CONTACTSYNC® V8.5

Quick Start Guide

NETsec

04. December 2024

NETsec GmbH & Co.KG | Schillingsstrasse 117 | 52355 Düren | Germany

Introduction **5**
contactSync 5
GALsync 5
Prerequisites **6**
System Requirements 6
Overview 7
Service Account (on-premises) 8
Exchange mailbox for the contactSync Service Account 8
On-premises mailbox 8
Exchange Online mailbox 8
Local service account on a standalone server 9
Execution Policy (Microsoft 365 Exchange Online) 9
ExchangeOnlineManagement PowerShell module 10
Install ExchangeOnlineManagement PowerShell module 10
Update ExchangeOnlineManagement PowerShell module 10
Installation **11**
Install contactSync 11
Configure contactSync Service 15
Apply contactSync License 18
Create an Environment Configuration **19**
Create an Environment Configuration for on-premises Exchange environment 19
Create an Environment Configuration for Hybrid Exchange environment 24
Create Environment Configuration for Exchange Online environment 32
Exchange Online certificate-based authentication via App Registration 38
Register an Enterprise Application in Microsoft Entra ID 40
Where to find the domain name of the Microsoft 365 tenant? 42
Certificate for the registered Application 44
Upload certificate file for the registered Application 48
Assign API permissions to the registered Application 50
Exchange Administrator role for the registered Application 62
Overview of the registered Application in App registrations 64
Test the Exchange Online PowerShell connection and the Exchange mailbox 70
Exchange Online authentication via Service Account 73
Service Account (Microsoft 365 Exchange Online) 73
Modern Authentication OAuth 2.0 for Exchange Web Services (EWS) to access Exchange Online 74
Create and Run contactSync Policies **91**

Synchronize Contacts from Exchange On-Premises into Mailboxes 91
Create new policy 91
Synchronization mode 92
Access to Mailboxes for on-premises Exchange 93
Access to Mailboxes for Exchange Online 94
Select the Mailboxes from On-Premises Exchange 95
Select the Mailboxes from Exchange Online 99
Select mail-enabled objects on the Directory tab from On-Premises 101
Select the Mailbox Contact Folder 105
Status notification email 106
Schedule policy run 107
Policy name and description 108
Execute Policy and Check Log File 109
Synchronize Contacts from Exchange Online into Mailboxes 113
Create new policy 113
Synchronization mode 114
Access to Mailboxes for On-Premises Exchange 115
Access to Mailboxes for Exchange Online 116
Select the Mailboxes from On-Premises Exchange 117
Select the Mailboxes from Exchange Online 122
Select mail-enabled objects on the Directory tab from Exchange Online 125
Select the Mailbox Contact Folder 127
Status notification email 128
Schedule policy run 129
Policy name and description 130
Execute policy and check log files 131
Synchronize Contacts from Public Folder 135
Create a new policy 135
Synchronization mode 136
Access to Mailboxes for on-premises Exchange 137
Access to Mailboxes for Exchange Online 138
Select the Mailboxes from On-Premises Exchange 139
Select the Mailboxes from Exchange Online 144
Select Public Folder 147
Determine the primary SMTP address of the public folder located on-premises 148
Determine the primary SMTP address of the public folder located Exchange Online 151

Select the Mailbox Contact Folder 153
Status notification email 154
Schedule policy run 155
Policy name and description 156
Execute policy and check log files 158
Synchronize Contacts from Shared Mailbox 161
Create new policy 161
Synchronization mode 162
Access to Mailboxes for on-premises Exchange 163
Access to Mailboxes for Exchange Online 164
Select the Mailboxes from On-Premises Exchange 165
Select the Mailboxes from Exchange Online 170
Select Shared Mailbox 173
Select Contact Folder in the Shared Mailbox 175
Select the Mailbox Contact Folder 177
Status notification email 178
Schedule policy run 179
Policy name and description 180
Execute policy and check log files 182
How to 184
How to configure Exchange Application Impersonation 184
Exchange Impersonation in Exchange 2013, 2016, 2019 and Exchange Online 184
Support: What to do when I notice an error / bug? 190
Environment Overview 190
Description of the issue 190
Configuration and log files 190

Introduction

contactSync

contactSync synchronizes contacts contained in a Shared Mailbox or in a modern Public Folder into users' mailboxes in the same Exchange environment.

It also synchronizes the Global Address List (GAL) into users' mailboxes, that are in the same environment. Mail-enabled objects in an on-premises Active Directory can be synchronized into Exchange mailboxes in the same Exchange environment and mail-enabled objects in a Microsoft 365 tenant can be synchronized into Exchange mailboxes in the same Exchange environment.

contactSync synchronizes the contacts into a subfolder within the user's mailbox contacts.

This **Quick Start Guide** describes with examples how to create an **Environment Configuration** for an Exchange environment and how to configure the policy to synchronize contacts into Exchange mailboxes.

For more information about different synchronization scenarios and the configuration settings, please take a look at the contactSync manual.

contactSync Documentation

https://www.netsec.de/en/products/contactsync/documentation.html

GALsync

GALsync synchronizes the Global Address List (GAL) between different Exchange environments, which can be on-premises Exchange environments or Exchange Online of Microsoft 365 tenants.

For each Exchange environment, you can configure which mail-enabled objects will be synchronized as mail-enabled contacts to the other Exchange environments. Also, you can configure how the received mail-enabled objects from the other Exchange environments will be synchronized as mail-enabled contacts to your own Exchange environment.
This will make the mail-enabled objects from the other Exchange environments visible as contacts in the Global Address List (GAL).

Please take a look at the GALsync documentation for additional information.

GALsync Documentation

https://www.netsec.de/en/products/galsync/documentation.html

Prerequisites

System Requirements

Components	Required
OS (64Bit)	Windows Server 2016 Windows Server 2019 Windows Server 2022 Windows Server 2025
Hardware	Processor: minimum dual core RAM: minimum 4GB
Software	.NET Framework 4.8.0 and later Windows PowerShell 5.1 and ExchangeOnlineManagement PowerShell module version 3.6 or later for Exchange Online PowerShell V3
Recommendations	**Exchange On-Premises**: We recommend to install contactSync on a member server within the domain (e.g., dedicated contactSync server or file server). The machine should be uncritical (e.g., may be restarted without complications). The contactSync server must have a high bandwidth connection to the DC/GC. **Exchange Online**: See recommendations for on-premises; but you can use also a standalone computer.
Supported Exchange Versions*	Exchange 2013* SP1 and later Exchange 2016 and later Exchange 2019 and later Microsoft 365 Exchange Online

** Microsoft stopped supporting Exchange 2013 on the 11th April 2023. Microsoft stopped supporting for Windows Server 2012 and Windows Server 2012 R2 on the 10th October 2023.*

As much as we would like to keep up compatibility for all versions, we cannot support an Environment, which is no longer supported by the manufacturer.

Overview

contactSync requires a service account. The contactSync service account is only a domain user in the Active Directory and has an Exchange mailbox. The mailbox of the contactSync service account can be located at the on-premises Exchange or in Exchange Online.

On your contactSync server, the service account should be a local administrator and it should be possible to log on to the server as this account. Remote desktop connectivity may also be required.

Furthermore, the service account on the contactSync server needs the right to run as a service.

It is recommended to run the contactSync GUI always with the credentials of the local contactSync service account.

This can be confirmed on the information bar at the bottom of the contactSync GUI.

Exchange on-premises:

To access the mailboxes on your on-premises Exchange server, the contactSync service account needs to be member of the Exchange **Application Impersonation** role to gain access to the mailboxes to which the contacts are to be synchronized.

Please take a look at the chapter
How to configure Exchange Application Impersonation

Exchange Online:

To access the mailboxes in Exchange Online, you have the option of user-based authentication or certificate-based authentication. Certificate-based authentication for Exchange Online is recommended so the contactSync service account will not require any additional authorizations.

The certificate-based authentication for Exchange Online is described in the chapter
Exchange Online certificate-based authentication via App Registration

Service Account (on-premises)

The on-premises contactSync service account is a domain user of the on-premises Active Directory.

The on-premises service account is a member of the **Local Administrators** group on the Windows Server, where contactSync is installed.

The on-premises service account needs the local right to **run as a service** on the Windows Server, where contactSync is installed. This permission is added to the service account during the installation.

Make sure you can logon as the on-premises service account to the Windows Server, where contactSync is installed. It is likely that the on-premises service account requires membership in the local **Remote Desktop Users** group.

Note: We strongly recommend logging on as the service account to run the contactSync GUI.

The contactSync Service must run in the credentials of the on-premises service account.

In order to install contactSync you need administrative permission. Setup will also install the contactSync Service on the Windows Server you install contactSync on.

Important: If you configure the logon information for the Active Directory domain service account in the contactSync GUI using on-premises Exchange, it will be necessary use the format domain\username.

Exchange mailbox for the contactSync Service Account

The contactSync service account needs a licensed Exchange mailbox in the environment.

- contactSync must have direct access to the user mailbox of the service account via Exchange Web Services (EWS).
- Ensure that the mailbox is accessible (e.g., by Outlook Web Access).
- Ensure that the mailbox can send and receive email.

On-premises mailbox

For an on-premises Exchange scenario, the on-premises contactSync service account needs a mailbox located on the on-premises Exchange Server.

Exchange Online mailbox

An Exchange Online mailbox for the contactSync service account needs to be licensed with an Exchange Online license in the Microsoft 365 tenant.

For example: Microsoft 365 Business Basic, Exchange Online (Plan 1) or Microsoft 365 E1 license will work for the service account.

Local service account on a standalone server

If you run contactSync on a standalone Windows server, please create a local account for contactSync. This is only valid in Exchange Online cloud-only scenarios.

Please use the local account to configure and run the contactSync Service and the contactSync GUI in the credentials of this local account.

The local account needs the same local permissions as a domain user described above.

The local account will be required to use Modern Authentication for Microsoft 365 Exchange Online. The contactSync Service Account of the Microsoft 365 Exchange Online tenant is independent of this local account.

For example: **contactSync** is a local account of the **standalone Windows server**.

Please run also the contactSync GUI in the credentials of this local account.

Important: If you configure the logon information for the local service account in the contactSync GUI, it will be necessary use the format computername\username.

Execution Policy (Microsoft 365 Exchange Online)

If you configure a policy for Microsoft 365 Exchange Online, contactSync needs the parameter **ExecutionPolicy** to be set to **RemoteSigned** for the Windows PowerShell to connect to Exchange Online.

The reason for this is a security setting built into **Windows PowerShell** called execution policy. Execution policy determines how (or if) PowerShell runs scripts. By default, PowerShell's execution policy is set to Restricted; this means that scripts will not run. contactSync requires that scripts can be run.

```
Get-ExecutionPolicy
```

http://technet.microsoft.com/en-us/library/hh849821.aspx

```
Set-ExecutionPolicy RemoteSigned
```

https://technet.microsoft.com/en-us/library/hh849812.aspx

ExchangeOnlineManagement PowerShell module

contactSync requires **Windows PowerShell 5.1** and **ExchangeOnlineManagement PowerShell module version 3.6 or later** for Exchange Online PowerShell V3.

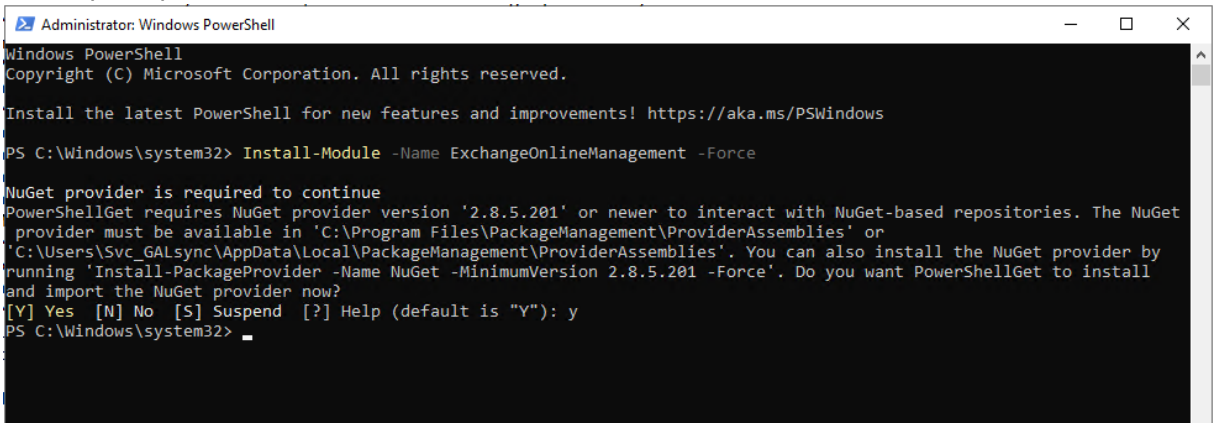
On the contactSync Server you need to install the **ExchangeOnlineManagement PowerShell module** so that contactSync direct can communicate with a Microsoft 365 Exchange Online tenant.

Install ExchangeOnlineManagement PowerShell module

On the contactSync Server, open **Windows PowerShell** as **Administrator**, then run the following to install:

```
Install-Module -Name ExchangeOnlineManagement -Force
```

When prompted, enter **Y** for Yes then Return



Please have look at the **Prerequisites for the Exchange Online PowerShell module** chapter of the **Microsoft Docs: About the Exchange Online PowerShell module**

https://learn.microsoft.com/en-us/powershell/exchange/exchange-online-powershell-v2?view=exchange-ps#install-the-exchange-online-powershell-module

Update ExchangeOnlineManagement PowerShell module

On the contactSync Server, open **Windows PowerShell** as **Administrator**, then run the following to update:

```
Update-Module -Name ExchangeOnlineManagement -Force
```

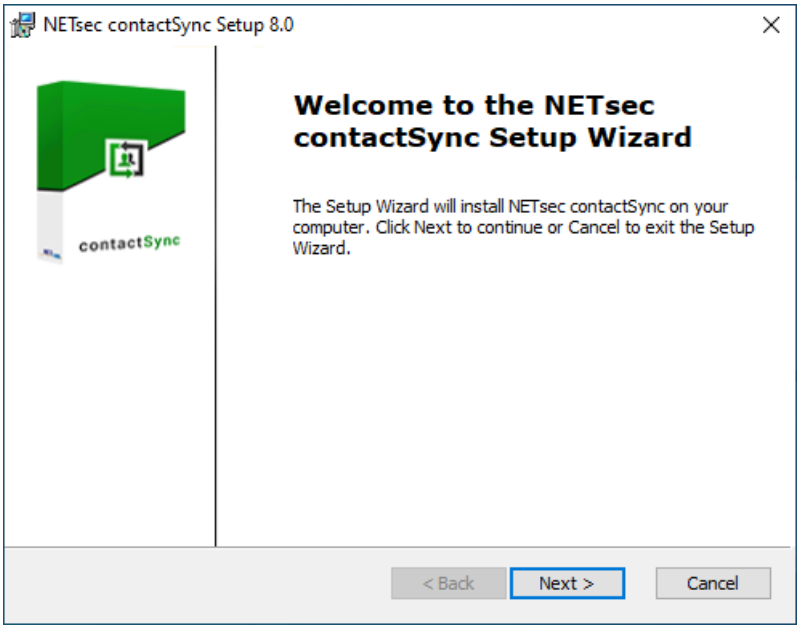
Please have look at the **Prerequisites for the Exchange Online PowerShell module** chapter of the **Microsoft Docs: About the Exchange Online PowerShell module**

https://learn.microsoft.com/en-us/powershell/exchange/exchange-online-powershell-v2?view=exchange-ps#update-the-exchange-online-powershell-module

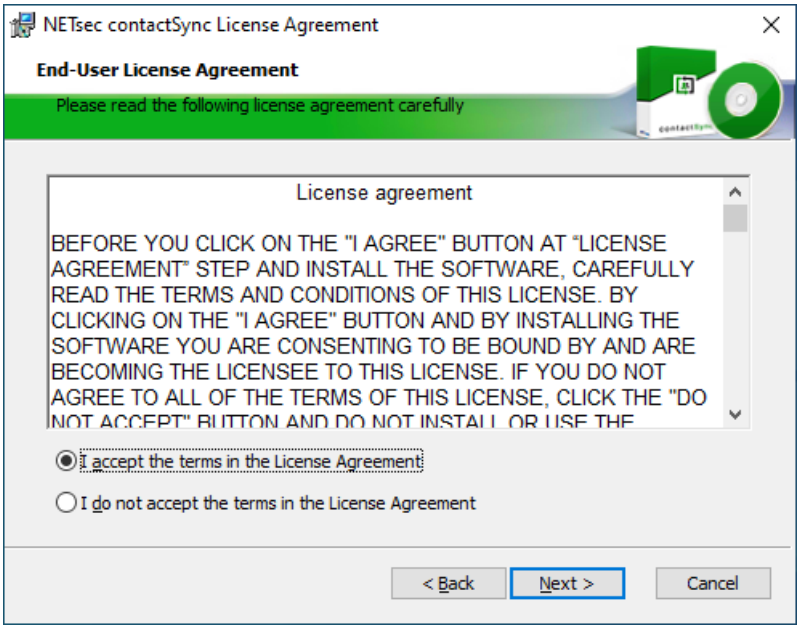
Installation

Install contactSync

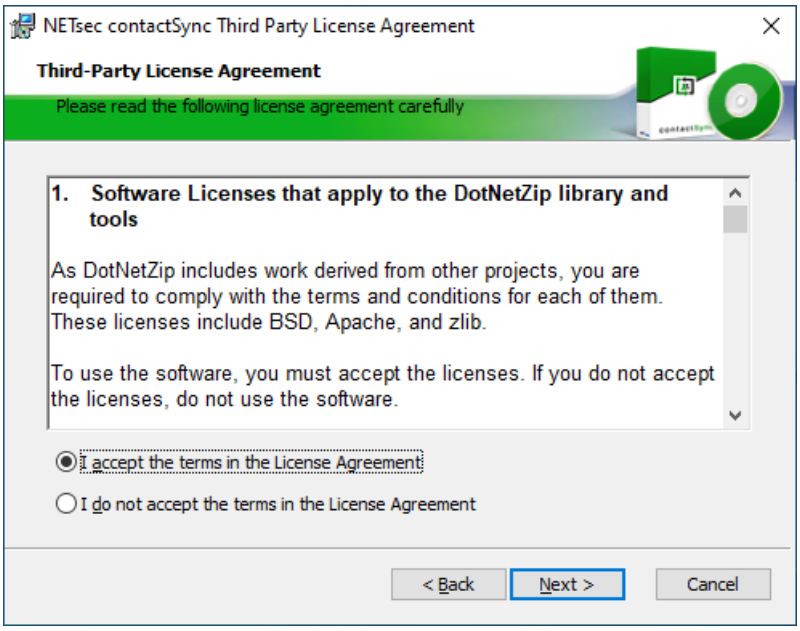
Open the **contactSyncSetup.msi** file and click **Next**



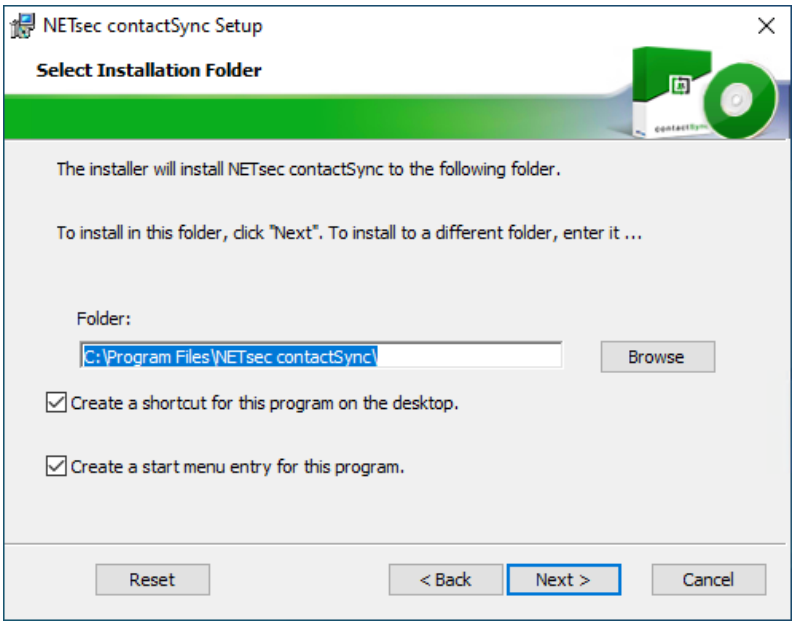
Accept the End-User License Agreement, then click **Next**



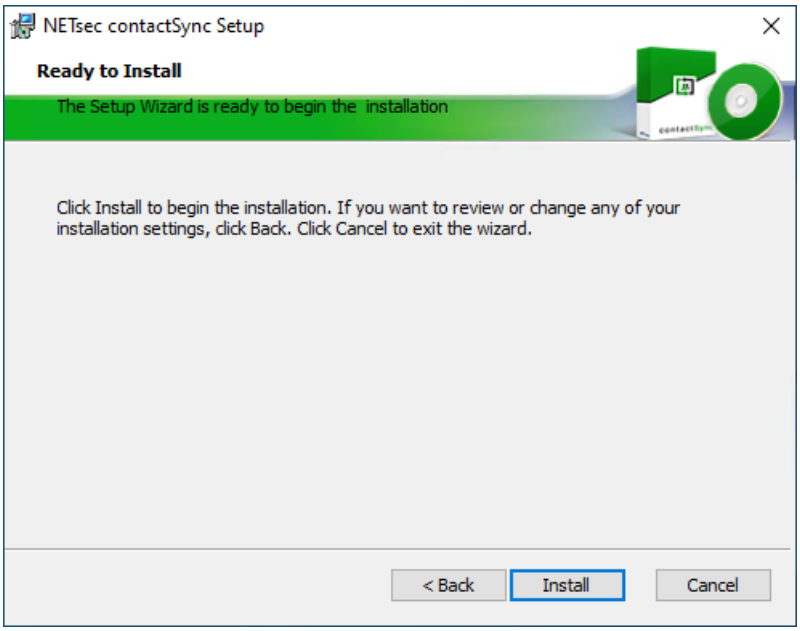
Accept third party license agreement to use the libraries and tools, then click **Next**



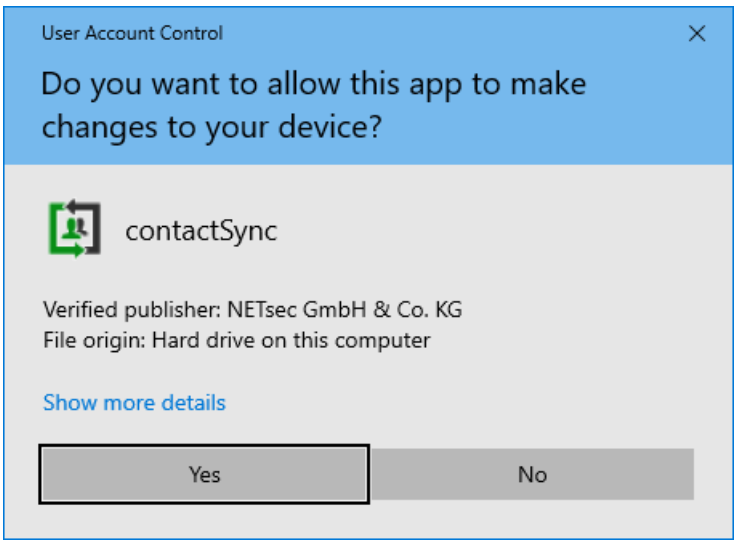
Select the install path for the contactSync binaries, then click **Next**



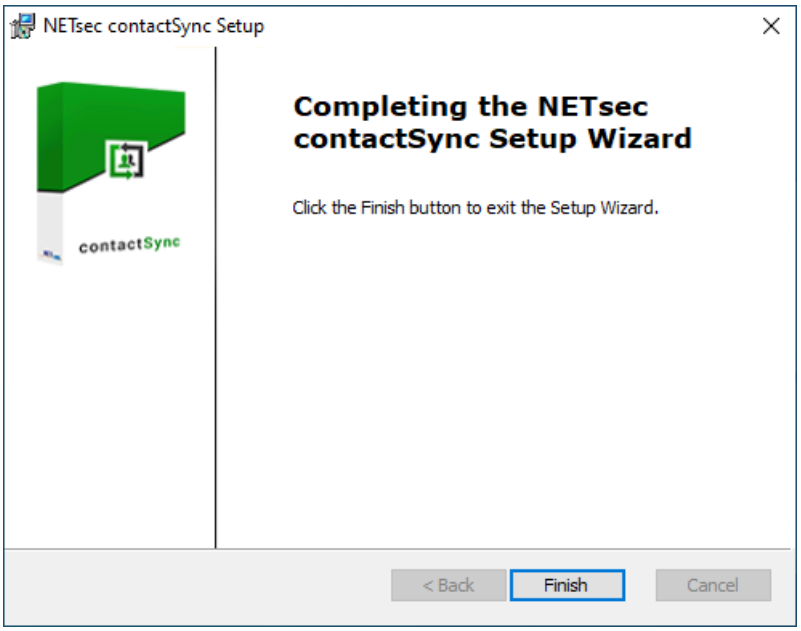
Click **Install**



Click **Yes**, if prompted



Click **Finish**

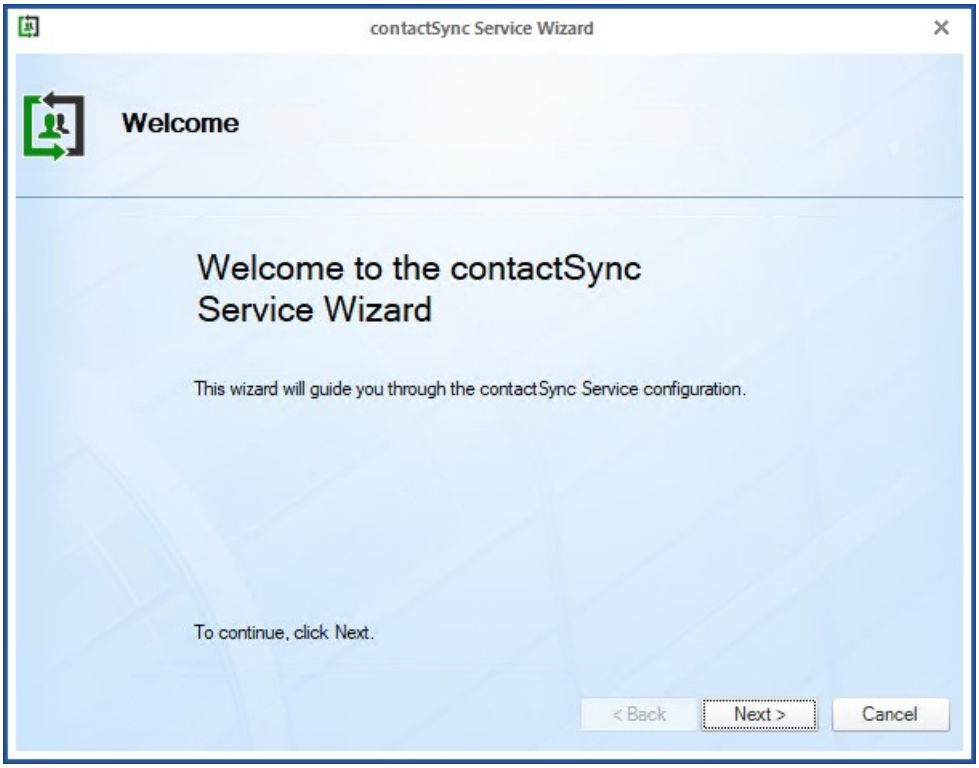


Configure contactSync Service

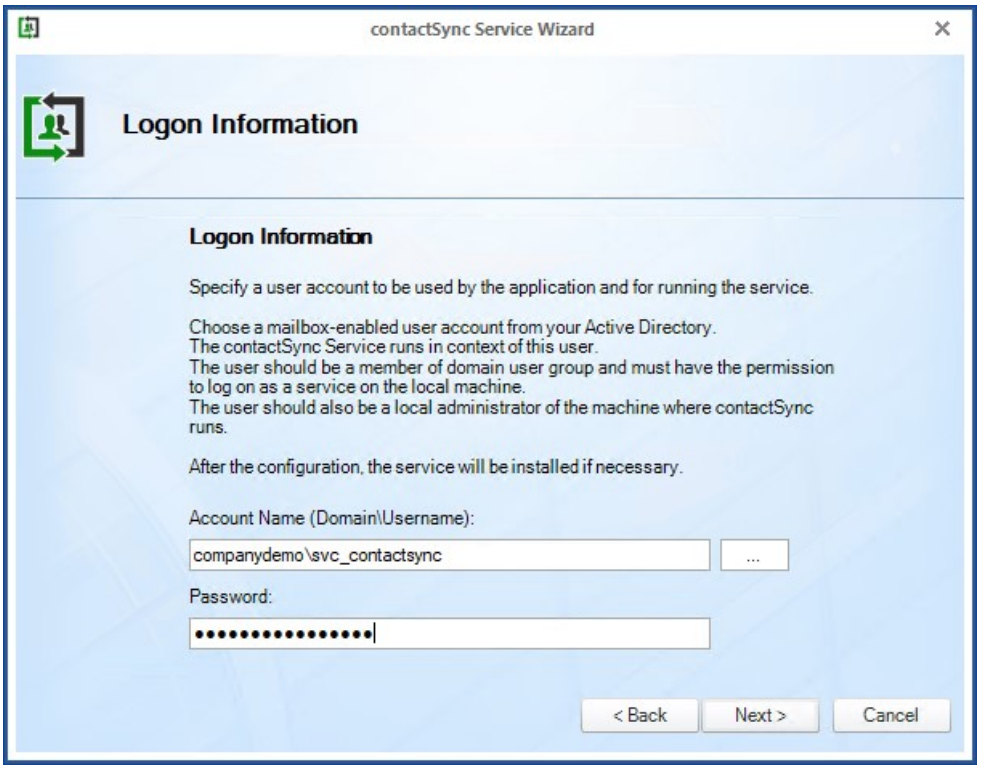
To launch contactSync, click the **NETsec contactSync** shortcut on the desktop.

When opened for the first time, the contactSync Service Wizard will open, prompting the user to enter the contactSync Service account credentials.

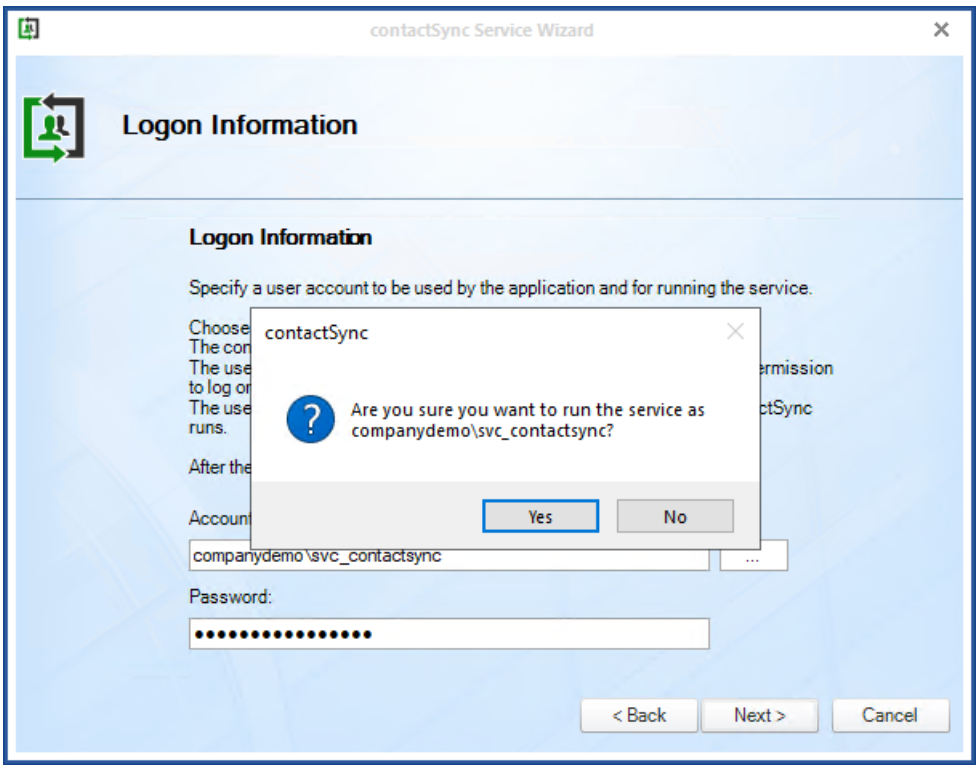
Click **Next**



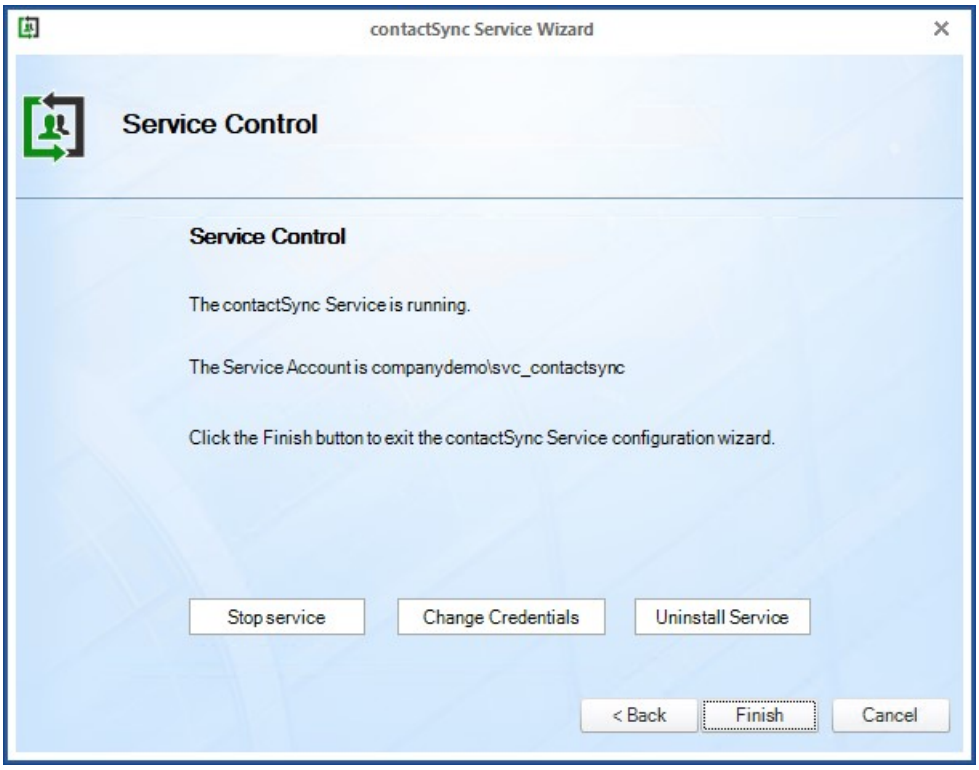
Enter the account credentials in **Domain\Username** format, then click **Next**.



If authentication is successful, the user is prompted to confirm the is the correct account to use. Click **Yes**, then click **Next**.

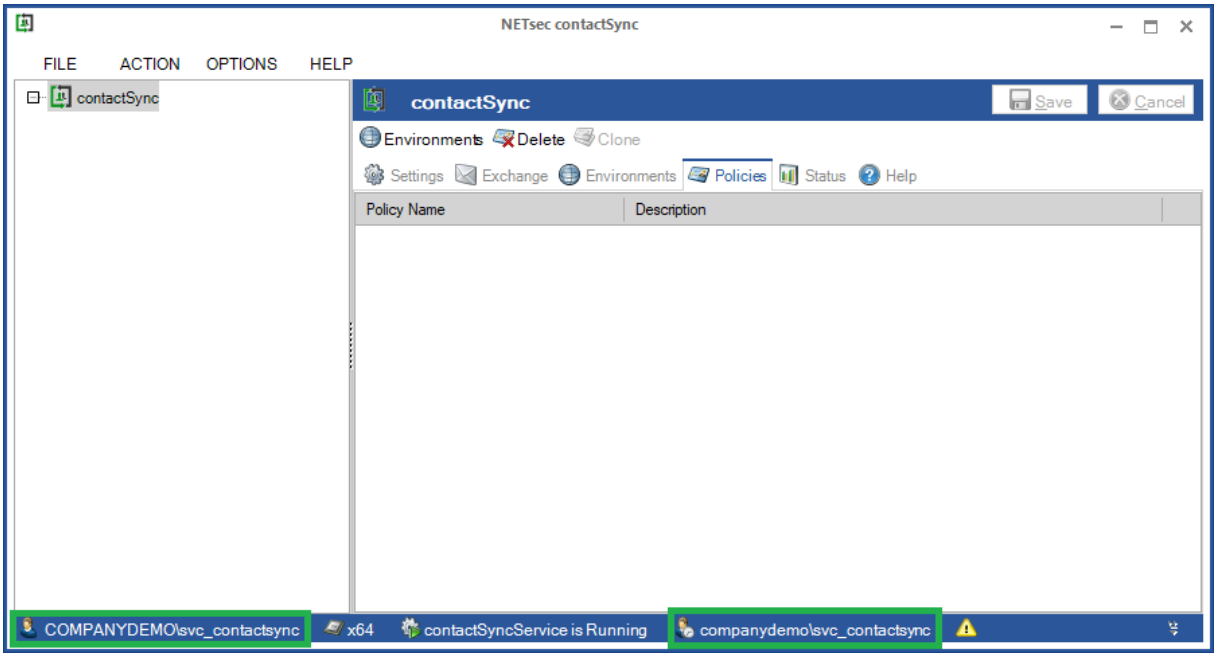


Click **Finish**.



The contactSync user interface opens upon completion of this wizard.

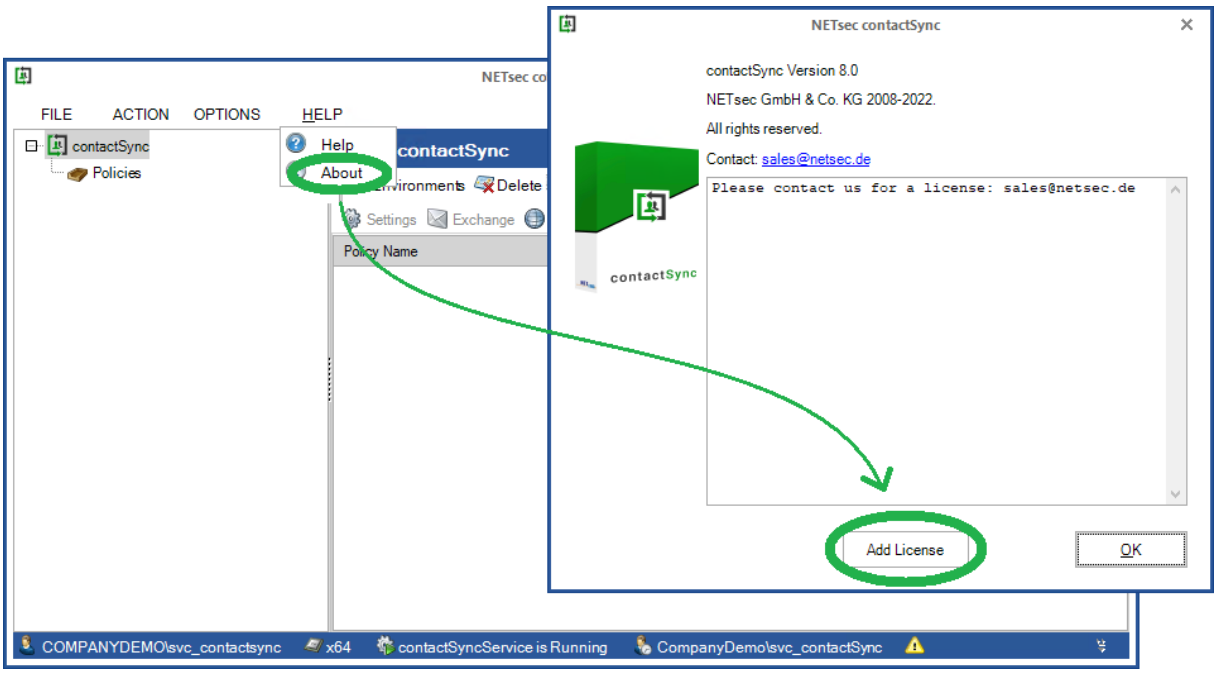
The bottom of the interface displays the current logged on user (on the left) and the contactSync user account (on the right).



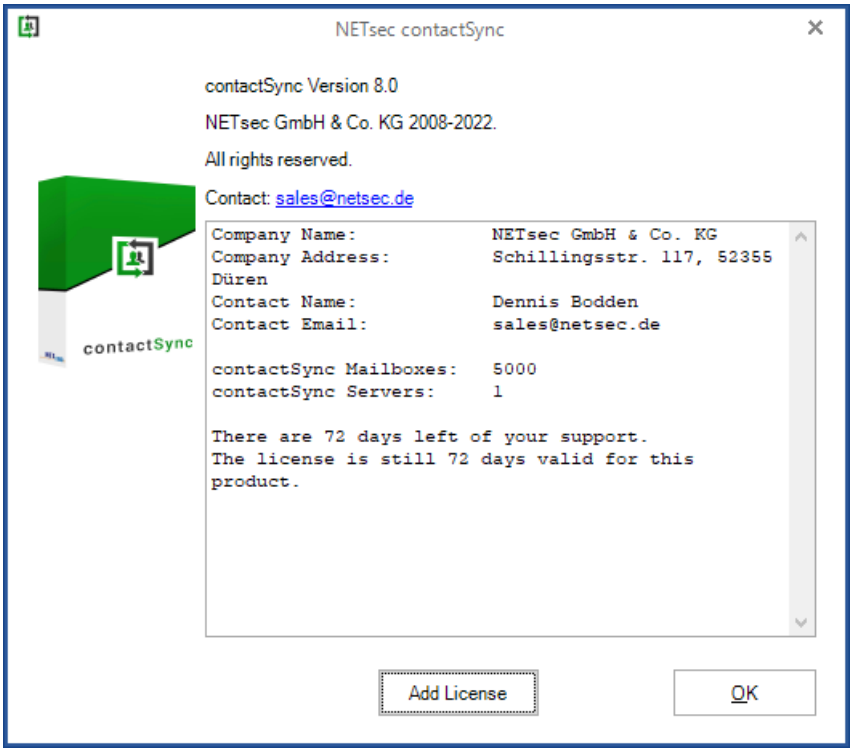
Apply contactSync License

Click the Help menu, then **About**

Click **Add license**, then browse to the location where the contactSync license was saved on the server, then select it and click **Open**.



Click **OK** to apply the license.



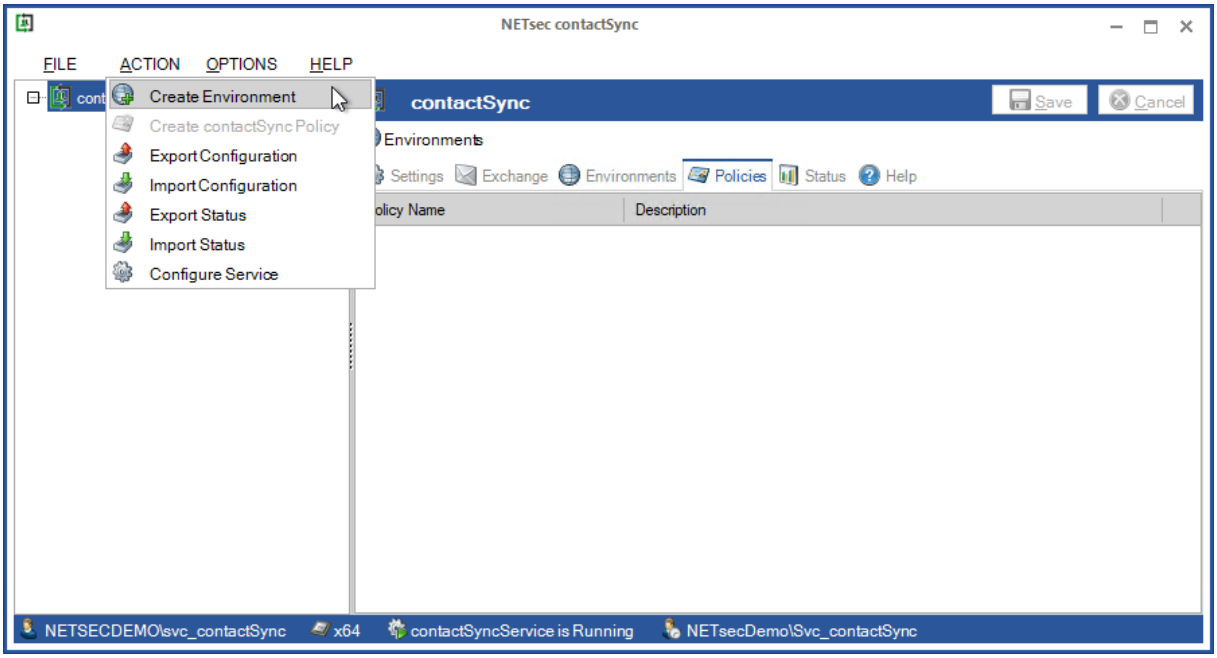
Create an Environment Configuration

Create an Environment Configuration for on-premises Exchange environment

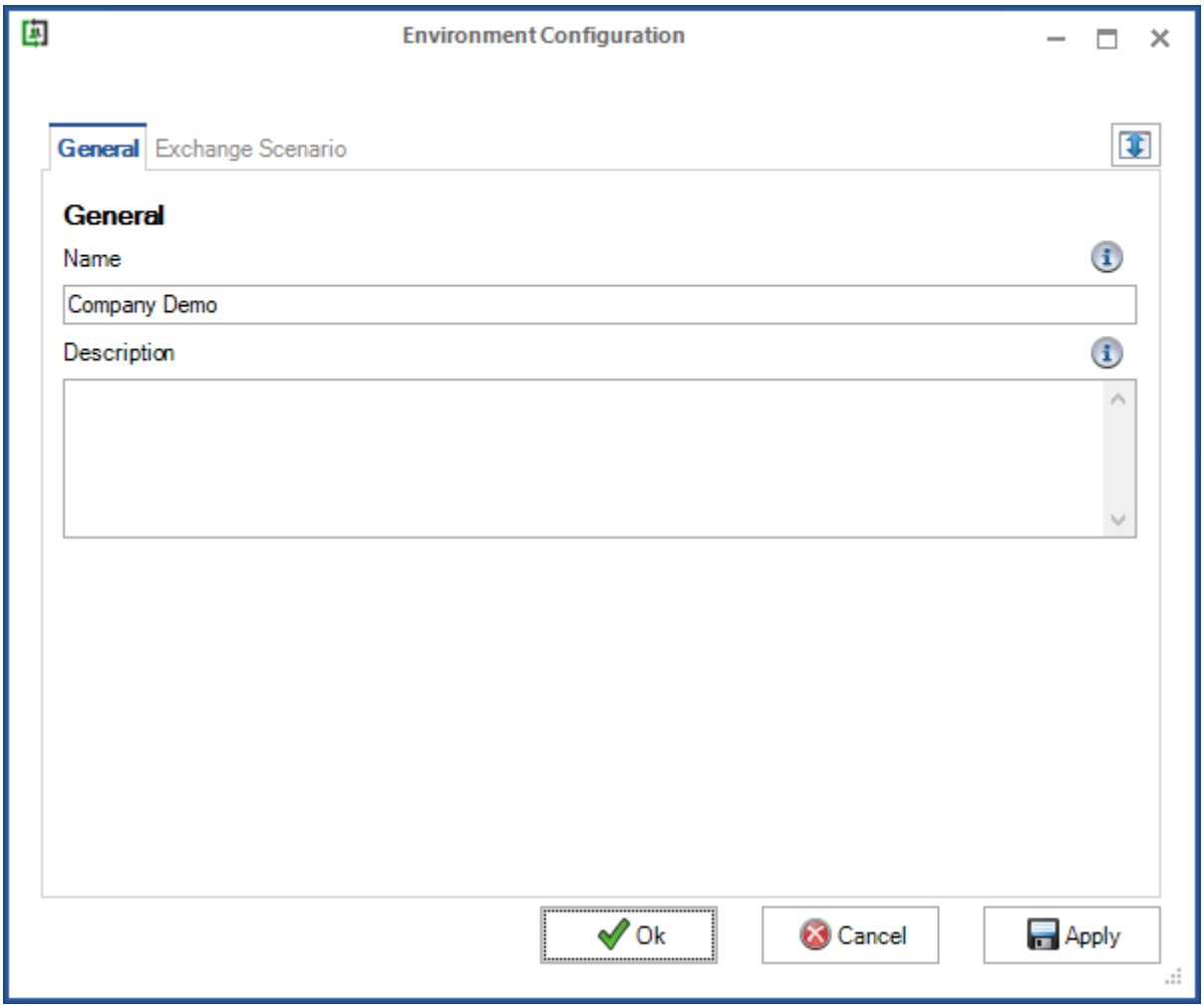
First, please verify the contactSync GUI is running in the credentials of the local contactSync service account, otherwise contactSync cannot access its mailbox.

This can be confirmed on the information bar at the bottom of the contactSync GUI.

From the **Action** menu select **Create Environment**.

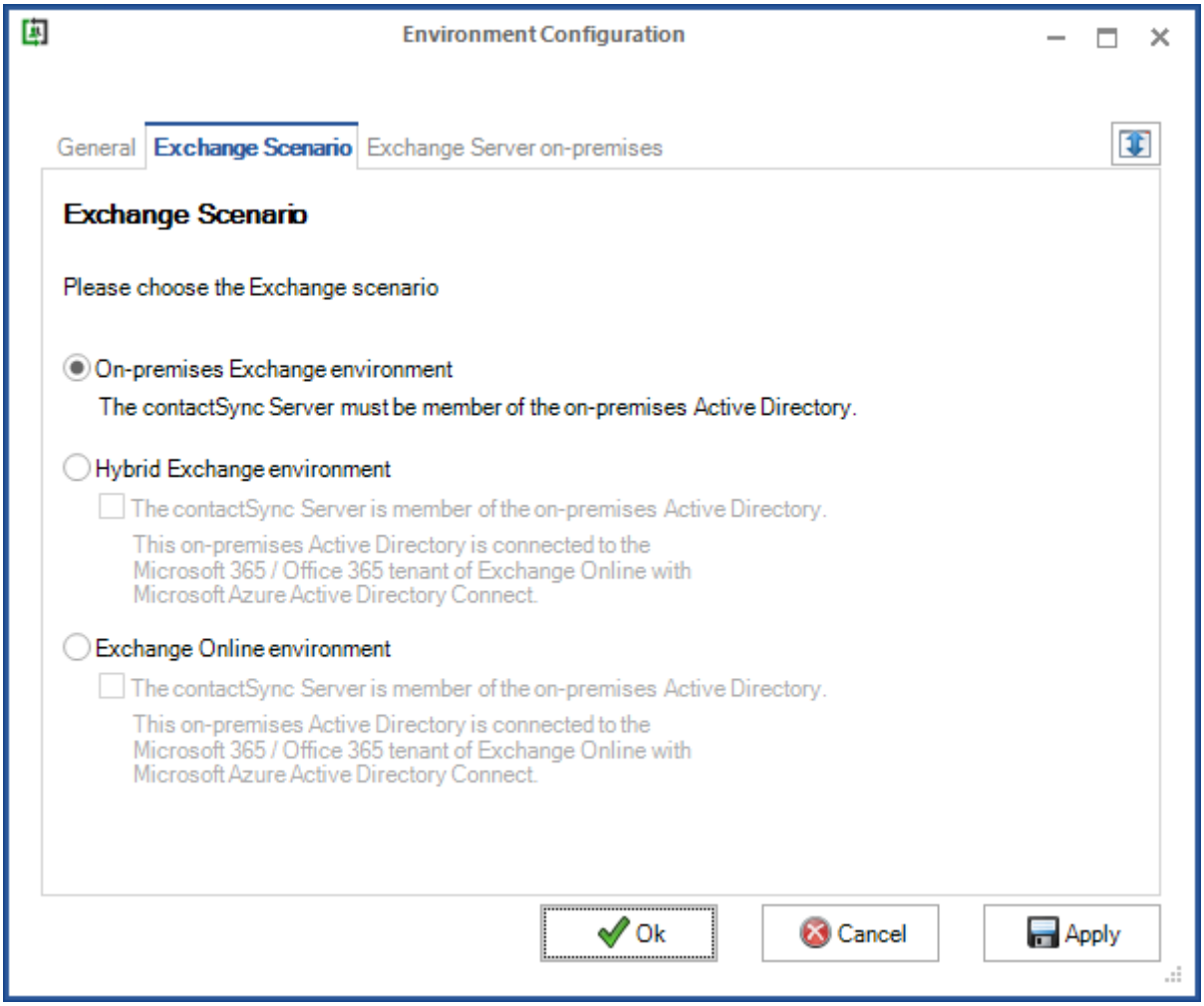


In the **General** tab, enter a name for the environment and optional description.



