – Field Mapping

The default field mapping for the SharePoint Agent is as follows:

SharePoint	vCard
Title	Last Name
FirstName	First Name
Company	Company
JobTitle	Title
WorkAddress	Business Address Street Address
WorkCity	Business Address City
WorkState	Business Address State or Province
WorkZip	Business Address Postal Code
WorkCountry	Business Address Country or Region
WorkPhone	Work Phone
HomePhone	Home Phone
CellPhone	Mobile Phone
WorkFax	Work Fax
Email	Email Address
Webpage	Web Page

9.7 Salesforce Agent – Field Mapping

The default field mapping for the Salesforce Agent is as follows:

SharePoint	vCard
LastName	Last Name
FirstName	First Name
Name	Display Name
Department	Department
AccountName	Company
ReportsToName	Manager
	Initials
Title	Title
MailingStreet	Business Address Street Address
MailingCity	Business Address City
MailingState	Business Address State or Province
MailingPostalCode	Business Address Postal Code
MailingCountry	Business Address Country or Region
Phone	Work Phone
OtherPhone	Other Phone
HomePhone	Home Phone

SharePoint	vCard
	Other Home Phone
MobilePhone	Mobile Phone
Fax	Work Fax
AccountFax	Other Fax Number
	Pager
AssistantPhone	Telephone Assistant
Email	Email Address
AccountWebsite	Web Page

Supported Attributes:

- AccountNumber
- AccountSource
- AnnualRevenue
- AssistantName
- AssistantPhone
- BillingCity
- BillingCountry
- BillingLatitude
- BillingLongitude
- BillingPostalCode
- BillingState
- BillingStreet
- Birthdate
- CreatedDate
- CreatedDate
- DandbCompanyId
- Department
- Description
- Description
- DunsNumber
- Email
- EmailBouncedDate

- EmailBouncedReason
- Fax
- Fax
- FirstName
- HomePhone
- Industry
- IsEmailBounced
- LastActivityDate
- LastActivityDate
- LastCURequestDate
- LastCUUpdateDate
- LastModifiedDate
- LastModifiedDate
- LastName
- LastReferencedDate
- LastReferencedDate
- LastViewedDate
- LastViewedDate
- LeadSource
- MailingCity
- MailingCountry
- MailingLatitude
- MailingLongitude
- MailingPostalCode
- MailingState
- MailingStreet
- MasterRecordId
- MobilePhone
- NaicsCode
- NaicsDesc
- Name
- Name
- NumberOfEmployees
- OtherCity
- OtherCountry
- OtherLatitude
- OtherLongitude
- OtherPhone
- OtherPostalCode
- OtherState
- OtherStreet
- Ownership
- ParentId
- Phone
- Phone
- Rating
- ReportsToFirstName
- ReportsToId
- ReportsToLastName
- ReportsToName
- Salutation
- ShippingCity

- ShippingCountry
- ShippingLatitude
- ShippingLongitude
- ShippingPostalCode
- ShippingState
- ShippingStreet
- Sic
- SicDesc
- Site
- SystemModstamp
- TickerSymbol
- Title
- Tradestyle
- Type
- Website
- YearStarted

9.8 Microsoft CRM Agent – Field Mapping

The default field mapping for the Microsoft CRM Agent is as follows:

SharePoint	**vCard**
LastName	Last Name
FirstName	First Name
FullName	Display Name
Department	Department
ParentCustomerId_Name	Company
	Manager
	Initials
JobTitle	Title
Address1_Line1	Business Address Street Address
Address1_City	Business Address City
Address1_StateOrProvince	Business Address State or Province
Address1_PostalCode	Business Address Postal Code
Address1_PostOfficeBox	Post Office Box
Address1_Country	Business Address Country or Region
Telephone1	Work Phone

SharePoint	vCard
Telephone2	Other Phone
	Home Phone
	Other Home Phone
MobilePhone	Mobile Phone
Fax	Work Fax
	Other Fax Number
	Pager
	Telephone Assistant
EMailAddress1	Email Address
WebSiteUrl	Web Page

Version History

Version	Changes
1.00	▪ First Public Release

Copyright

The description of the CRON-like Sync Schedules is partly copied from the Wikipedia encyclopedia (http://en.wikipedia.org/wiki/Cron).

Contact us

messageconcept software GmbH

Grosse Witschgasse 17

50676 Cologne · Germany

Phone +49 221 677 855 0

Fax +49 221 677 855 99

E-Mail info@messageconcept.com

Internet www.messageconcept.com

messageconcept Hotline Numbers

For technical sales and software support please use the following contact details.

Languages	Countries	Hotline Numbers
German	DE/AT/CH	+49 221 677 855 49
English	US/CA	+1 778 786 3475
	UK	+44 870 479 8657
	Other	+49 221 677 855 44

Our hotlines are available 24/7. Outside European business hours you will be connected to one of our call center agents and will receive a callback during business hours of your time zone.