Click the **Exchange Scenario** tab, and select the **On-premises Exchange environment**.

When an 'On-premises Exchange environment' is selected, contactSync will authenticate to the mailbox of the account that runs the contactSync service.

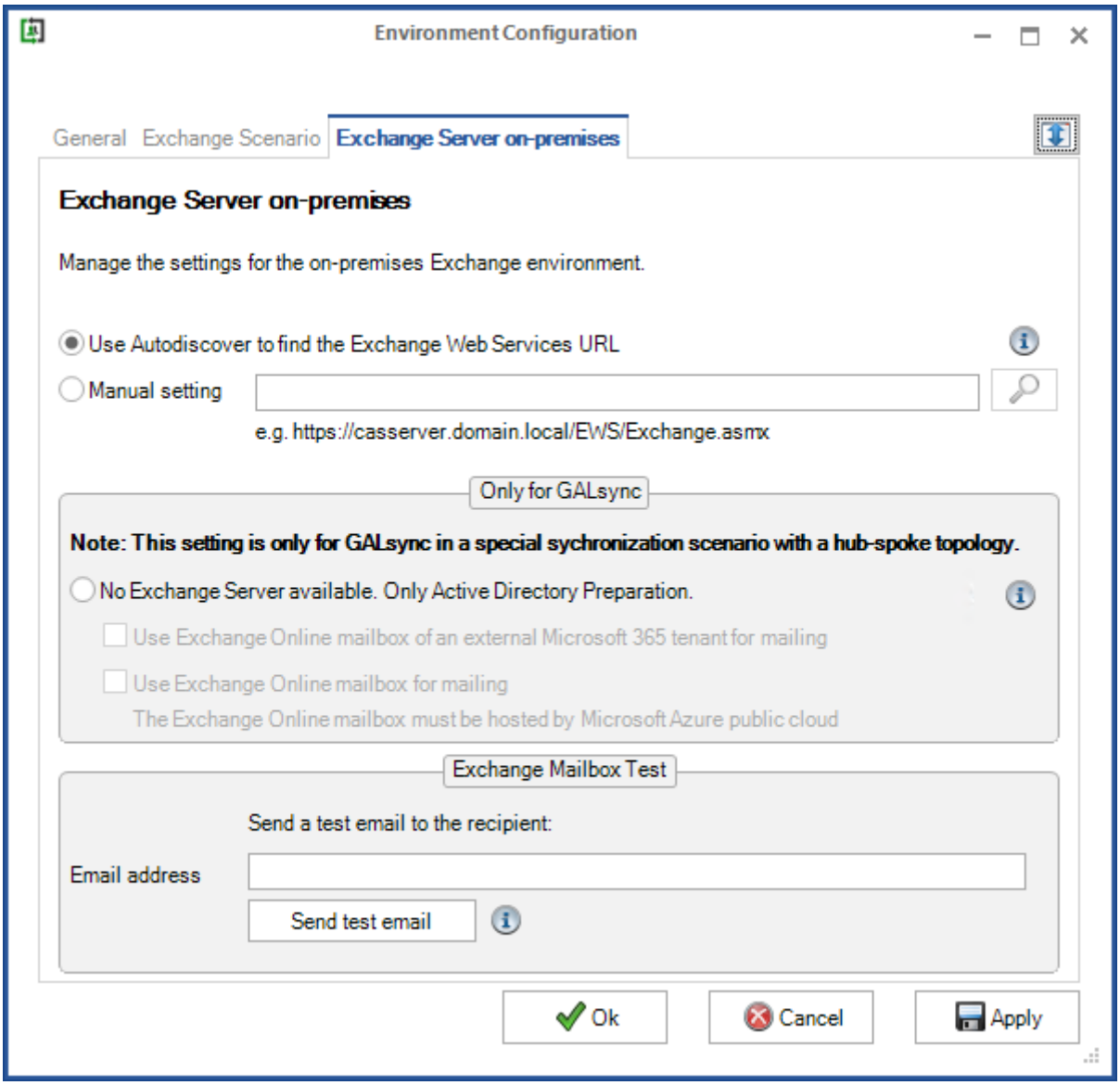


Select the **Exchange Server on-premises** tab.

To verify connectivity to the mailbox, enter a recipient email then click **Send test email**.

Autodiscover is used by default to locate the Exchange Web Services URL and connect to its mailbox. If an error is returned which indicates the EWS URL cannot be resolved, a manual setting has been provided to enter a valid Exchange Web Services URL, such as the one shown below, which resolves the issue in most situations.

If the connection to the mailbox is successful, a test email will be sent to the specified recipient, and a popup message similar to the one below will be returned.



Apply the changes, then click **OK**.

Account for access to the on-premises Exchange mailboxes

contactSync uses the local contactSync service account to access the on-premises Exchange mailboxes by default.

Please verify the contactSync GUI and the contactSyncService is always running in the credentials of the local contactSync service account.

This can be confirmed on the information bar at the bottom of the contactSync GUI.

In this case contactSync requires the **Exchange Application Impersonation** role in on-premises Exchange for this service account to access the on-premises Exchange mailboxes.

contactSync can also use a dedicated on-premises Exchange mailbox user, which has the **Exchange Application Impersonation** role in the on-premises Exchange to access the on-premises Exchange mailboxes.

Please take a look at the chapter:

How to configure Exchange Application Impersonation

Create an Environment Configuration for Hybrid Exchange environment

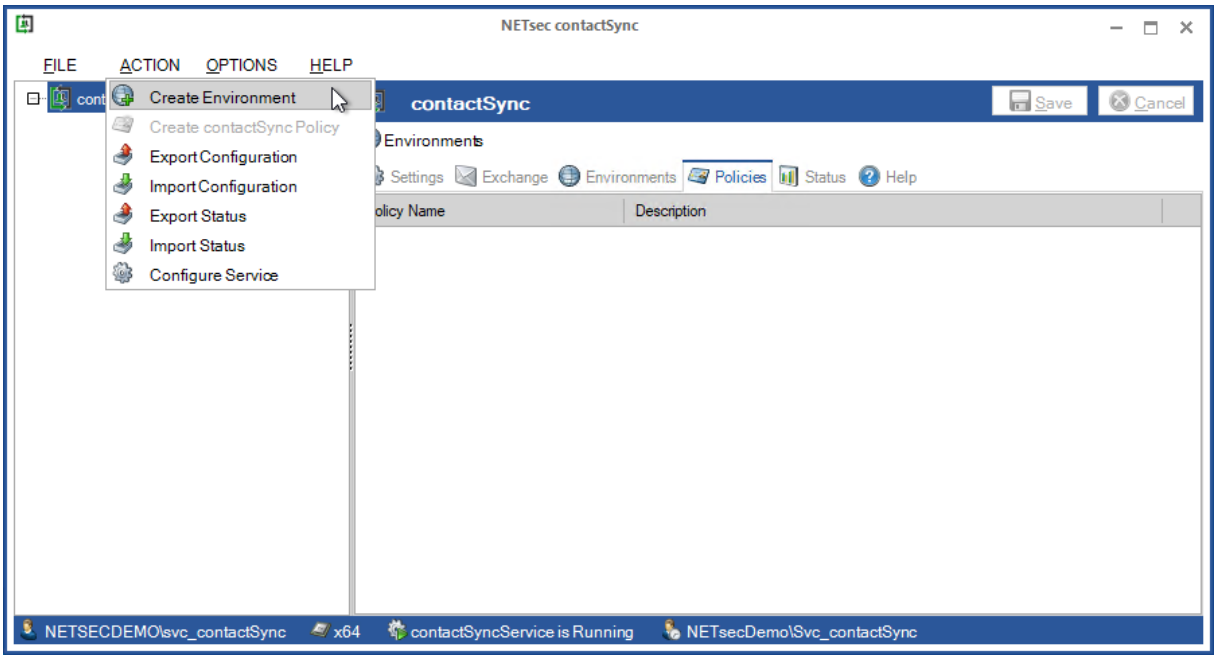
First, please verify the contactSync GUI is running in the credentials of the local contactSync service account, otherwise contactSync cannot access its mailbox and cannot communicate with Exchange Online.

This can be confirmed on the information bar at the bottom of the contactSync GUI.

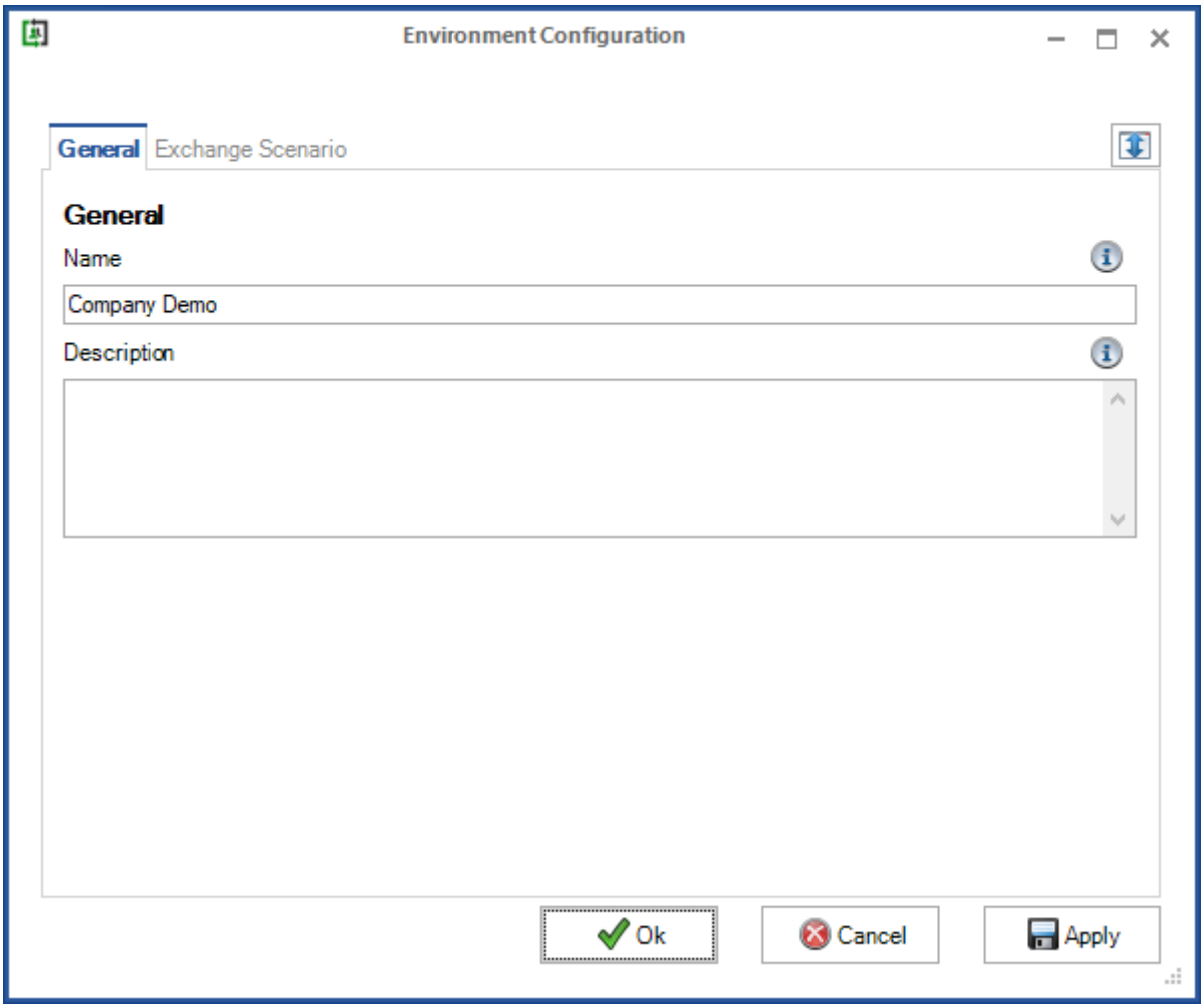
Important: When creating an environment, it is necessary that you logon to the contactSync server as the contactSync Service account. contactSync uses Windows authentication when accessing its mailbox (when on-premises). When creating an Exchange Online environment with certificate-based authentication the certificate will be stored in the certificate store of the current logged on user. The contactSync account will not be able to find and read the certificate when logged on as a different user.

If your Exchange Environment is a hybrid, you have the option to establish your synchronization focal point to either on-premises Exchange (Active Directory), or Exchange Online. A connection to on-premises Exchange and Exchange Online is configured in a hybrid environment. Since on-premises Active Directory hosts the master copy of all objects synced through Azure AD Connect, it is recommended an on-premises connection is used.

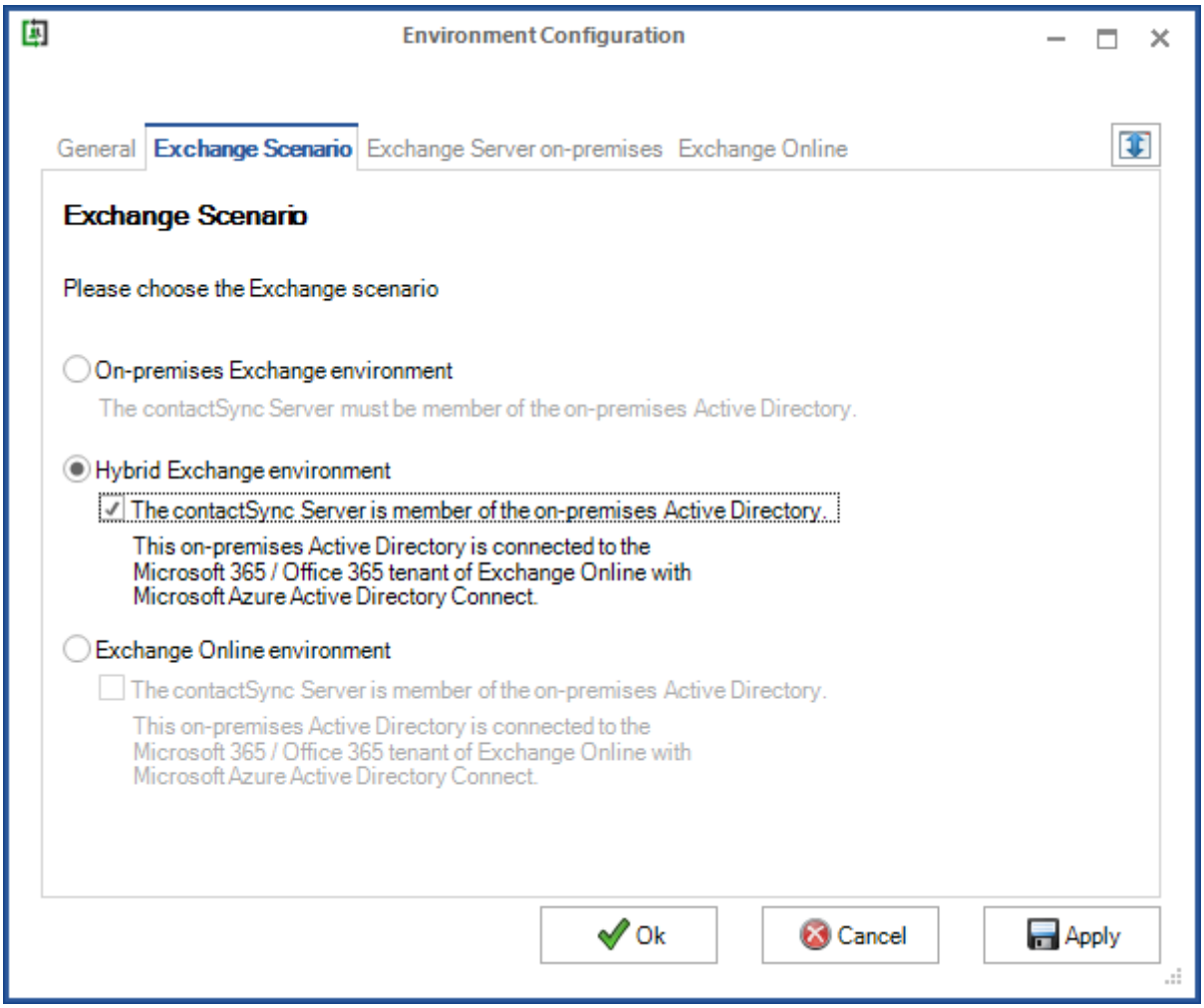
From the **Action** menu select **Create Environment**.



In the **General** tab, enter a name for the environment and optional description.



Click the **Exchange Scenario** tab, then select **Hybrid Exchange environment**. The **Exchange Online** tab will be displayed. After checking the checkbox: **The contactSync Server is a member of the on-premises Active Directory**, the **Exchange Server on-premises** tab will be displayed. Select this tab.



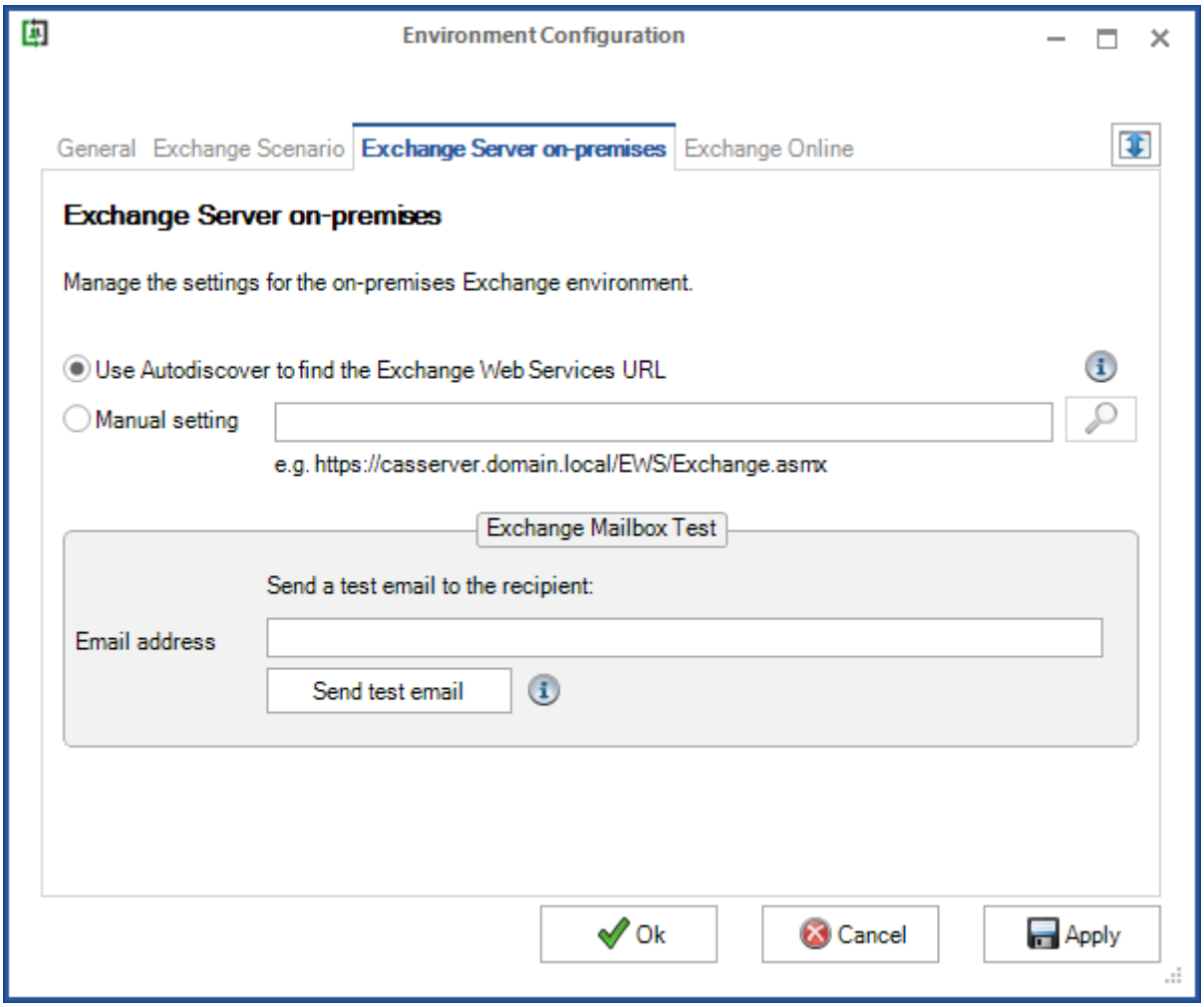
Select the **Exchange Server on-premises** tab.

contactSync connects to the on-premises mailbox of the contactSync service account. To test this connection, enter a recipient email address and click **Send test email**.

Autodiscover is used by default to locate the Exchange Web Services URL and connect to its mailbox. If an error is returned which indicates the EWS URL cannot be resolved, a manual setting has been provided to enter a valid Exchange Web Services URL, such as the one shown below, which resolves the issue in most situations.

Please note: If the mailbox of the contactSync on-premises service account is located in Exchange Online, it will be necessary to enter the Exchange Web Services URL for the on-premises Exchange Server.

A popup will be returned similar to the one below upon a successful connection to the contactSync mailbox, indicating the email was successfully sent to the target mailbox.



Account for access to the on-premises Exchange mailboxes

contactSync uses the local contactSync service account to access the on-premises Exchange mailboxes by default.

Please verify the contactSync GUI and the contactSyncService is always running in the credentials of the local contactSync service account.

This can be confirmed on the information bar at the bottom of the contactSync GUI.

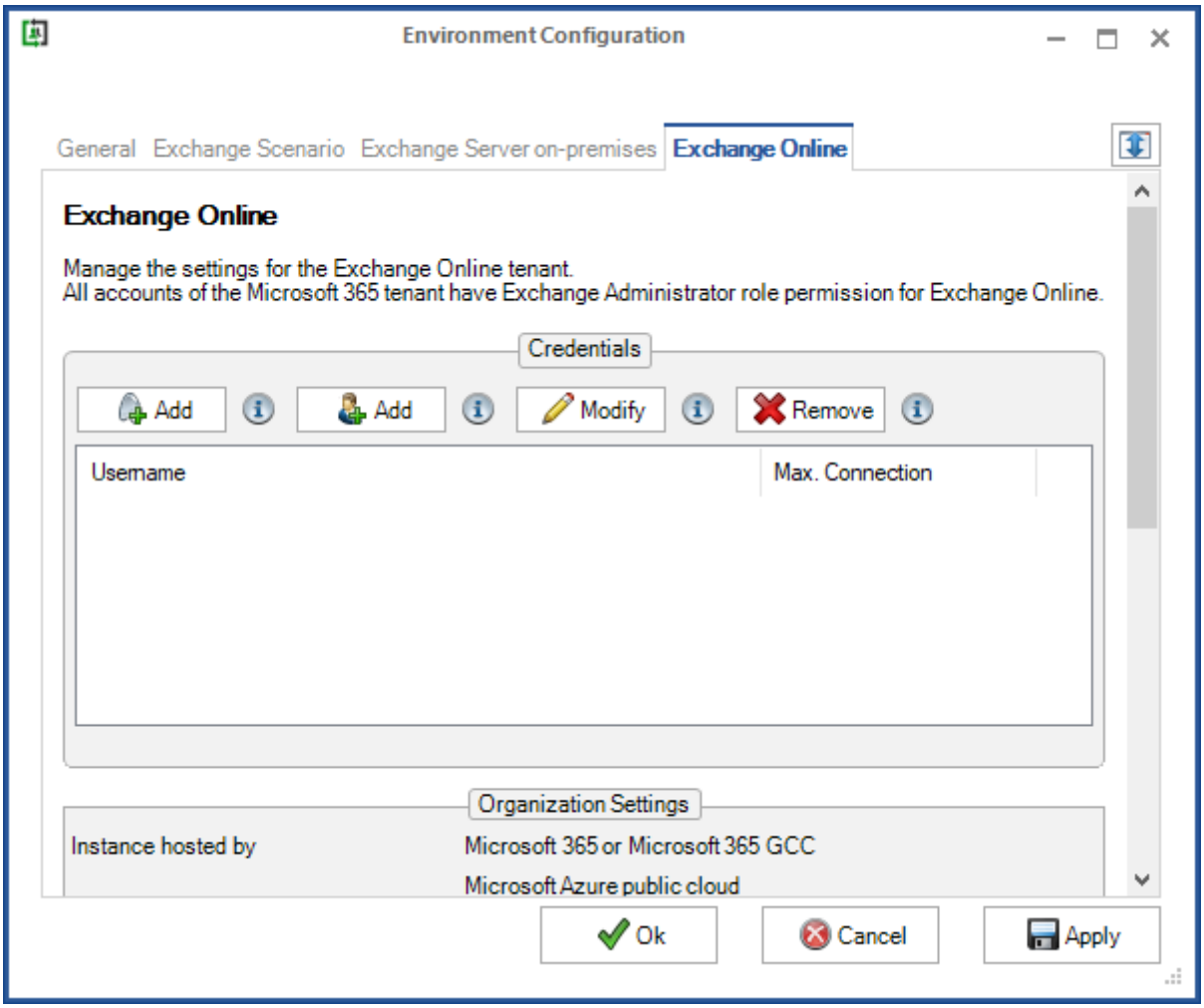
In this case contactSync requires the **Exchange Application Impersonation** role in on-premises Exchange for this service account to access the on-premises Exchange mailboxes.

contactSync can also use a dedicated on-premises Exchange mailbox user, which has the **Exchange Application Impersonation** role in the on-premises Exchange to access the on-premises Exchange mailboxes.

Please take a look at the chapter:

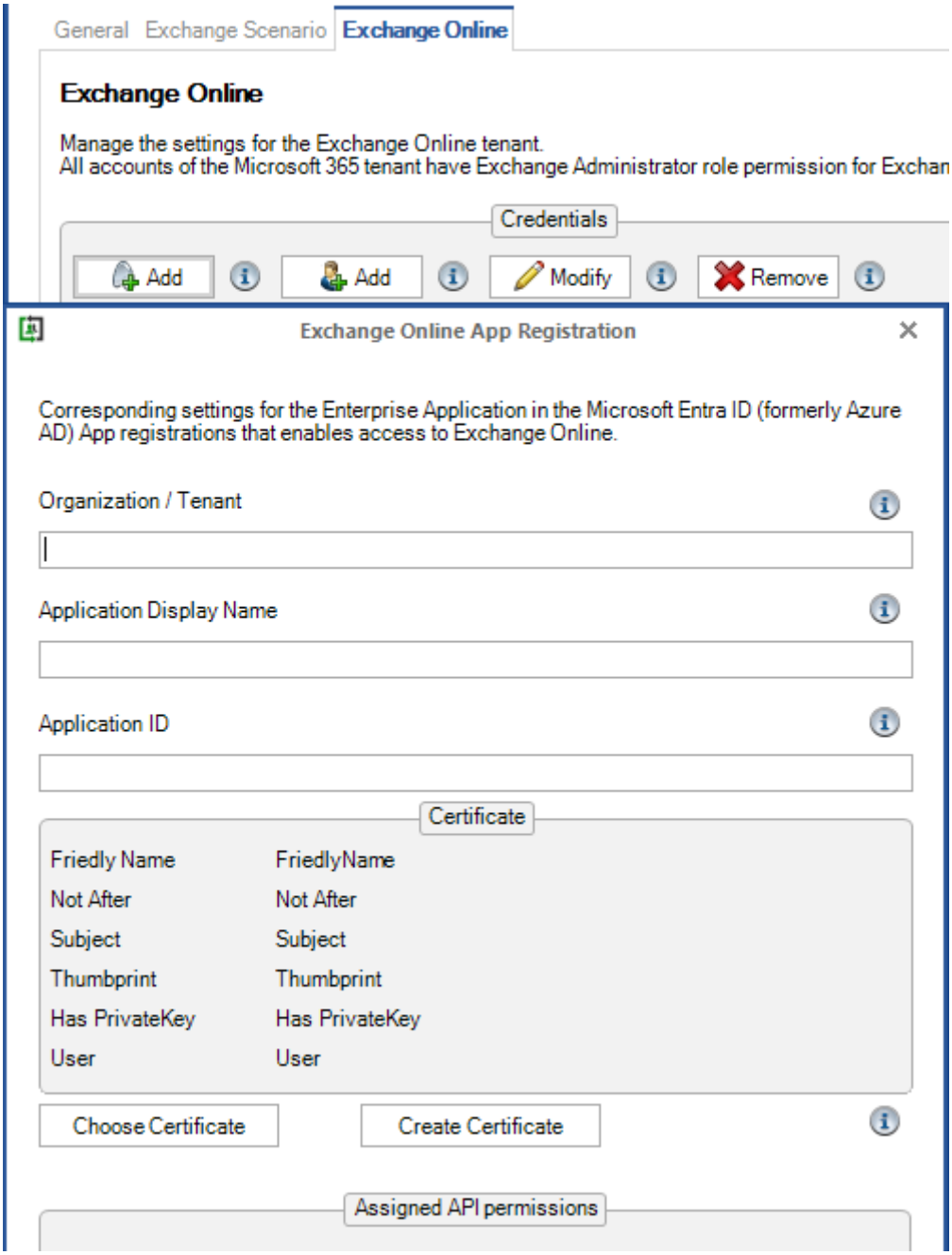
How to configure Exchange Application Impersonation

Select the **Exchange Online** tab.



There are two available methods to establish a connection to Exchange Online.

1. The **Add** button on the left, will open a dialog window in which to configure **certificate-based authentication** via **App registration** for the Exchange Online tenant.

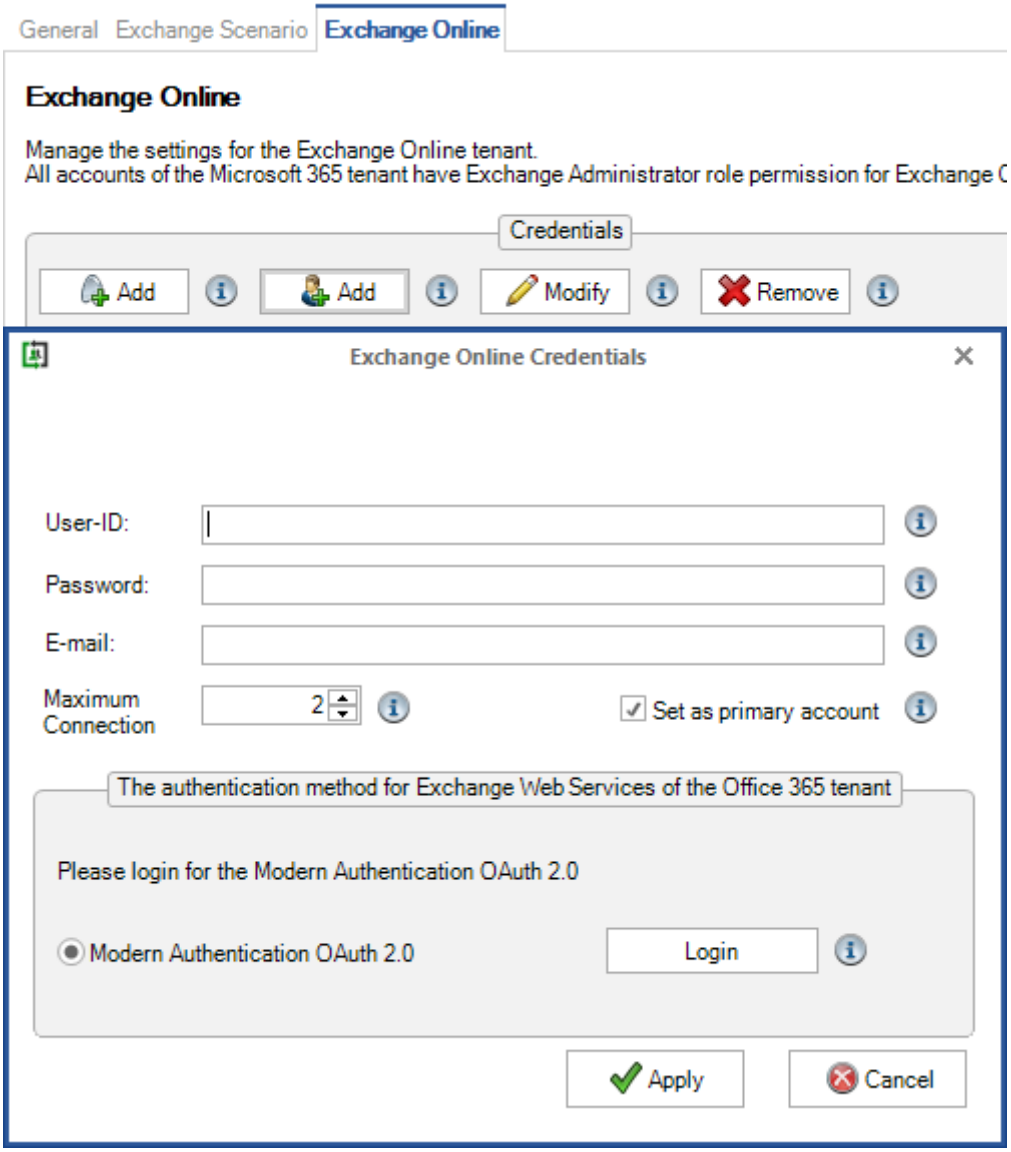


A detailed description is in chapter
Exchange Online certificate-based authentication via App Registration

2. The **Add** button on the right, will open a dialog window in which to configure **user-based authentication** via **Service Account** for the Exchange Online tenant.

Note, the user-based authentication is deprecated. The certificate-based authentication is recommended.

Please note, that user-based authentication via OAuth 2.0 works only for the Microsoft Azure Public Cloud instance. If your Microsoft 365/Office 365 instance is hosted by a national cloud, please configure **Exchange Online certificate-based authentication via App Registration**.



A detailed description is in chapter
Exchange Online authentication via Service Account

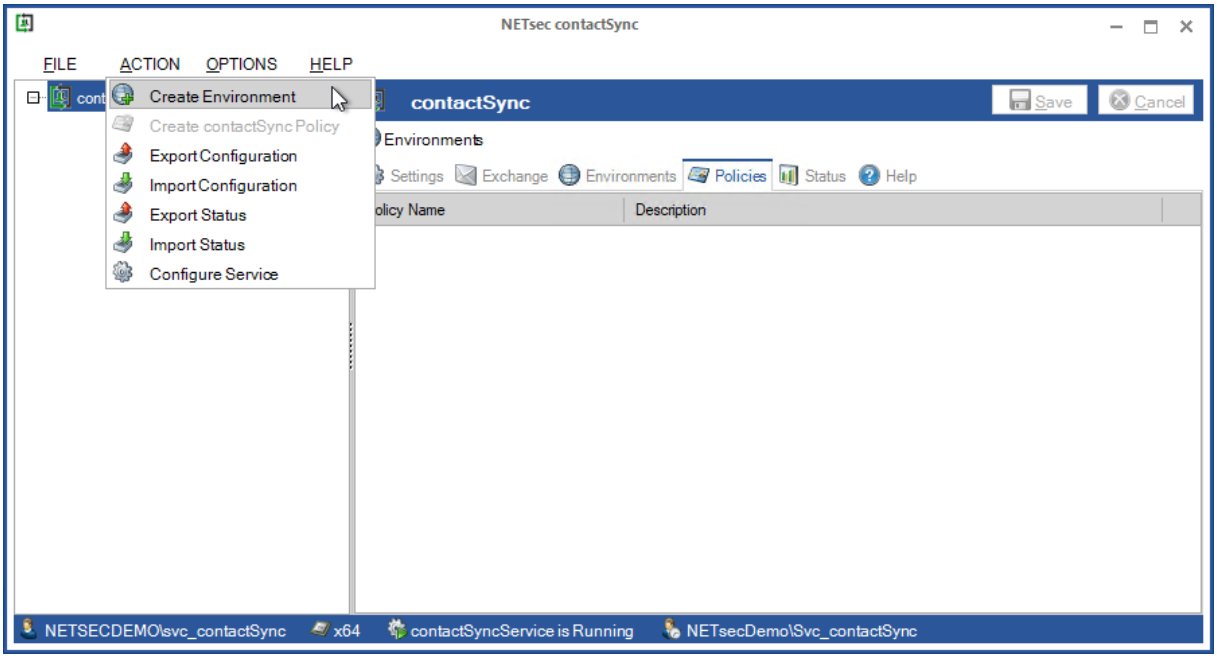
Create Environment Configuration for Exchange Online environment

First, please verify the contactSync GUI is running in the credentials of the local contactSync service account, otherwise contactSync cannot communicate with Exchange Online.

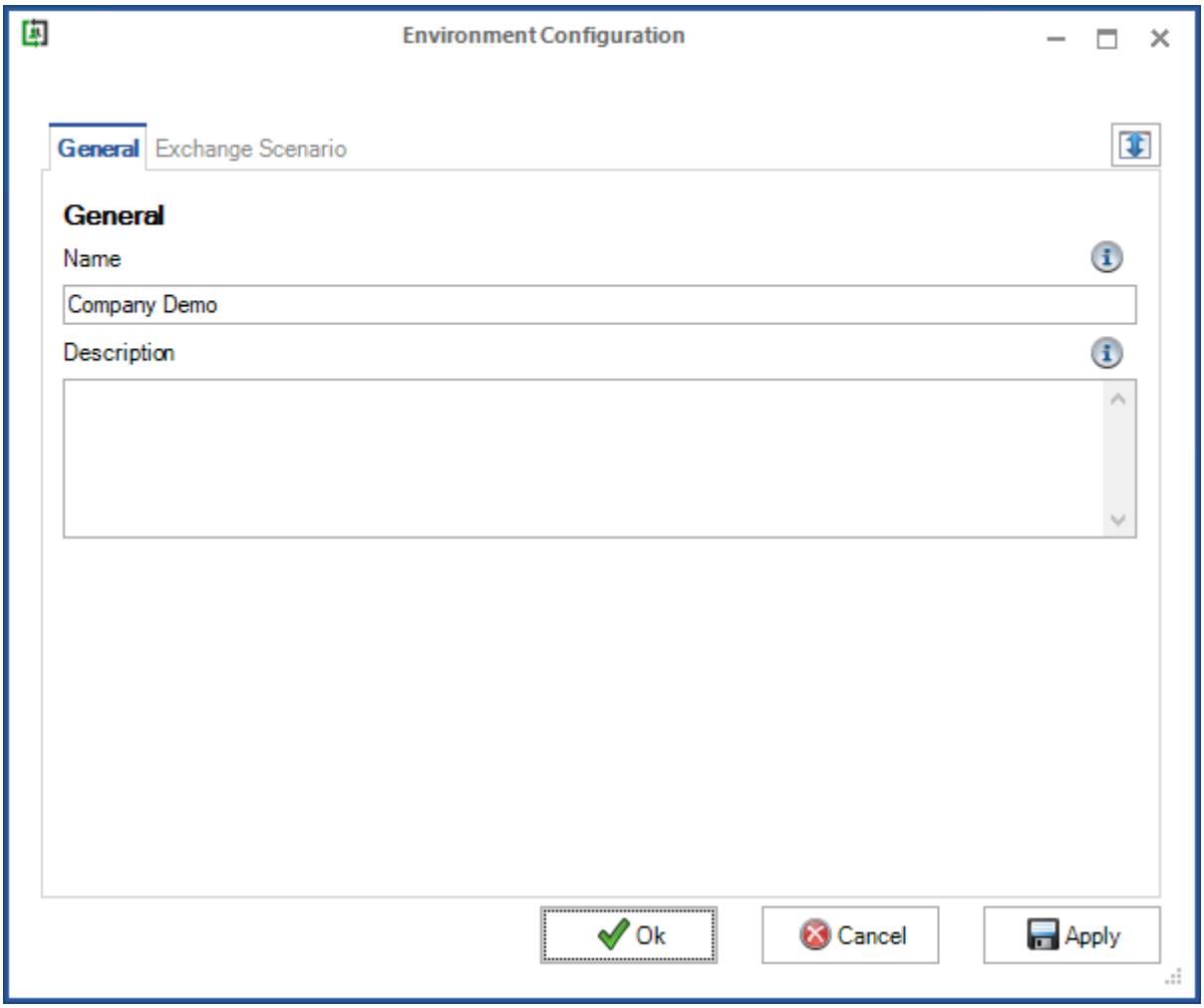
This can be confirmed on the information bar at the bottom of the contactSync GUI.

Important: When creating an environment, it is necessary that you logon to the contactSync server as the contactSync Service account. contactSync uses Windows authentication when accessing its mailbox (when on-premises). When creating an Exchange Online environment with certificate-based authentication the certificate will be stored in the certificate store of the current logged on user. The contactSync account will not be able to find and read the certificate when logged on as a different user.

From the **Action** menu select **Create Environment**.

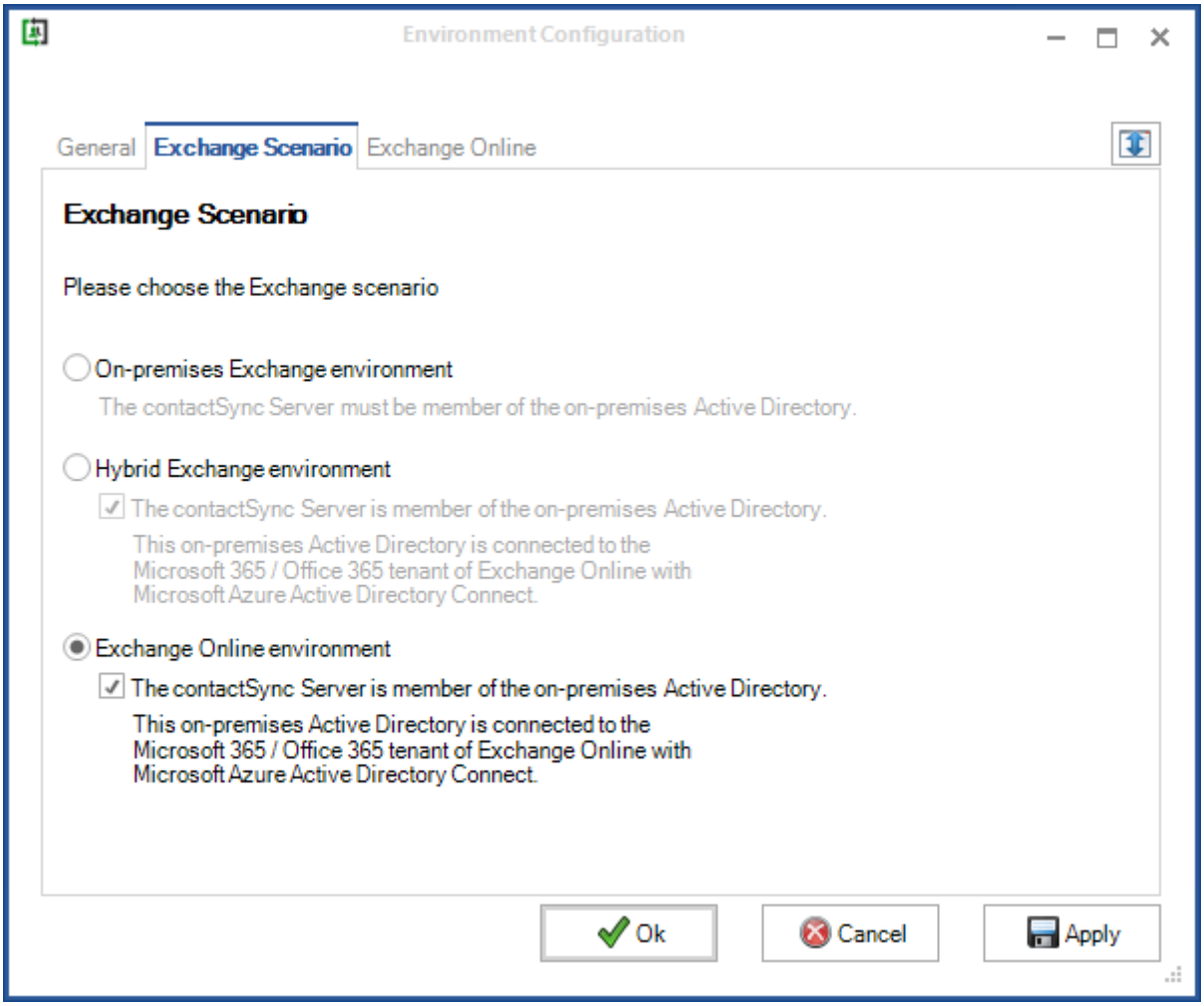


In the **General** tab, enter a name for the environment and an optional description.

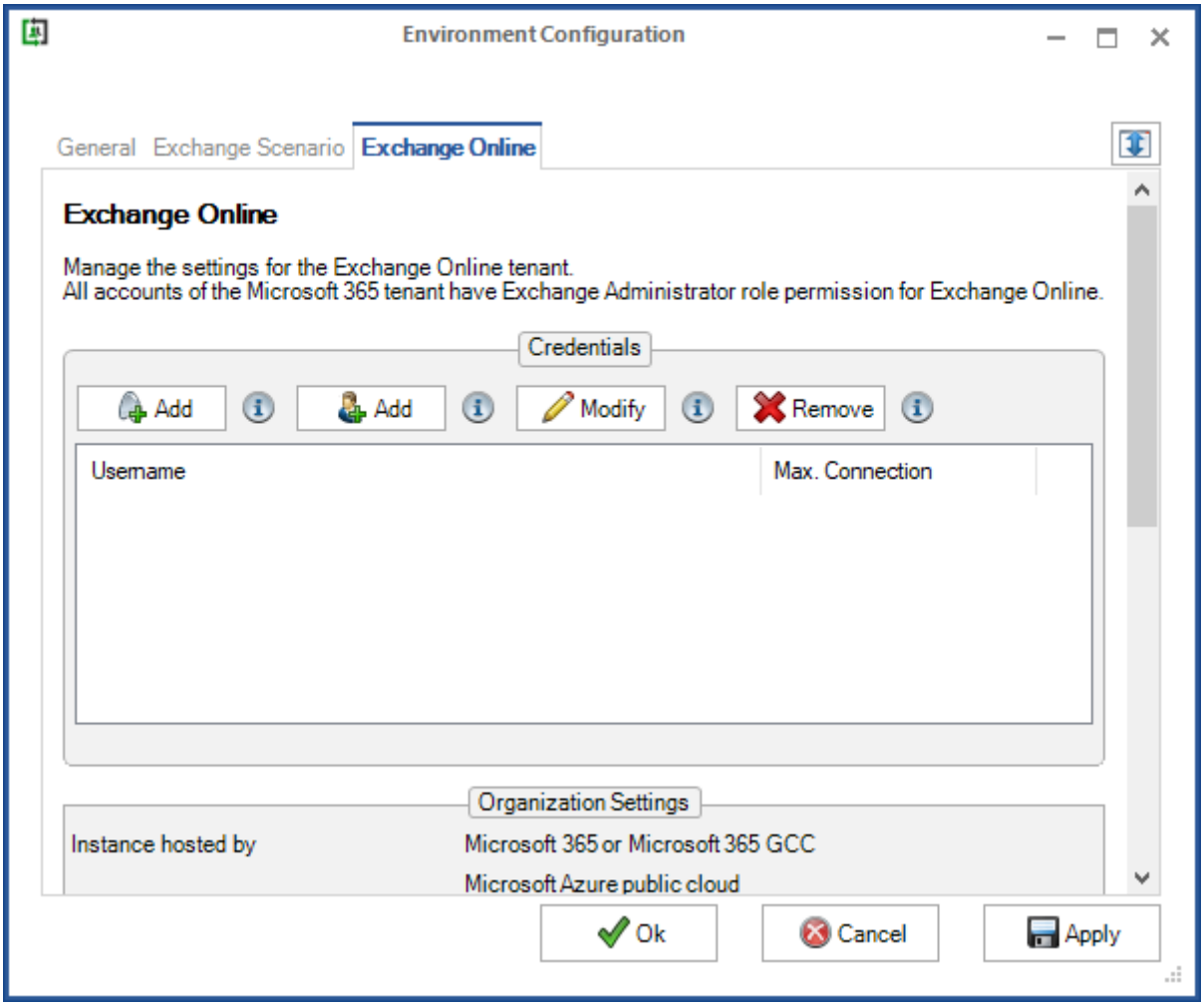


Select the **Exchange Scenario** tab, then select **Exchange Online environment**.

Check **The contactSync server is a member of the on-premises Active Directory**, if applicable.

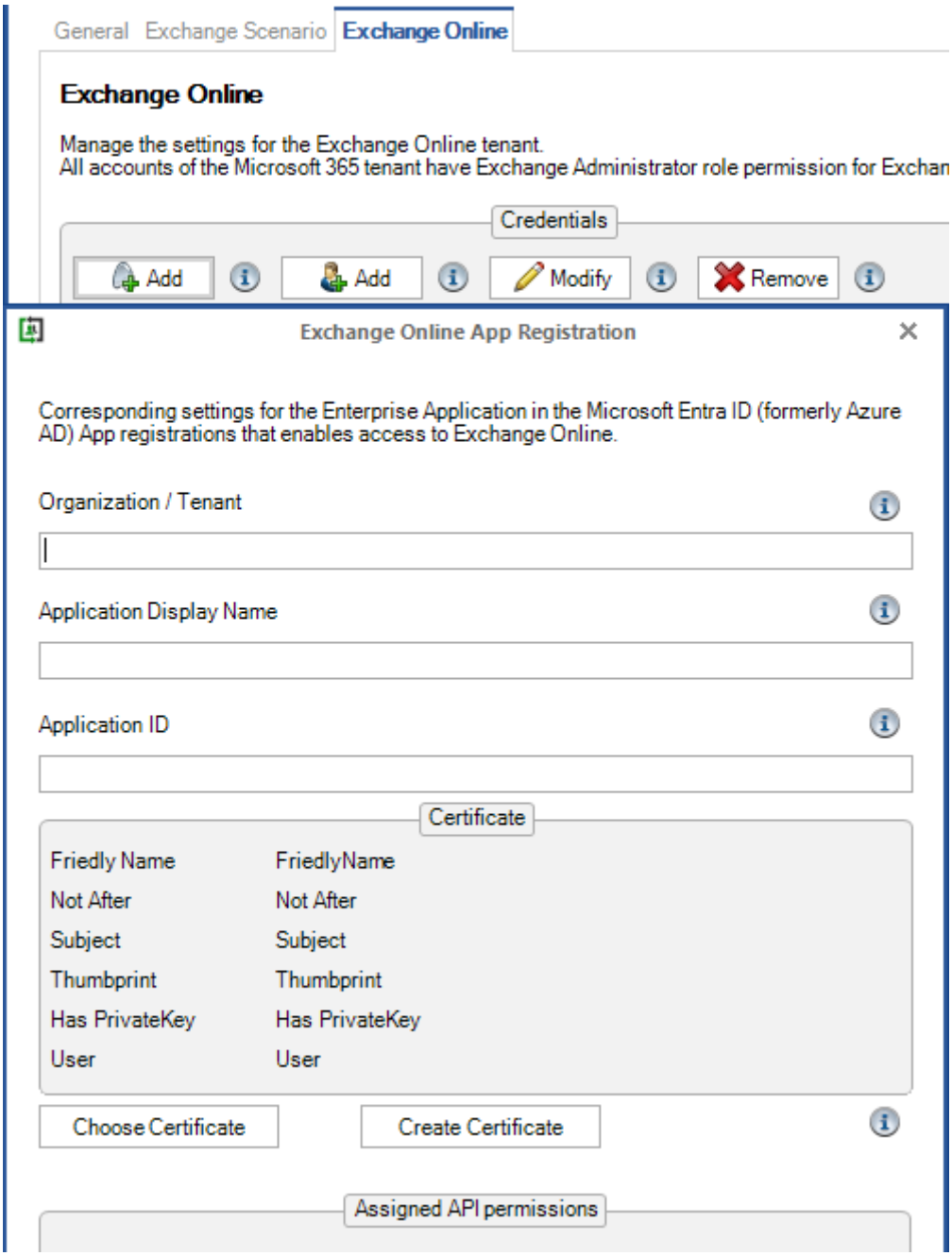


Select the **Exchange Online** tab.



There are two available methods to establish a connection to Exchange Online.

1. The **Add** button on the left, will open a dialog window in which to configure **certificate-based authentication** via **App registration** for the Exchange Online tenant.

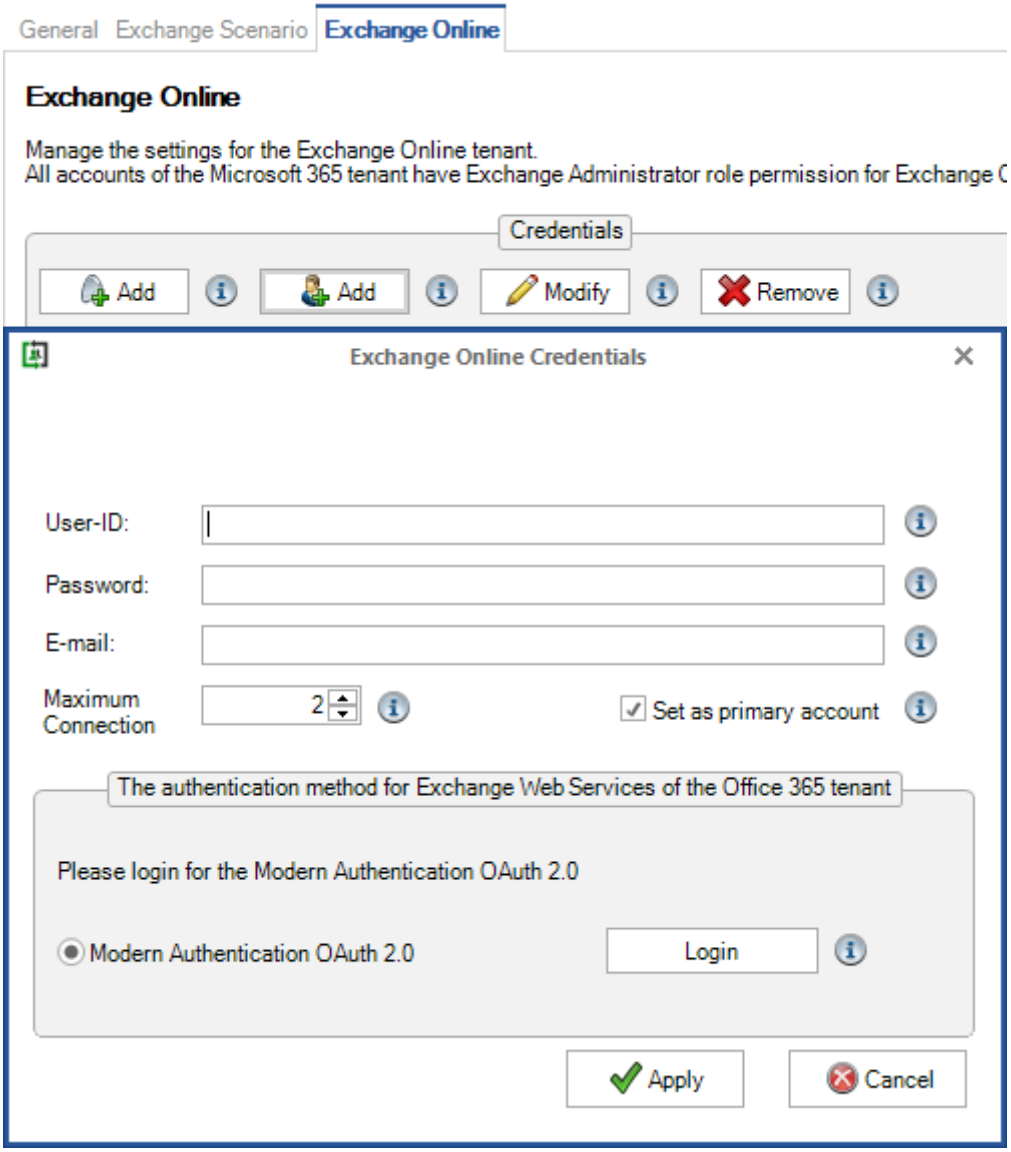


A detailed description is in chapter
Exchange Online certificate-based authentication via App Registration

2. The **Add** button on the right, will open a dialog window in which to configure **user-based authentication** via **Service Account** for the Exchange Online tenant.

Note, the user-based authentication is deprecated. The certificate-based authentication is recommended.

Please note, that user-based authentication via OAuth 2.0 works only for the Microsoft Azure Public Cloud instance. If your Microsoft 365/Office 365 instance is hosted by a national cloud, please configure **Exchange Online certificate-based authentication via App Registration**.



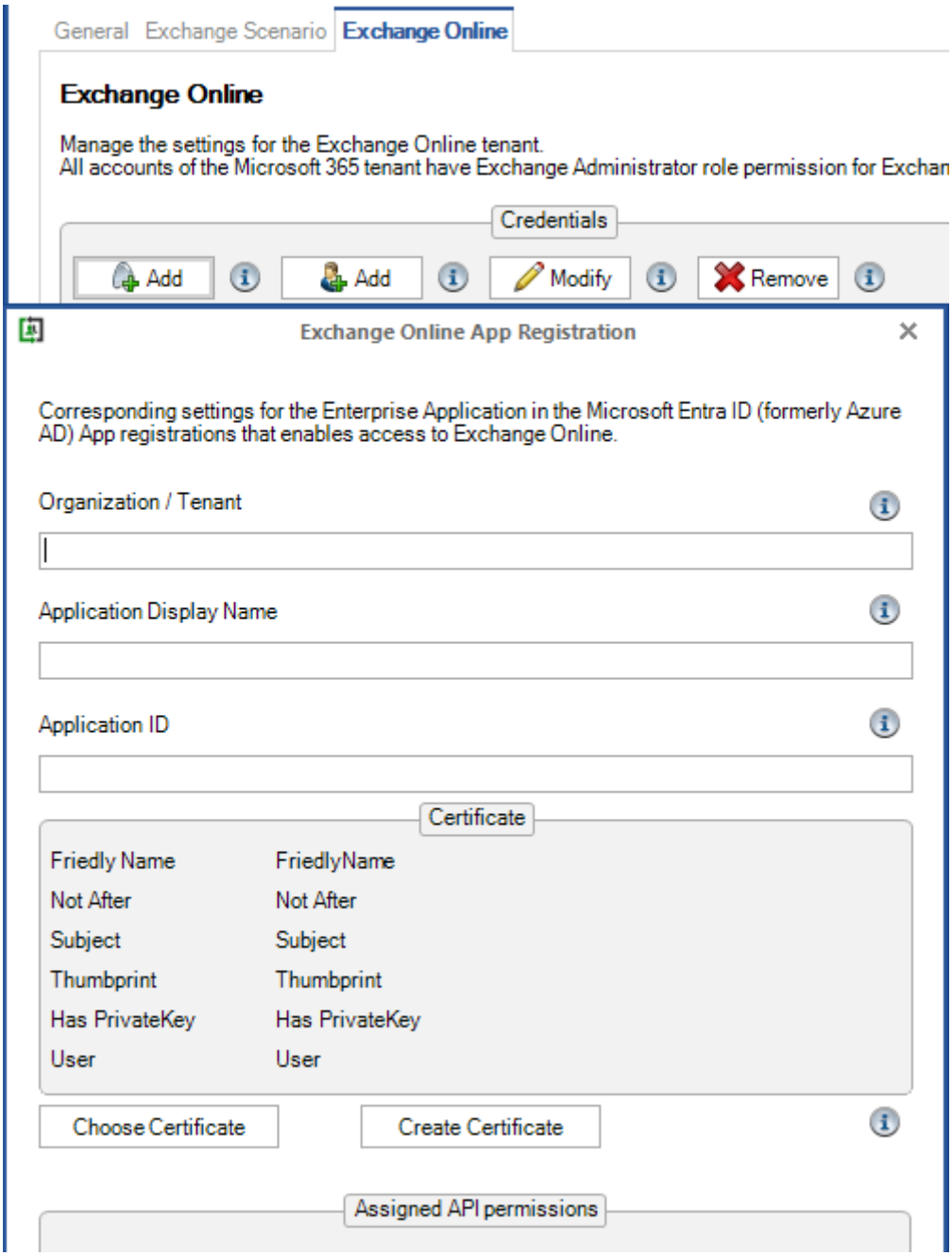
A detailed description is in chapter
Exchange Online authentication via Service Account

Exchange Online certificate-based authentication via App Registration

First, please verify the contactSync GUI is running in the credentials of the local contactSync service account, otherwise contactSync cannot decrypt the Application Id and cannot find the certificate later.

This can be confirmed on the information bar at the bottom of the contactSync GUI.

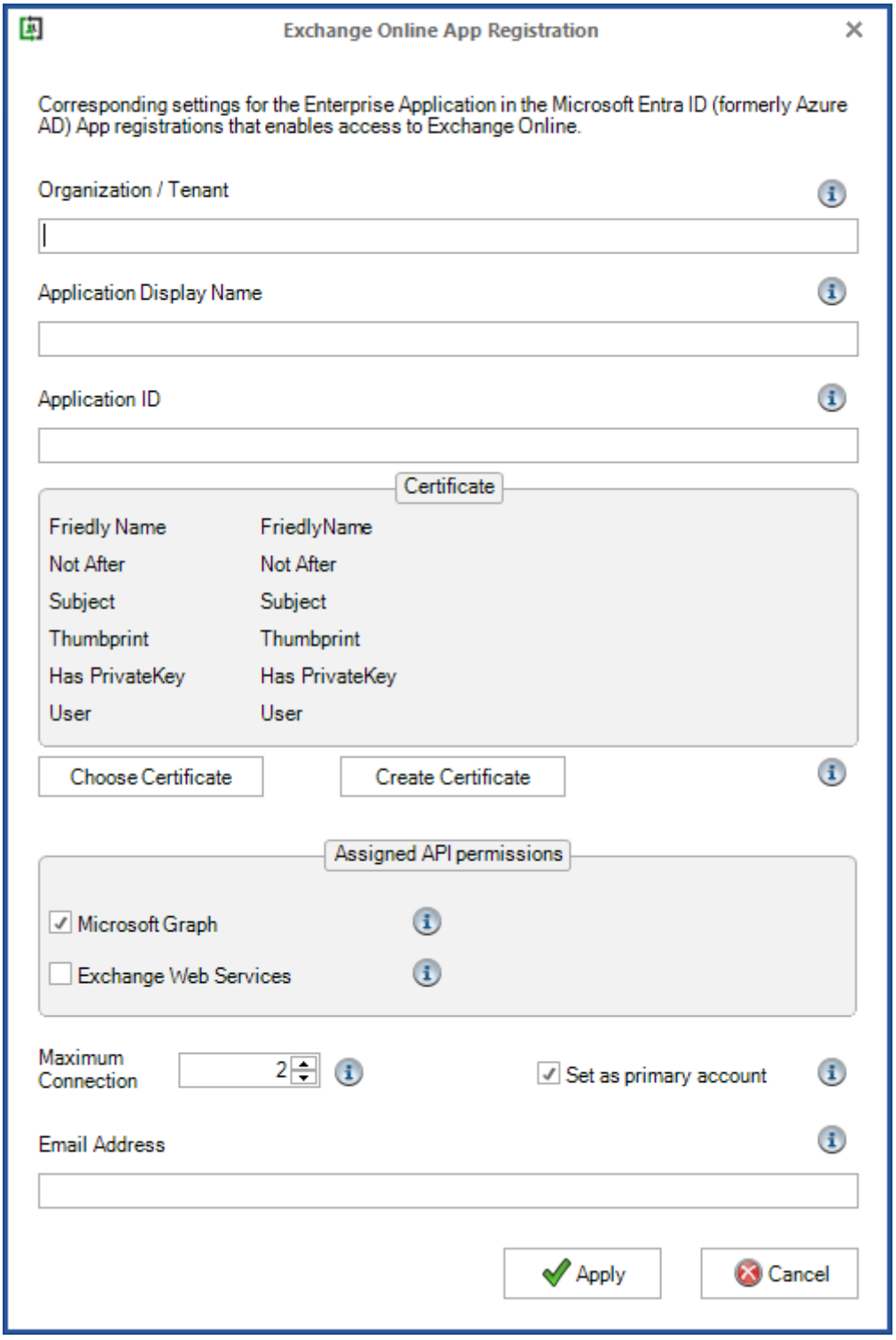
Register an Enterprise Application in the **Microsoft Entra admin center** (formerly known as **Azure Active Directory admin center**) and enter the corresponding values in the **Exchange Online App Registration** dialog.



The following description is based on the **Microsoft Documentation** article:

App-only authentication for unattended scripts in Exchange Online PowerShell and Security & Compliance PowerShell

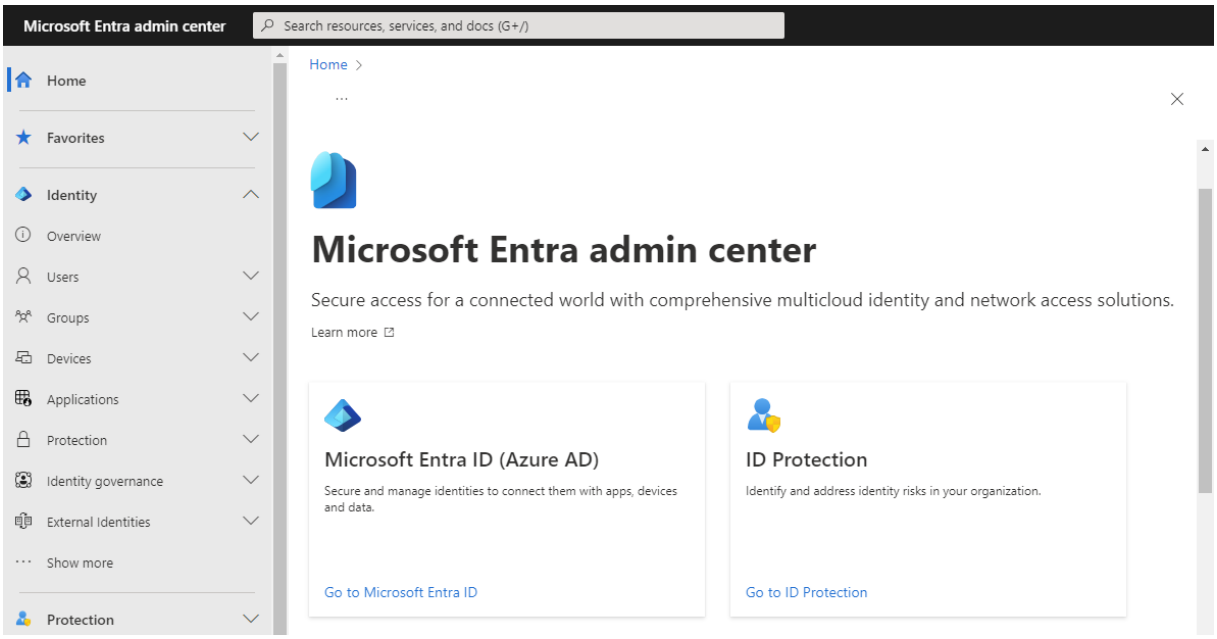
https://learn.microsoft.com/en-us/powershell/exchange/app-only-auth-powershell-v2?view=exchange-ps



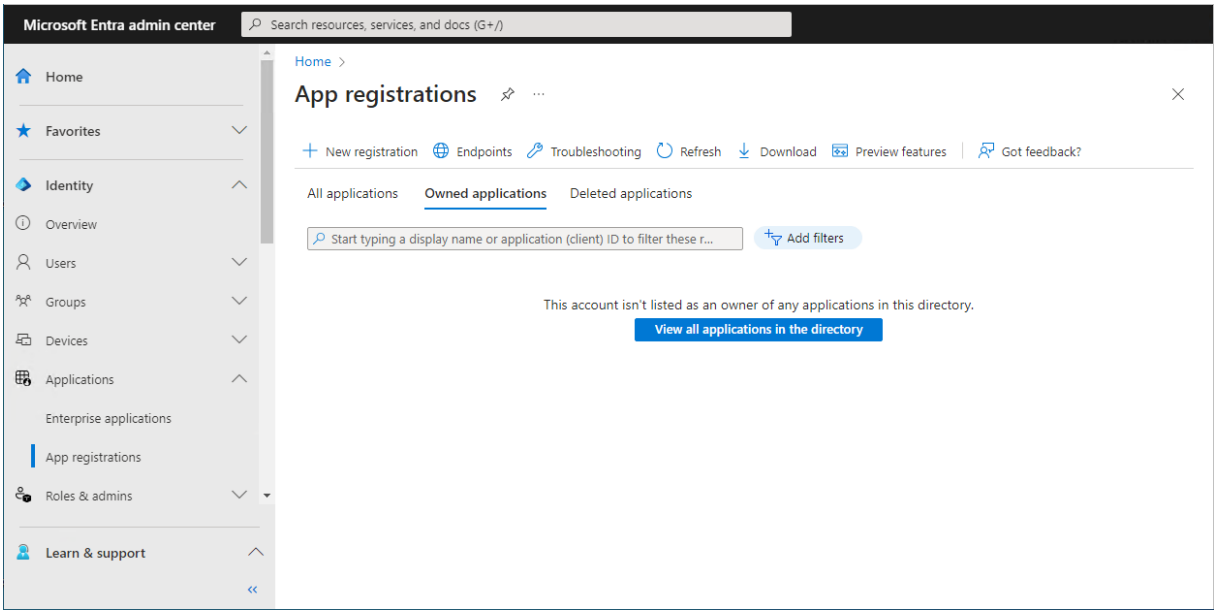
Register an Enterprise Application in Microsoft Entra ID

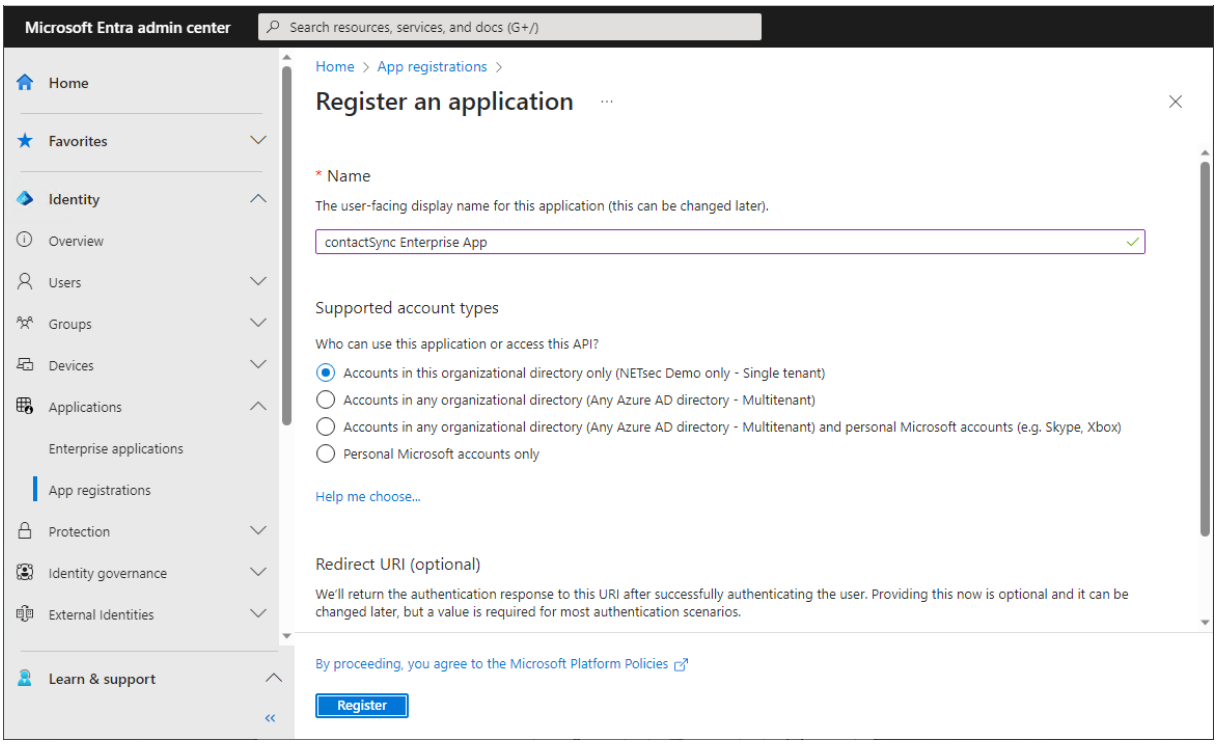
Logon to the **Microsoft Entra admin center** https://entra.microsoft.com

as a global administrator and expand **Identity** (formerly Azure Active Directory).



Expand **Applications** and go to **App registrations**. Then select **New registration**.

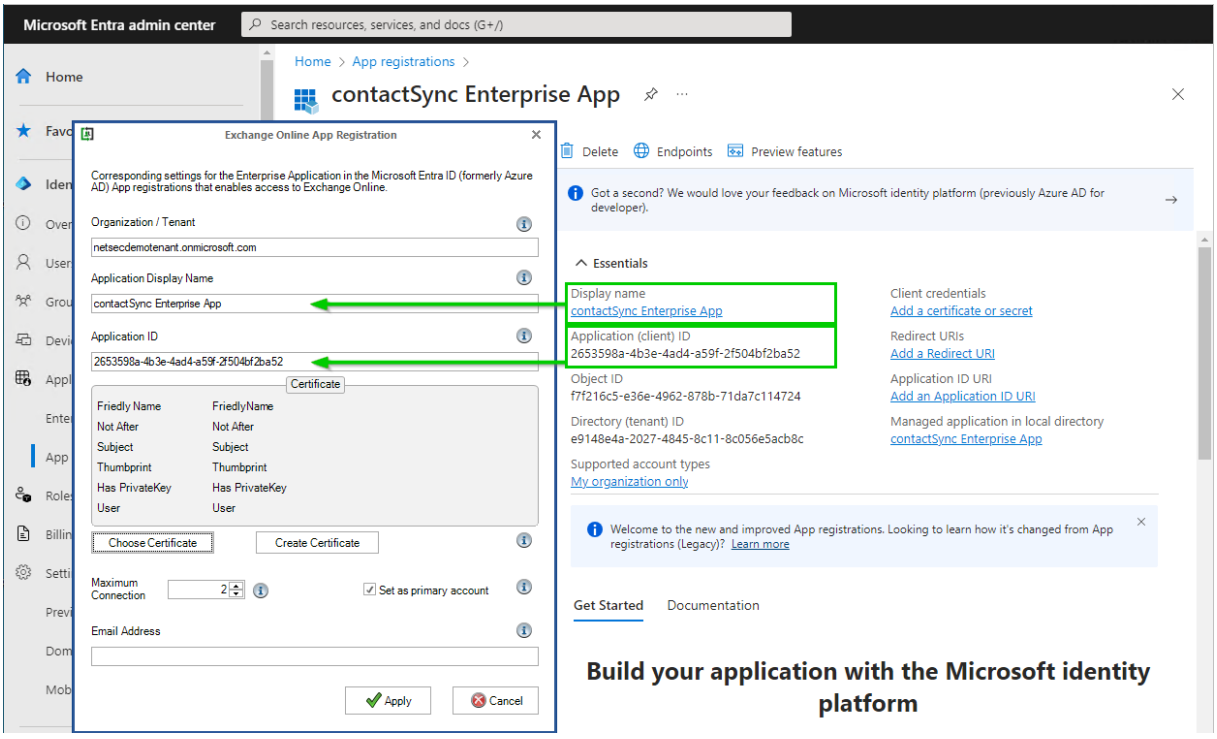




Enter a name for the **Application**.
In this example, it has been named **contactSync Enterprise App**.

Select the **Accounts in this organizational directory only (<*YourOrganizationName*> only - Single tenant)** radio button and click **Register**.

Transfer the information of the registered Application to the **Exchange Online App Registration** dialog.



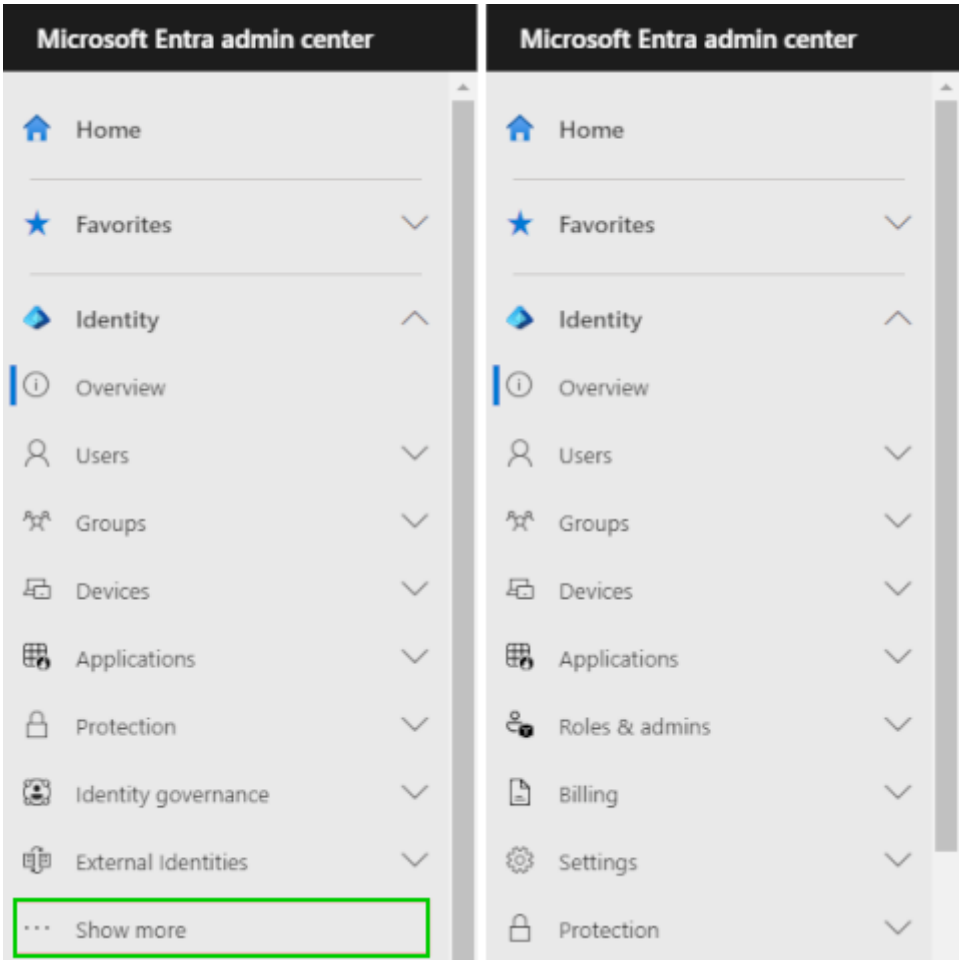
Organization / Tenant needs the **.onmicrosoft.com** domain name of the Microsoft 365 tenant. Otherwise, you may encounter cryptic permission issues when you run a policy in the app context. The next chapter will describe where to find the domain name of the Microsoft 365 tenant.

Application Display Name must have the value of the **Display name** of the registered Application.

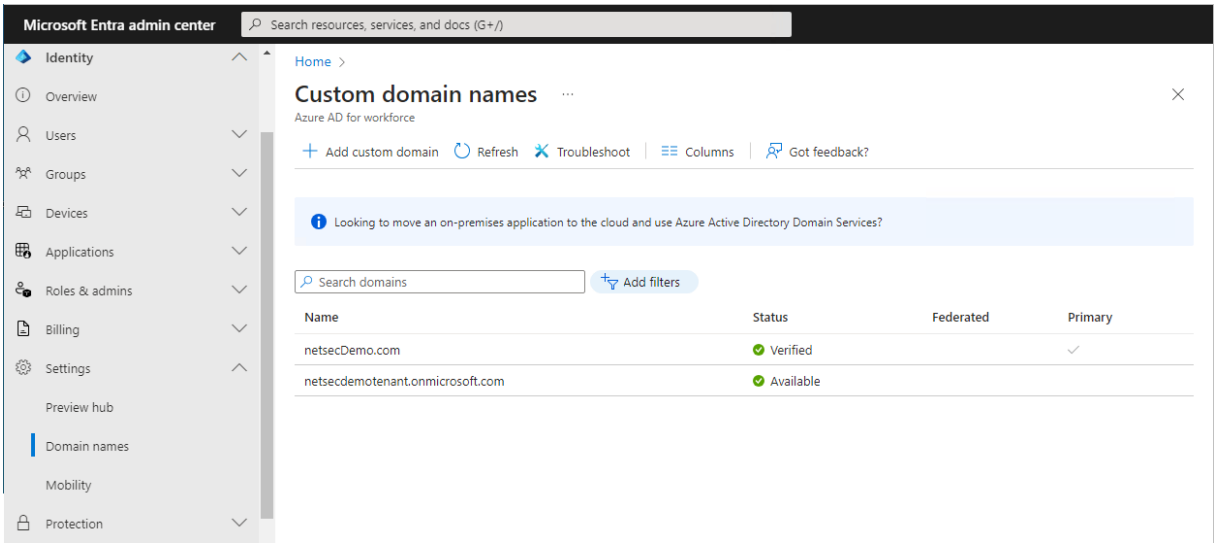
Application ID must have the value of the **Application (Client) ID** of the registered Application.

Where to find the domain name of the Microsoft 365 tenant?

Click **Show more** to see **Settings**



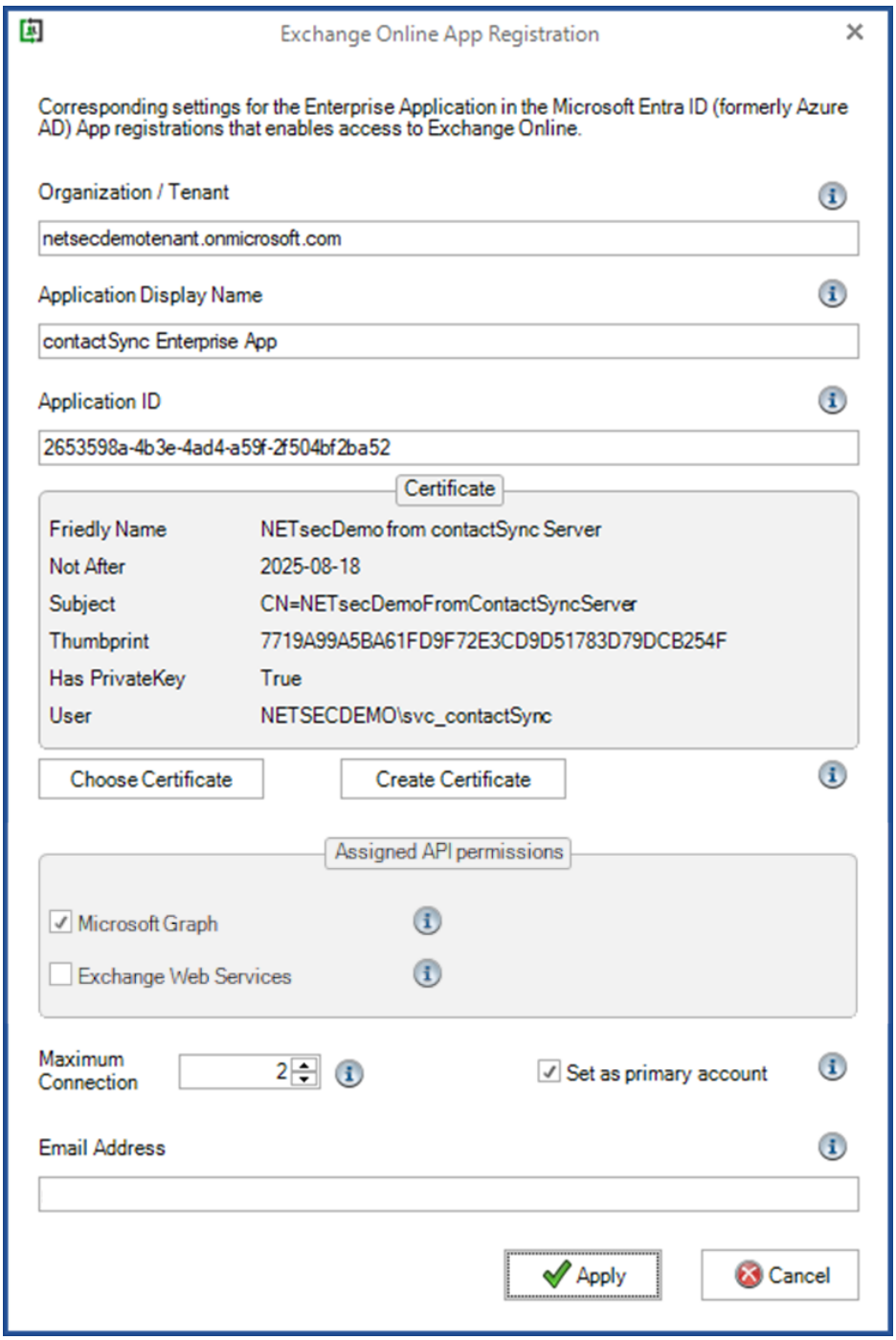
Expand **Settings,** go to **Domain names** and use the **.onmicrosoft.com** domain name.



Please do not confuse the Microsoft 365 tenant domain names with the Exchange Online accepted domains.

Certificate for the registered Application

For app-only authentication in **Microsoft Entra ID** (formerly known as Azure Active Directory), you typically use a certificate to request access. Anyone who has the certificate and its private key can use the application, and the permissions granted to the application.



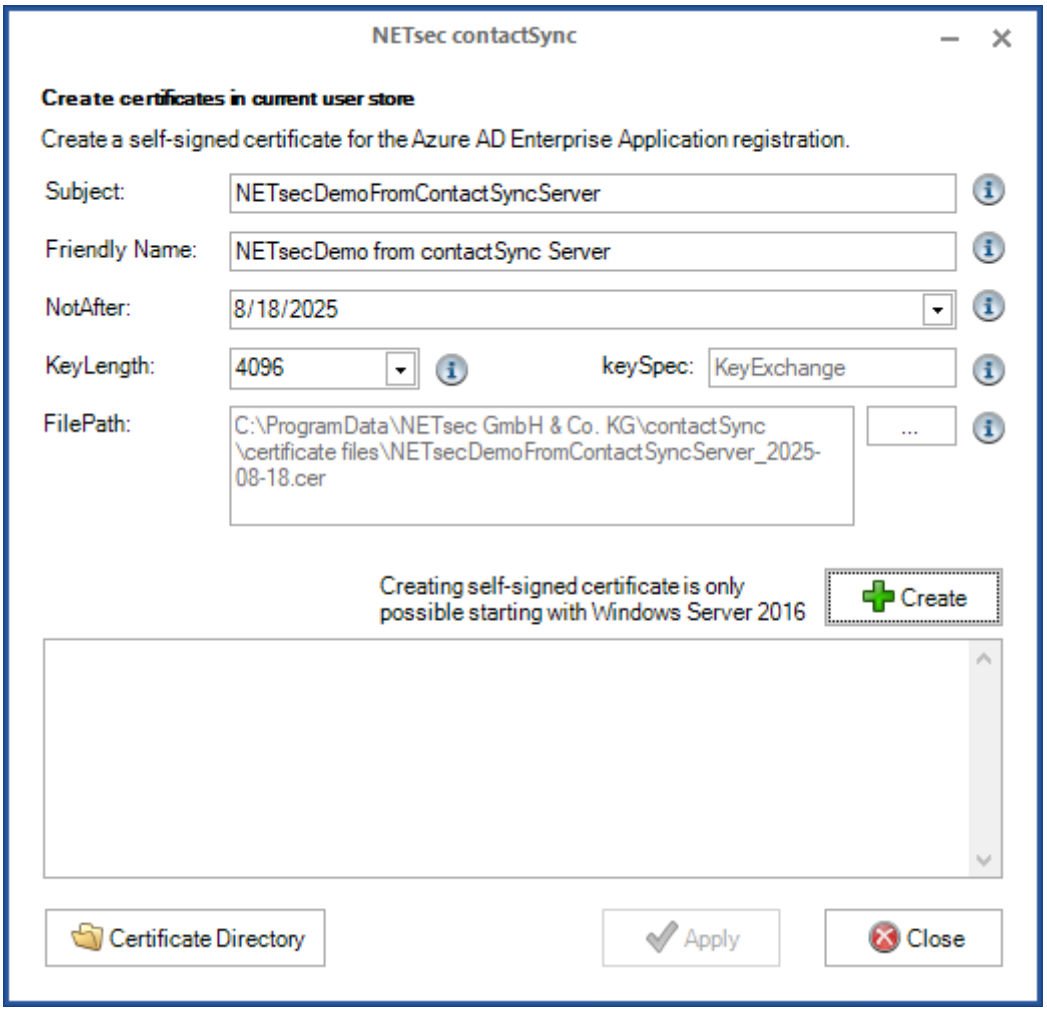
Choose Certificate

Choose an existing certificate and its private key from the user certificate store of the current user, which runs the contactSync GUI.

The corresponding public key file of this selected certificate must be uploaded to the registered Application.

Create Certificate

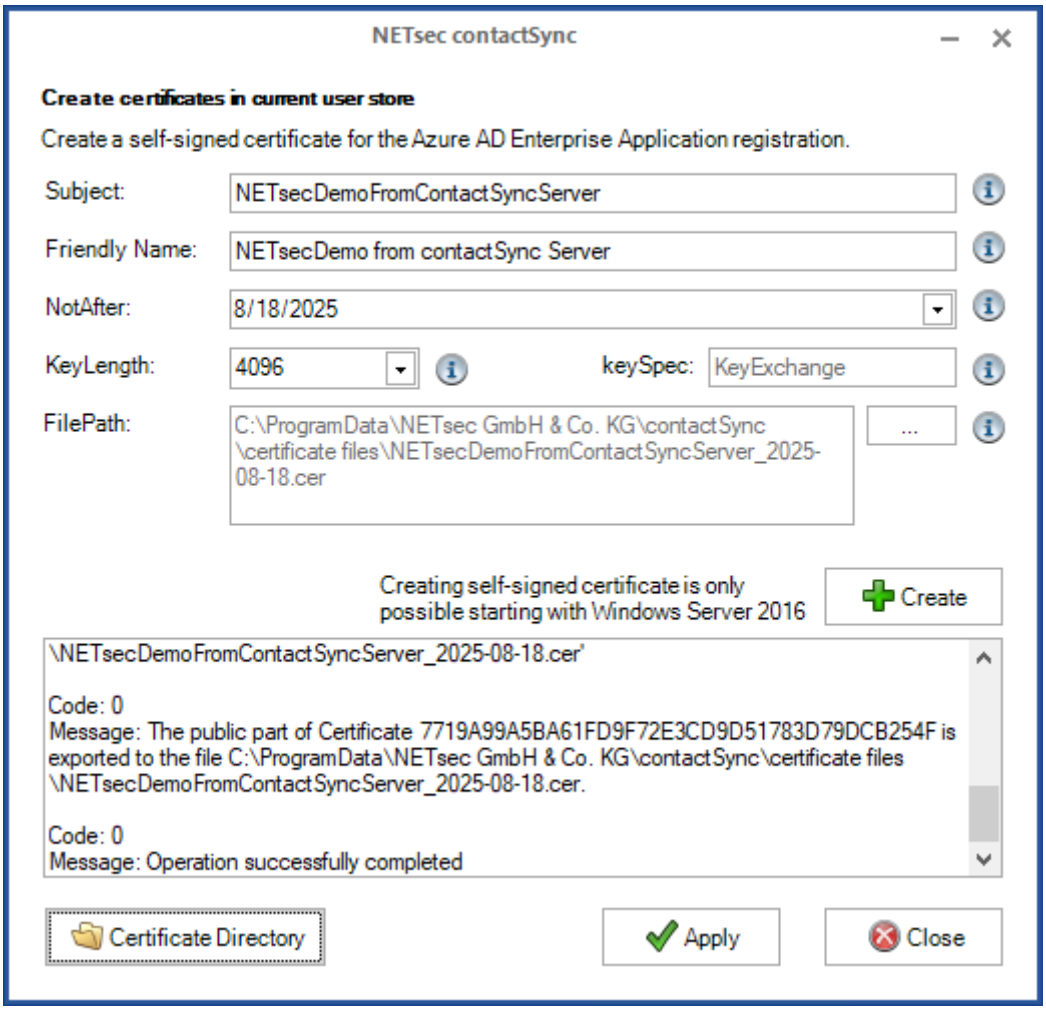
Create a self-signed certificate, which will be saved in the current user certificate store and will be used to authenticate your Application against **Identity** (formerly Azure Active Directory), while requesting the app-only access token.



Enter the **Subject**, and **Friendly Name** of the certificate.

In the example above, the forest name (NETsecDemo) and the name of the server (contactSync Server) from which the connection is established will be incorporated in both.

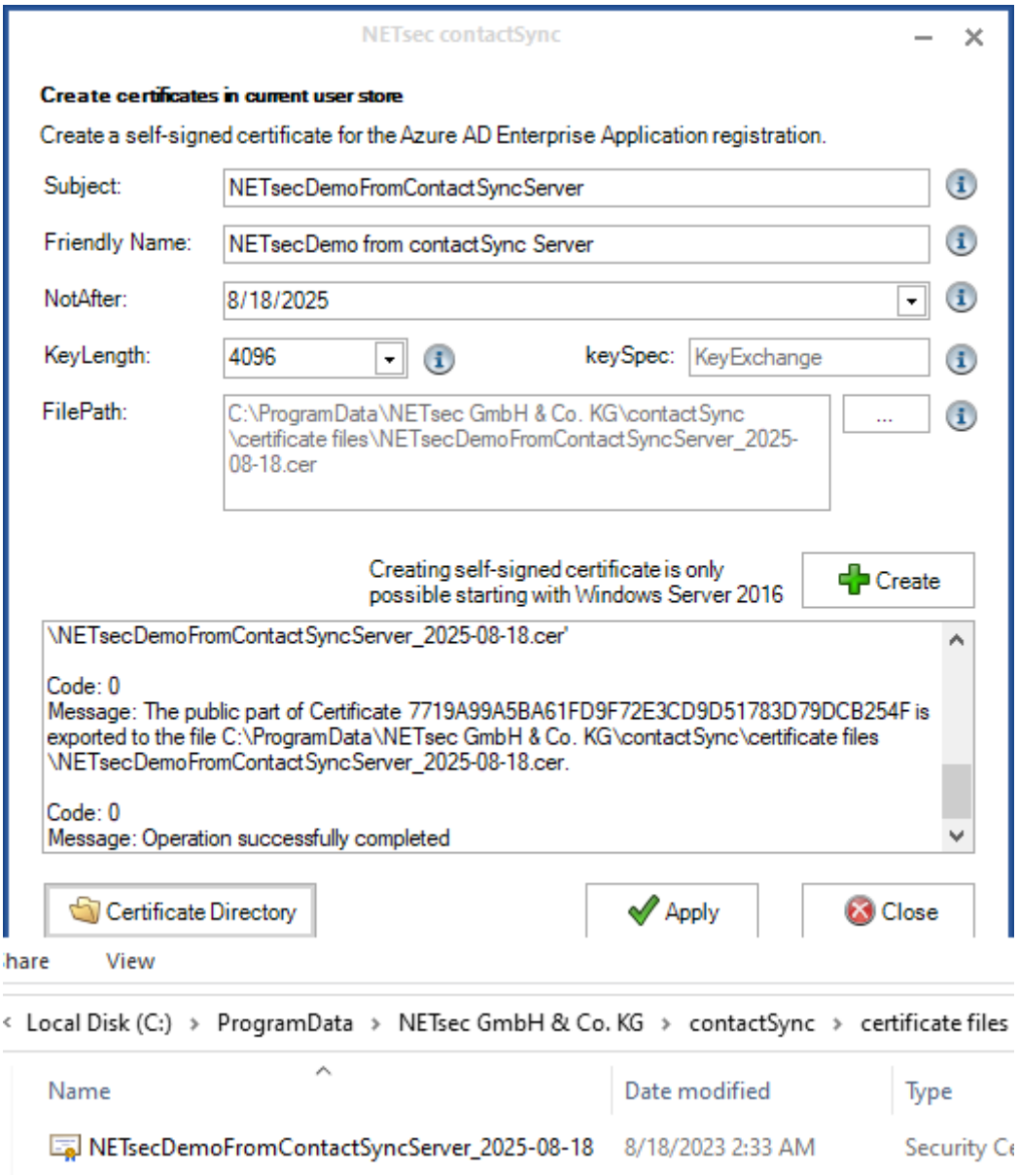
Click **Create** to generate a new certificate.



The public key file is created in the default path

```
C:\ProgramData\NETsec GmbH & Co. KG\contactSync\certificate files\
```

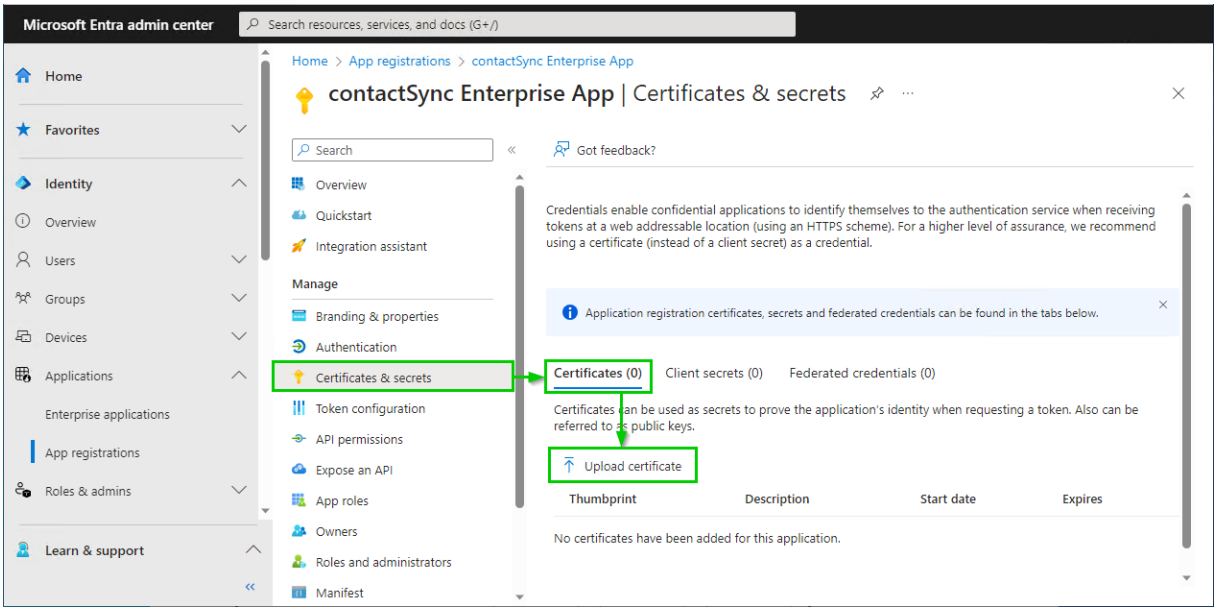
Click on the **Certificate Directory** button to open the folder in **File Explorer**



Then click **Apply** to close the Create Certificate dialog.

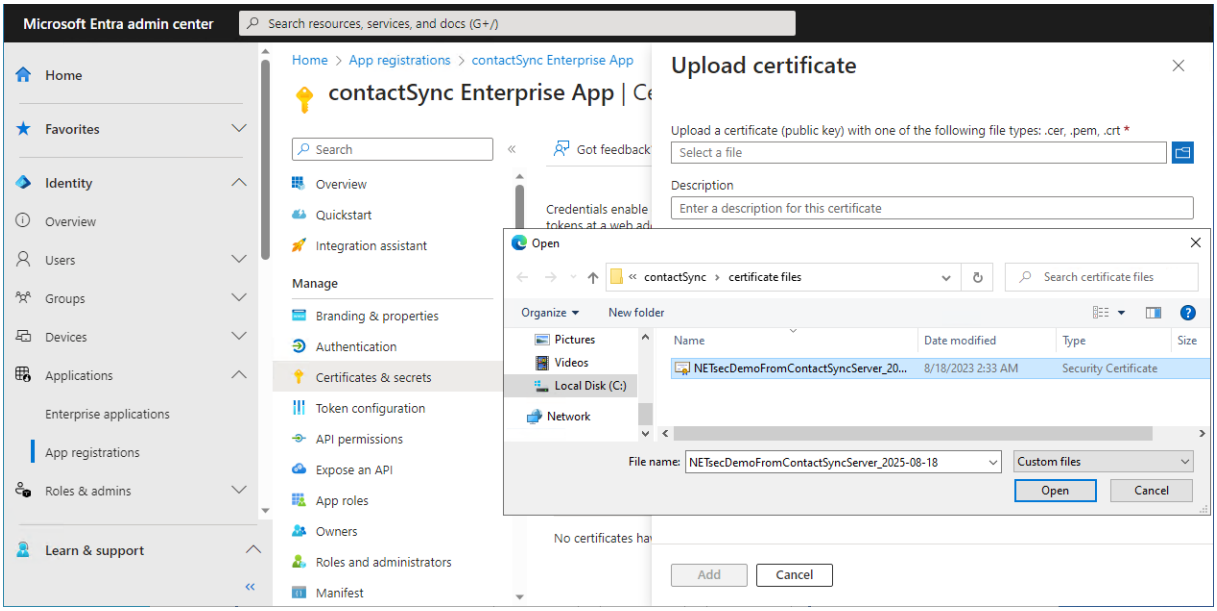
Upload certificate file for the registered Application

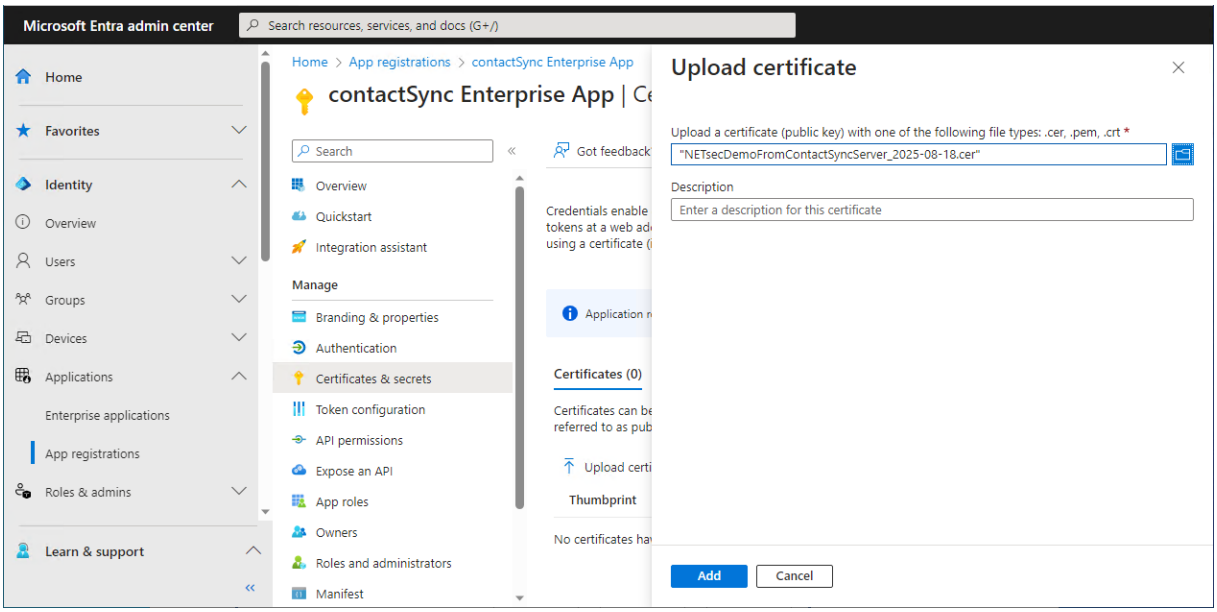
Go to **Certificates & secrets** of the registered Application in **Microsoft Entry ID** (Azure AD), and select the **Certificates** tab.



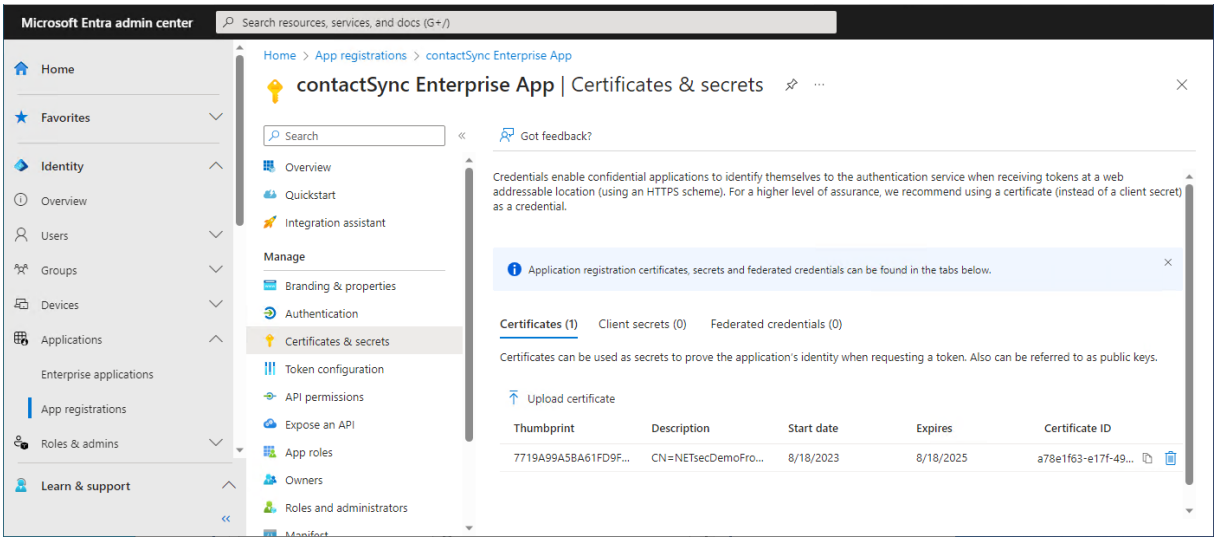
Select **Upload certificate**, then browse to the location where the certificate was saved. Select, and open it. The default path is:

```
C:\ProgramData\NETsec GmbH & Co. KG\contactSync\certificate files
```





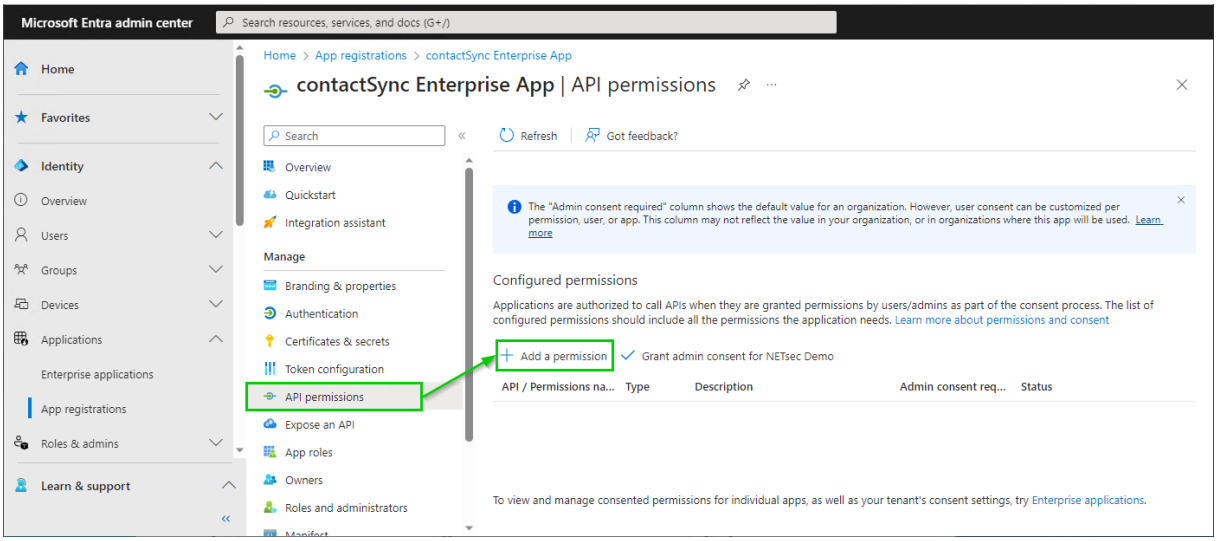
Add the selected certificate.



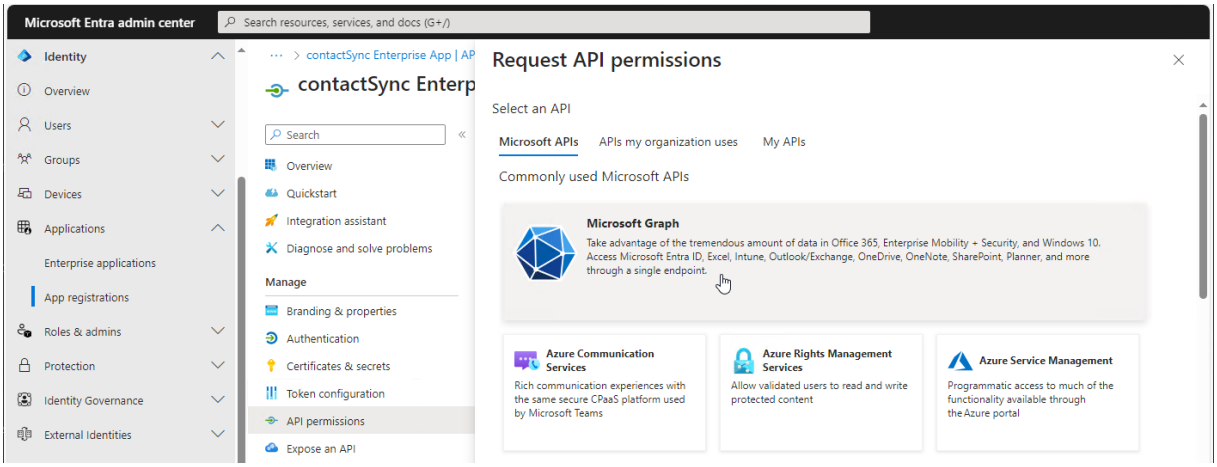
Assign API permissions to the registered Application

API permissions for Microsoft Graph

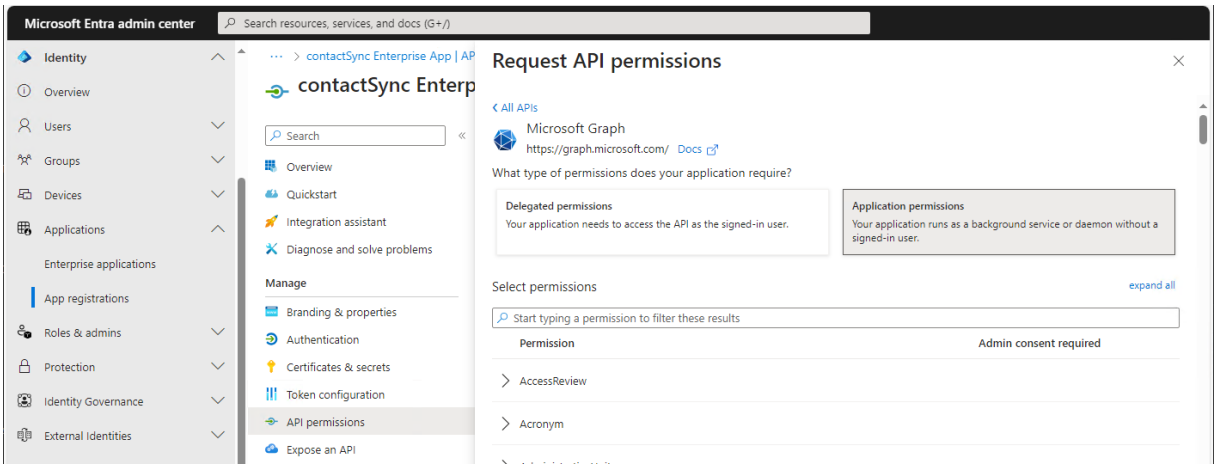
Go to **API permissions**, then select **Add a permission**



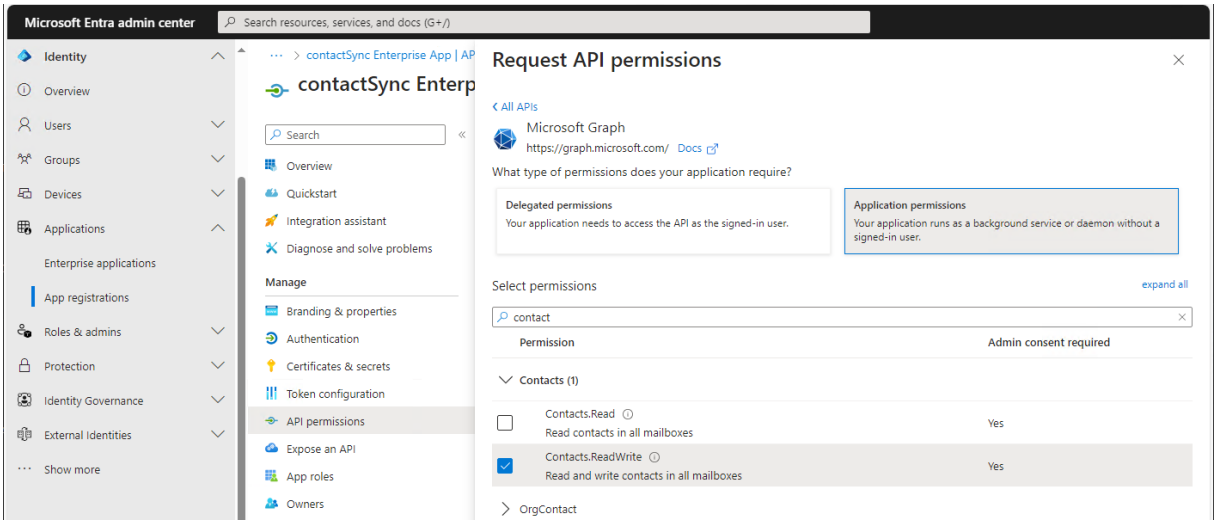
Select the **Microsoft APIs** and click on **Microsoft Graph**



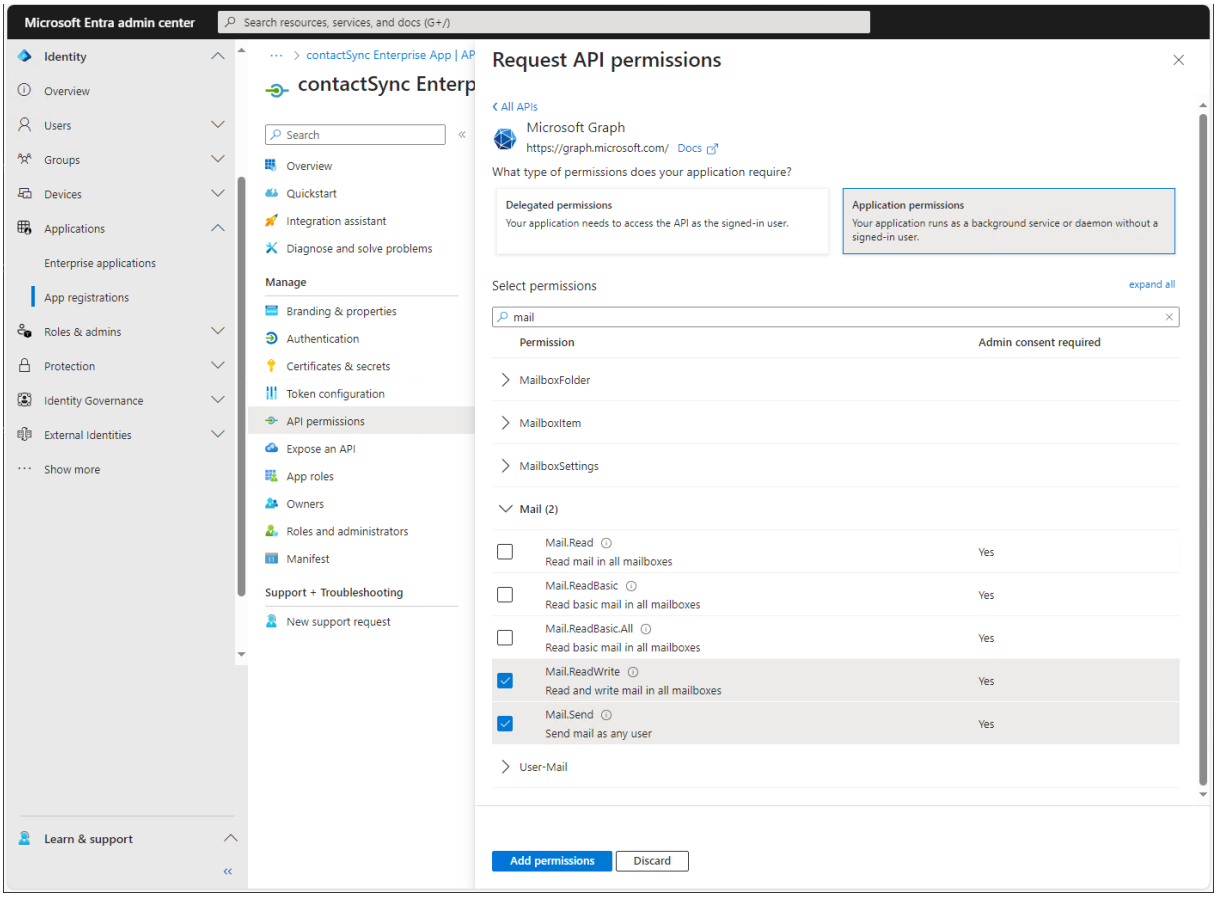
Select **Application permissions**



Search for **contact** and expand the **Contacts** in the result list.
Select
Contacts.ReadWrite

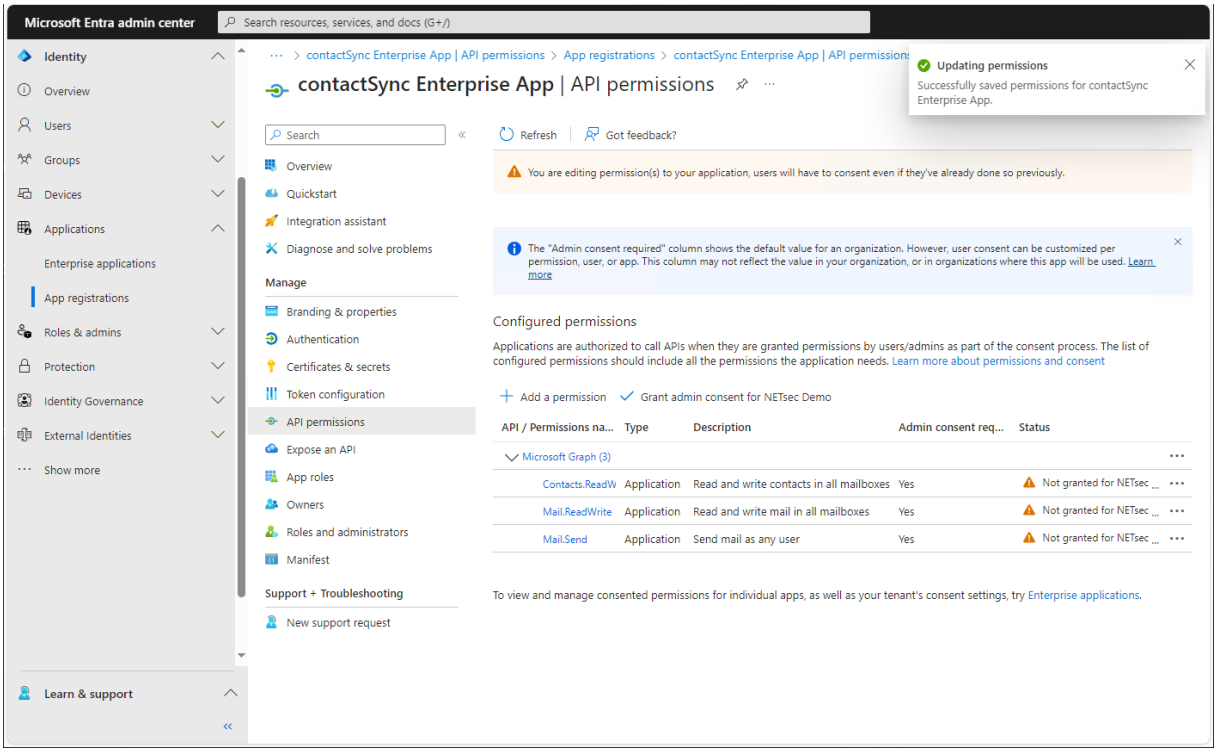


Search for **mail** and expand the **Mail** in the result list.
Select
Mail.ReadWrite
and
Mail.Send

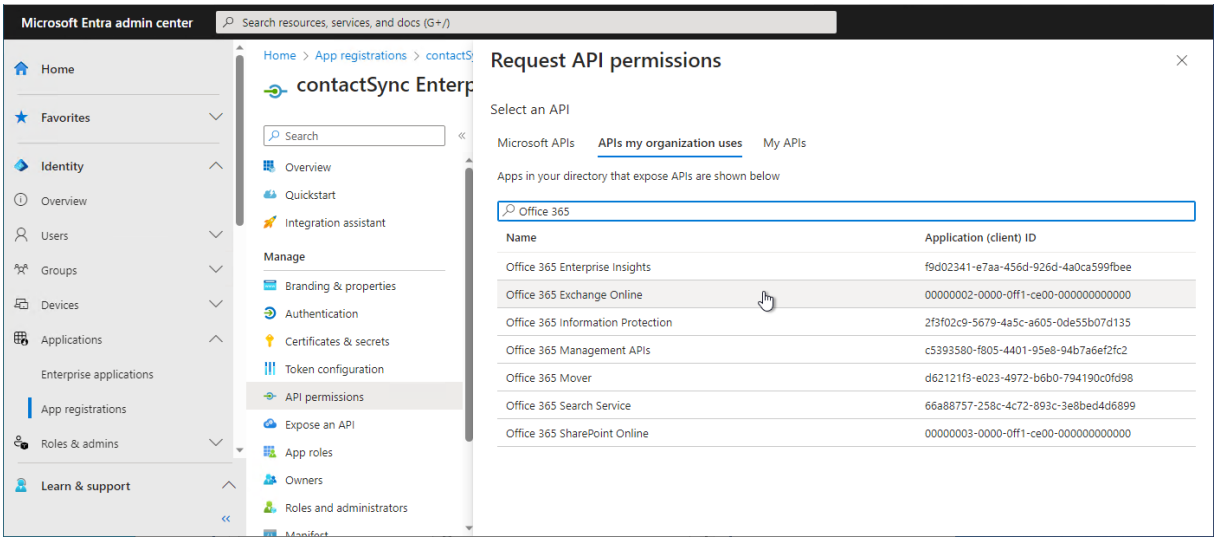


Click **Add permissions**

Select **Add a permission** again.

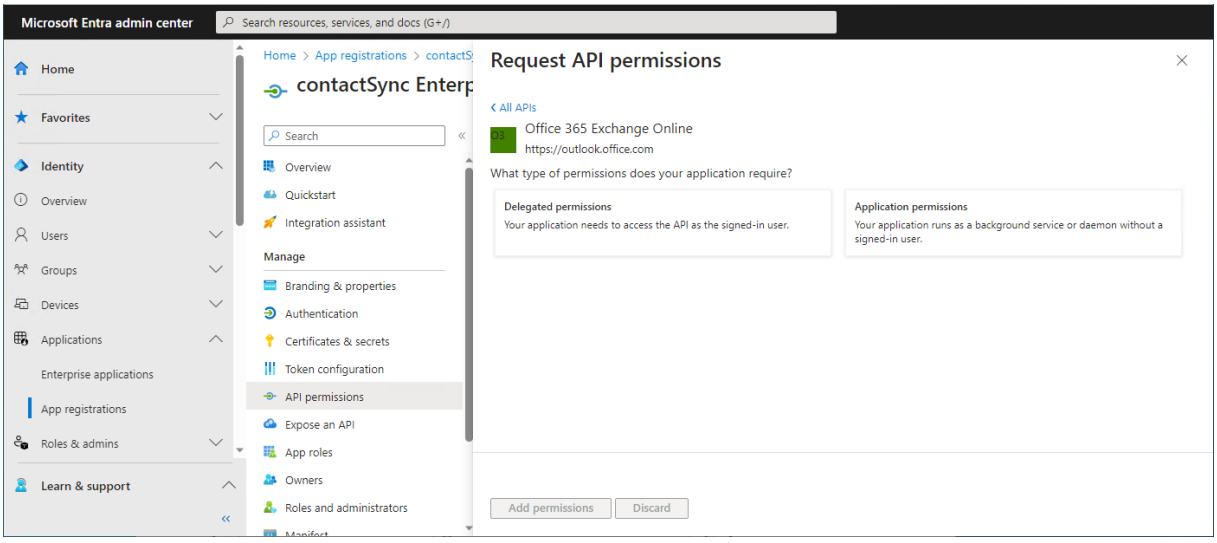


Select the **APIs my organization uses** tab on the **Request API permissions** dialog and search for **Office**.



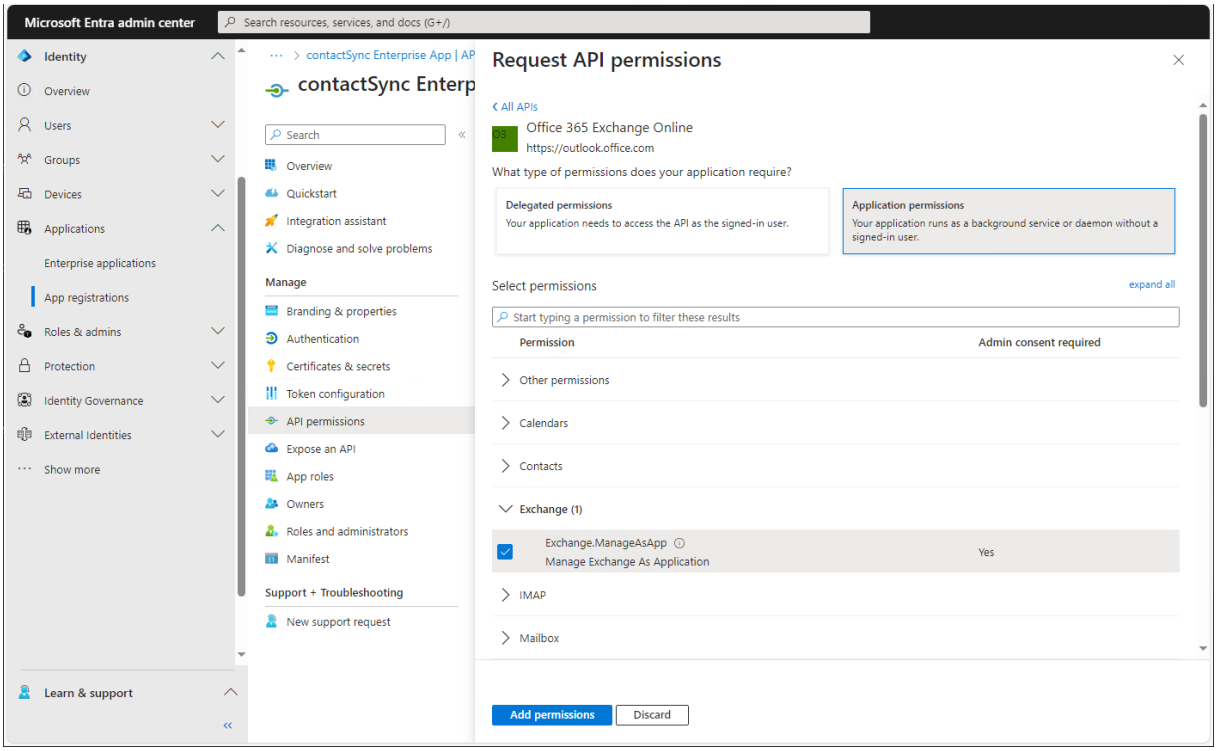
Click on **Office 365 Exchange Online** in the result list to open it.

Select **Application permissions**



Policies synchronizing contacts from Exchange Online and from Shared Mailboxes, which are located in Exchange Online, need only Microsoft Graph permissions.

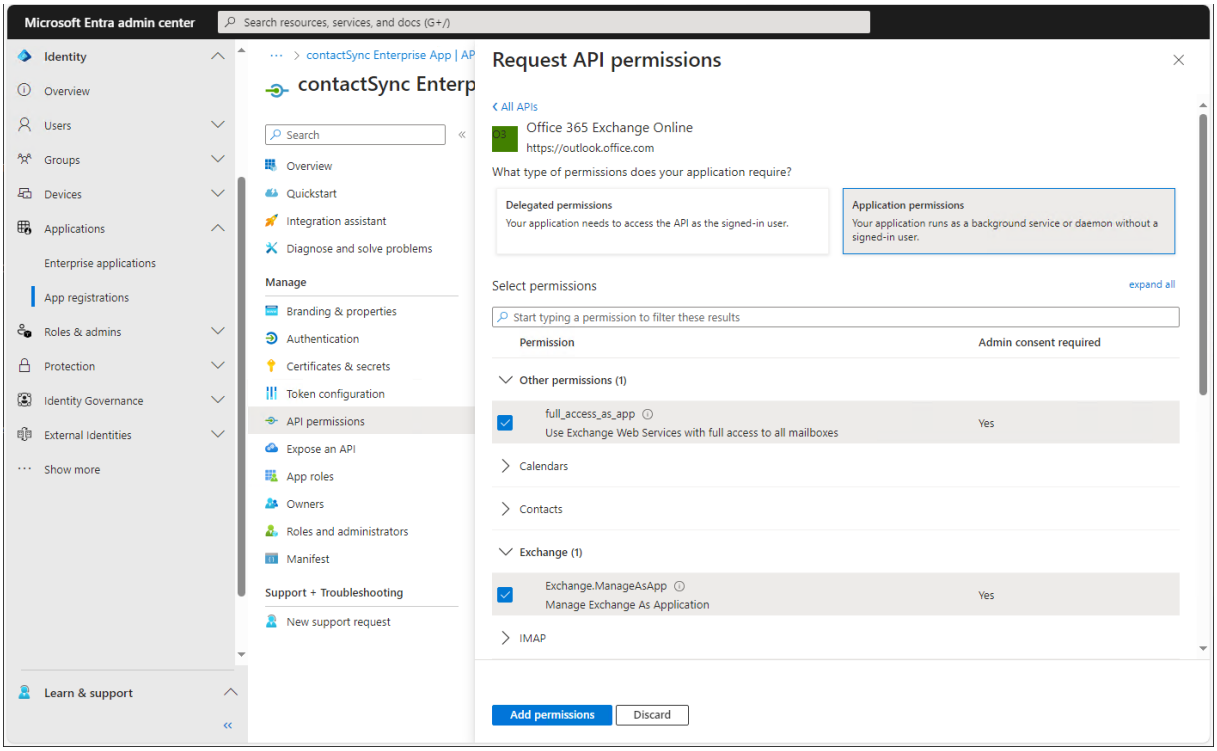
Select
Exchange.ManageAsApp
Manage Exchange As Application



Click **Add permissions**

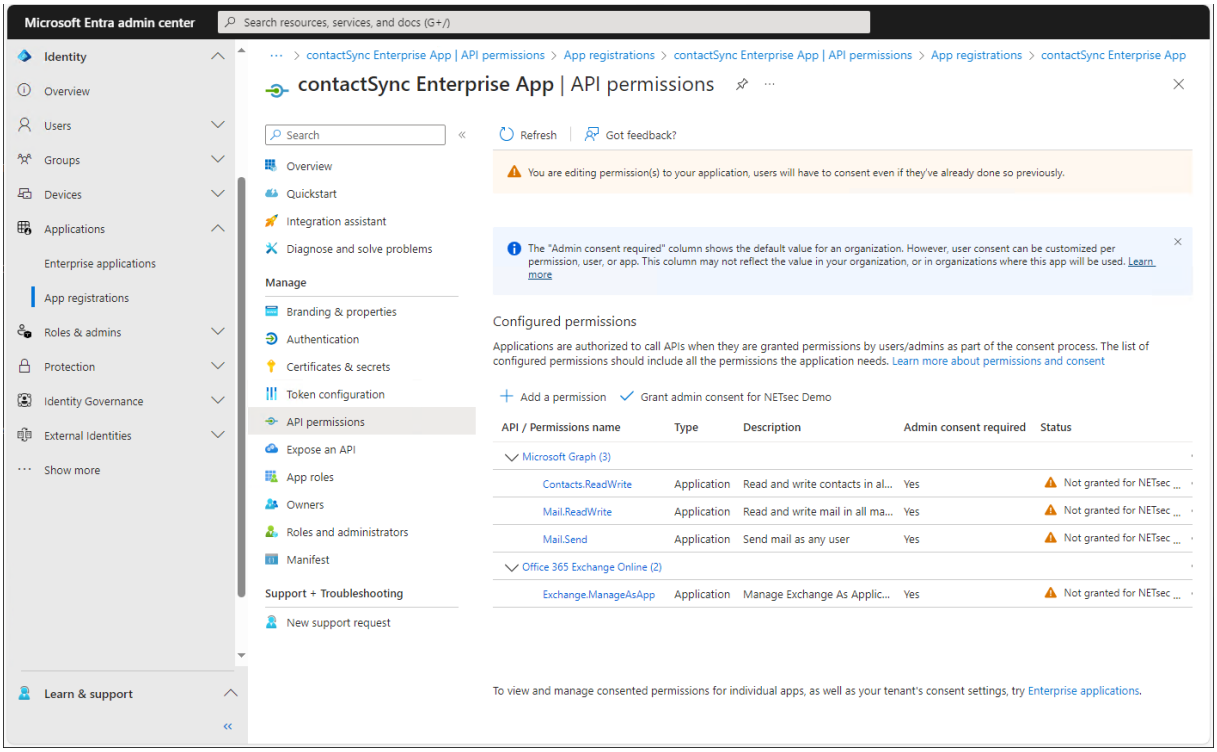
Policies synchronizing contacts from Public Folder, which are located in Exchange Online, need additionally the permission for Exchange Web Services at the moment.

Select
full_access_as_app
Use Exchange Web Services with full access to all mailboxes
and
Exchange.ManageAsApp
Manage Exchange As Application

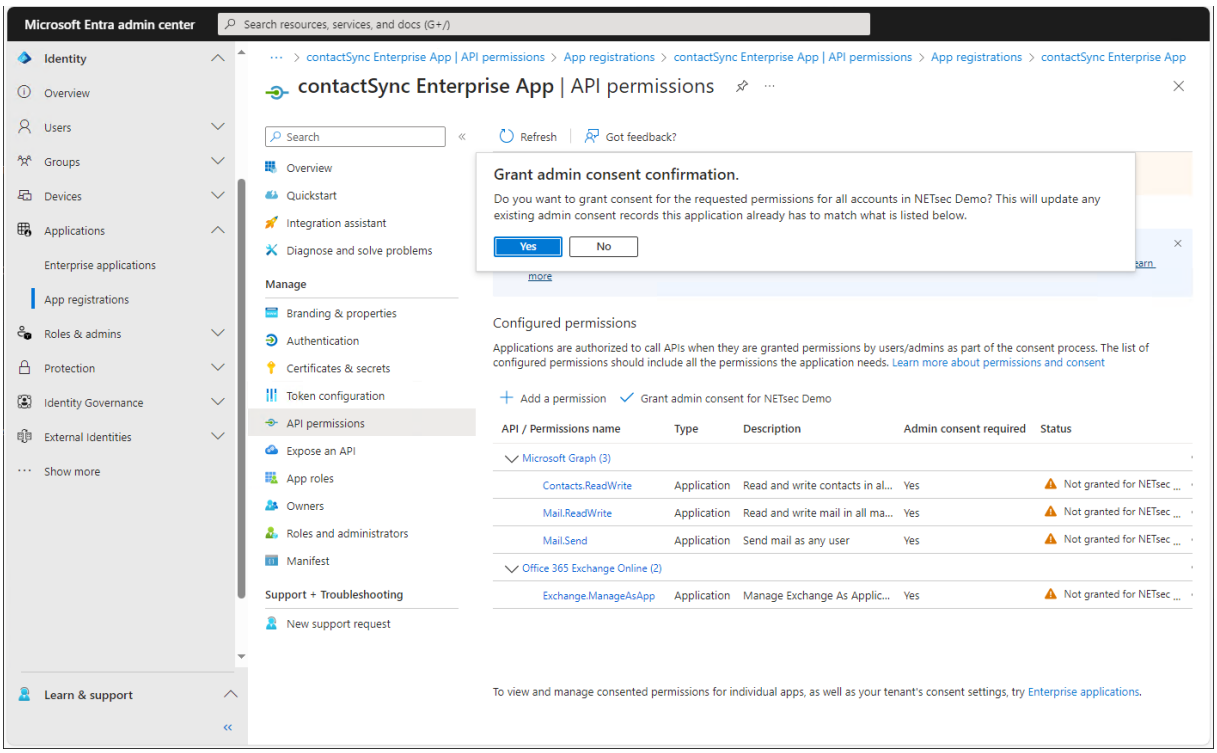


Click **Add permissions**

Click **Grant admin consent for** your tenant.

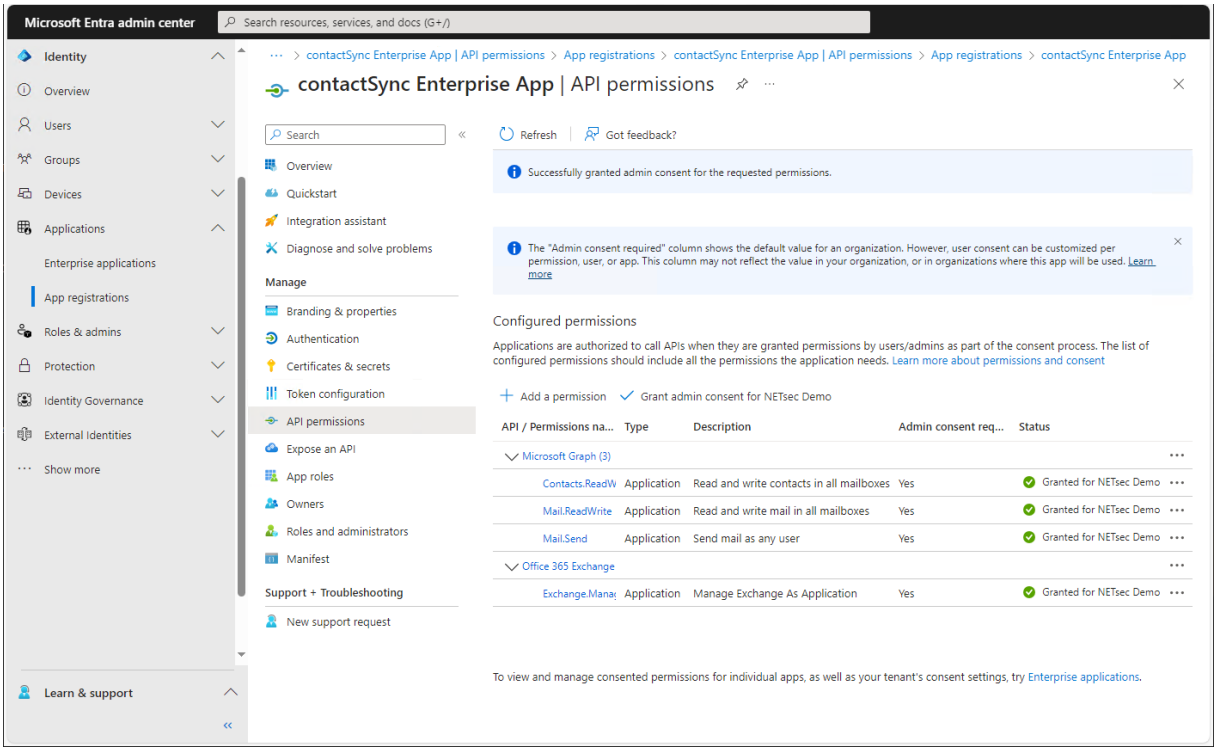


Click **Yes** to confirm the consent.

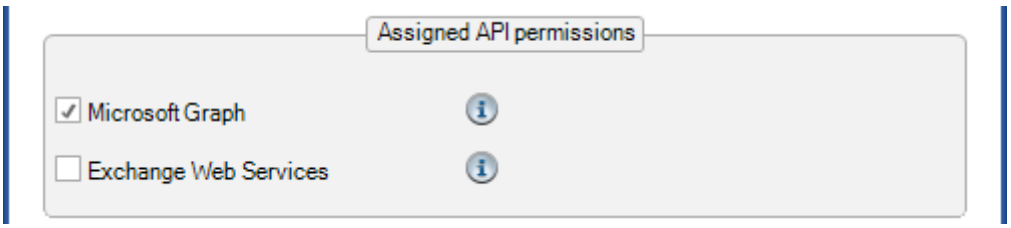


API permissions are assigned to the registered Application.

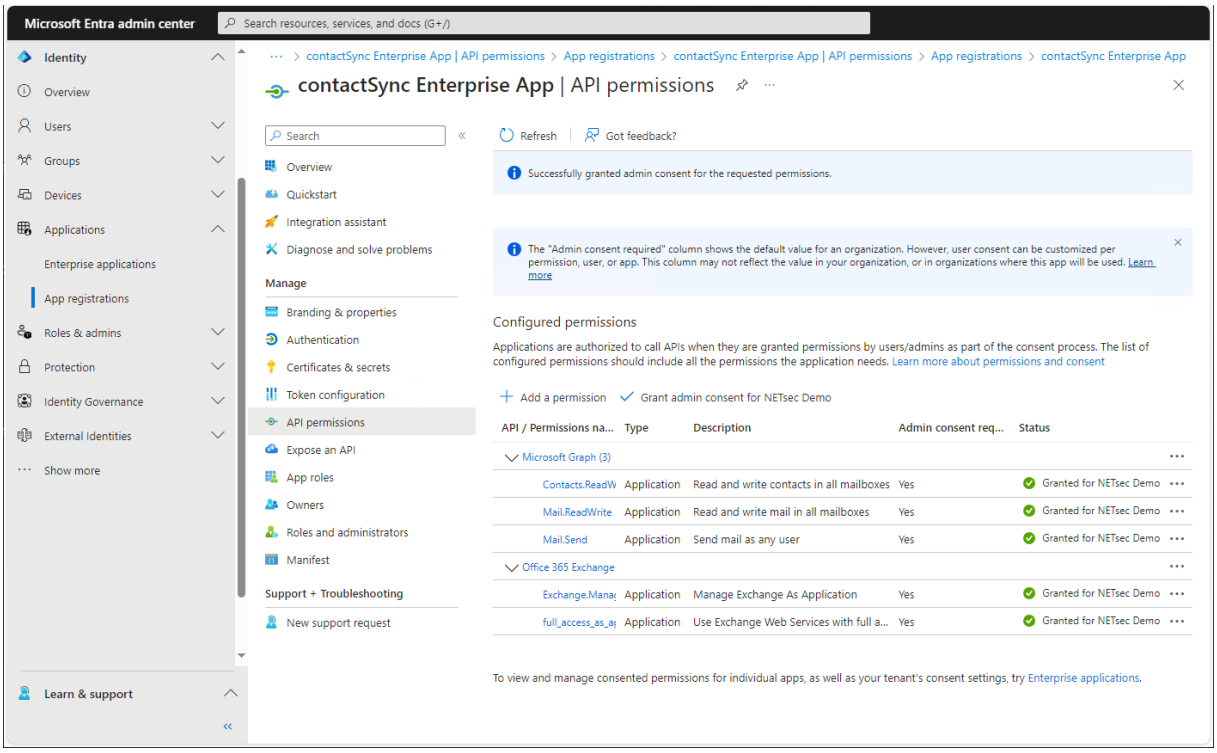
Policies synchronizing contacts from Exchange Online and from Shared Mailboxes, which are located in Exchange Online, need these API permissions.



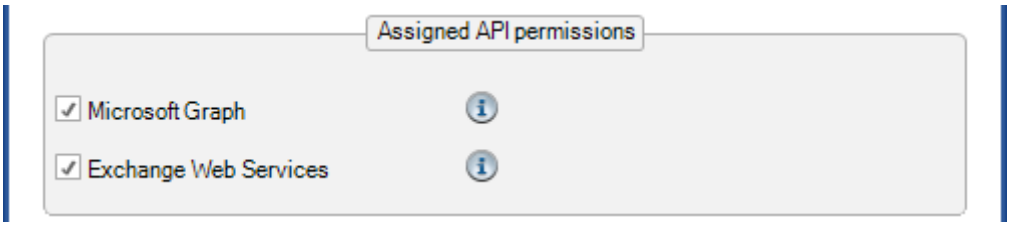
Accordingly, select **Microsoft Graph** at the **Assigned API permissions** group box in the Exchange Online App Registration dialog.



Policies synchronizing contacts from Public Folder, which are located in Exchange Online, need additionally the permission for Exchange Web Services at the moment.



Accordingly, select **Microsoft Graph** and **Exchange Web Services** at the **Assigned API permissions** group box in the Exchange Online App Registration dialog.

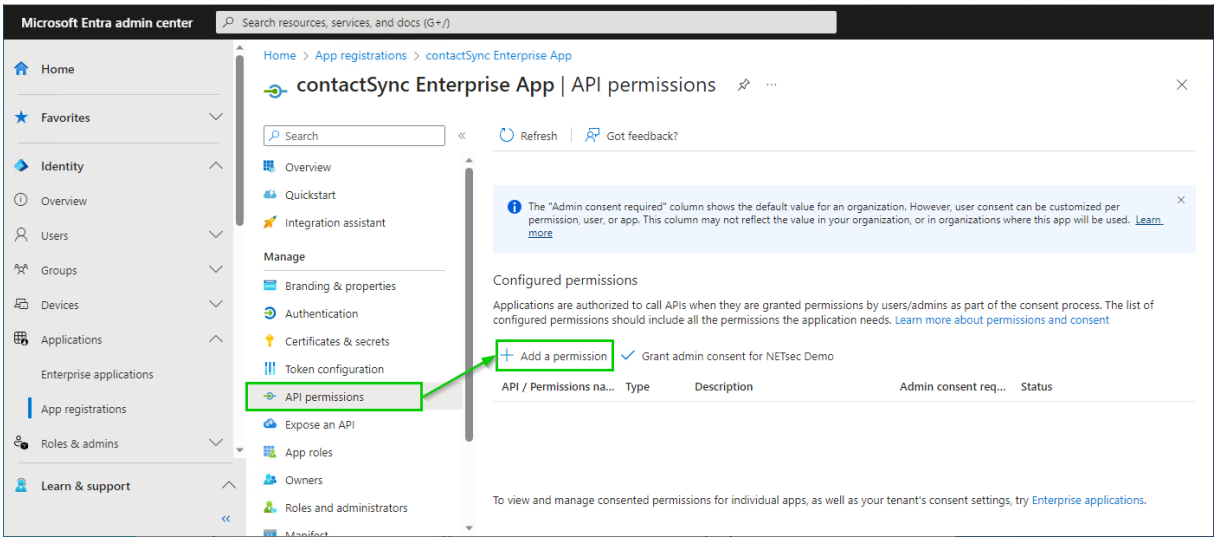


API permissions for Exchange Web Services (deprecated)

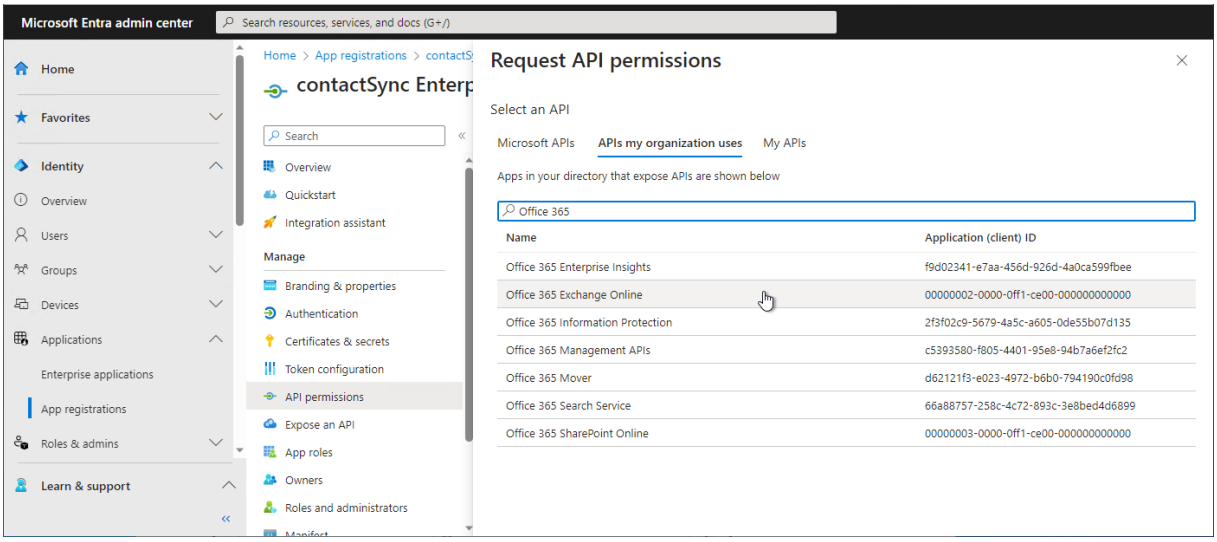
Please note, Microsoft has announced that on 1. October 2026 blocking Exchange Web Services (EWS) requests from non-Microsoft apps to Exchange Online.

Retirement of Exchange Web Services in Exchange Online
https://techcommunity.microsoft.com/t5/exchange-team-blog/retirement-of-exchange-web-services-in-exchange-online/ba-p/3924440

Go to **API permissions**, then select **Add a permission**

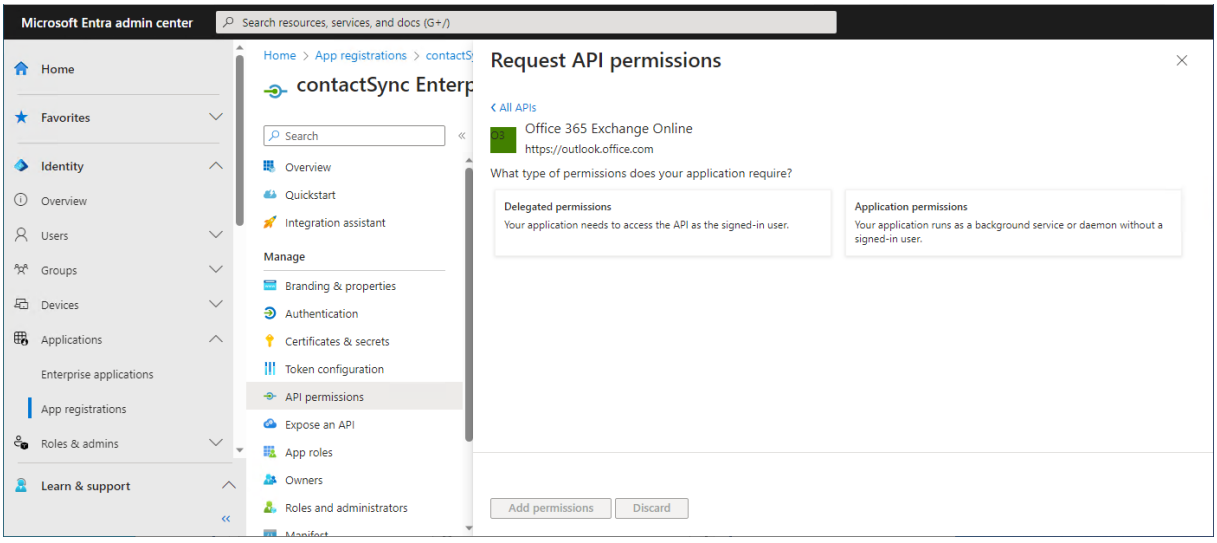


Select the **APIs my organization uses** tab on the **Request API permissions** dialog and search for **Office**.

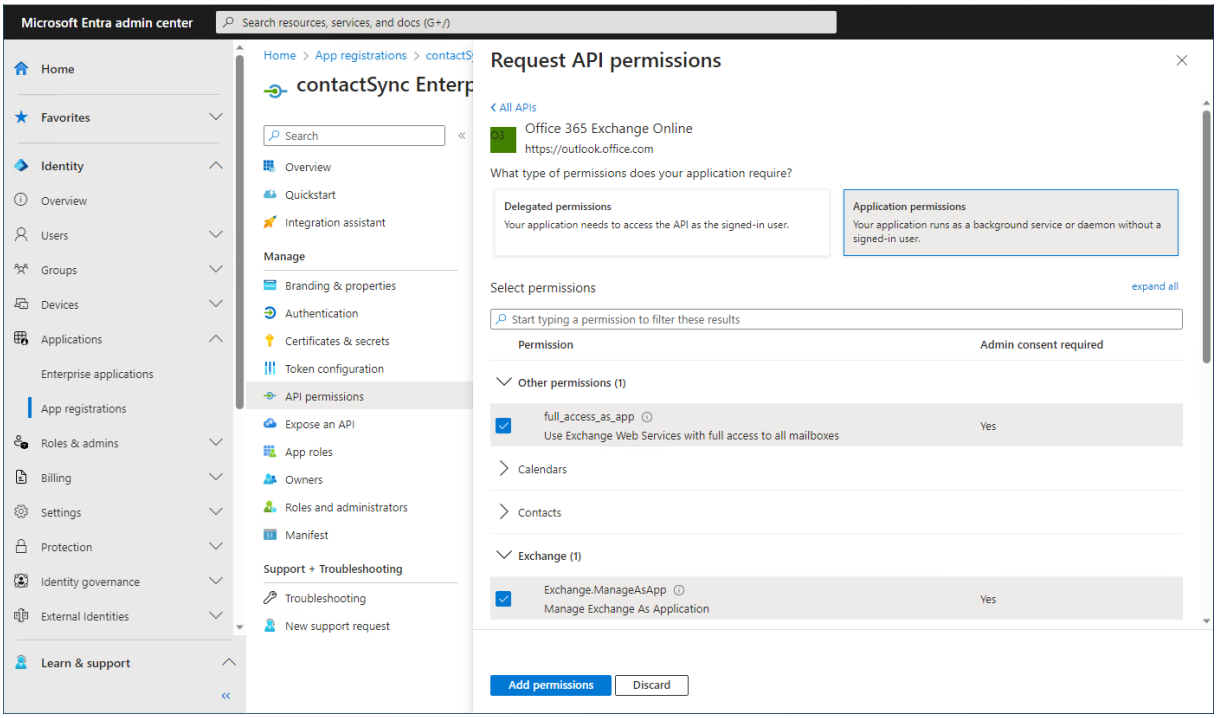


Click on **Office 365 Exchange Online** in the result list to open it.

Select **Application permissions**

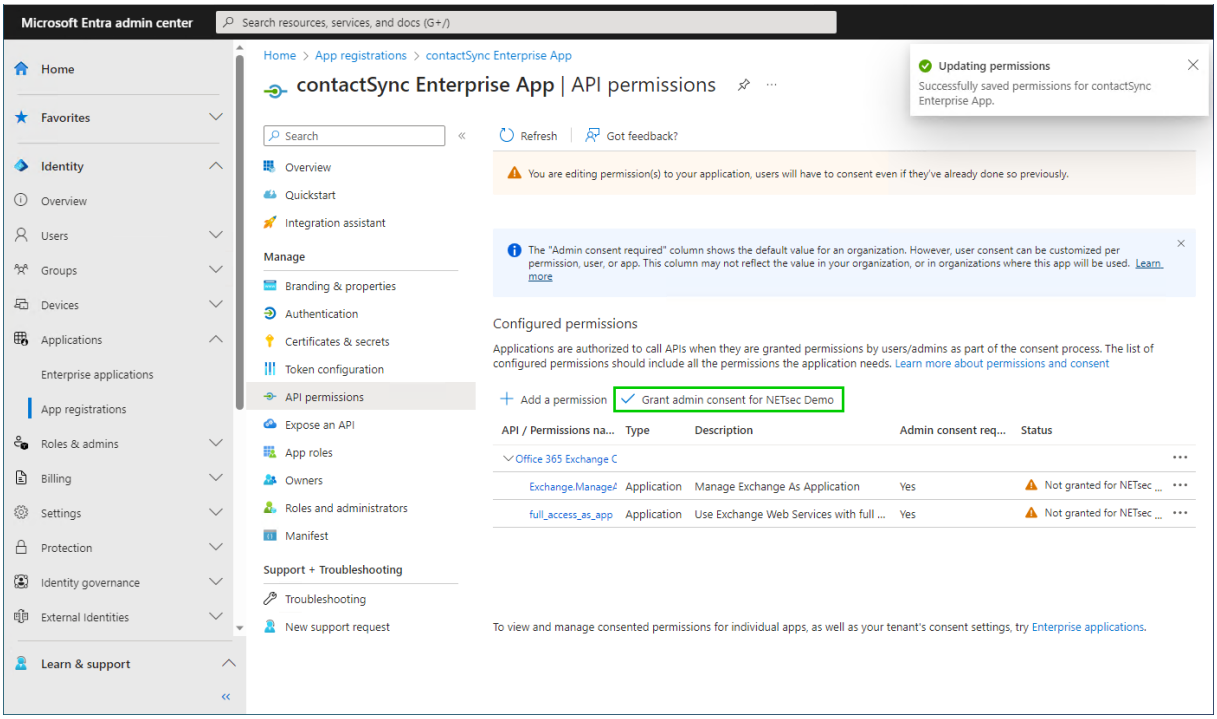


Select
full_access_as_app
Use Exchange Web Services with full access to all mailboxes
and
Exchange.ManageAsApp
Manage Exchange As Application

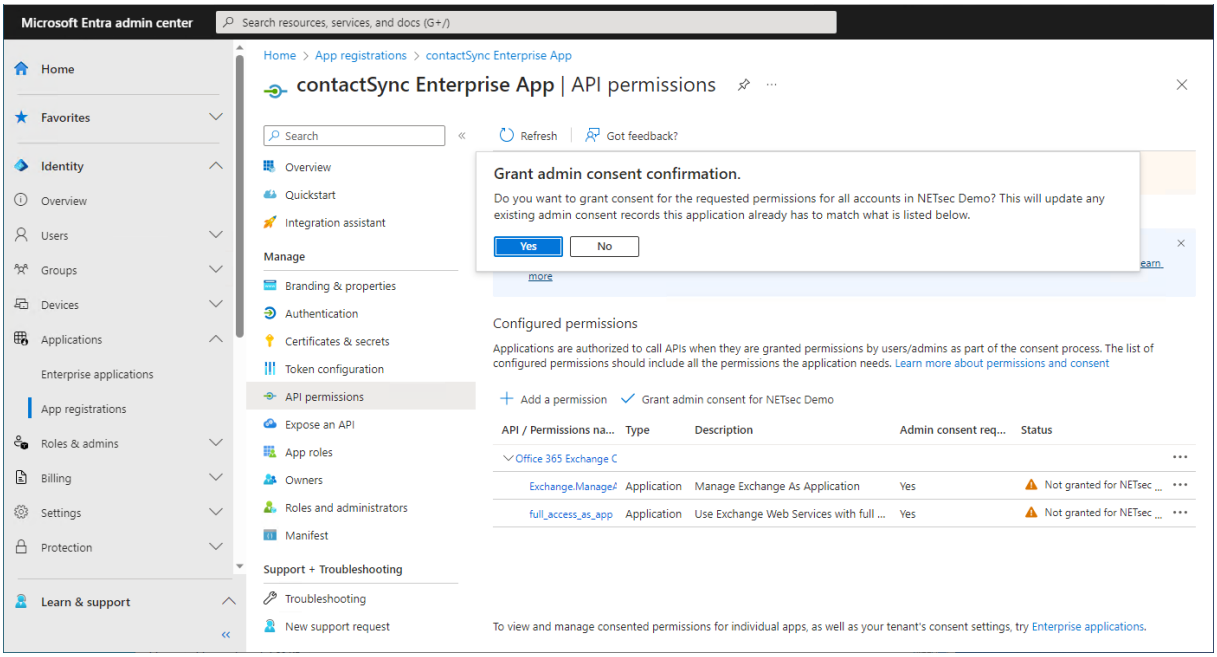


Click **Add permissions**

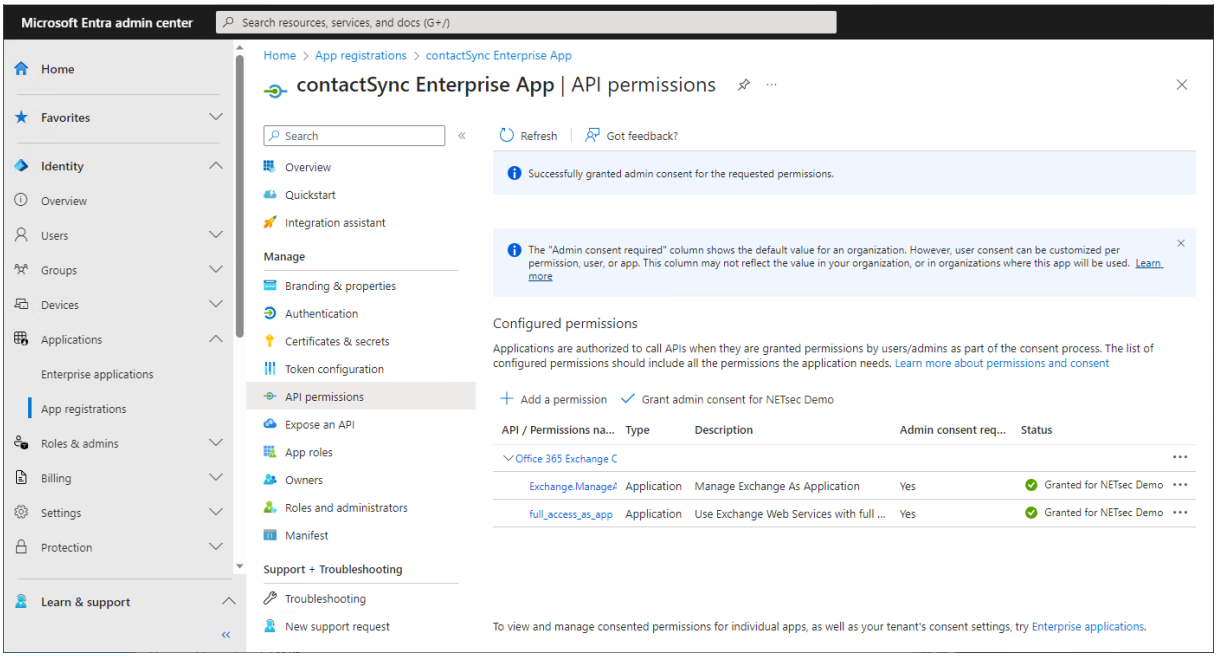
Click **Grant admin consent for** your tenant.



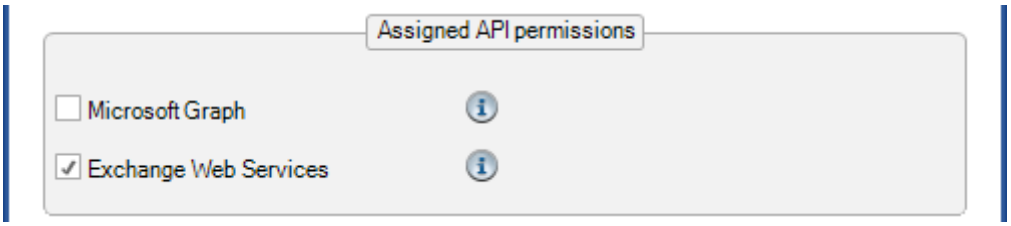
Click **Yes** to confirm the consent.



API permissions are assigned to the registered Application.



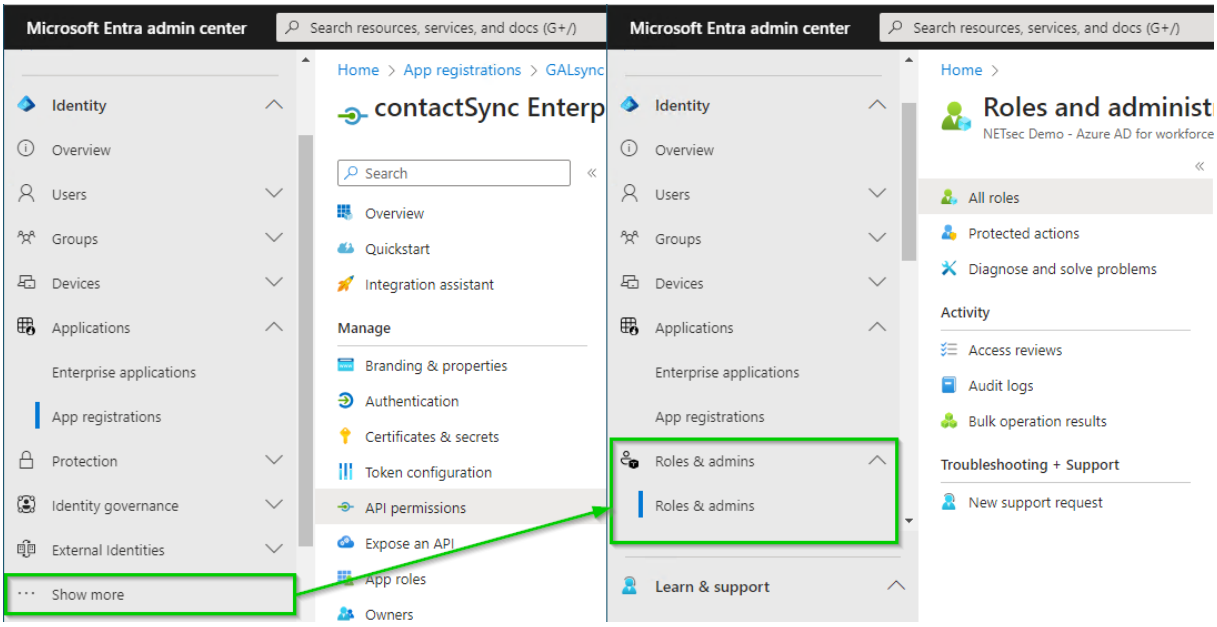
Accordingly, select **Exchange Web Services** at the **Assigned API permissions** group box in the Exchange Online App Registration dialog.



Exchange Administrator role for the registered Application

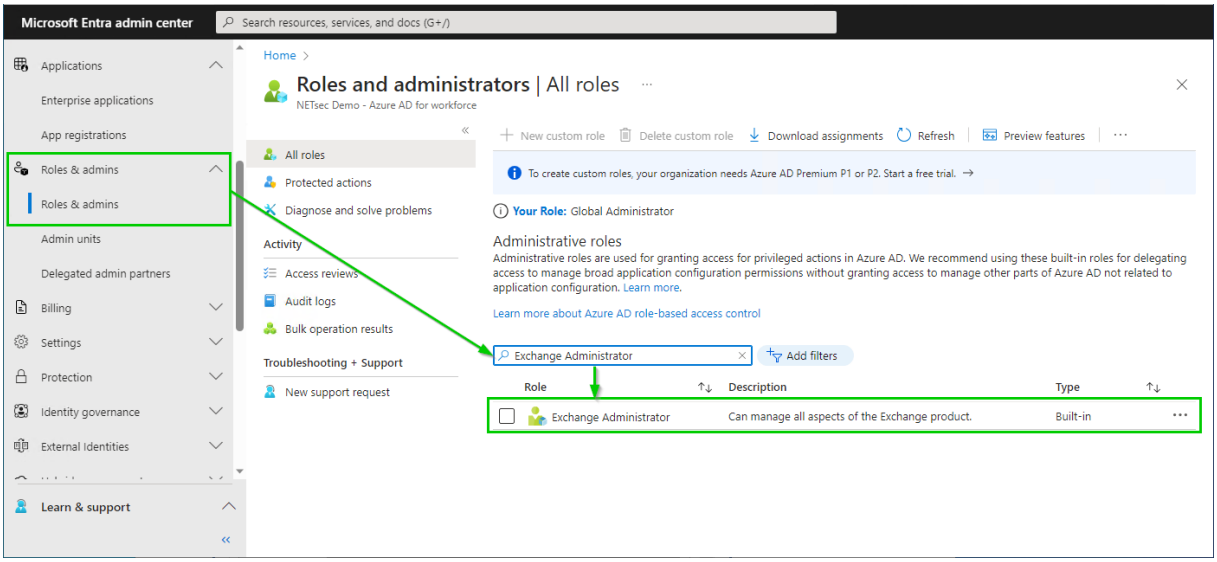
The **Exchange Administrator role** for **Exchange Online** is necessary because contactSync communicates via the **Exchange Online PowerShell** with the Microsoft 365 tenant.

The application requires **Exchange Administrator role** in the Microsoft 365 tenant, otherwise contactSync will not have access to the complete set of Exchange Online PowerShell cmdlets which are needed to function properly.

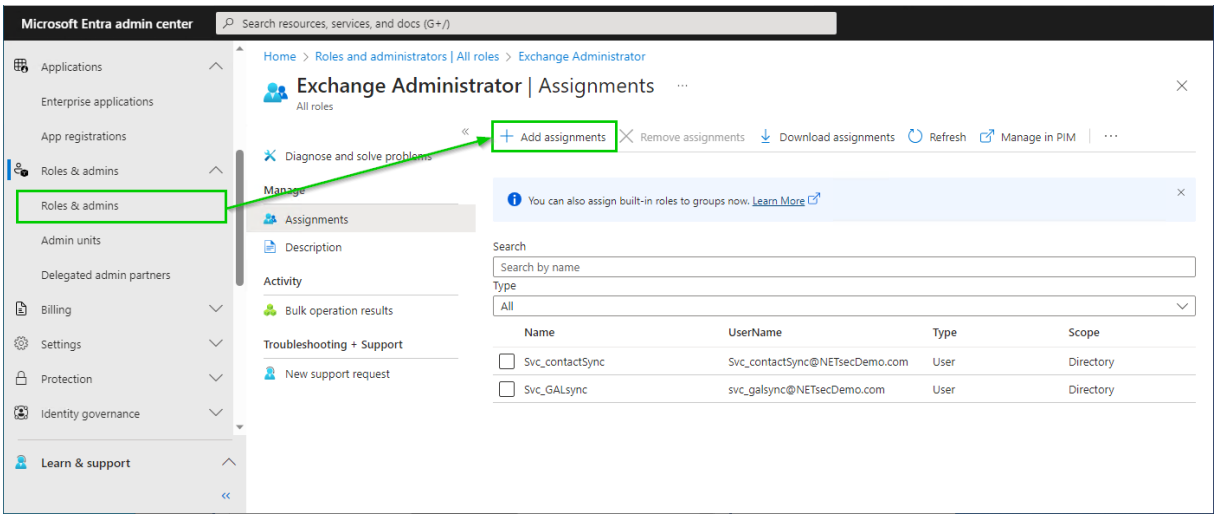


Expand **Roles & admins**. If you do not see **Roles & admins** in the **Identity** menu, click **Show more ...** .

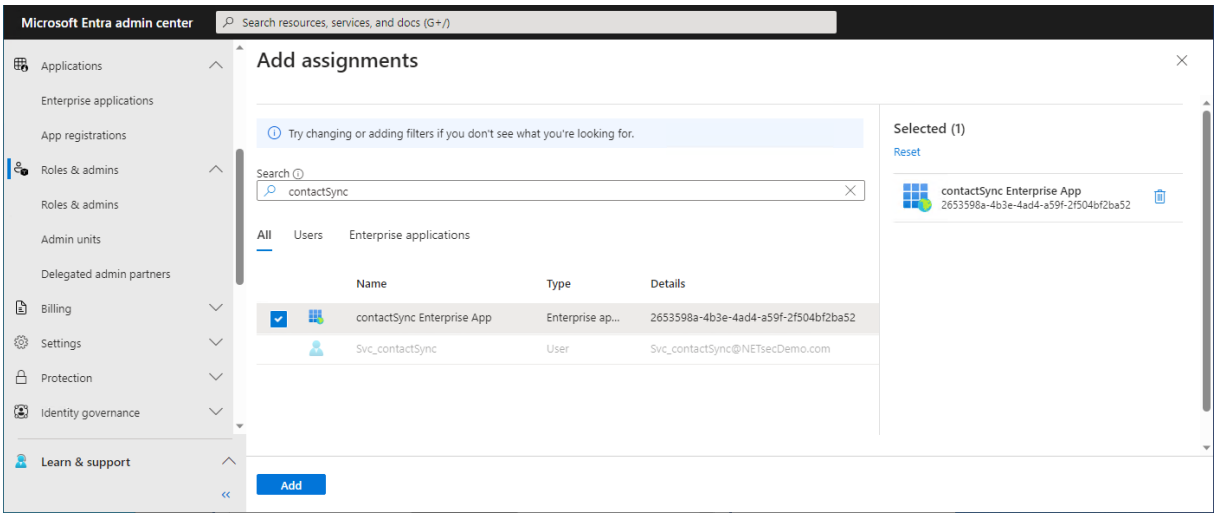
Go to **Roles & admins** in the expanded **Roles & admins** menu and search for **Exchange Administrator**.



Click on the **Exchange administrator** in the result list to open the **Exchange administrator role**.

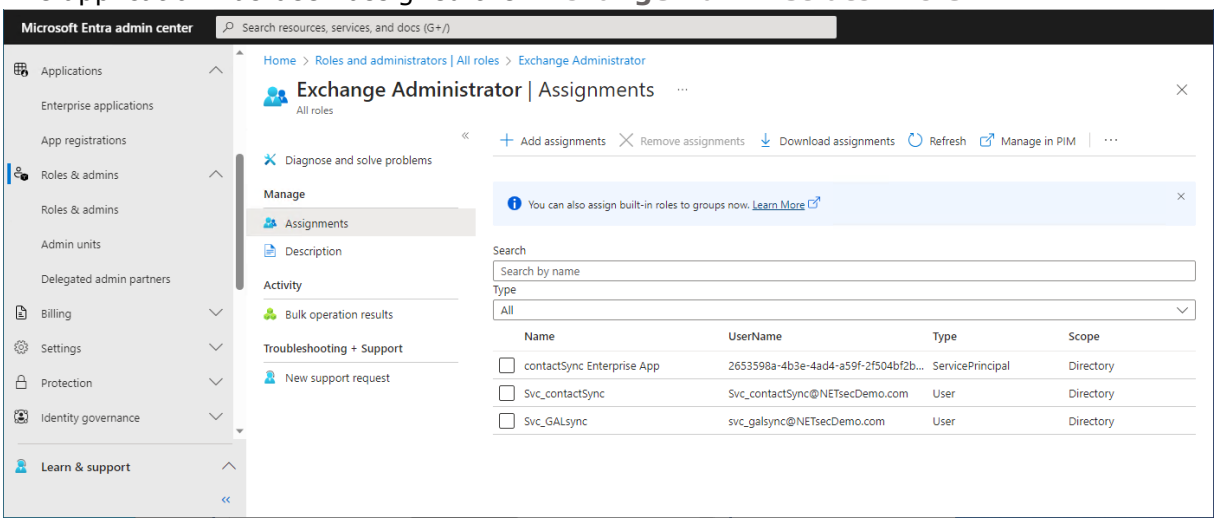


Click **Add assignments**, then search for the newly registered application.



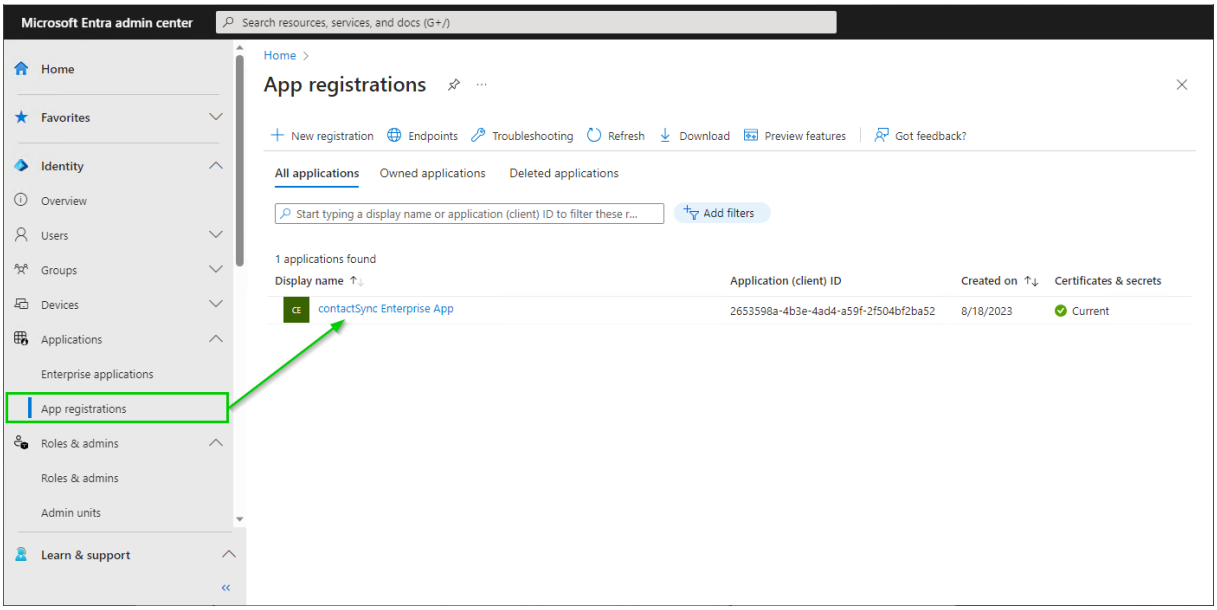
Select the newly registered application and click **Add**.

The application has been assigned the **Exchange Administrator Role**.

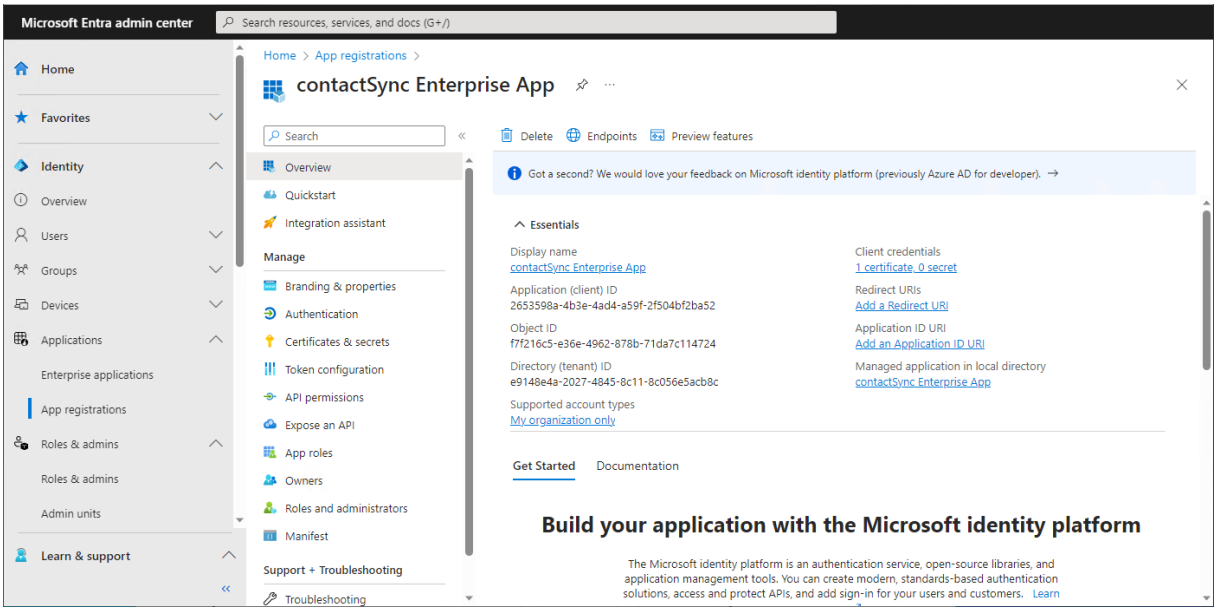


Overview of the registered Application in App registrations

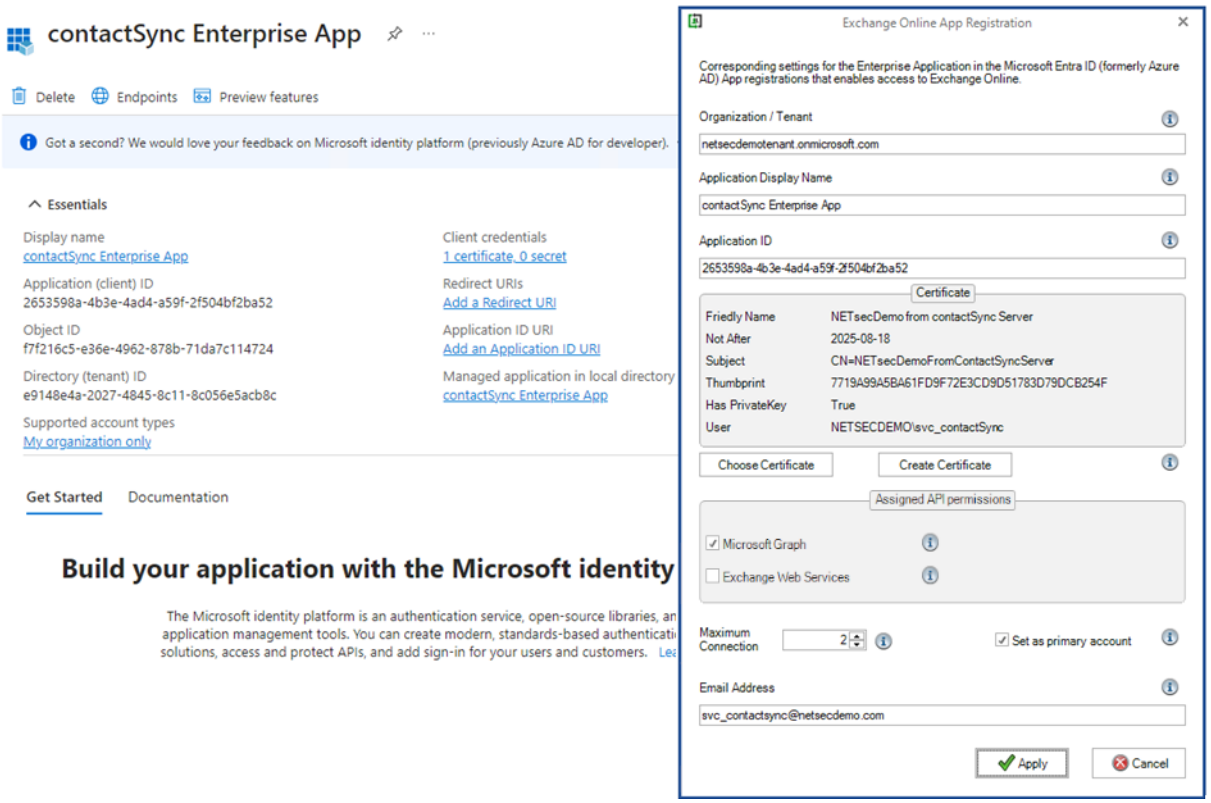
Go to **Identity** in the **Microsoft Entra admin center** menu, expand **Applications** and select **App registrations**.



Select the registered Application to see the overview.



Please check whether the values of the registered Application are corresponding with the values in the **Exchange Online App Registration** dialog.

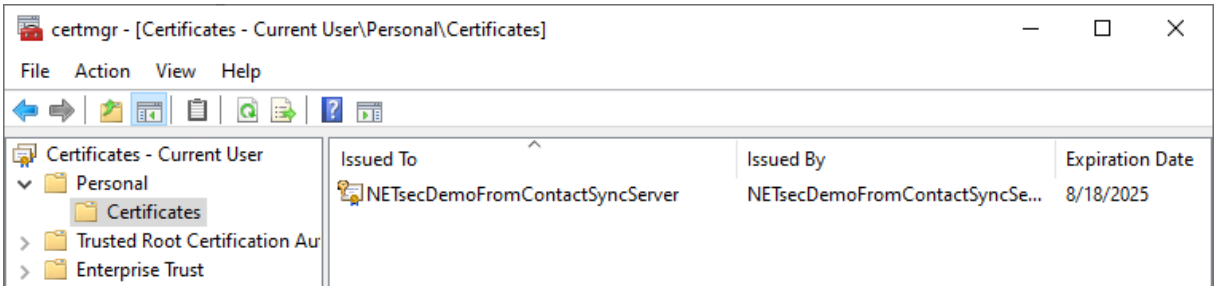


Organization / Tenant needs the **.onmicrosoft.com** domain name of the Microsoft 365 tenant. Otherwise, you might encounter cryptic permission issues when you run a policy in the app context.

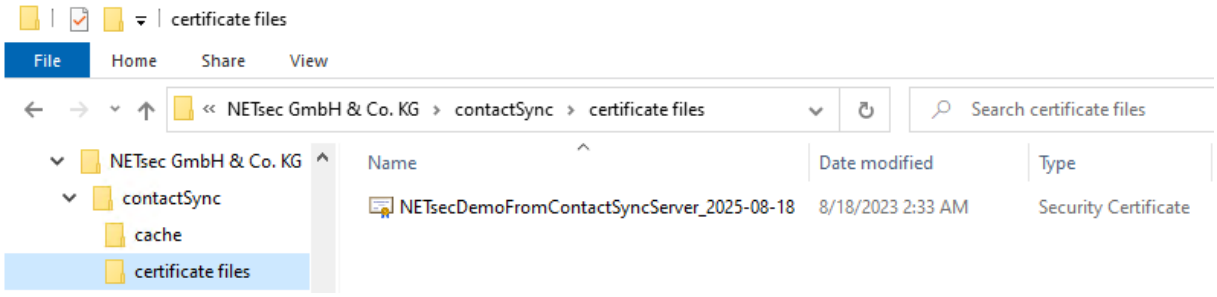
Application Display Name must have the value of the **Display name** of the registered Application.

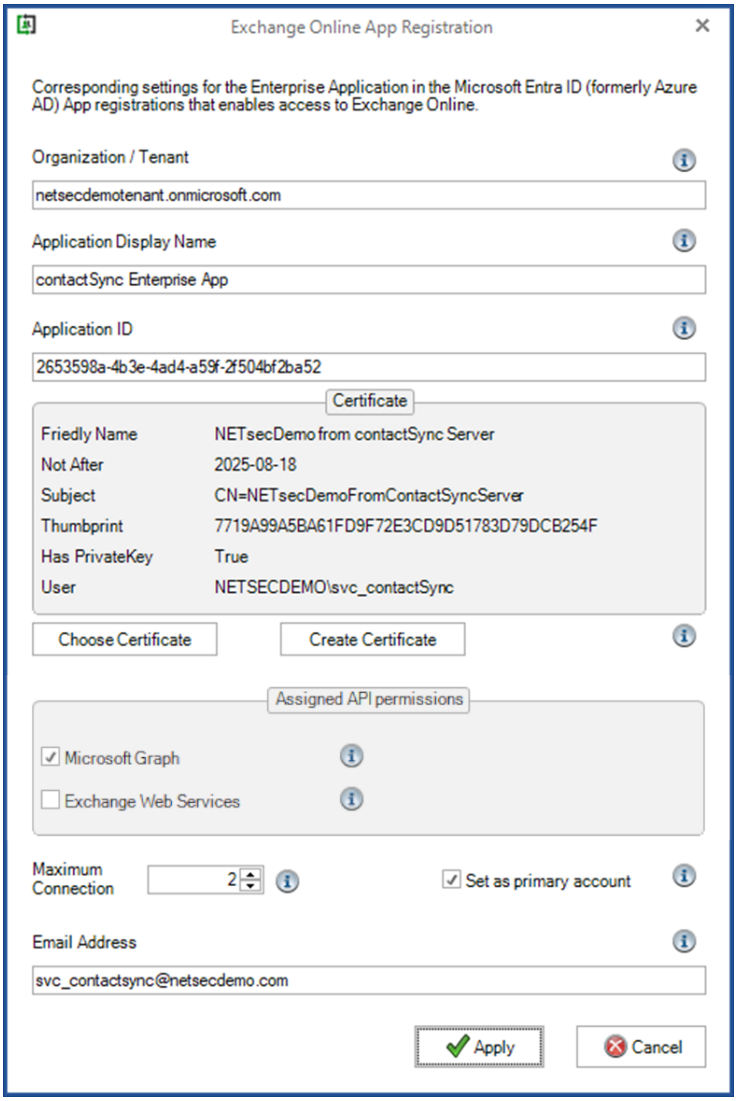
Application ID must have the value of the **Application (Client) ID** of the registered Application.

A **Certificate** is created and selected from **Current User Personal Certificates store**



and the corresponding certificate file is attached to the **Entra ID application**.

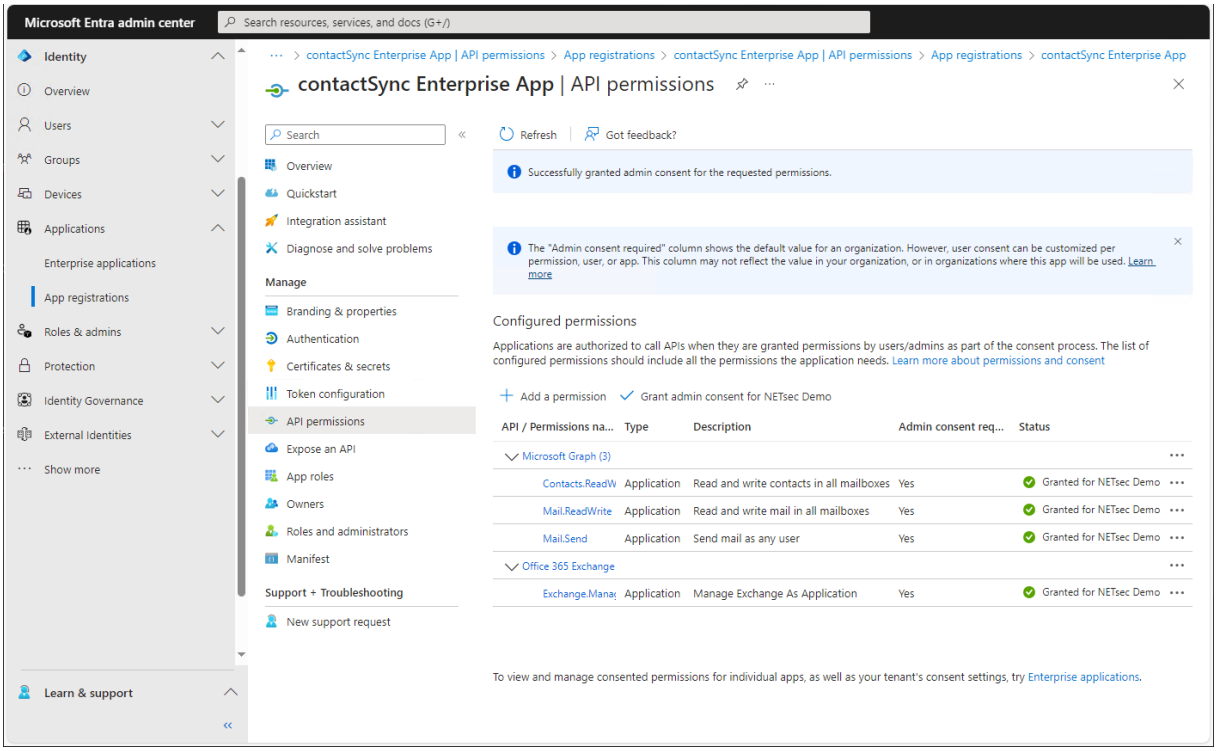




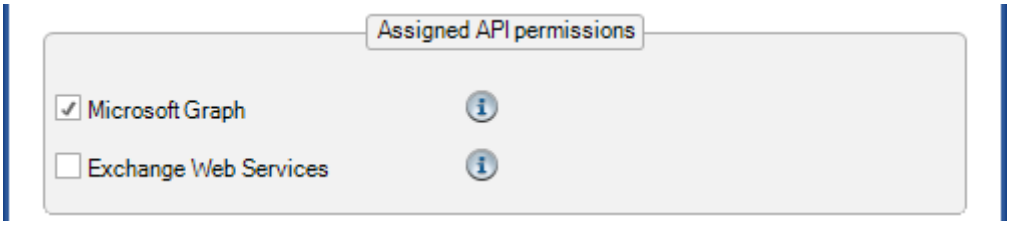
The selection of the **Assigned API permissions** group box in the **Exchange Online App Registration** dialog must be corresponding with the **API permissions** in the App Registration.

Please check the settings of the **API permissions for Microsoft Graph**.

Policies synchronizing contacts from **Exchange Online** and from **Shared Mailboxes**, which are located in Exchange Online, need these API permissions.

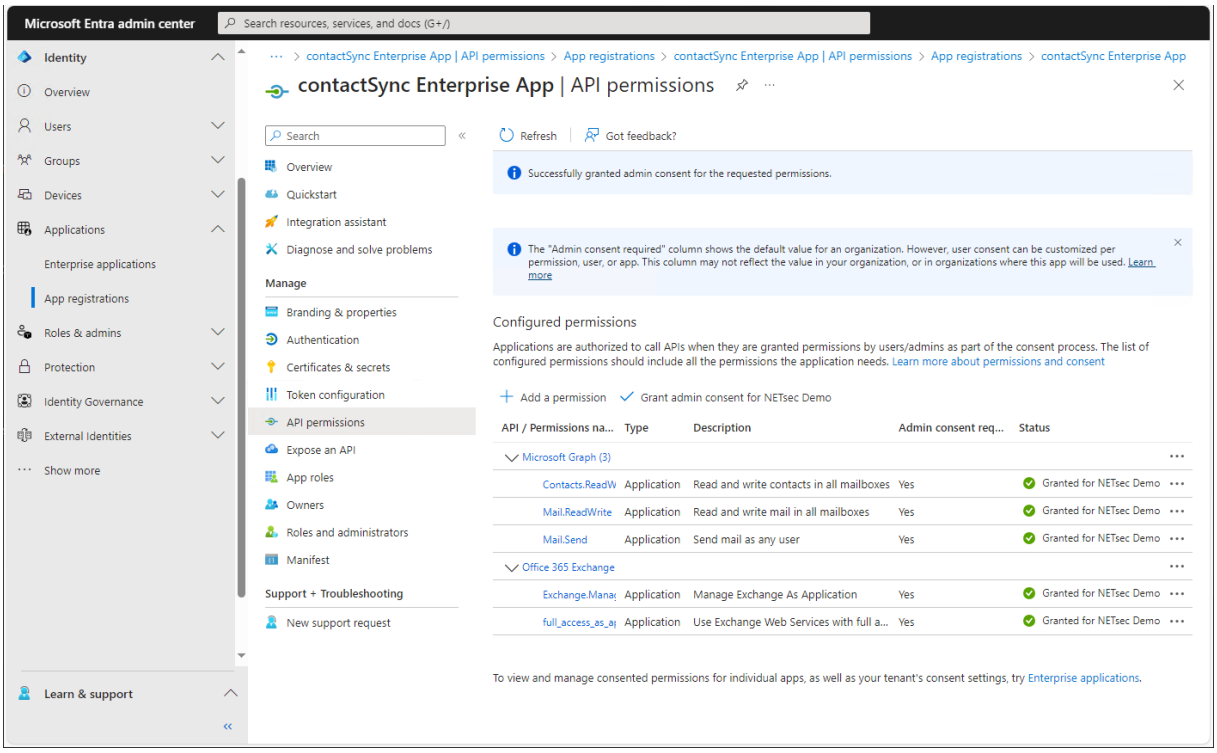


Accordingly, the **Microsoft Graph** at the **Assigned API permissions** group box must be selected in the Exchange Online App Registration dialog.

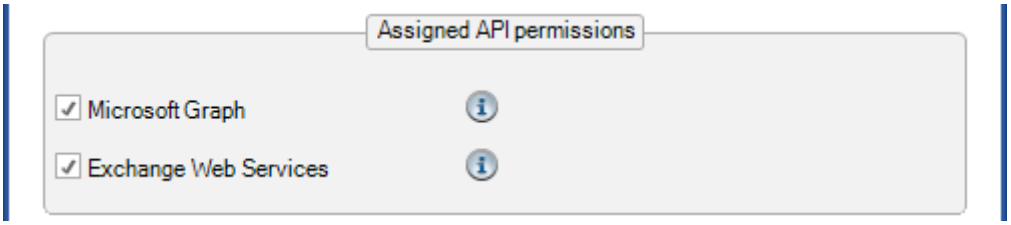


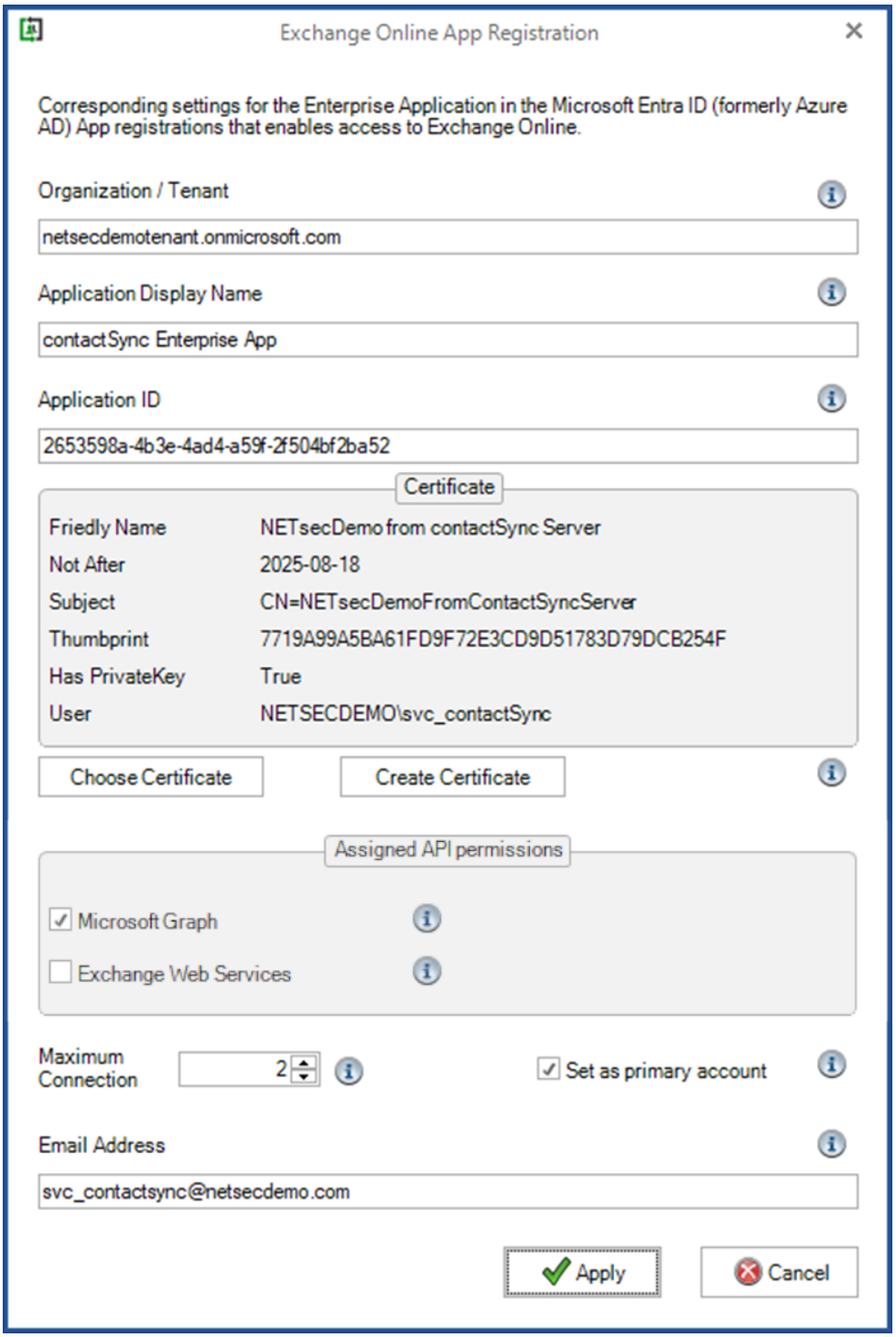
Please check the settings of the **API permissions for Microsoft Graph** and **Exchange Web Services**, if **Public Folder contacts from Exchange Online** need to be synchronized in the users´ mailboxes.

Policies synchronizing contacts from **Public Folder**, which are located in Exchange Online, need additionally the permission for Exchange Web Services at the moment.



Accordingly, the **Microsoft Graph** and **Exchange Web Services** at the **Assigned API permissions** group box must be selected in the Exchange Online App Registration dialog at the moment.



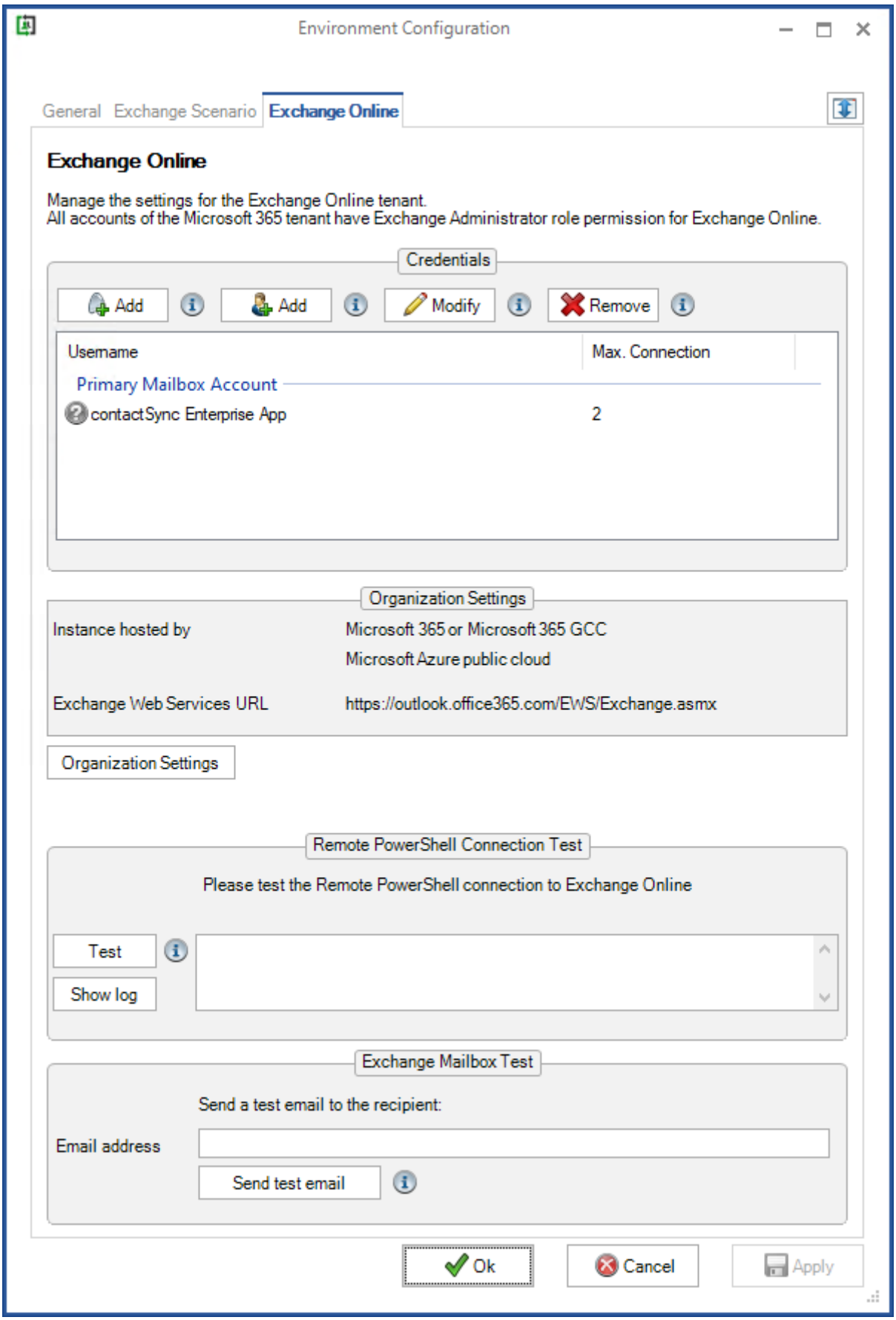


To complete the **Exchange Online App Registration** dialog, insert an **Email Address** of an Exchange Online mailbox.

Email Address of an Exchange Online mailbox is necessary to send and receive email. We recommend to use a dedicated Exchange Online mailbox for this purpose.

Click **Apply** to finish and close the **Exchange Online App Registration** dialog.

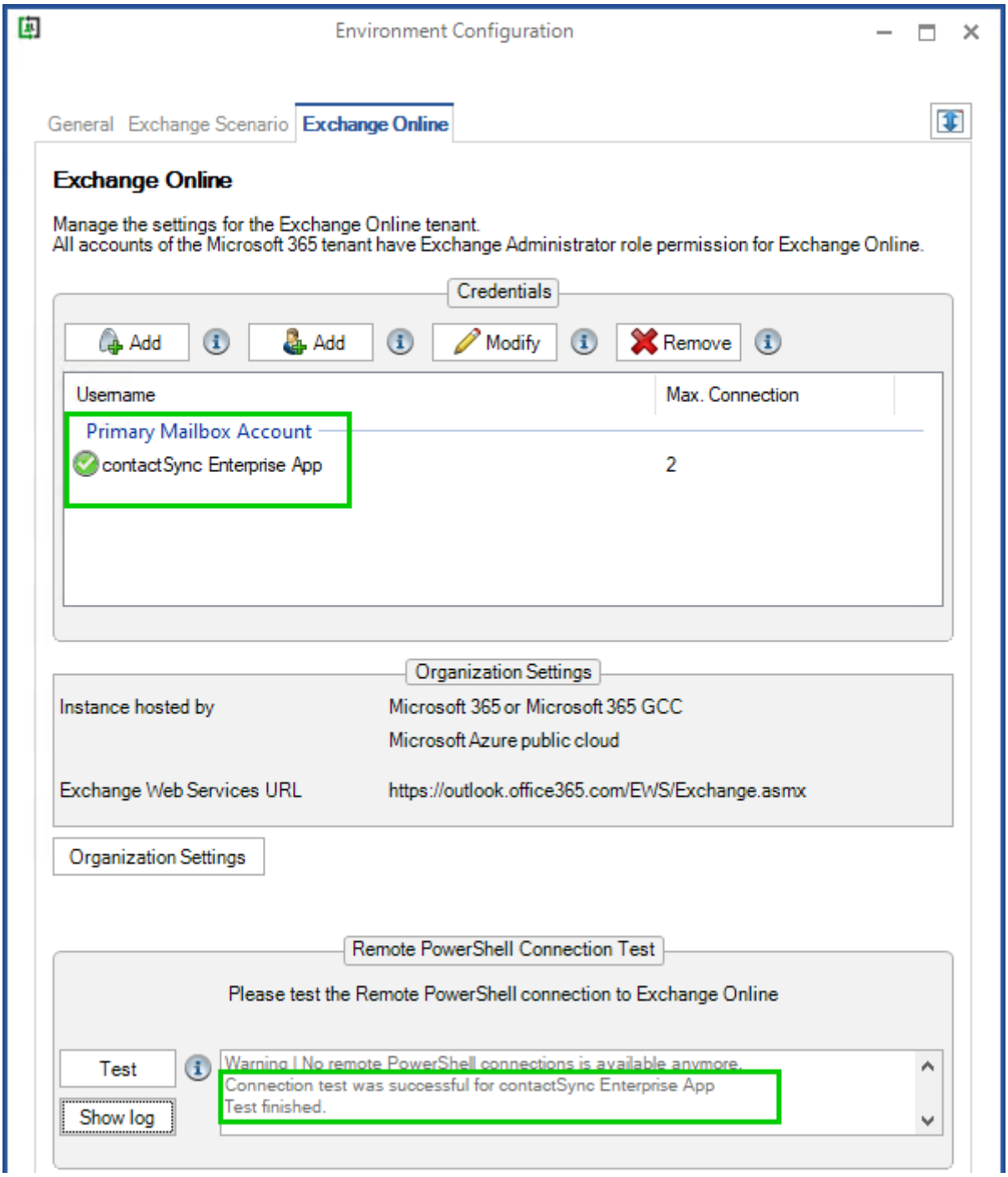
Test the Exchange Online PowerShell connection and the Exchange mailbox



Click the **Test** button for the **Remote PowerShell Connection Test**, to test connectivity to Exchange Online PowerShell.

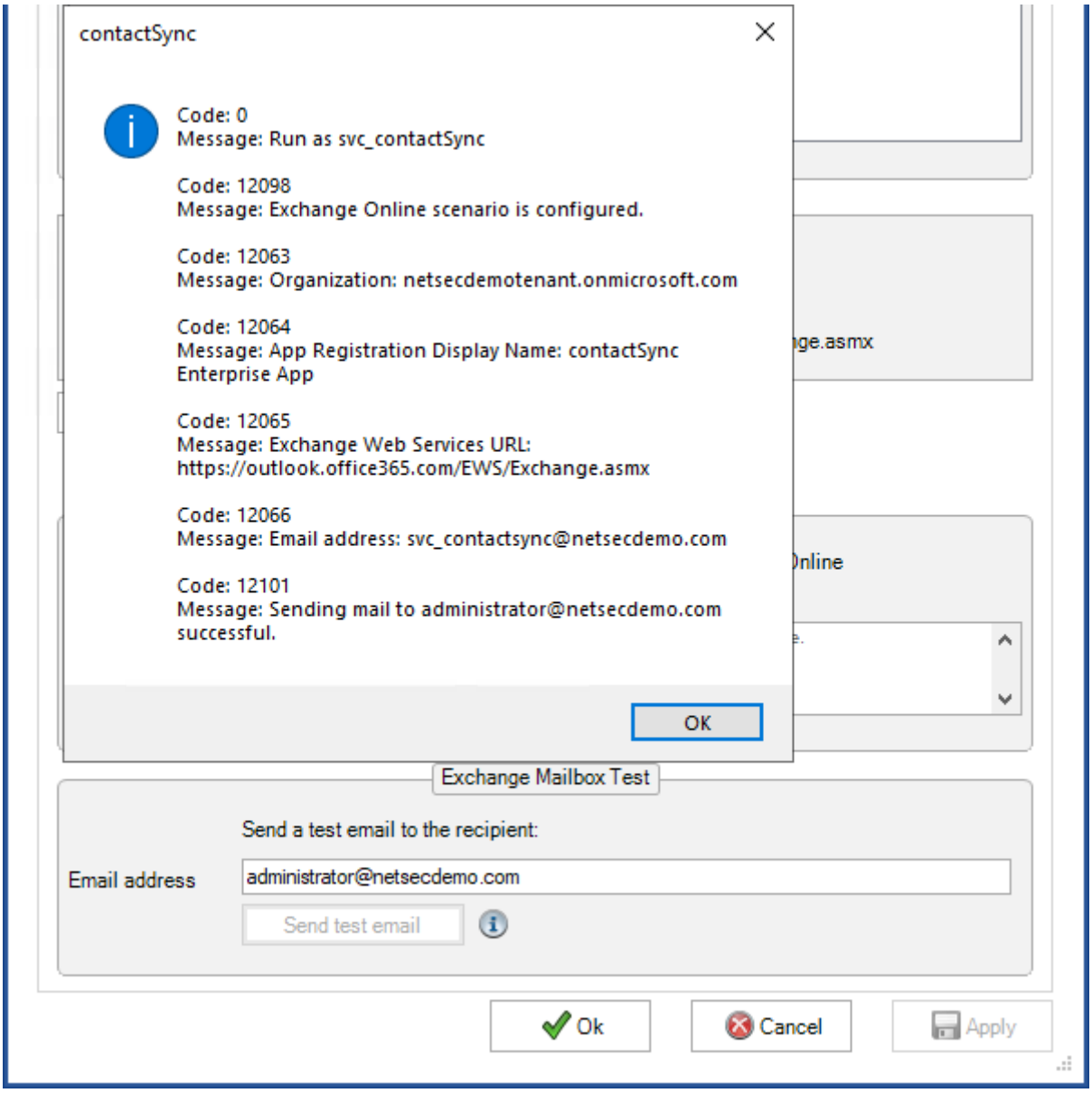
Please wait for the test to finish before proceeding.

Upon a successful connection, a green circle with a checkmark will be displayed.



If the connection test failed, click the **Show log** button for detailed information.

A test email can also be sent to the desired recipient as an additional test to validate mail flow. To do this, click the **Send test email** button for the **Exchange Mailbox Test**.



Please note, that the e-mail address of the recipient for the test email will not be saved.

Exchange Online authentication via Service Account

Please note, that user-based authentication via OAuth 2.0 works only for the Microsoft Azure Public Cloud instance. If your Microsoft 365 instance is hosted by a national cloud, please use **Exchange Online certificate-based authentication via App Registration**.

Note, the user-based authentication is deprecated. The certificate-based authentication is recommended.

Service Account (Microsoft 365 Exchange Online)

The contactSync service account needs to be a licensed Exchange Online mailbox user in the Microsoft 365 tenant.

For example: Microsoft 365 Business Basic, Exchange Online (Plan 1) or Microsoft 365 E1 license will work for the service account.

The service account must be a member of the **Exchange Administrator** role. contactSync uses the Exchange Online PowerShell commands, which are incomplete if the service account is not an Exchange Administrator for Exchange Online.

Note: By default, the Exchange Online password has to be changed within 30 days. To ensure, that contactSync works properly, you have to configure user passwords to never expire. To configure your password please follow the steps described in the following article:

https://support.office.com/en-us/article/Set-a-user-s-password-expiration-policy-0f54736f-eb22-414c-8273-498a0918678f

- contactSync must have direct access to the user mailbox of the service account via Exchange Web Services (EWS) of Exchange Online.
- Ensure that the mailbox is accessible (e.g., by Outlook Web Access).
- Ensure that the mailbox can send email.

Please note, service accounts are non-human privileged accounts used by applications, automated services, and that execute other IT processes. Because these are machine accounts, they cannot be protected by **multi-factor authentication (MFA)**, since there is no way for it to interactively logon.

We recommend disabling **multi-factor authentication (MFA)** for this account, and use conditional access policies to lock down this account, such as allowing login only from trusted public IP addresses.

Modern Authentication OAuth 2.0 for Exchange Web Services (EWS) to access Exchange Online

The contactSync service account of a Microsoft 365 tenant needs access to its own mailbox, therefore, Modern Authentication OAuth 2.0 for Exchange Web Services (EWS) must be configured.

Please note, that user-based authentication via OAuth 2.0 works only for the Microsoft Azure Public Cloud instance. If your Microsoft 365 instance is hosted by a national cloud, please use **Exchange Online certificate-based authentication via App Registration**.

First, please verify the contactSync GUI is running in the credentials of the local contactSync service account, otherwise contactSync cannot decrypt the token later.

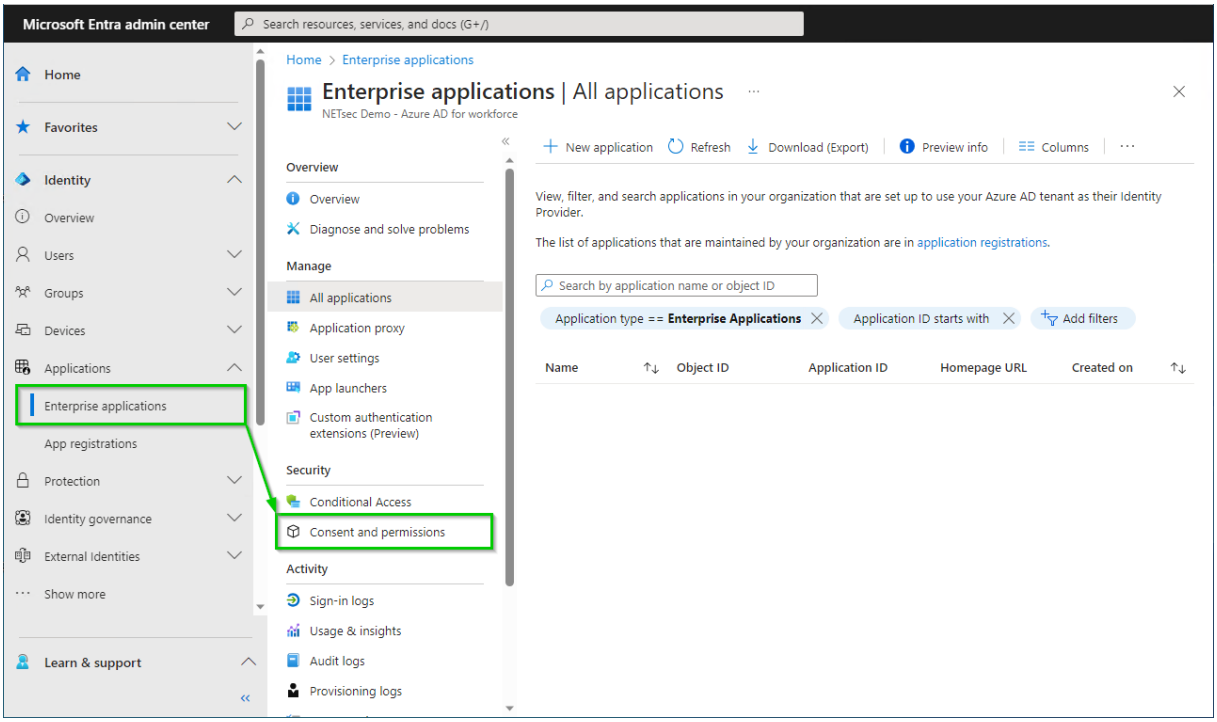
This can be confirmed on the information bar at the bottom of the contactSync GUI.

Admin consent requires in Entra ID Enterprise Applications (formerly Azure AD Enterprise Applications) to register NETsec contactSync as Enterprise Application.

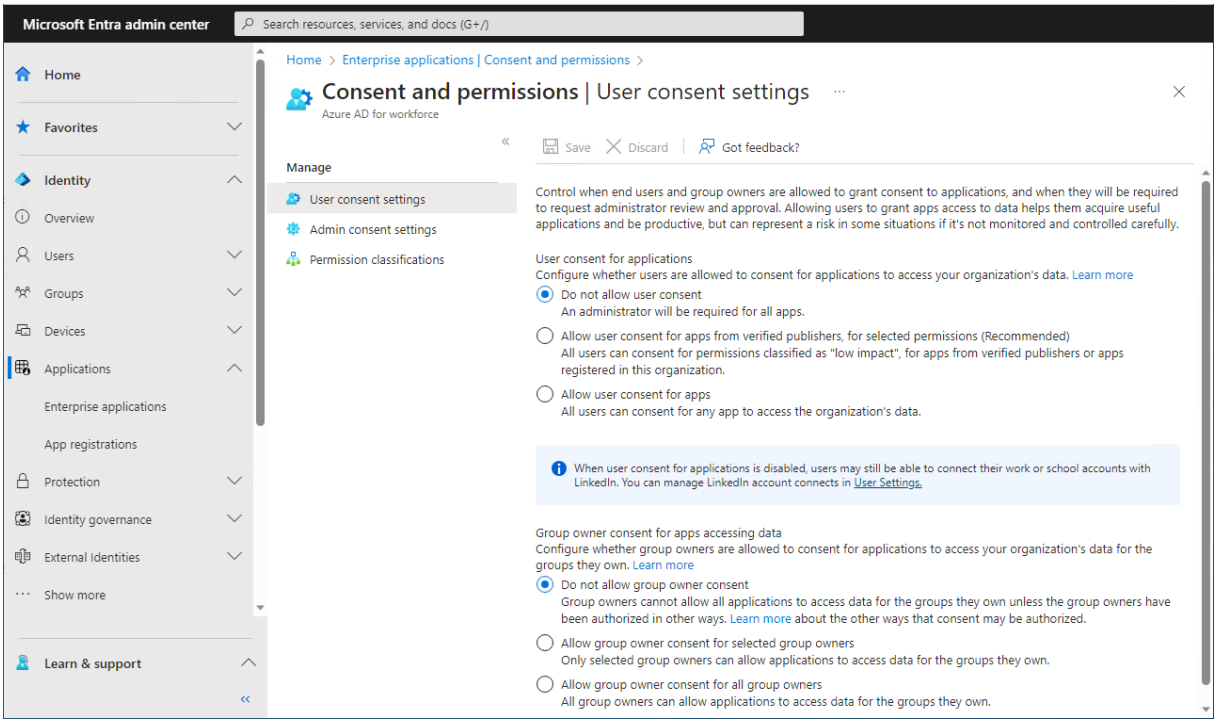
*Please note, that contactSync cannot request the necessary **User consent** for a non admin user with restricted settings **Consent and permissions** for Modern Authentication OAuth 2.0 for Exchange Web Services (EWS) of Exchange Online.*

How to check the Consent and permissions settings for Enterprise Applications?

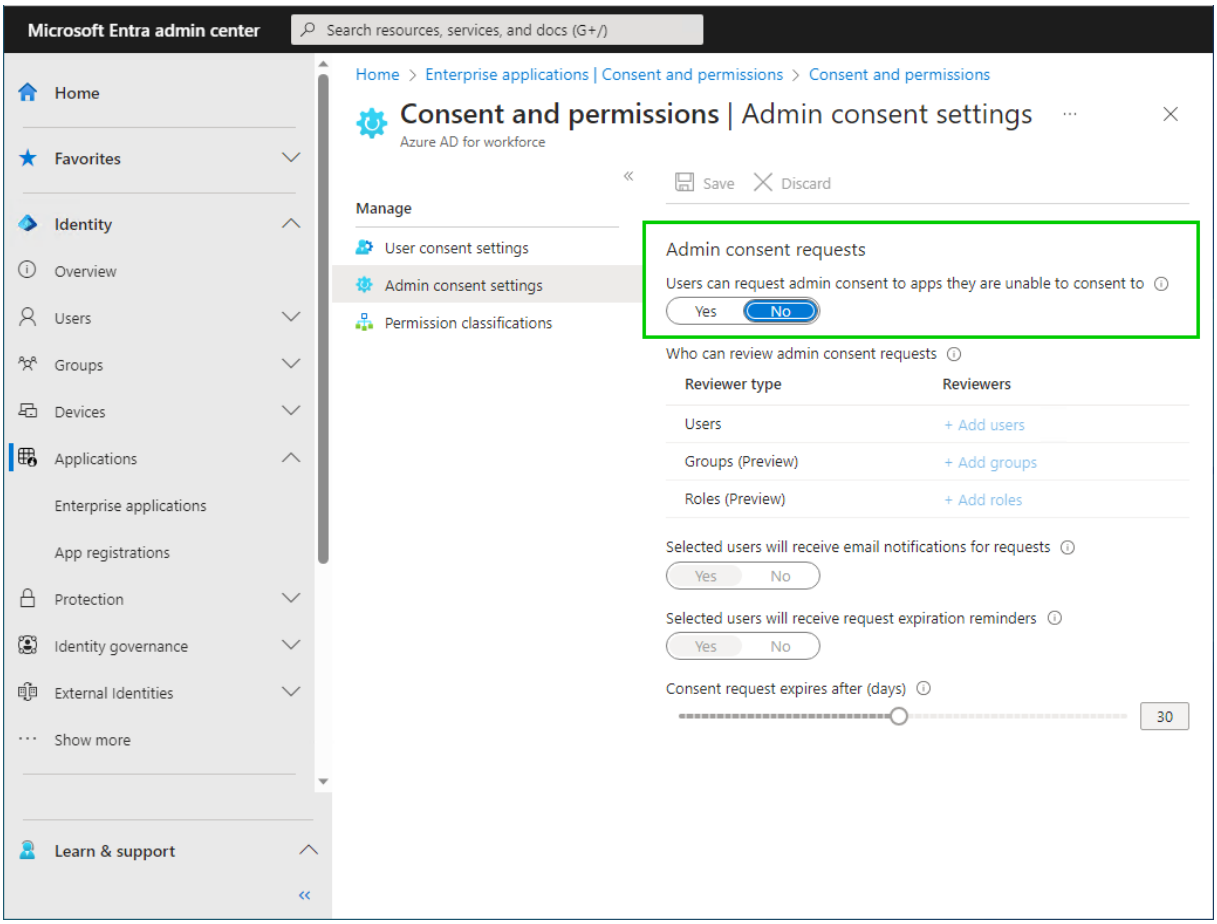
Microsoft Entra admin center -> Identity -> Applications -> Enterprise applications -> Consent and permissions



The **Consent and permissions** settings of the **Enterprise applications** are restricted:



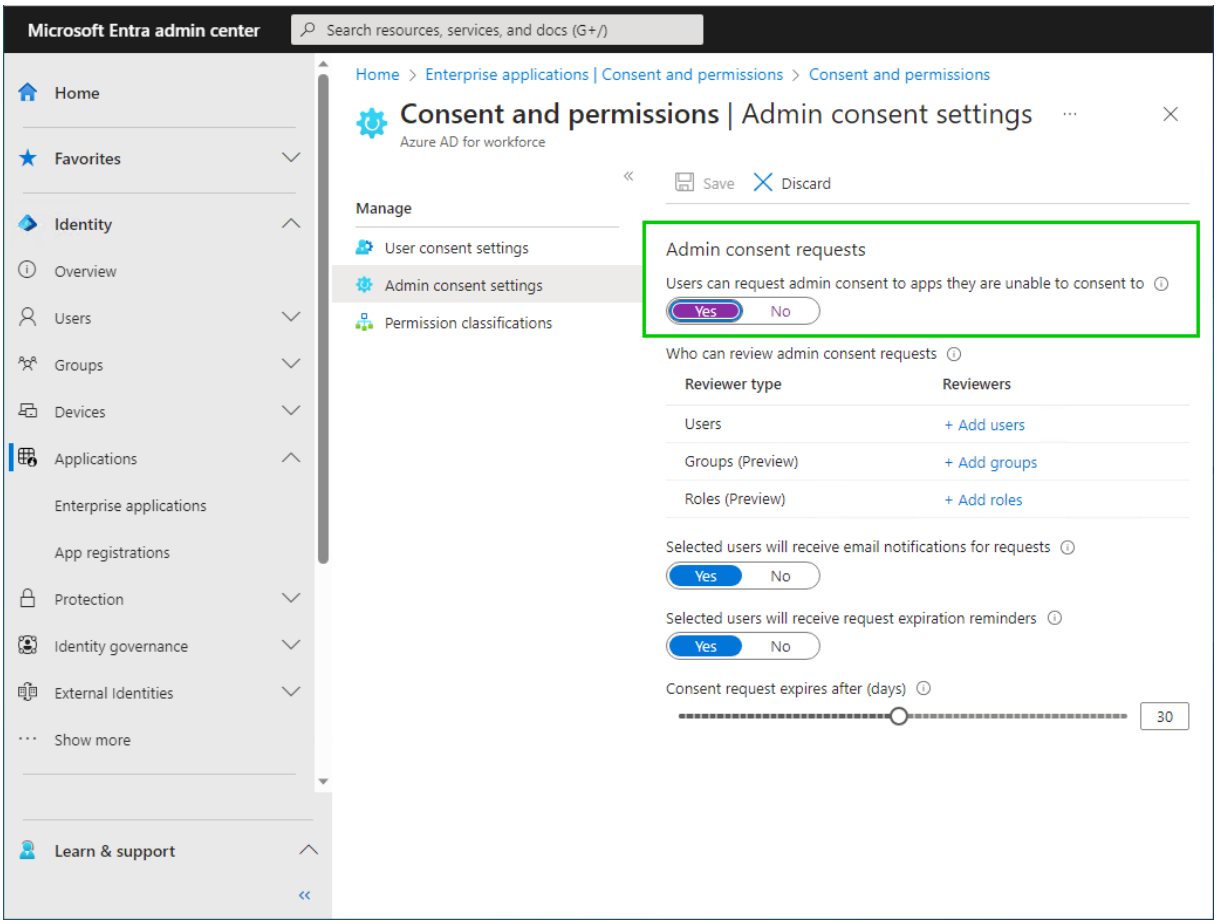
The **Consent and permissions** settings of the **Enterprise applications** are restricted and a Global Administrator account of the Microsoft 365 tenant must grant admin consent for the permissions of the Enterprise Application.



If the **Admin consent requests** in the **Admin consent settings** is **No**, the admin consent for the permissions of the Enterprise Application can be done with a sign in of a Global Administrator account during the first login process for Modern Authentication OAuth 2.0 for Exchange Web Services (EWS) of Exchange Online. This process is described in the following chapter.

*Please note, the contactSync service account should only be an Exchange Administrator of Exchange Online, but **not** a Global Administrator of the Microsoft 365 tenant.*

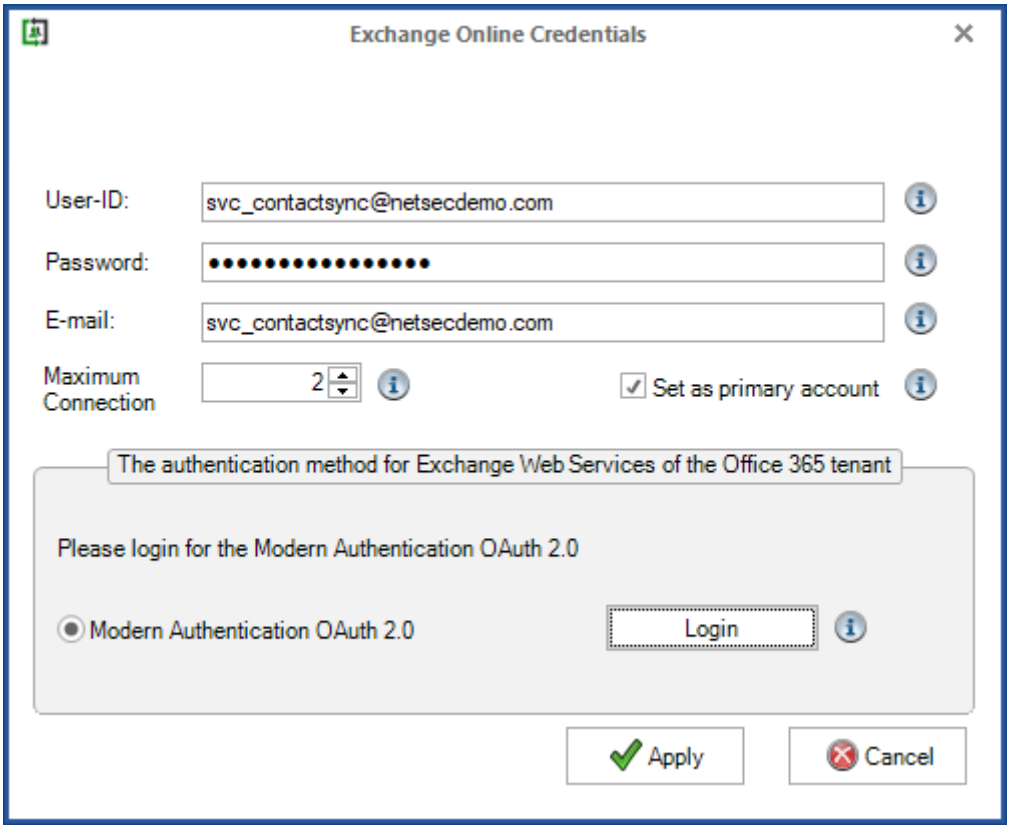
If the **Admin consent requests** in the **Admin consent settings** is **Yes**, the contactSync service account will send an admin consent request during the first login process for Modern Authentication OAuth 2.0 for Exchange Web Services (EWS) of Exchange Online.



After that a user, who can review admin consent requests, must accept the request, before the contactSync service account does the login for Modern Authentication OAuth 2.0 for Exchange Web Services (EWS) of Exchange Online a second time to get the token successfully.

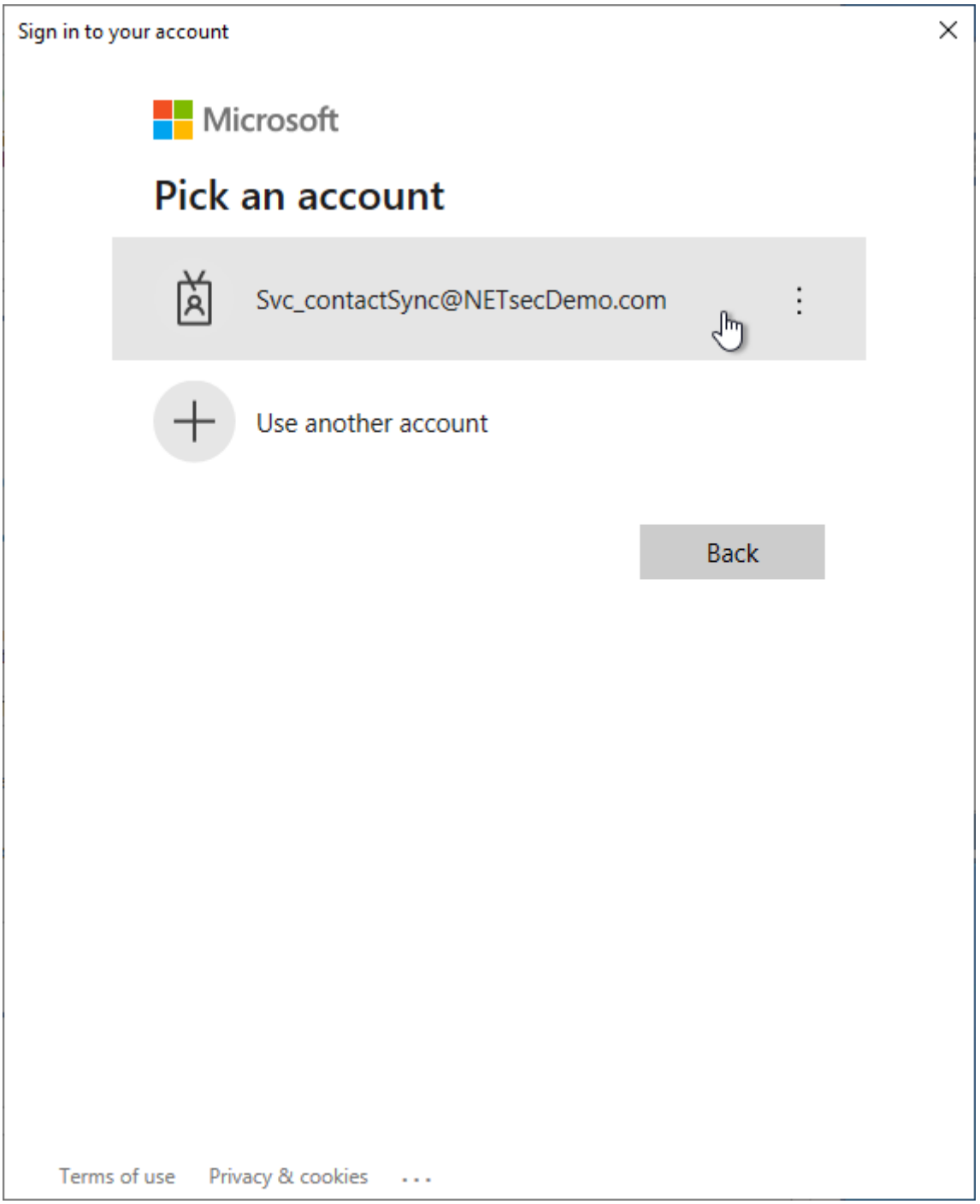
Login for Modern Authentication OAuth 2.0 for Exchange Web Services (EWS) of Exchange Online

Proceed with the Login for Modern Authentication OAuth 2.0 for Exchange Web Services (EWS) of Exchange Online with your contactSync Service Account.

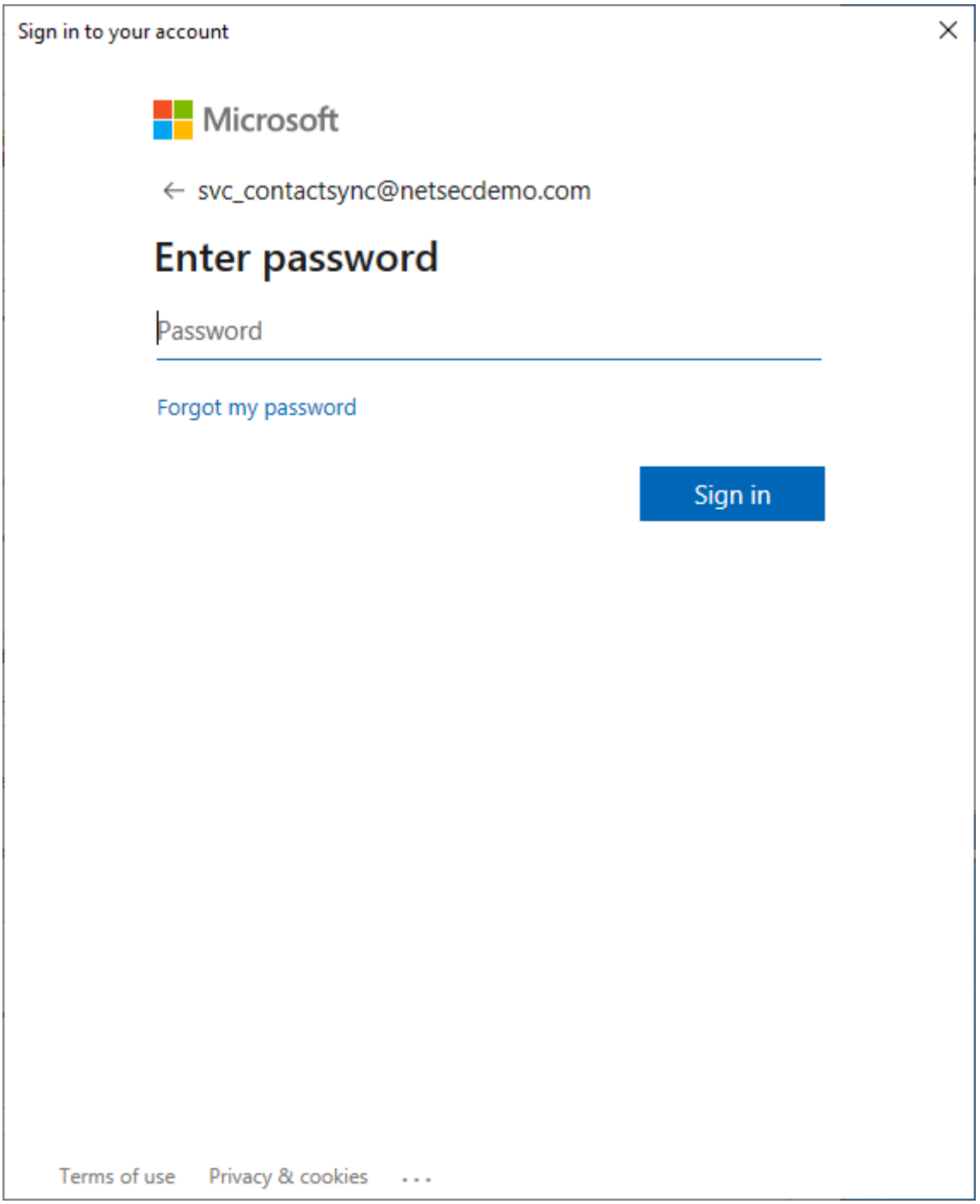


Please note, that the User-ID and the E-mail address can be different for an Exchange Online mailbox user. This depends on your Microsoft 365 Exchange Online tenant.

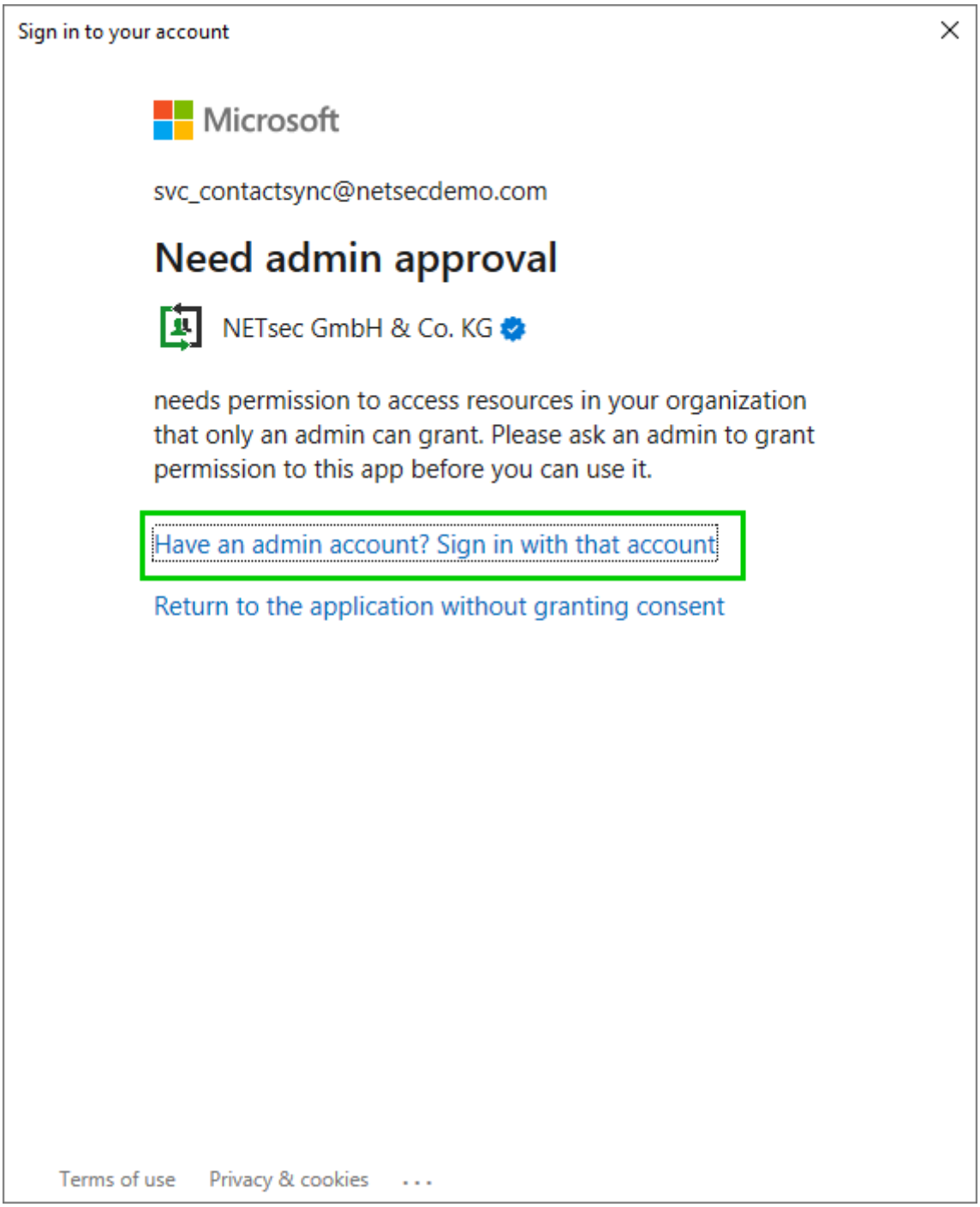
Insert the credentials for the contactSync service account, and click the **Login** button.



Select the same contactSync service account, which you have used in the **Exchange Online Credentials** dialog before.



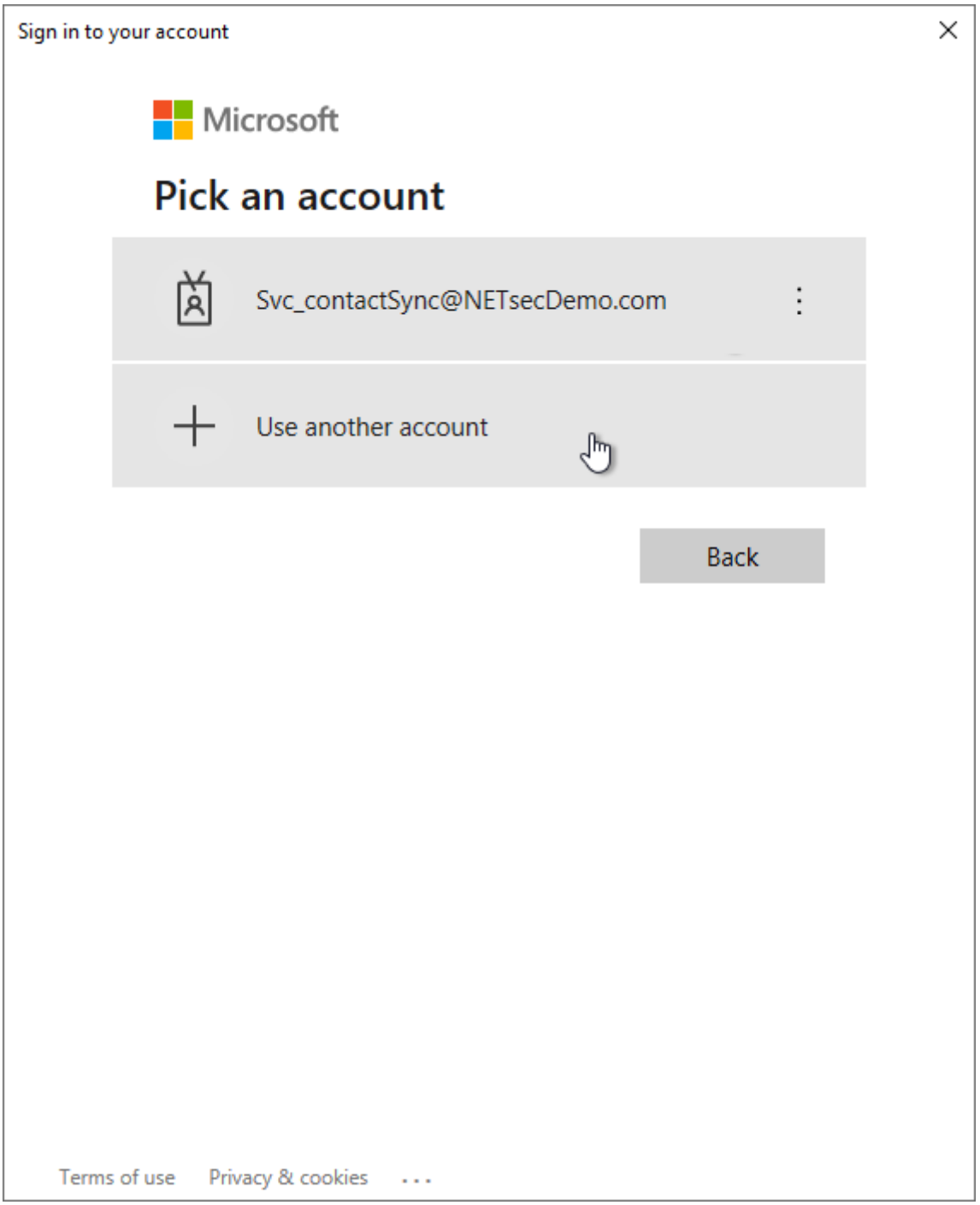
Insert the password of the contactSync service account.



NETsec contactSync needs a sign in of a Global Administrator, who will accept the requested permissions for the Enterprise Application.

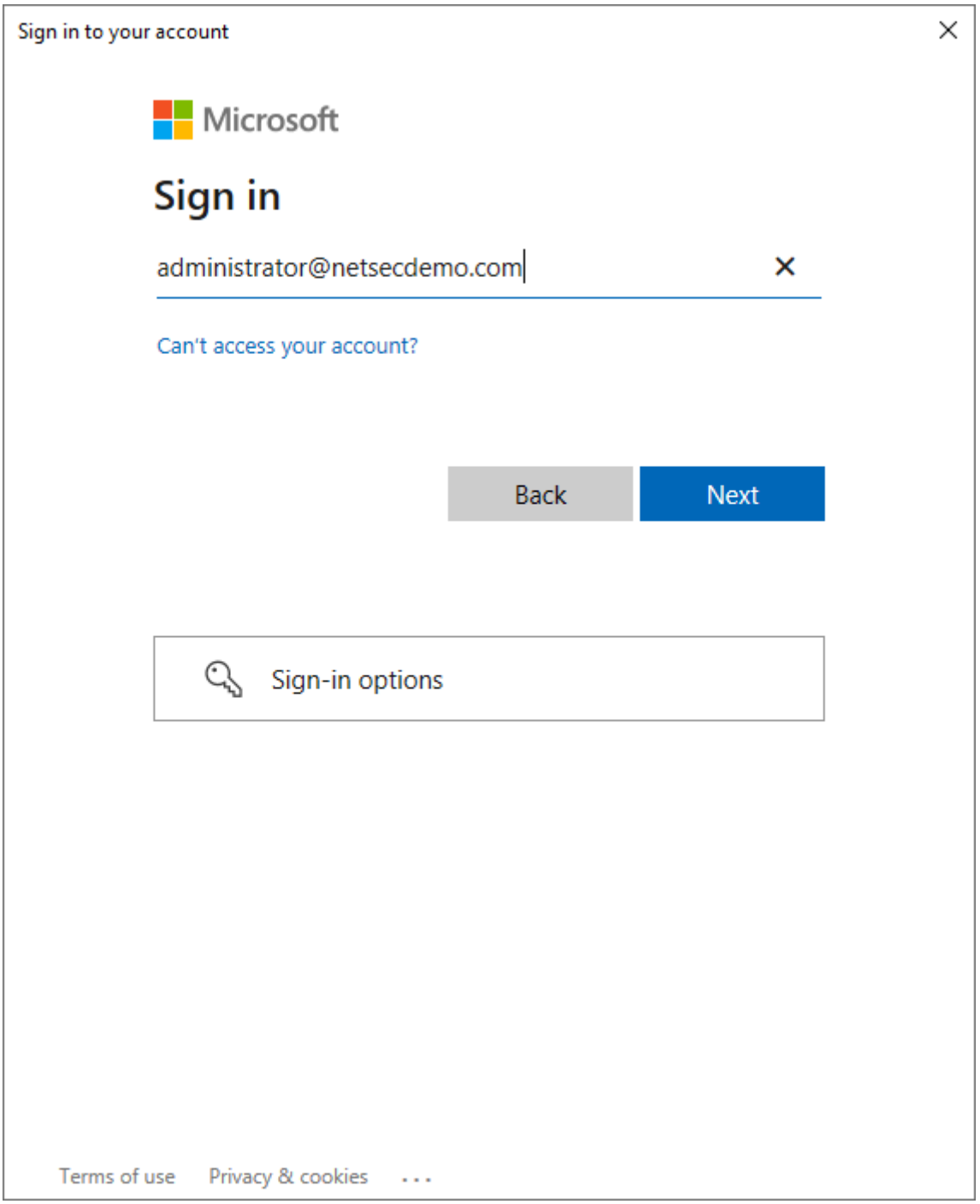
Click on **Have an admin account? Sign in with that account**.

Otherwise, a Global Administrator account grants consent for the requested permissions to the application under **Permissions** of the **NETsec contactSync Enterprise Application** in the **Microsoft Entra ID**, before the contactSync service account does the login for Modern Authentication OAuth 2.0 for Exchange Web Services (EWS) of Exchange Online a second time to get the token successfully.

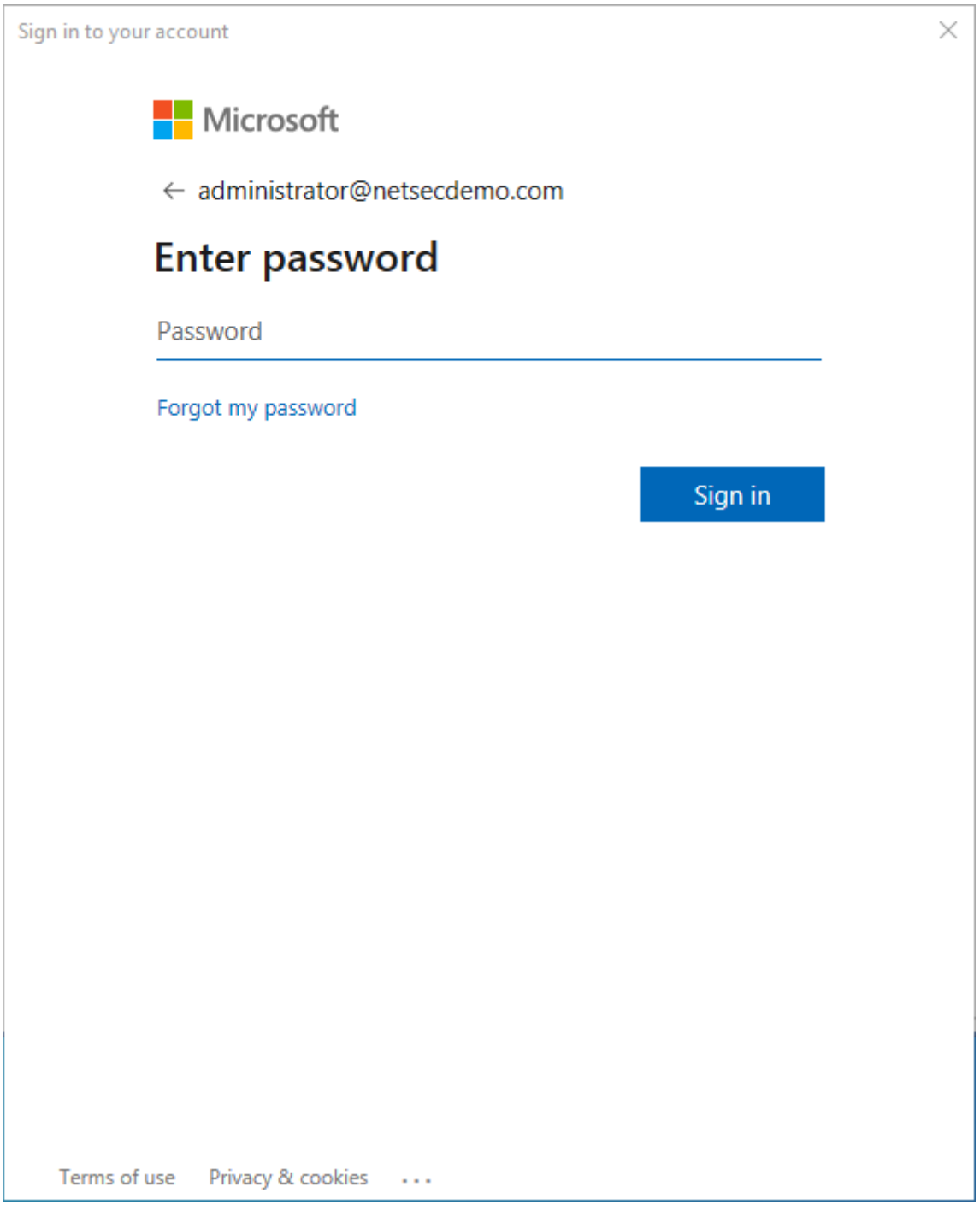


Use another account to sign in as a Global Administrator.

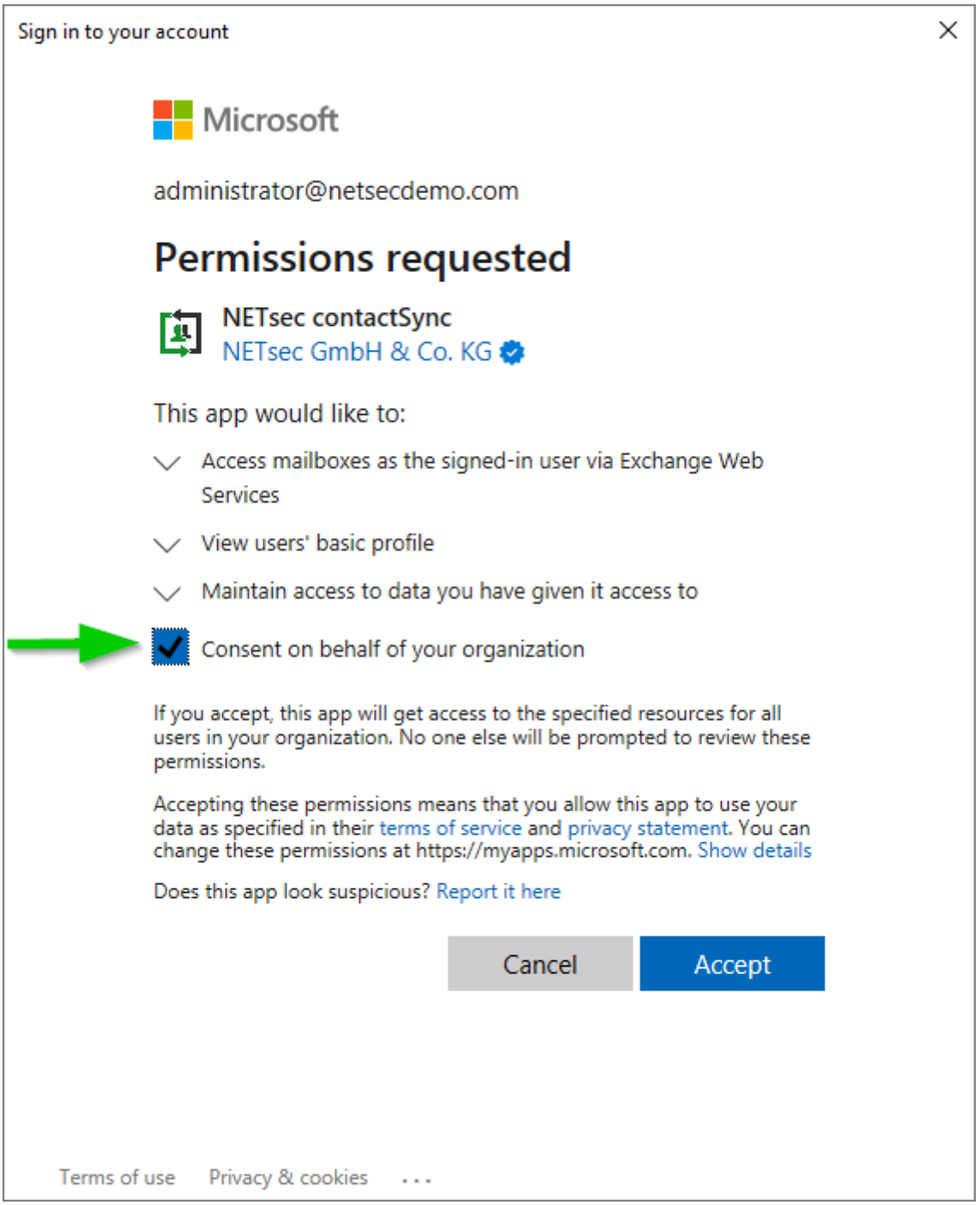
*Please note, the contactSync service account should only be an Exchange Administrator of Exchange Online, but **not** a Global Administrator of the Microsoft 365 tenant.*



Sign in with a **Global Administrator** account of the Microsoft 365 tenant.

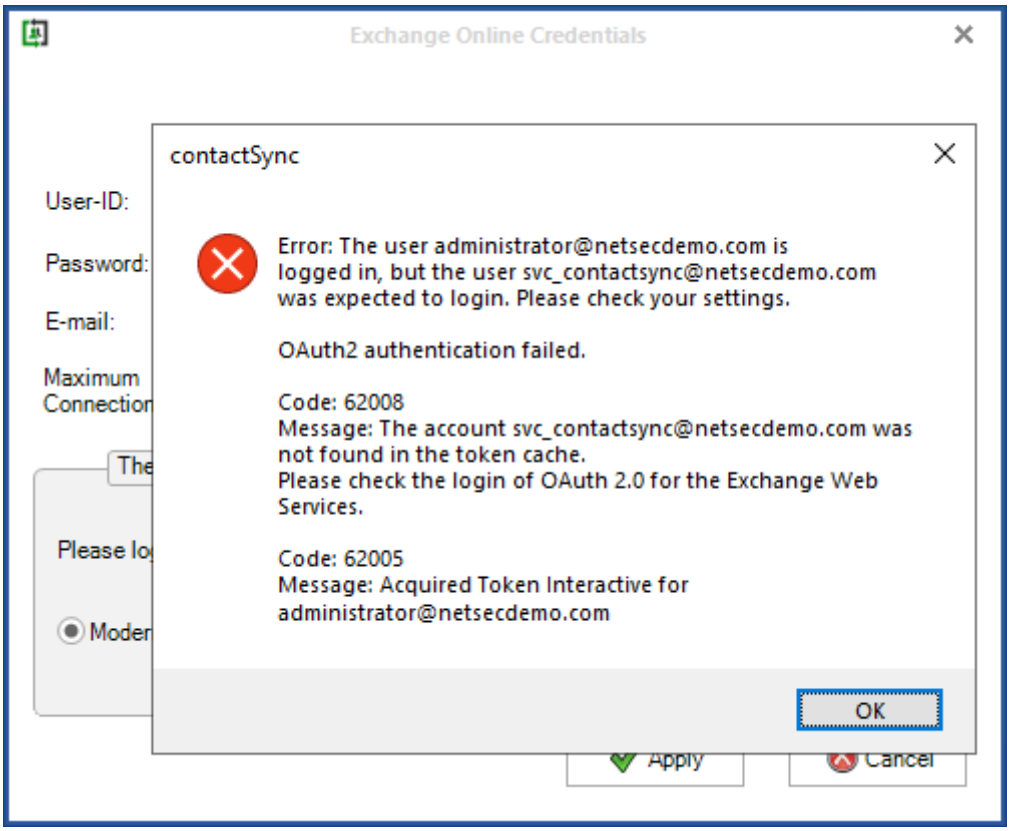


Insert the password of the **Global Administrator** account.

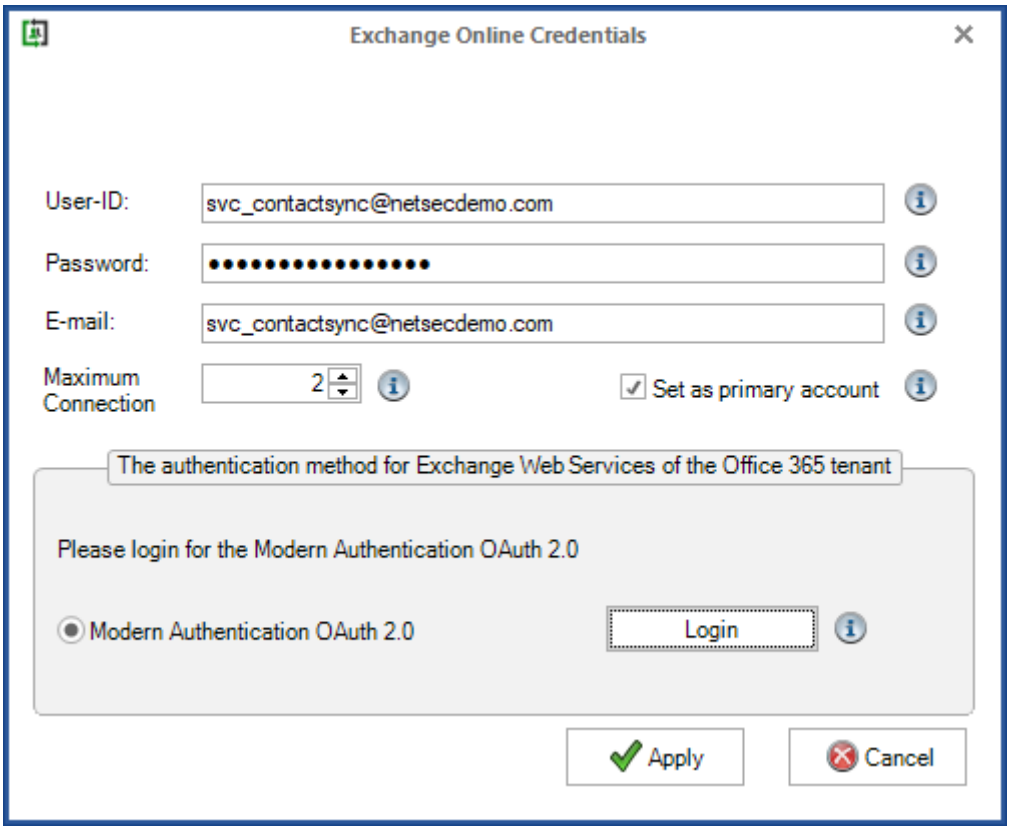


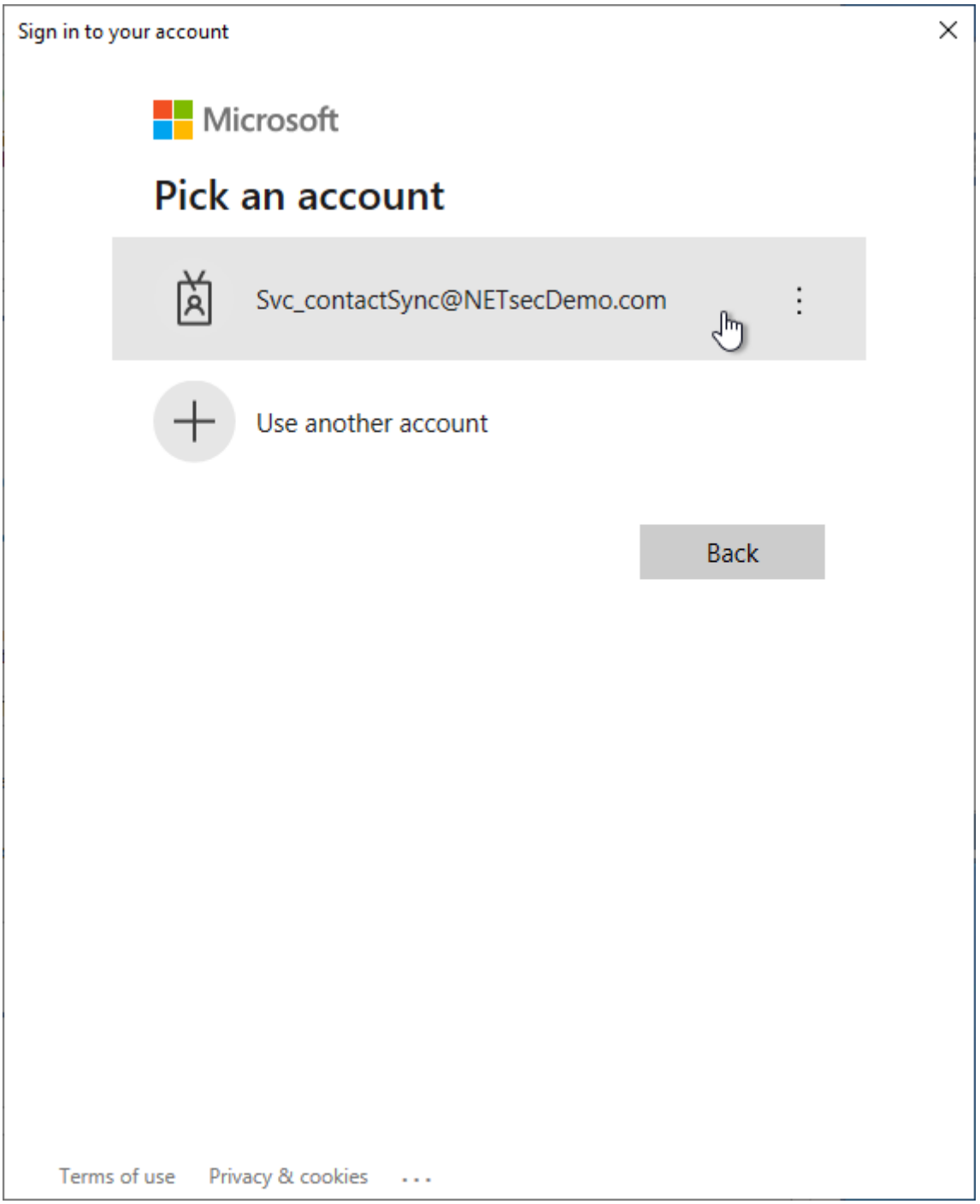
Enable **Consent on behalf of your organization**, then click **Accept**.

The OAuth2 authentication will fail after the first login process.

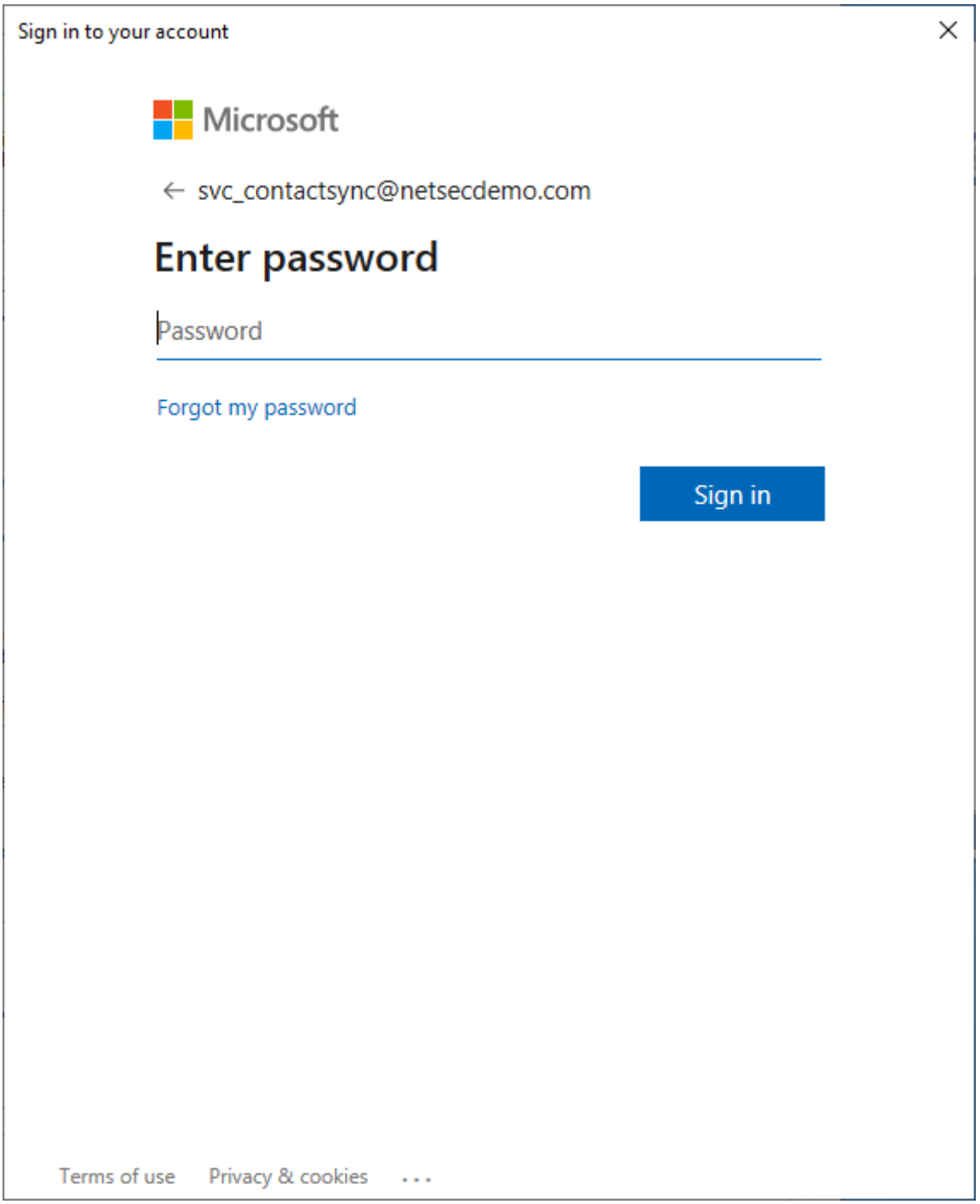


Proceed with the **Login** for Modern Authentication OAuth 2.0 for Exchange Web Services (EWS) of Exchange Online with your contactSync Service Account again.



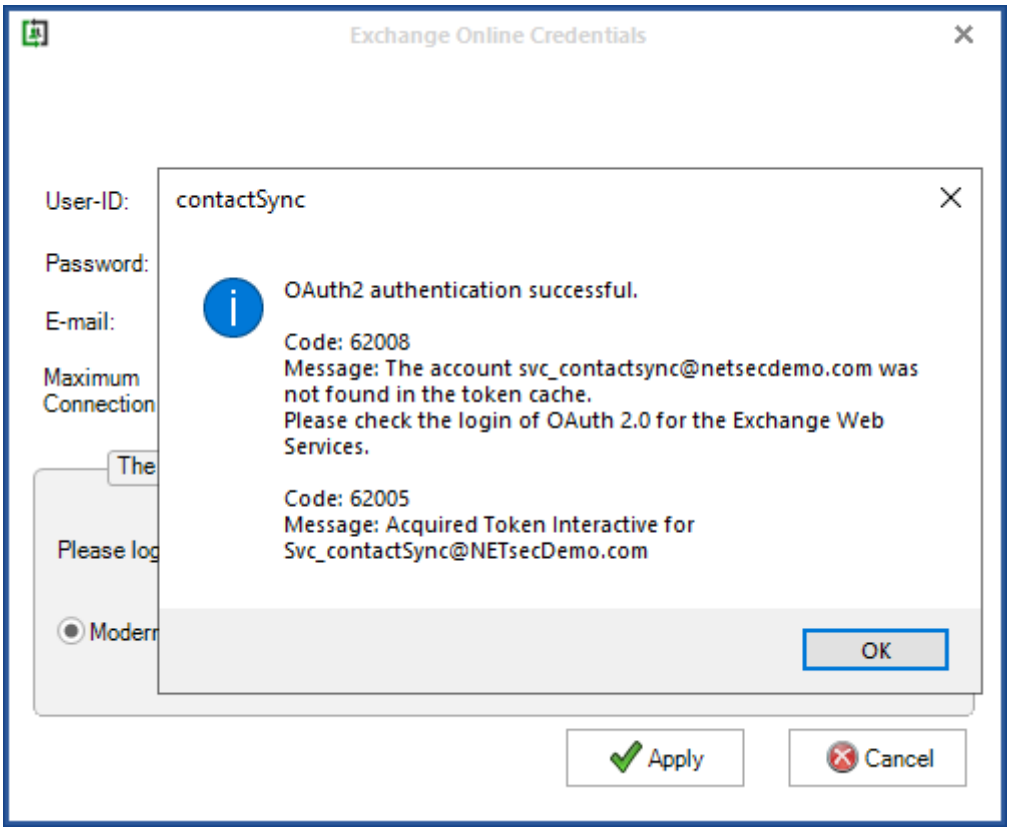


Once again select the same contactSync service account, which has been previously used in the **Exchange Online Credentials** dialog.



Insert the password of the contactSync service account.

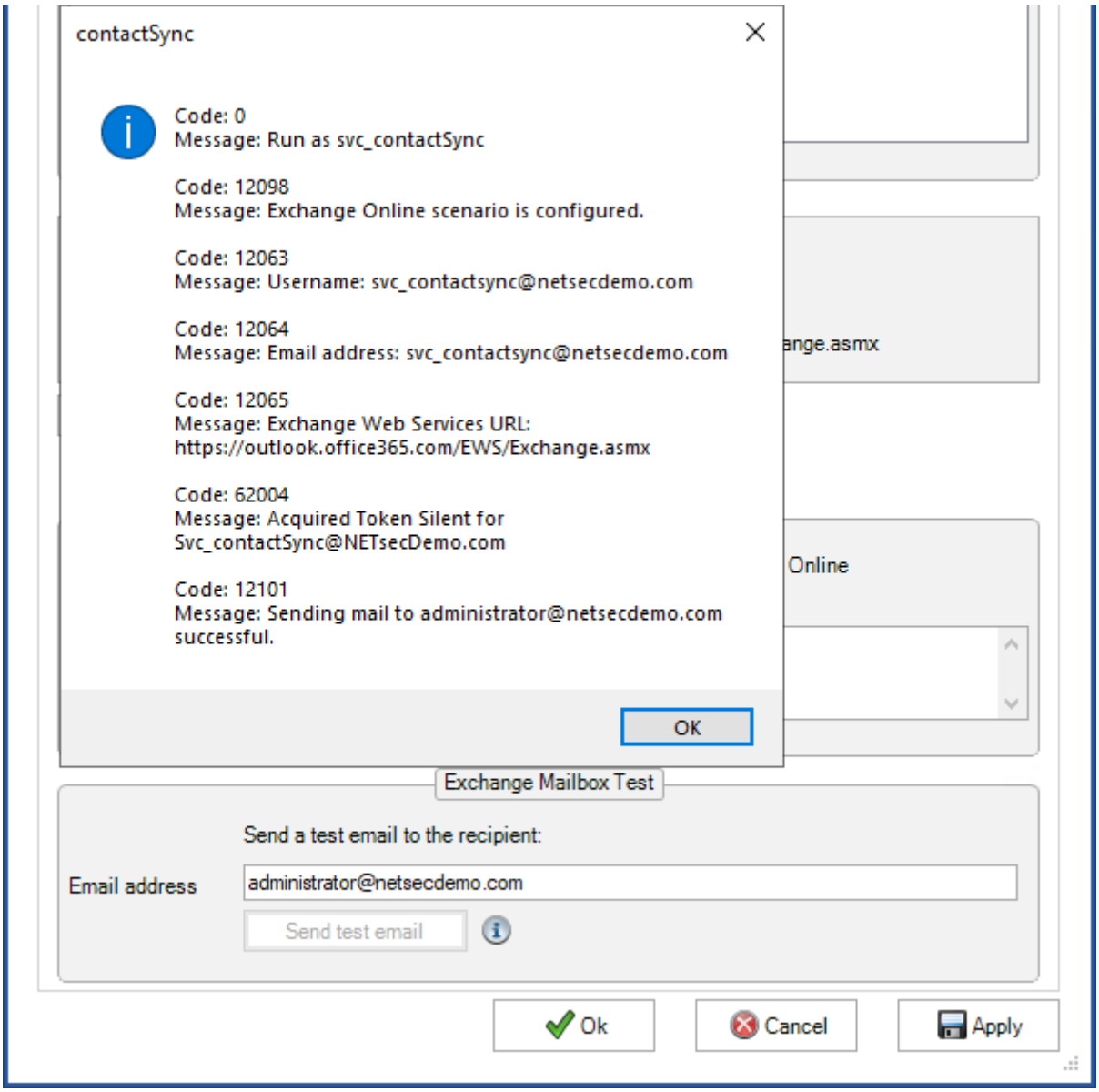
The login will now be successful.



contactSync can now use OAuth tokens for authentication to access the Exchange Web Services (EWS) for your Exchange Online during the policy runs.

Click **Apply** to close the **Exchange Online Credentials** dialog.

A test email can also be sent to the desired recipient as an additional test to validate mail flow. To do this, click the **Send test email** button for the **Exchange Mailbox Test**.



Please note, that the email address of the recipient for the test email will not be saved.

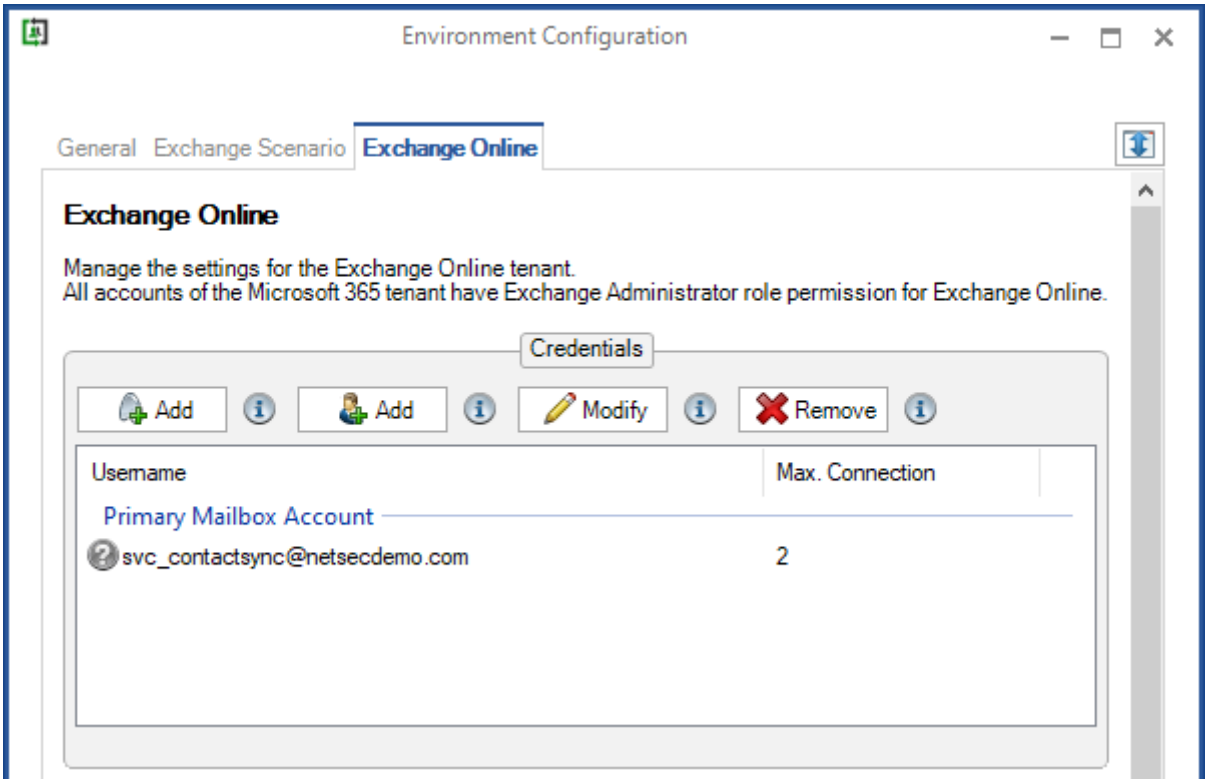
Also, please see the contactSync manual chapter:

12010 - Error getting Exchange Online connection

Account for access of Exchange Online mailboxes

contactSync uses the **Primary Mailbox Account** on the Exchange Online tab of the Environment Configuration to access Exchange Online mailboxes by default.

In this example, the user credentials of a service account are configured as a **Primary Mailbox Account**.



If the user credentials of a service account are configured for Exchange Online, contactSync requires the **Exchange Application Impersonation** role in Exchange Online for this service account to access Exchange Online mailboxes.

contactSync can also use a dedicated Exchange Online mailbox user, which has the **Exchange Application Impersonation** role in Exchange Online to access Exchange Online mailboxes.

Please take a look at the chapter:

How to configure Exchange Application Impersonation

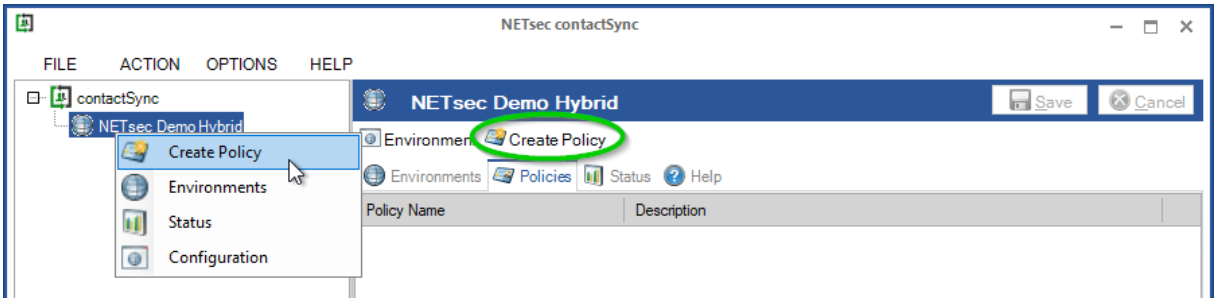
Create and Run contactSync Policies

Synchronize Contacts from Exchange On-Premises into Mailboxes

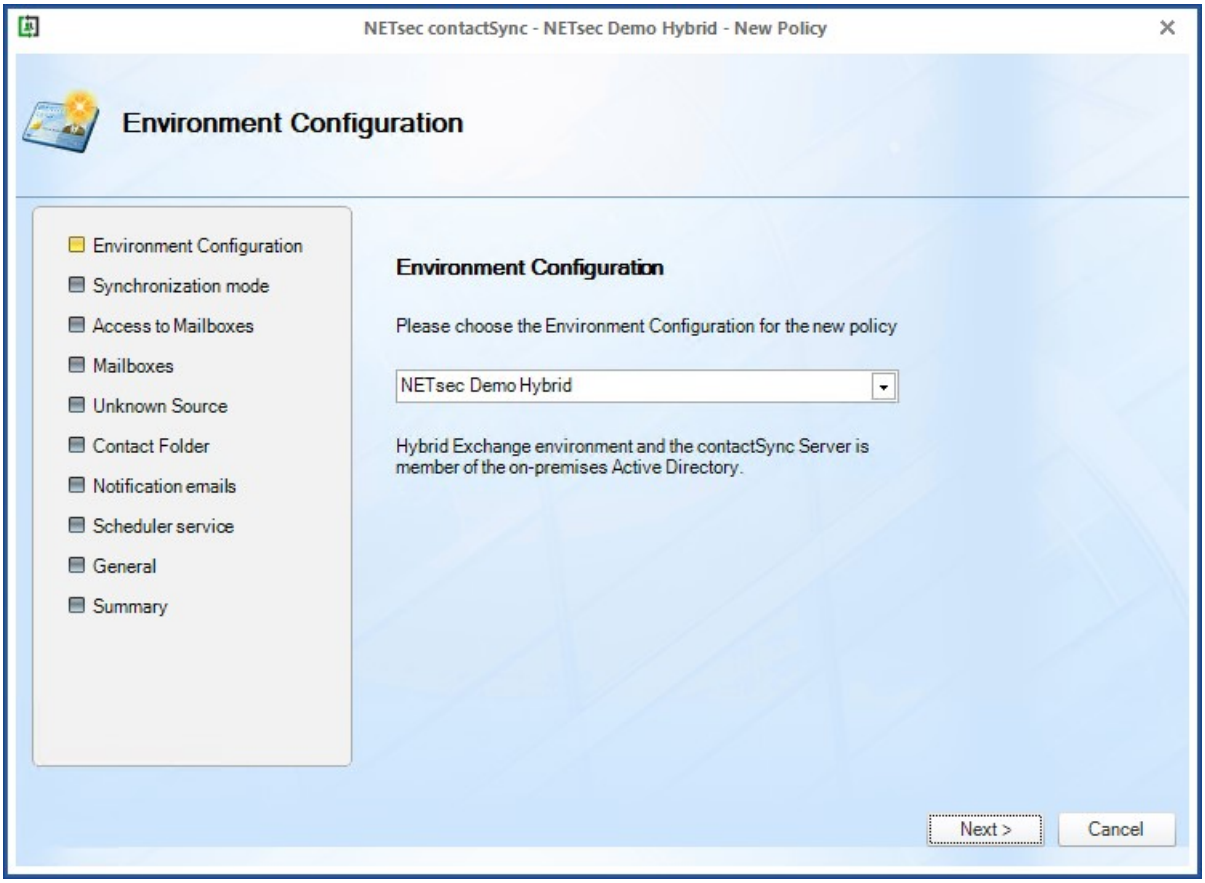
contactSync allows you to synchronize mail-enabled objects directly from on-premises as contacts into user mailboxes. It will connect to user mailboxes in your local Exchange Environment, whether it is in Exchange on-premises or Exchange Online if in hybrid mode.

Create new policy

Right click the desired environment and select **Create Policy** from the context menu or click **Create Policy** to the right.



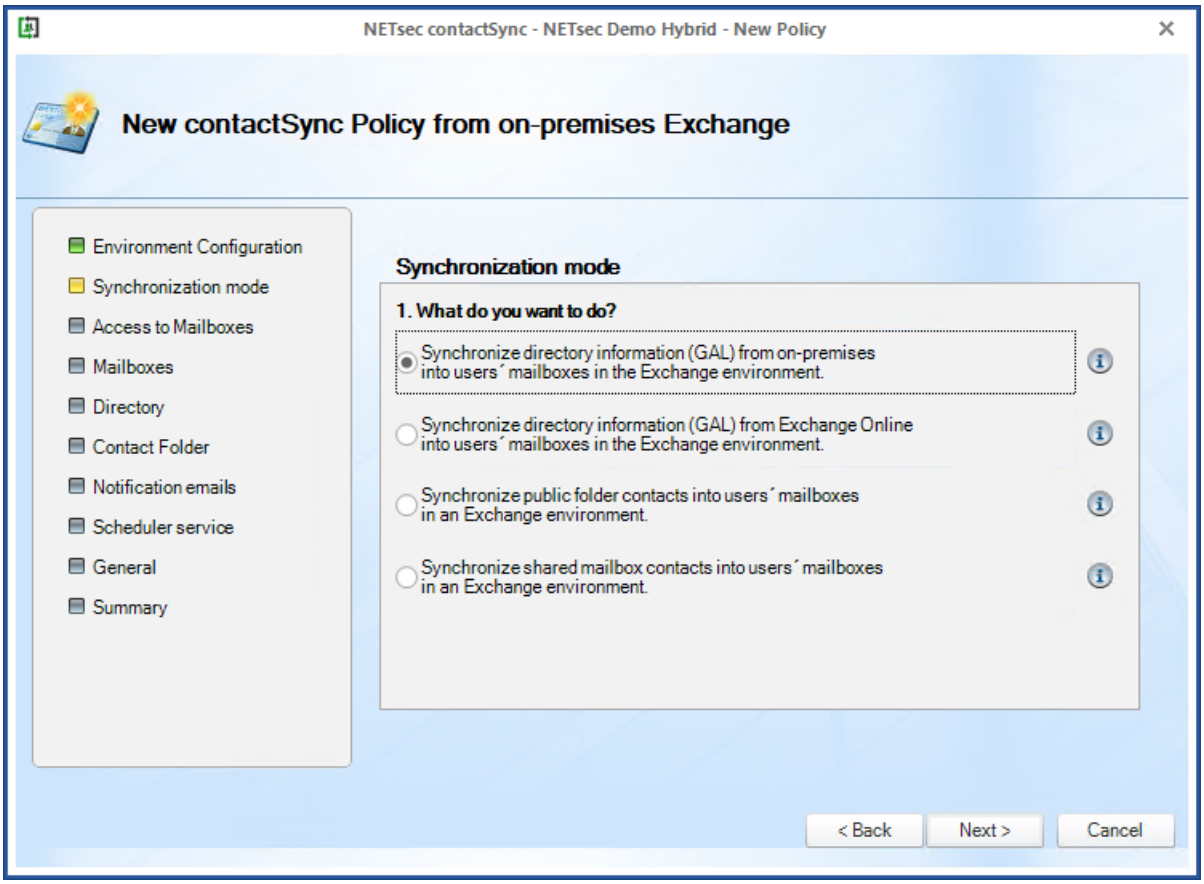
Ensure the desired environment has been selected from the dropdown.



Synchronization mode

Select **Synchronize directory information (GAL) from on-premises into users' mailboxes in an Exchange environment**.

Click **Next**.

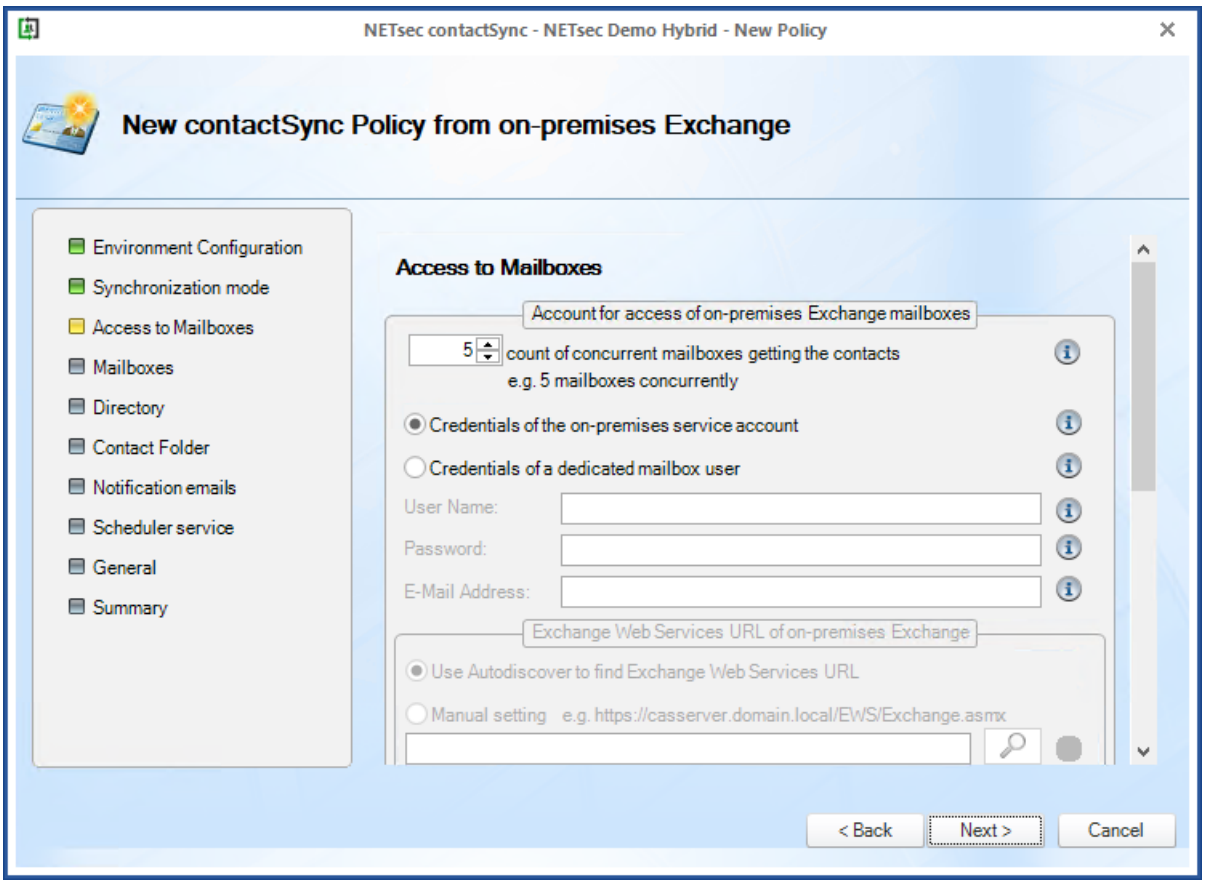


Access to Mailboxes for on-premises Exchange

contactSync requires access to user mailboxes in order to write to their contacts folder. The **Exchange Application Impersonation** can be configured for such access, which allows up to 5 concurrent connections to user mailboxes.

By default, contactSync will use the account which has been configured in the Environment configuration.

These two roles can be split between two separate accounts by entering the credentials of a dedicated mailbox user that has the **Application Impersonation** role.



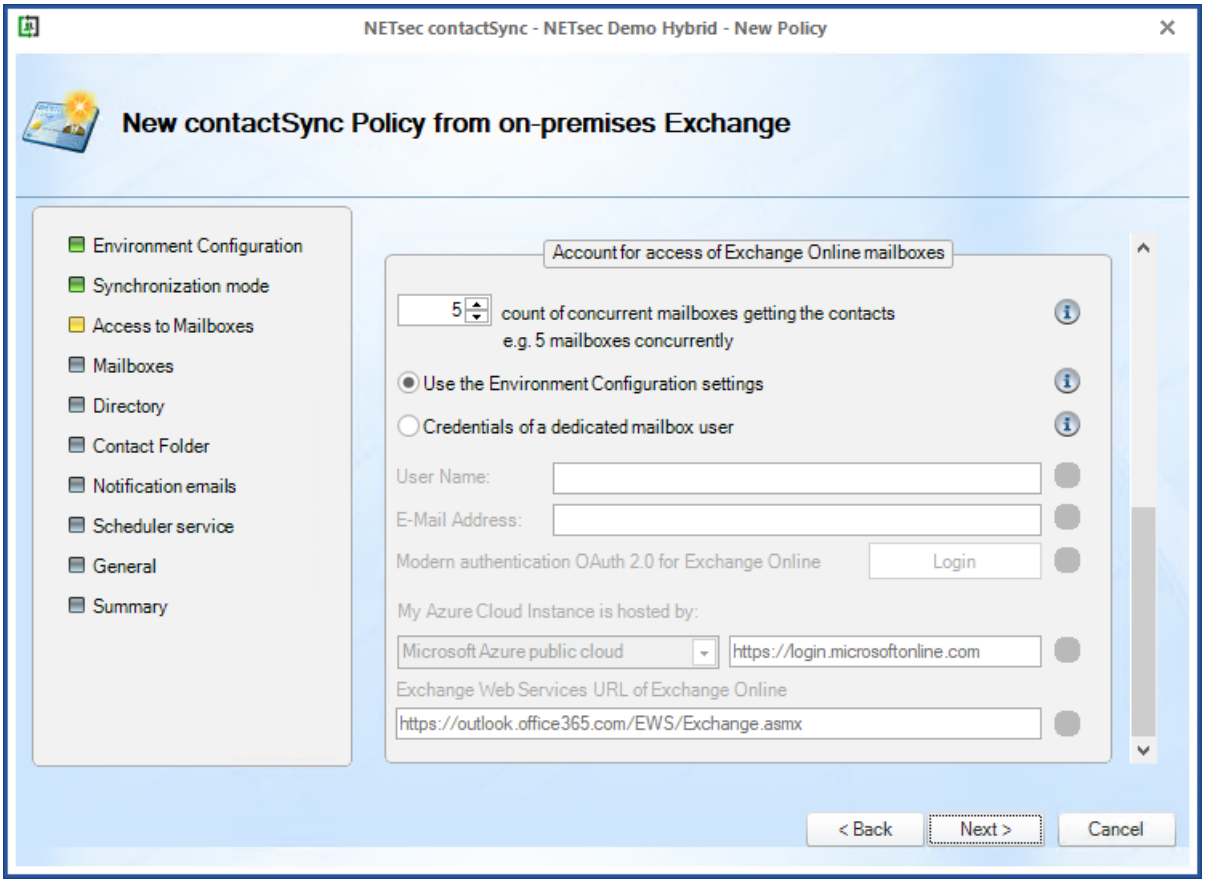
Please take a look at the chapter:

How to configure Exchange Application Impersonation

Access to Mailboxes for Exchange Online

By default, contactSync uses the Environment Configuration to access mailboxes. Application Impersonation, required for Exchange on-premises, will not be necessary when the certificate authentication via App Registration for Exchange Online is configured in the Environment Configuration.

Please take a look at the chapter
Exchange Online certificate-based authentication via App Registration

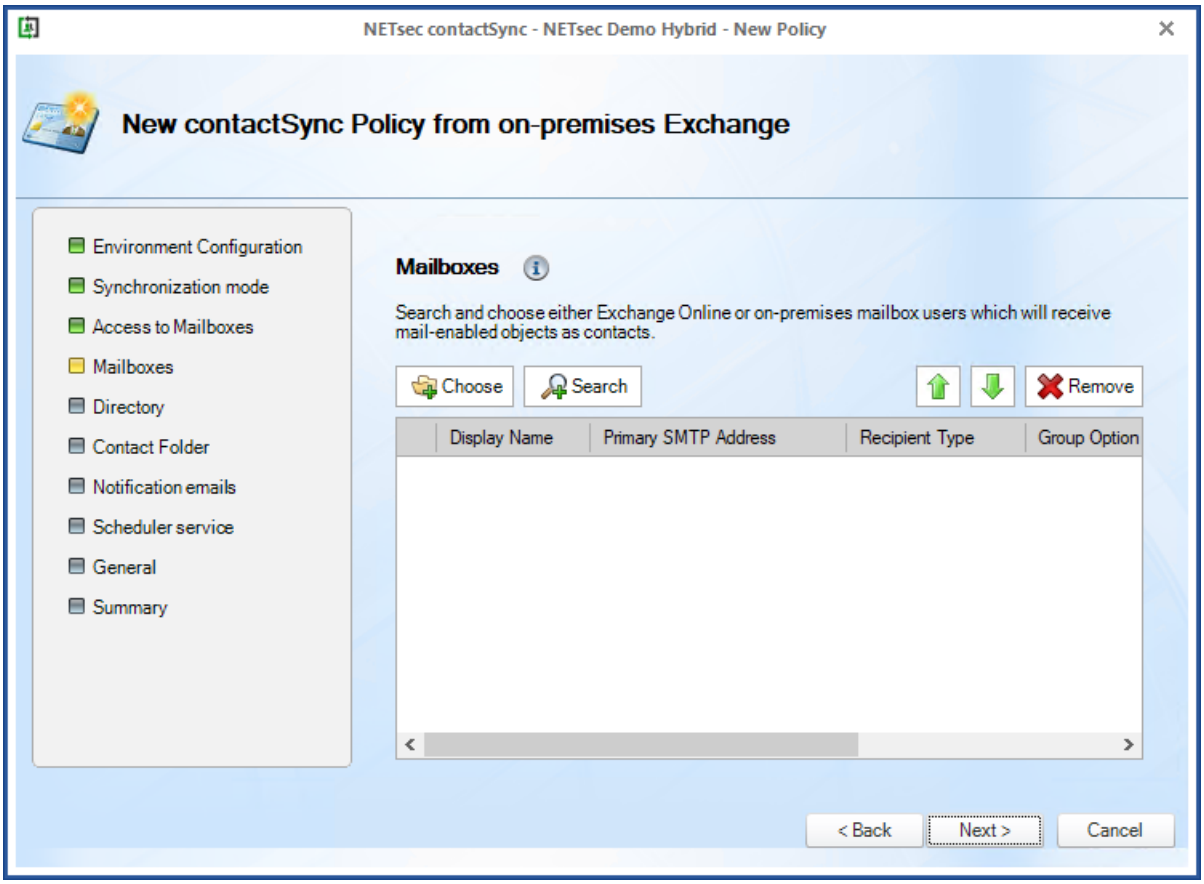


Click **Next**

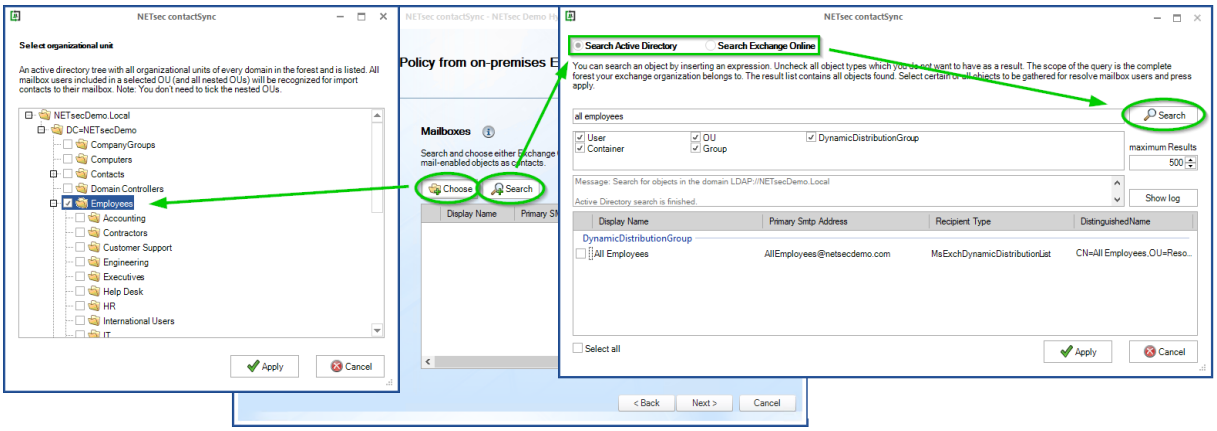
Select the Mailboxes from On-Premises Exchange

You can select Mailboxes located in an on-premises Exchange Server, which will receive contacts. It could be an on-premises Exchange environment or a part of a hybrid Exchange environment.

In the **Mailboxes** window, you are prompted to select the mailboxes which will receive the contacts. There are two ways to do make your selection.



1. Click **Choose** to select mailboxes by OU where they reside in Active Directory.
2. Click **Search** to open a search dialogue window from which you can search for the desired Active Directory objects. When searching Active Directory, mailboxes can be selected individually, by group membership, by container, or by OU. If you have a hybrid Exchange environment, an additional option is available to search for Exchange Online objects.

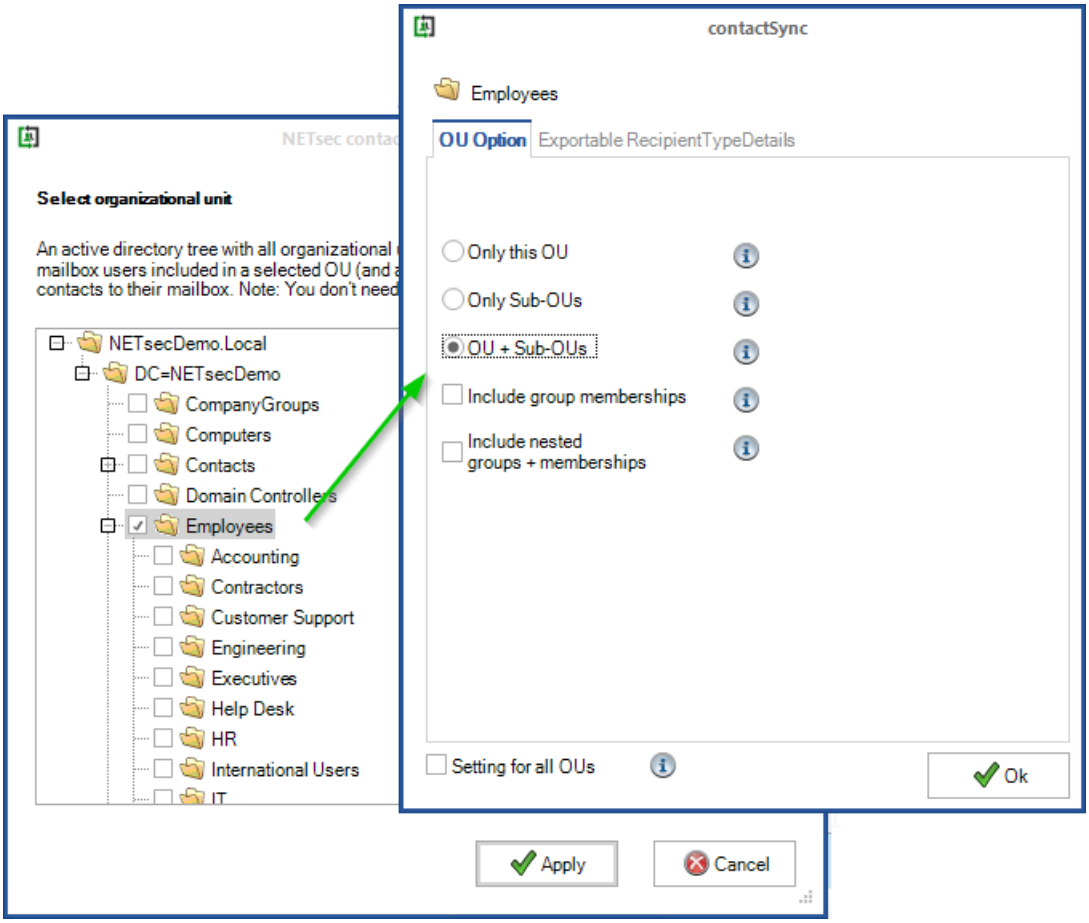


When the **Search Exchange Online** Radio Button has been selected, you can search for objects by Recipient Type, such as **UserMailbox**, **MailUniversalDistributionGroup**, **MailUniversalSecurityGroup**, **DynamicDistributionGroup**, or **Office365 Group**.

When OUs are selected, a prompt to select the OU depth is presented. If any groups are contained in the OU, contactSync will prompt the user to include mailboxes by group membership.

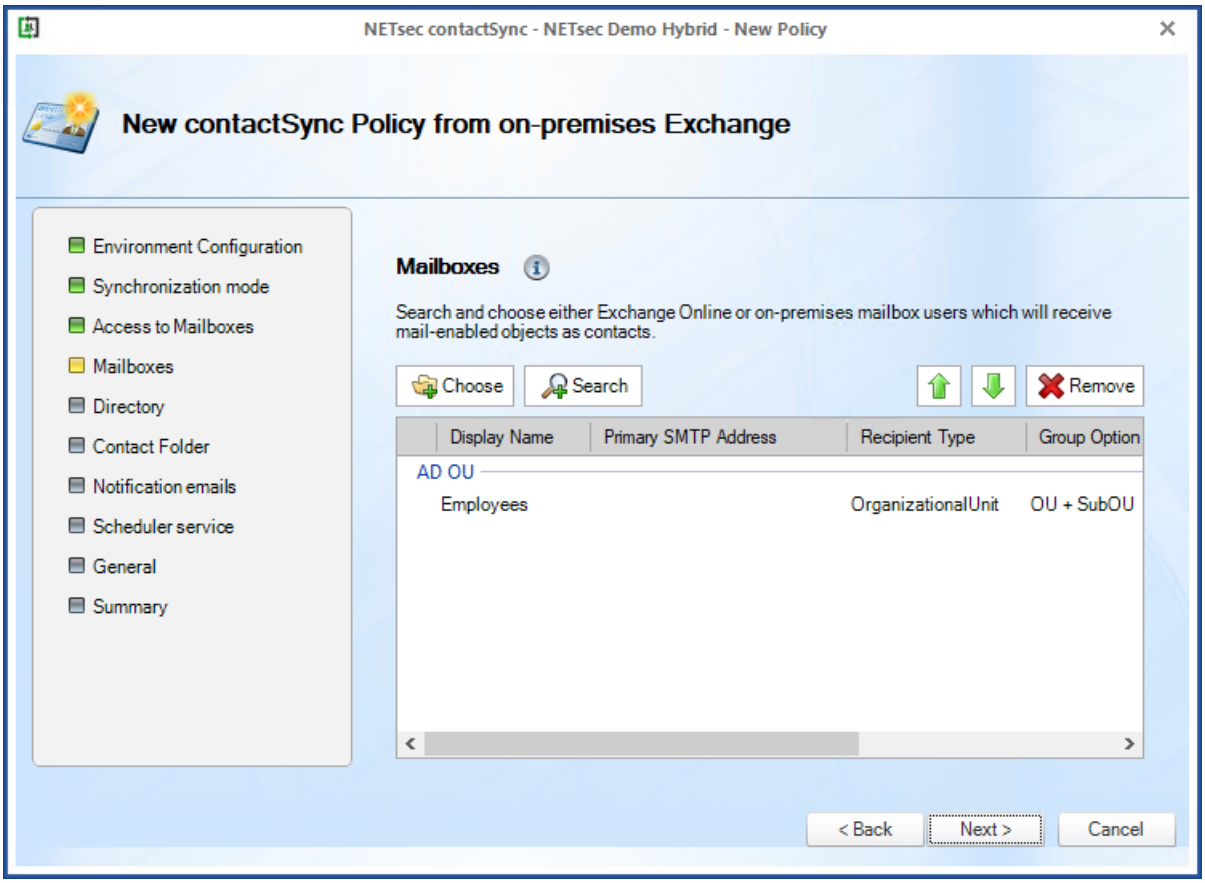
If multiple OUs have been selected, the checkbox at the bottom left will apply the settings to all selected OUs.

Click **OK**, then **Apply**.



Verify the selected OUs are displayed.

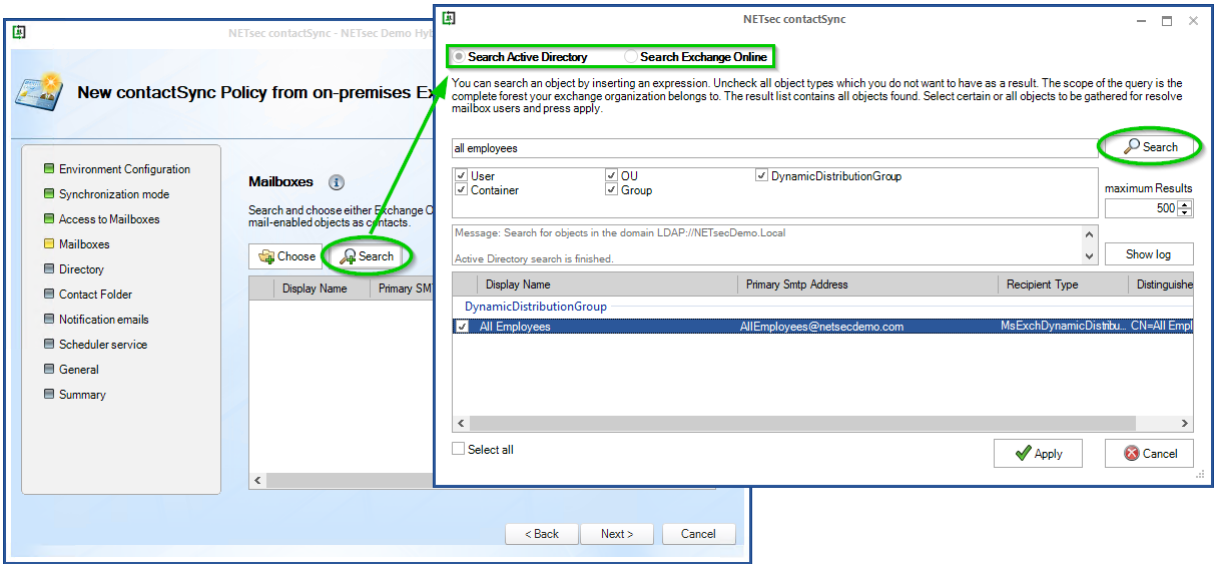
Click **Next**.



Click **Next**.

Instead of selecting OUs in Active Directory as described above, in the following example, the **All Employees** Dynamic Distribution Group has been selected from the Active Directory search.

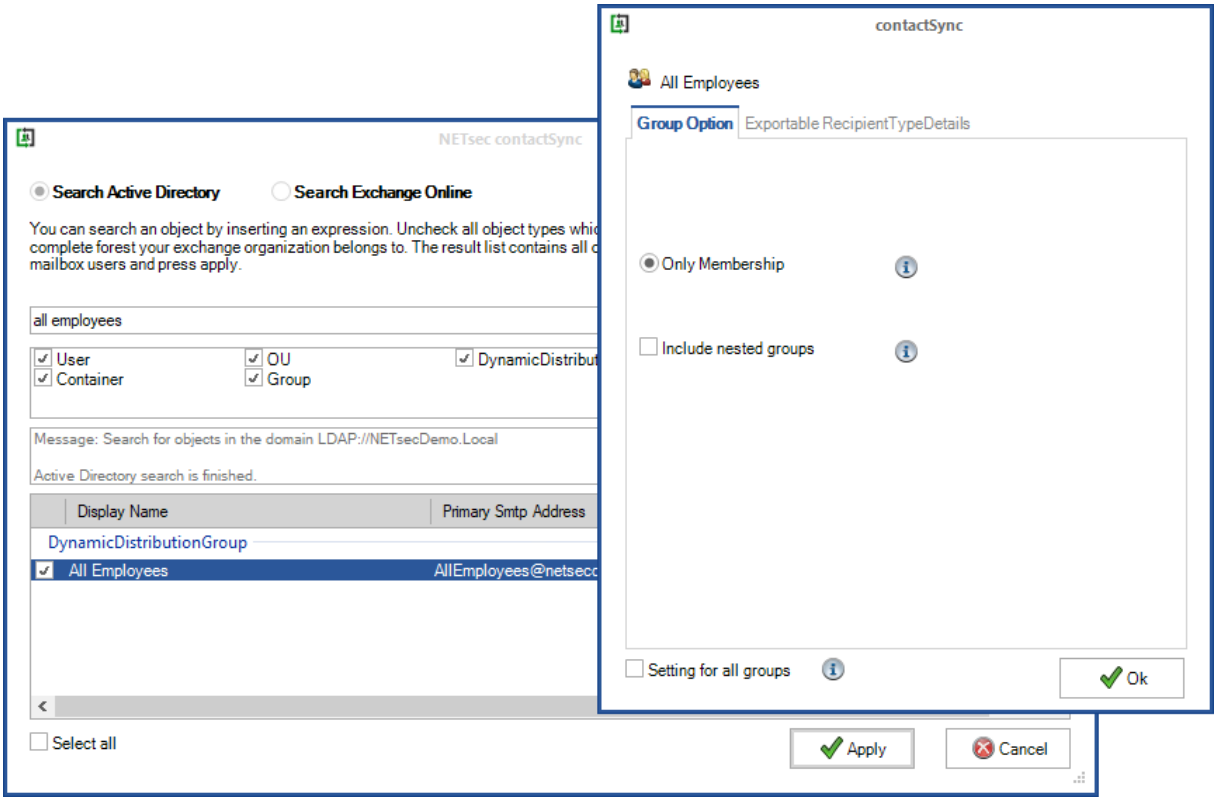
Click **Search** to search for objects through an LDAP query. They can be selected individually, by group membership, by container, or OU



All members with a mailbox in the selected group will receive the contacts, an option is also available to include nested groups.

Click **Apply**.

A new window opens with **Only Membership** preselected and the option to include nested groups.



Click **OK**

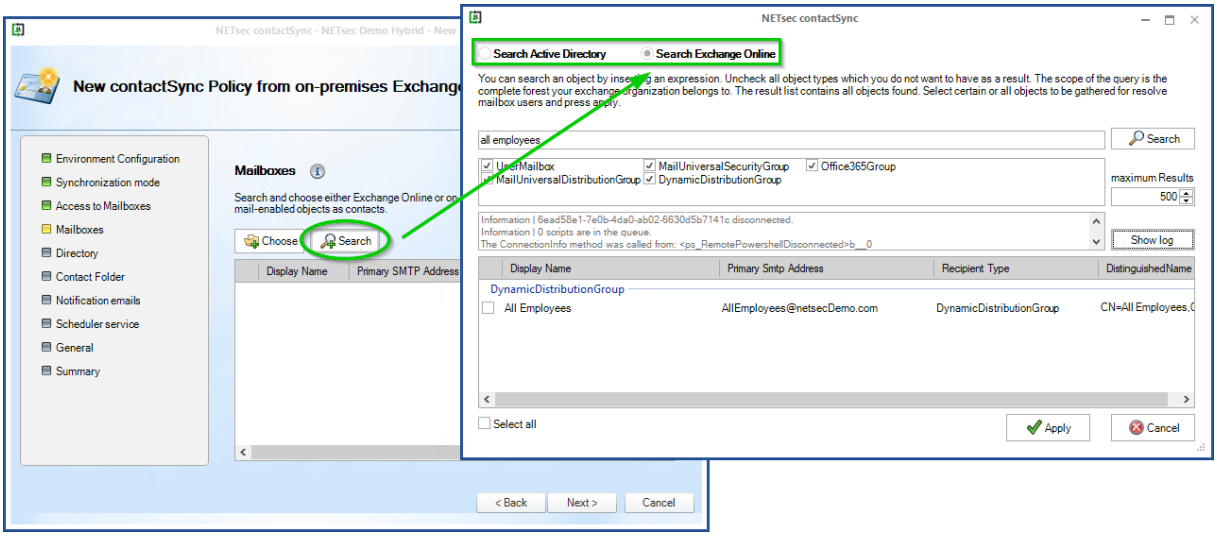
Then click **Apply**

For continued instructions, please see
Select mail-enabled objects on the Directory tab from On-Premises

Select the Mailboxes from Exchange Online

You can select Mailboxes located in Exchange Online which will receive the contacts. This is possible for an Exchange Online environment or a part of any hybrid Exchange environment.

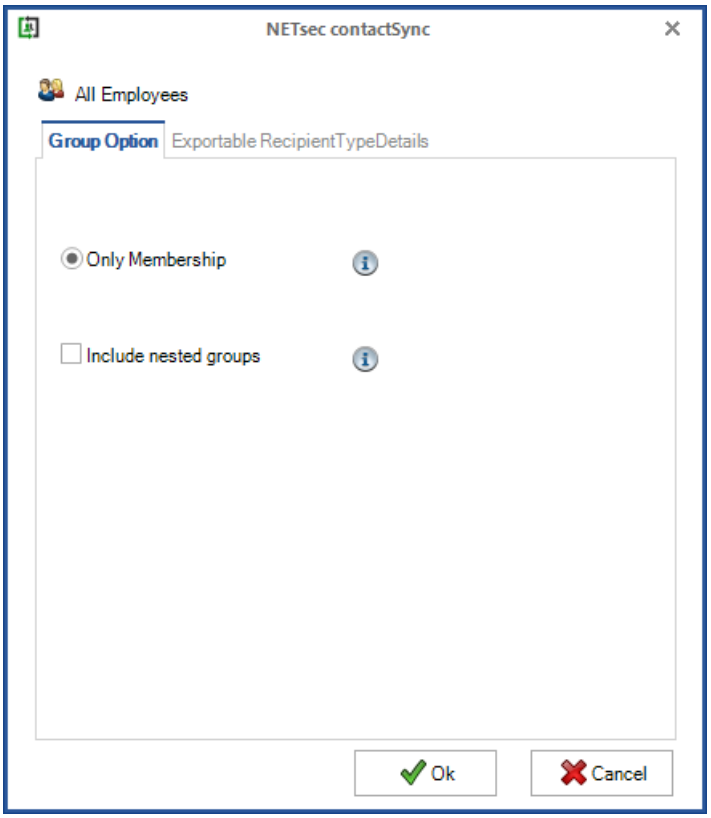
When searching for Exchange Online objects, you can search for objects by Recipient Type, such as **UserMailbox**, **MailUniversalDistributionGroup**, **MailUniversalSecurityGroup**, **DynamicDistributionGroup**, or **Office365 Group**.



In the example above, the **All Employees** Dynamic Distribution Group has been selected. You can expand your search by inserting a wild card character (*).

Click **Apply**.

All members with a mailbox in the selected group will receive the contacts, an option is also available to include nested groups.

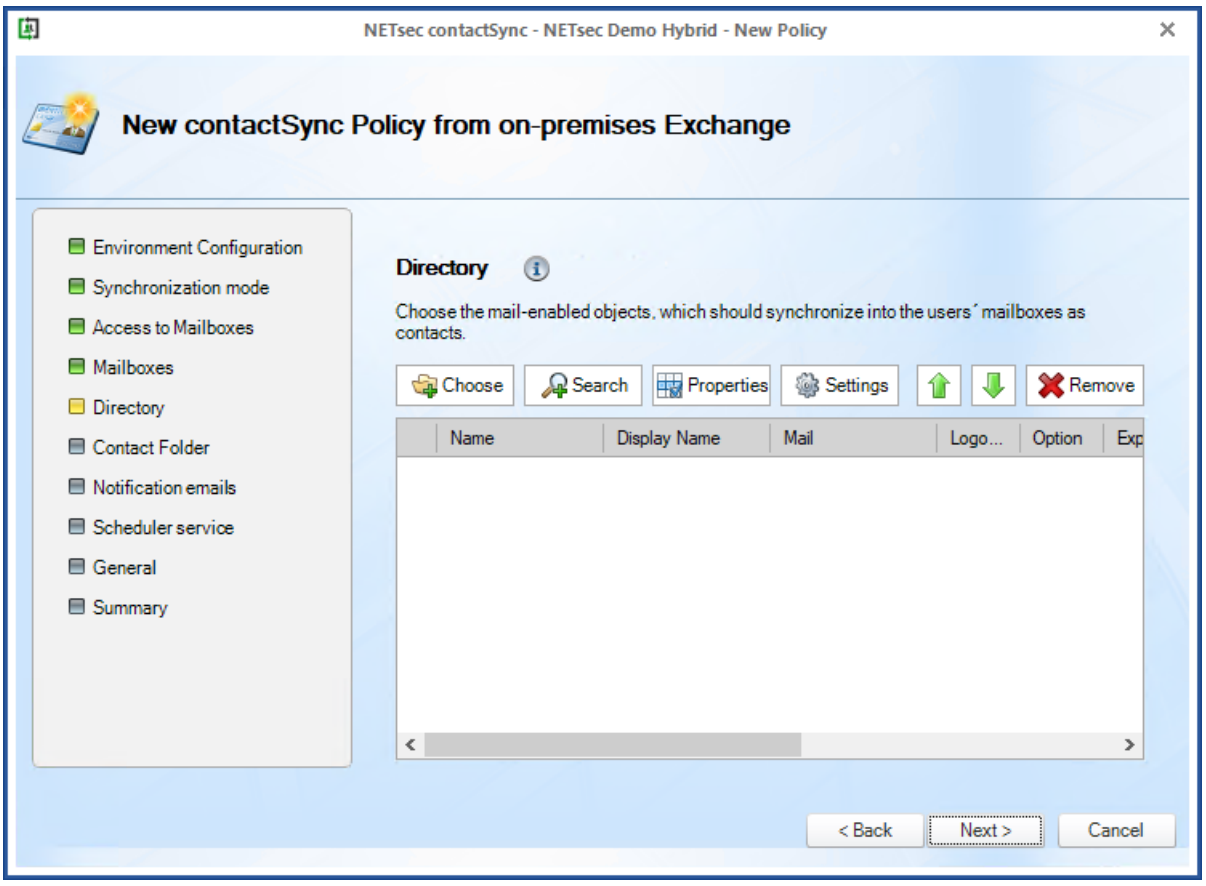


Click **OK**

Verify the selected group(s) are displayed.

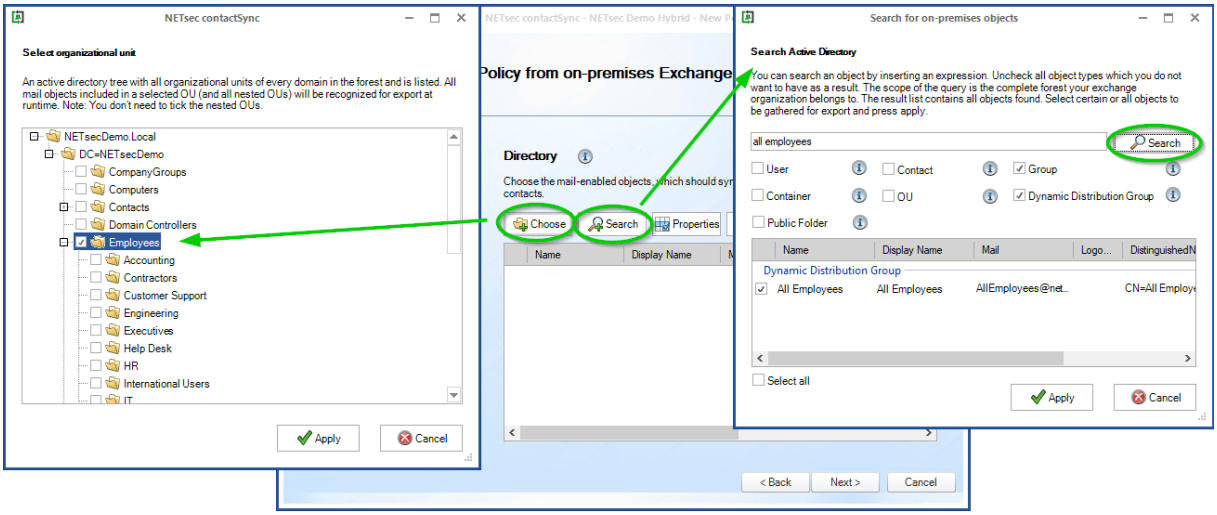
Click **Next**.

Select mail-enabled objects on the Directory tab from On-Premises



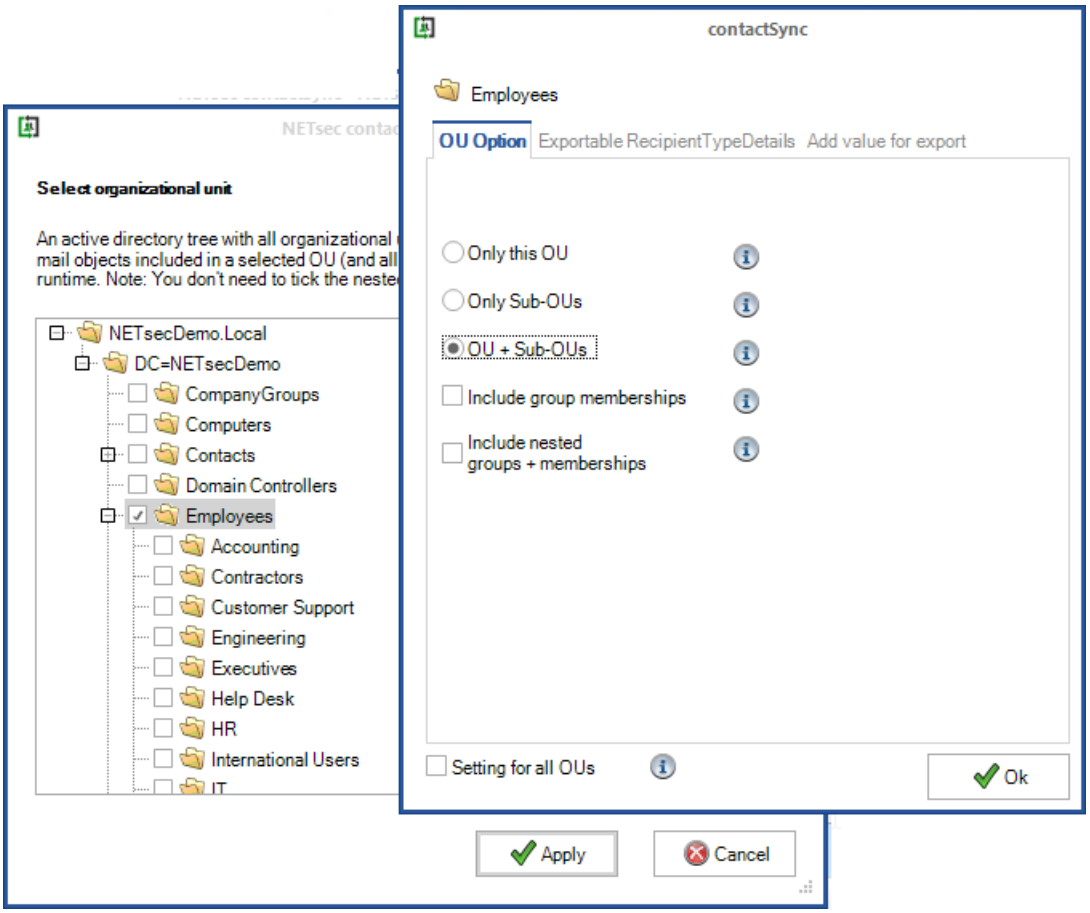
In the **Directory** window, it will be necessary to select mail-enabled objects to be synchronized as contacts into user mailboxes. This can be done 2 ways.

1. Click **Choose** to select OUs which contain the objects you would like to synchronize as contacts into user mailboxes.
2. (Preferred method) Click **Search** to search Active Directory for groups which contain the members you would like to be synchronized into user mailboxes.



Selection by OU

When OUs are selected, a prompt to select the OU depth is presented. If any groups are contained in the OU, an option is available to include group membership, which will be displayed in the group contact properties.



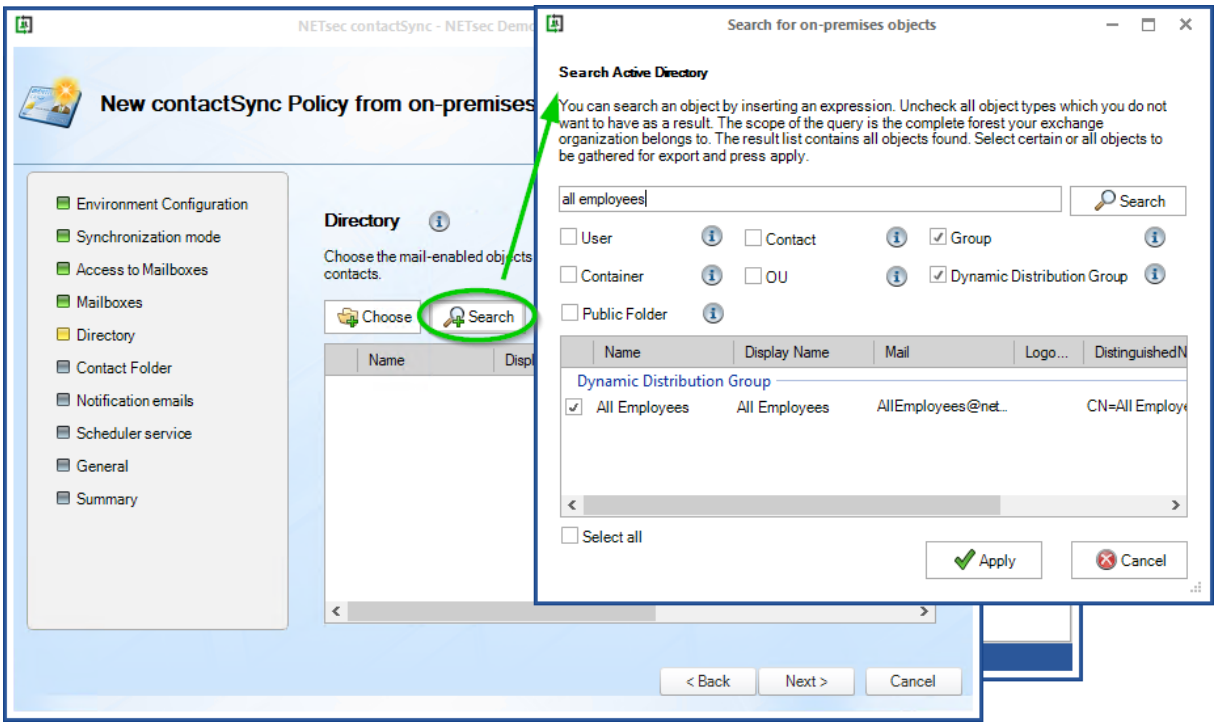
If multiple OUs have been selected, the checkbox at the bottom left will apply the settings to all selected OUs.

Click **OK**, then **Apply**.

Selection by Group and Membership

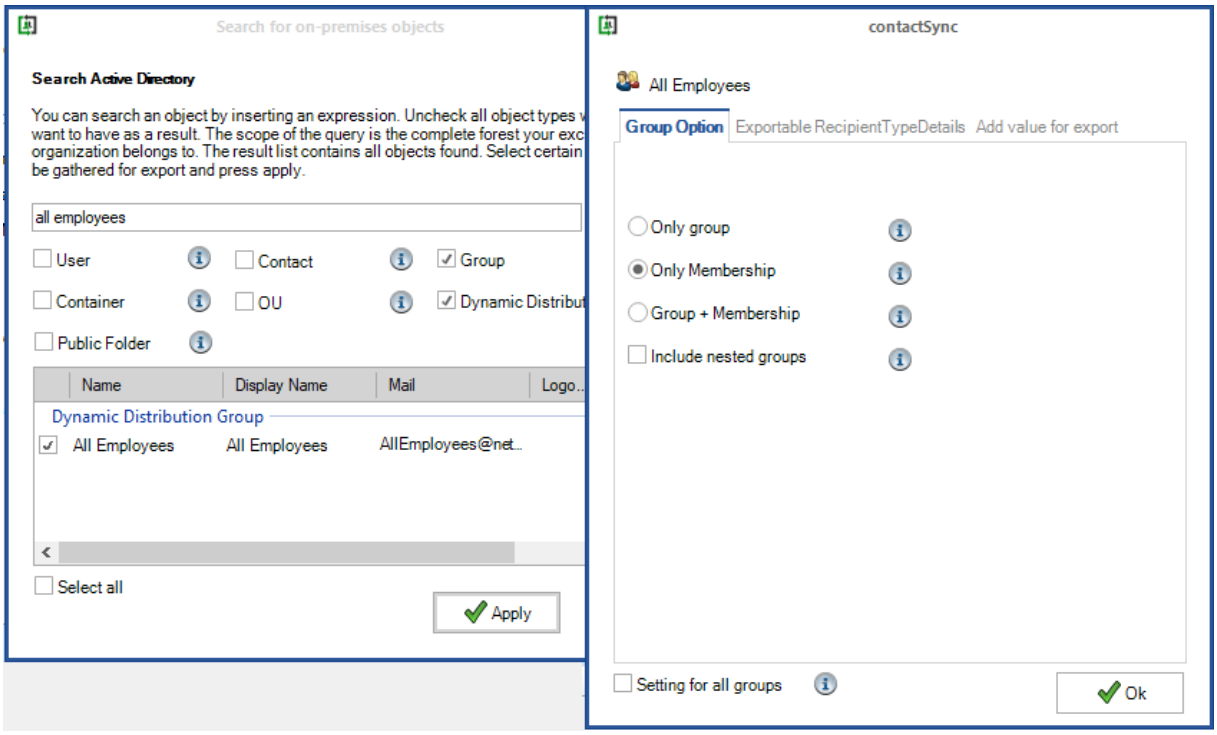
The preferred method for selecting contacts to be synchronized into user mailboxes is to search for a group which resides in Active Directory which contains all the desired mail-enabled object as group members.

The **All Employees** dynamic distribution group has been selected from the search query.

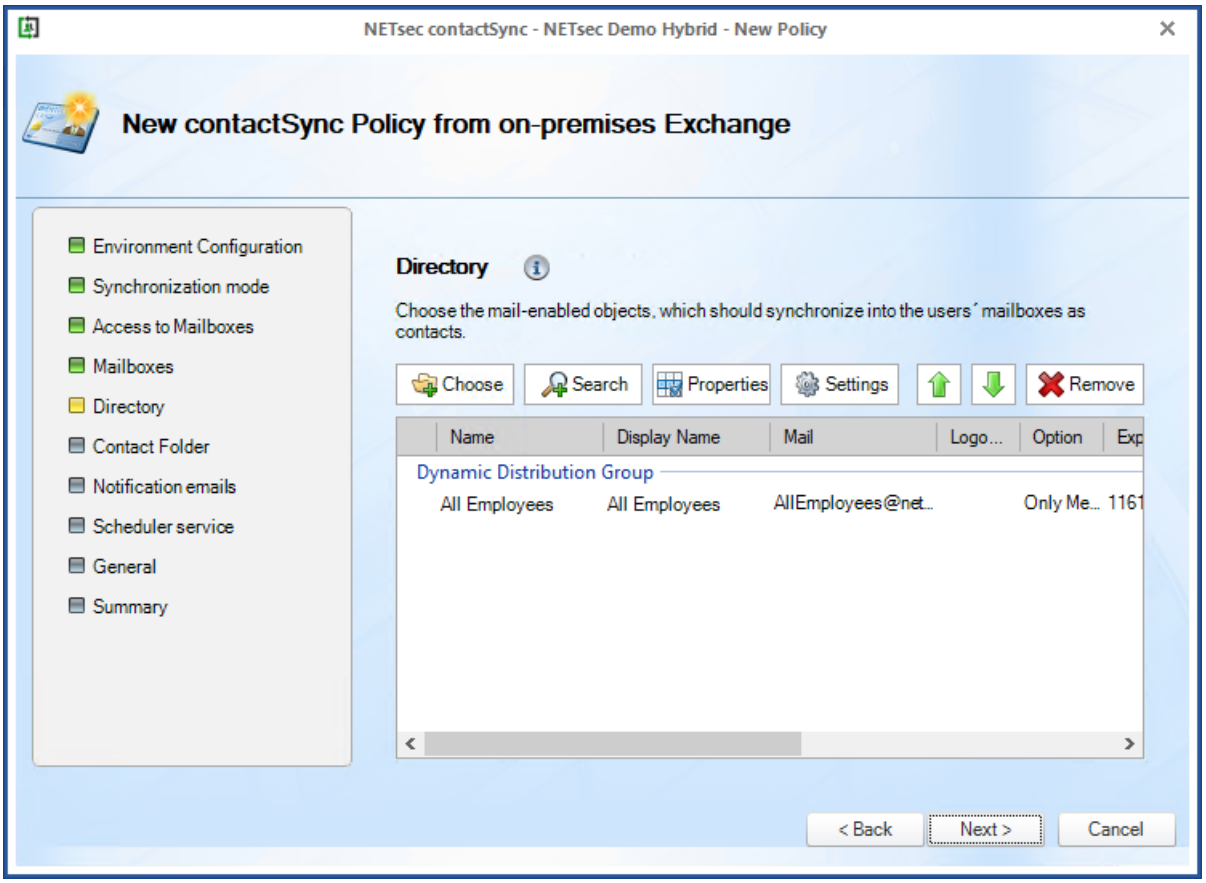


Click **Apply**

You will receive a prompt to select how the group will be synchronized into user mailboxes. The selection includes only the group, only membership, or the Group and Membership. The option is also available to include nested groups.



Ensure the selected group is displayed in the Directory window

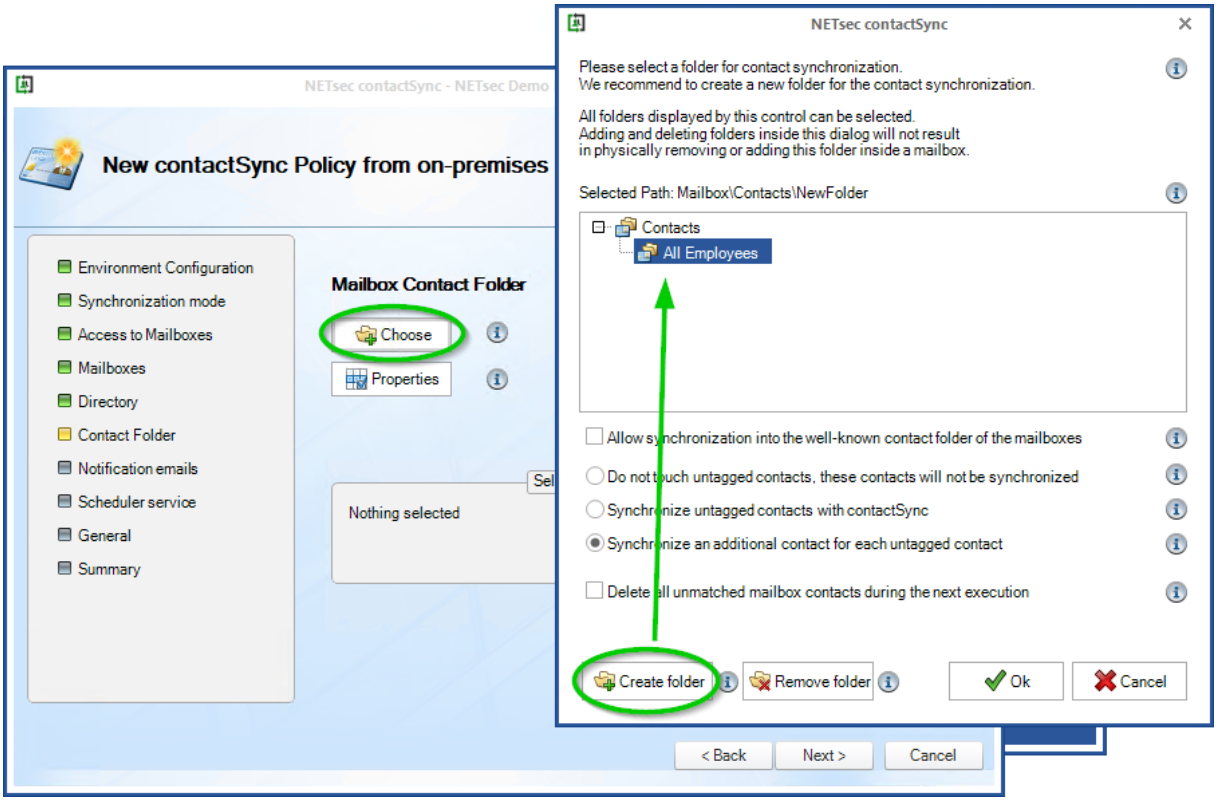


Then click **Next**

Select the Mailbox Contact Folder

Click **Choose** to select the contacts folder where the contacts will be synchronized to.

contactSync, can be configured to import contacts directly into the top-level Contacts folder. We recommend a new folder is created, which keeps the contactSync created contacts separate from the user-created contacts.



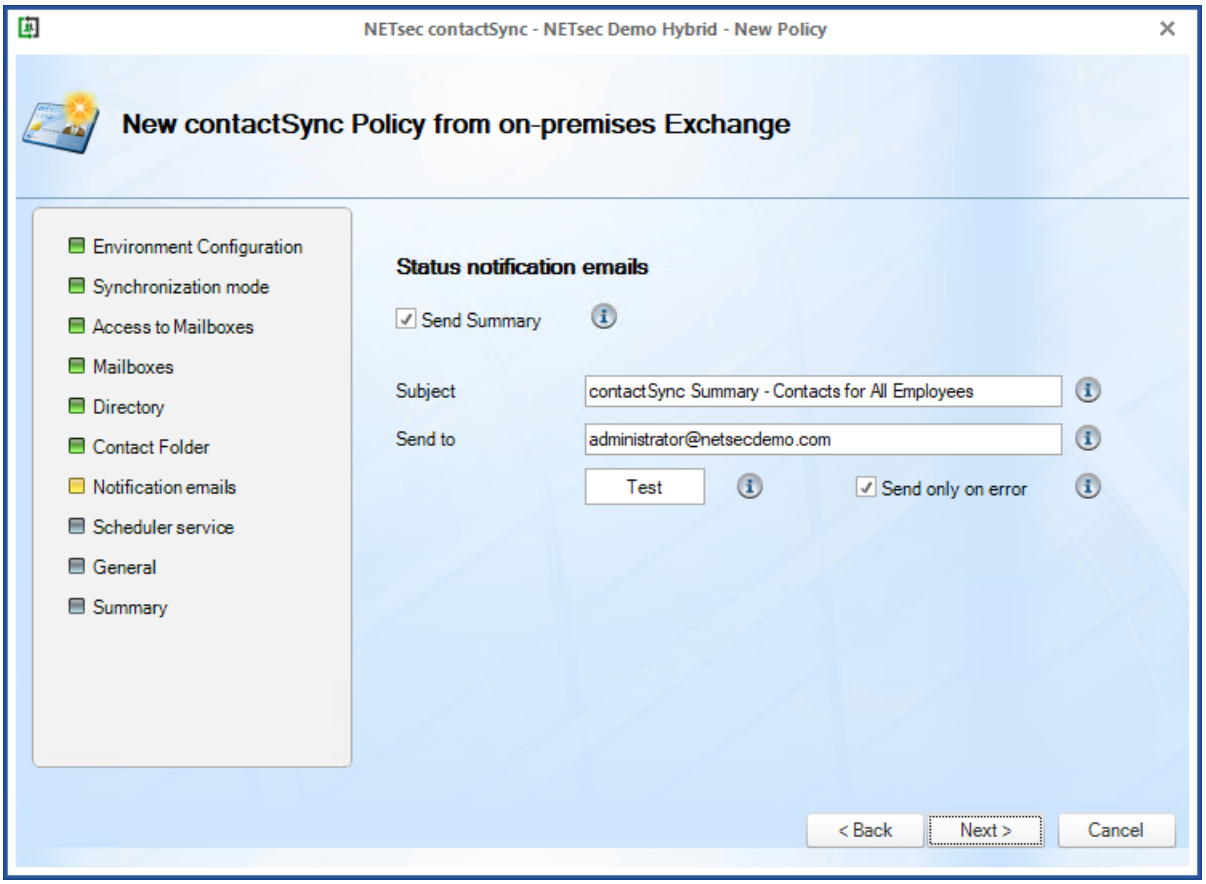
Select the top-level **Contacts** folder, then click **Create folder** to create a subfolder where the contacts will be synchronized, then give the new folder a name.

Click **OK**, then click **Next**.

Status notification email

An optional status notification email can be sent to the specified recipient(s) each time the policy runs, which provides a brief summary of activity. However, if your preference is to receive one only when an error has been logged, check the **Send only on error** checkbox. Click the **Test** button to send a test email. Then verify it has been received.

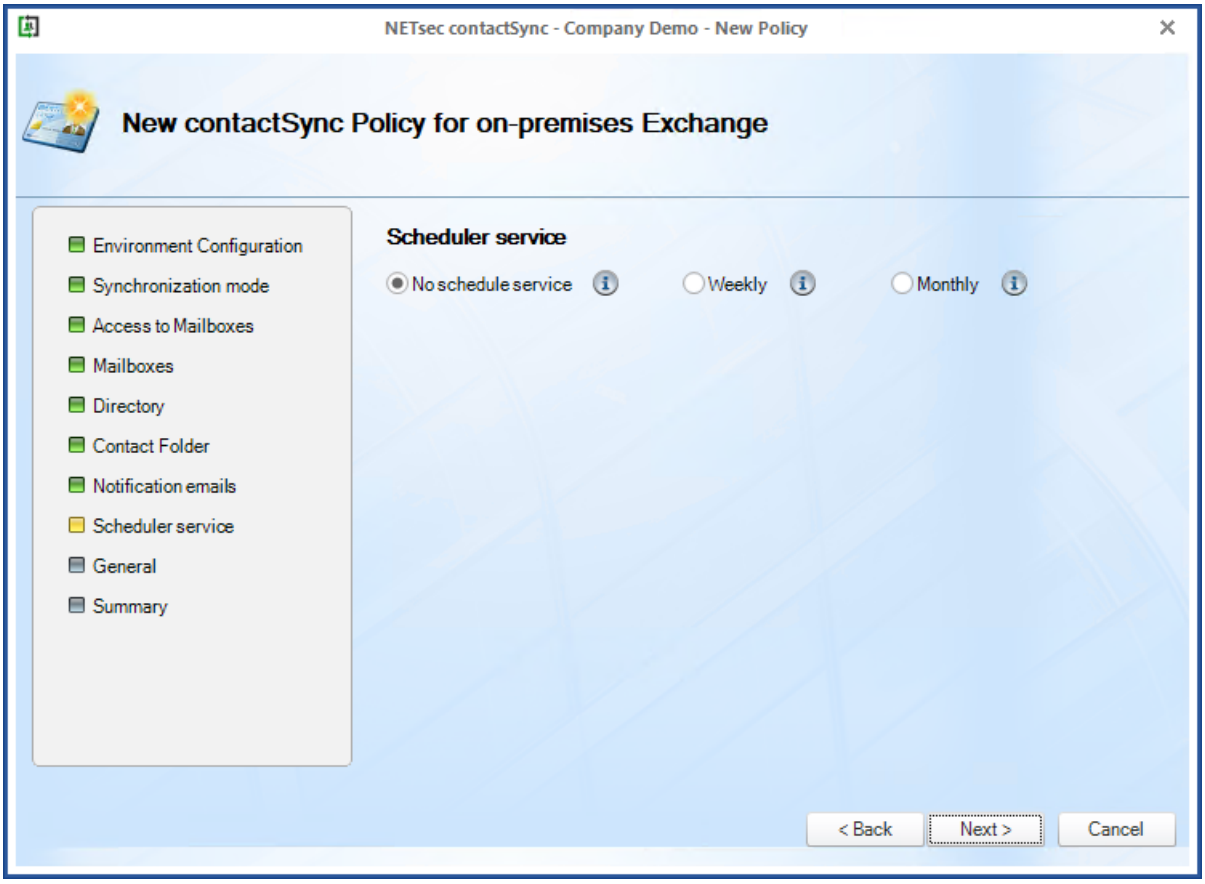
Click **Next**.



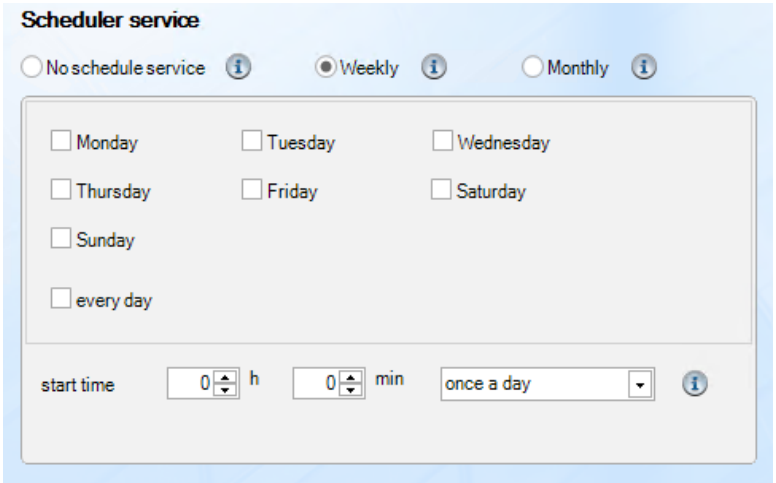
Schedule policy run

contactSync can be scheduled to run at regular intervals. We recommend the policy is manually run before any schedules are set. After the synchronization has completed successfully, you can go back and set it to run on the desired schedule.

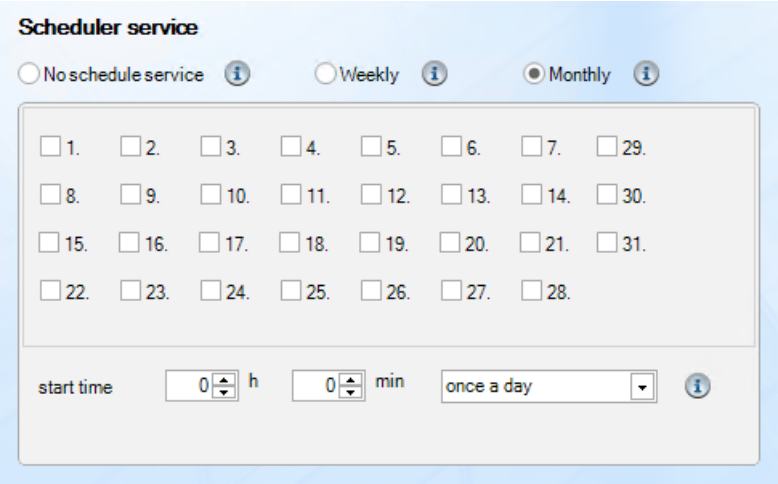
Click **Next**.



The **Weekly** schedule allows you to select which days of the week the policy runs, along with start time and frequency.

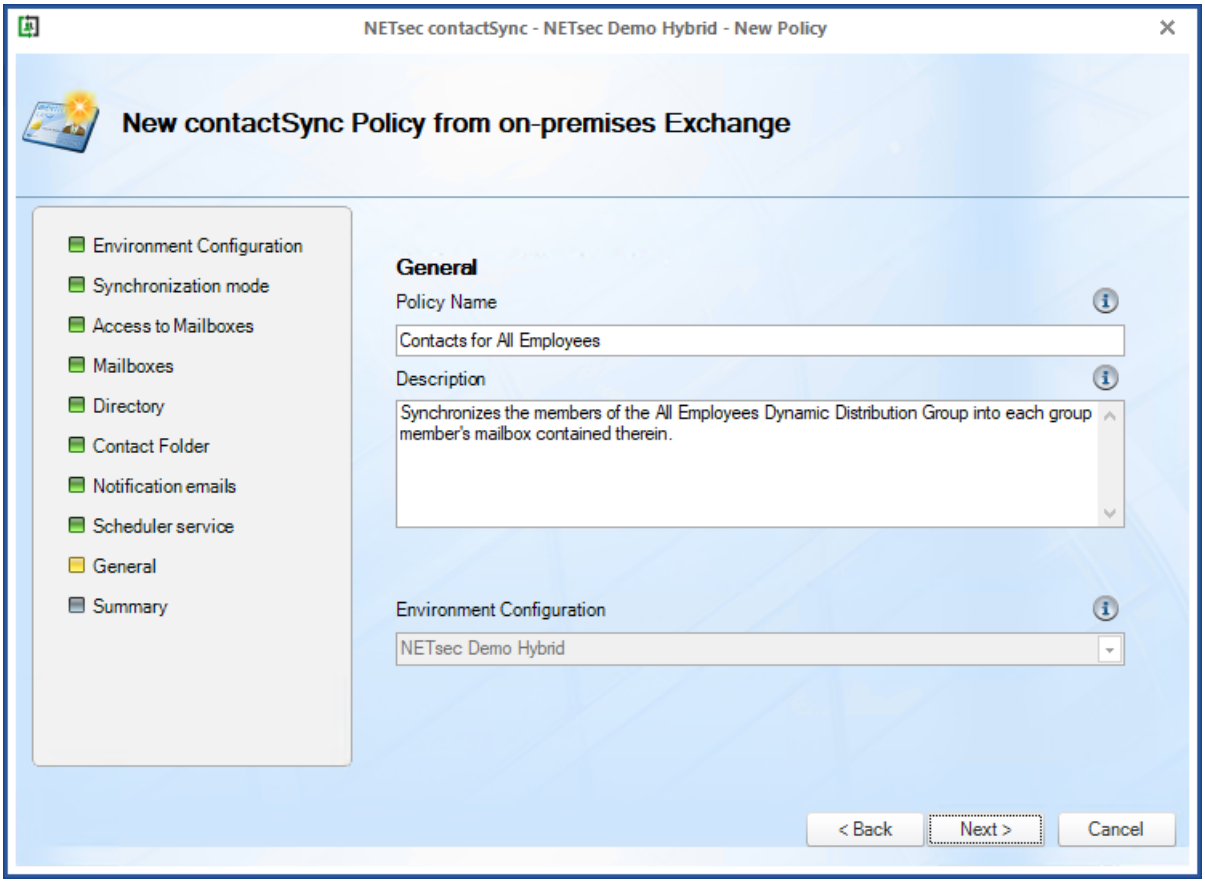


The **Monthly** schedule allows you to select which days of the month the policy runs, along with start time and frequency.



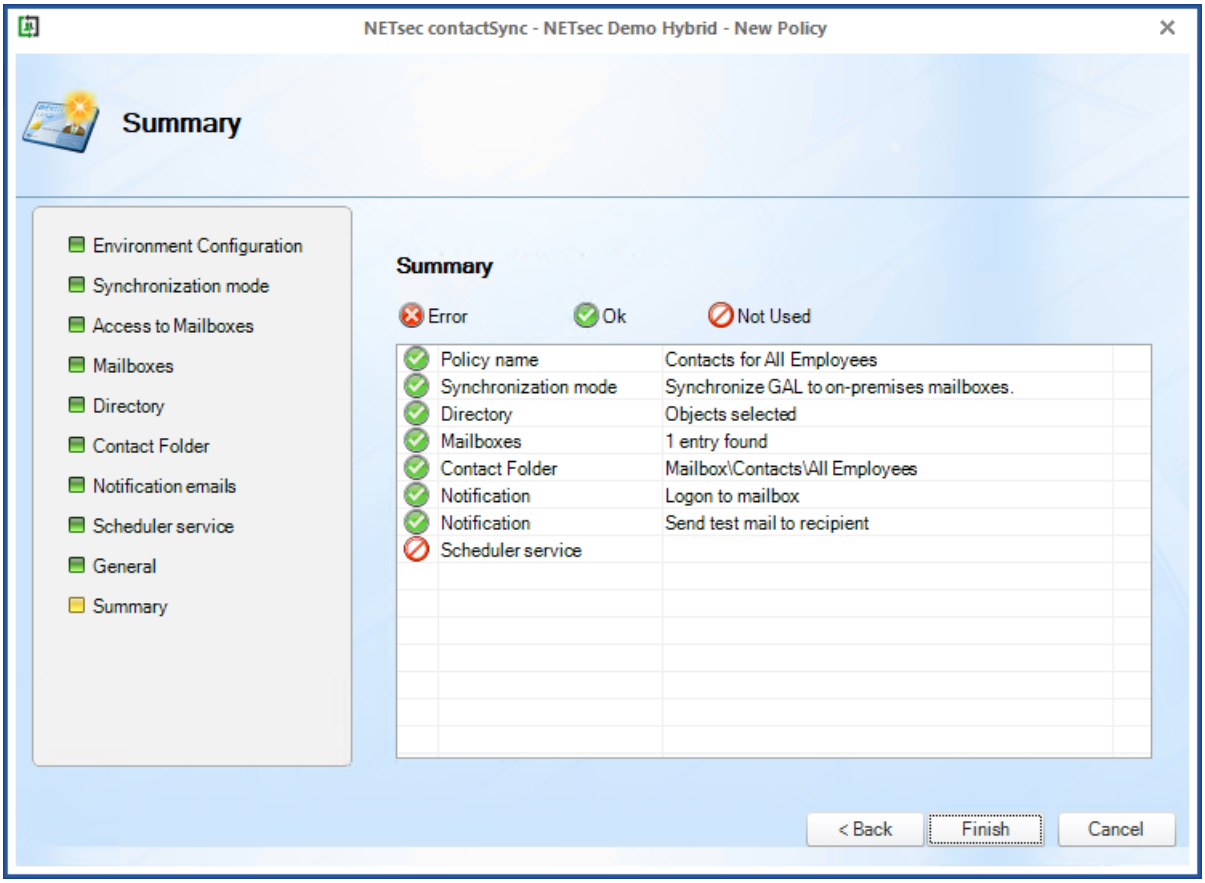
Policy name and description

Enter a policy name and optional description, then click **Next**.



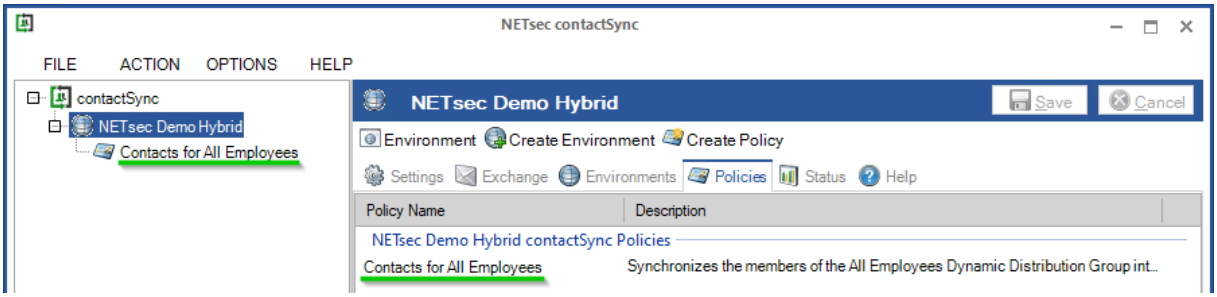
To ensure your settings have been properly configured contactSync will check your policy settings and notify you of any detected errors.

Click **Finish**.

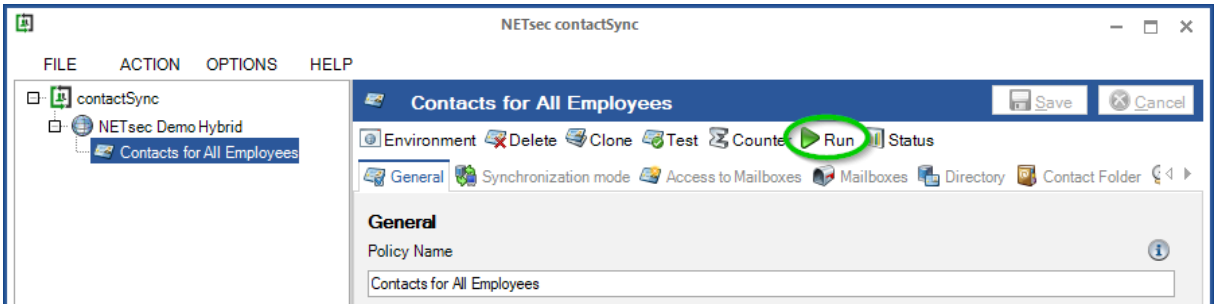


Execute Policy and Check Log File

The new policy is accessible by selecting it from either link shown below. Select the policy node.

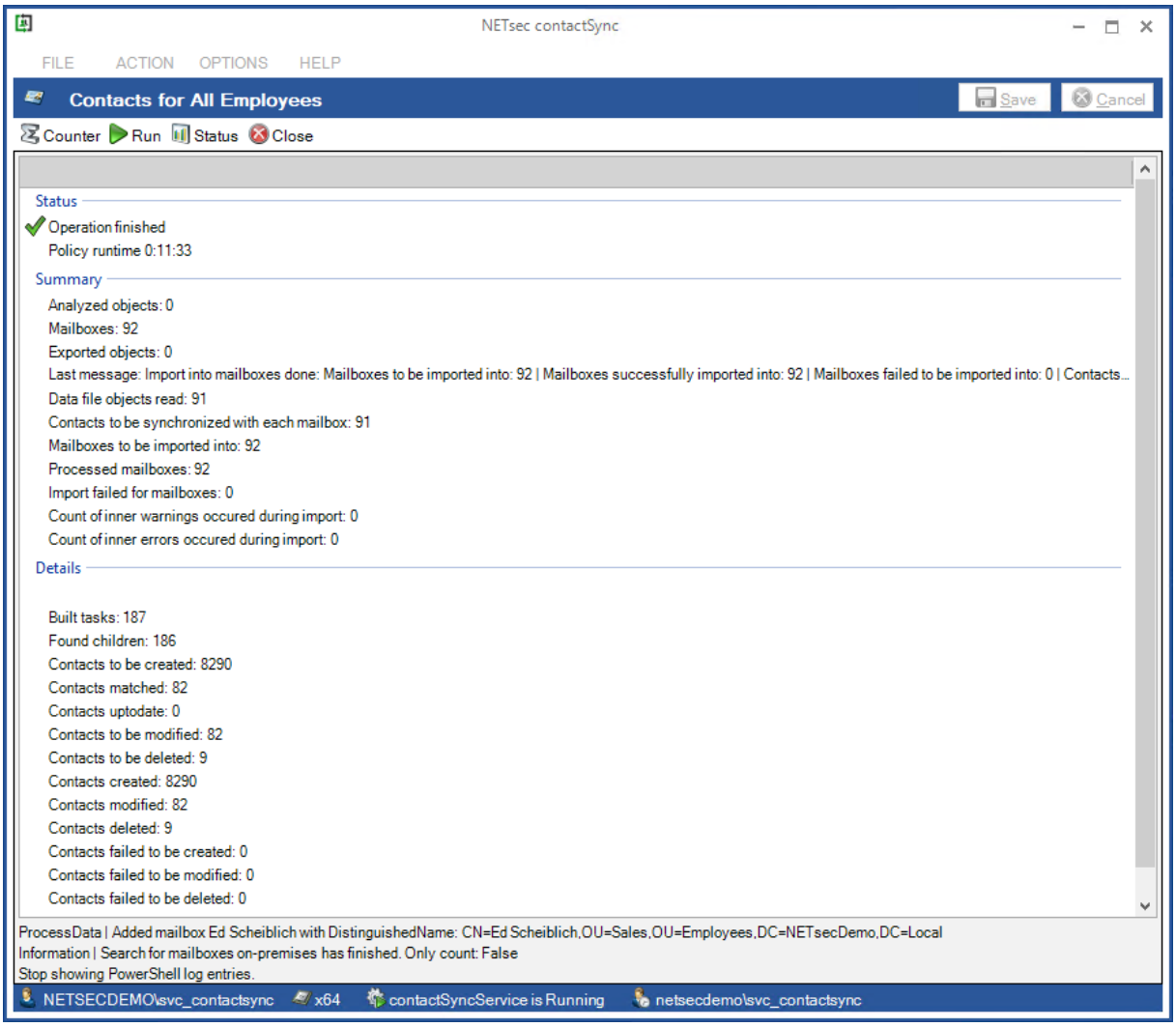


Click the **Run** button.

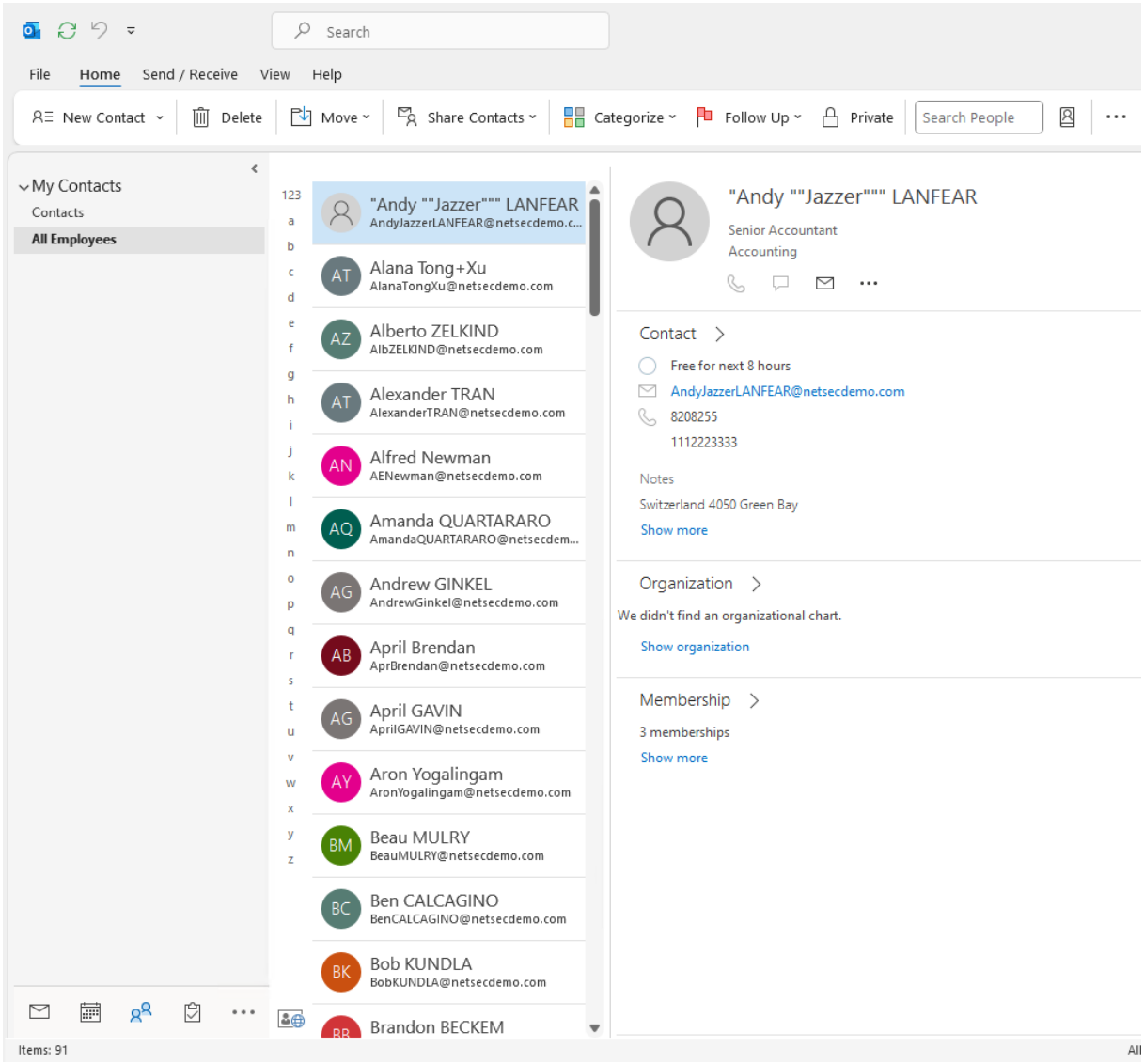


The status and a detailed summary are displayed upon completion.

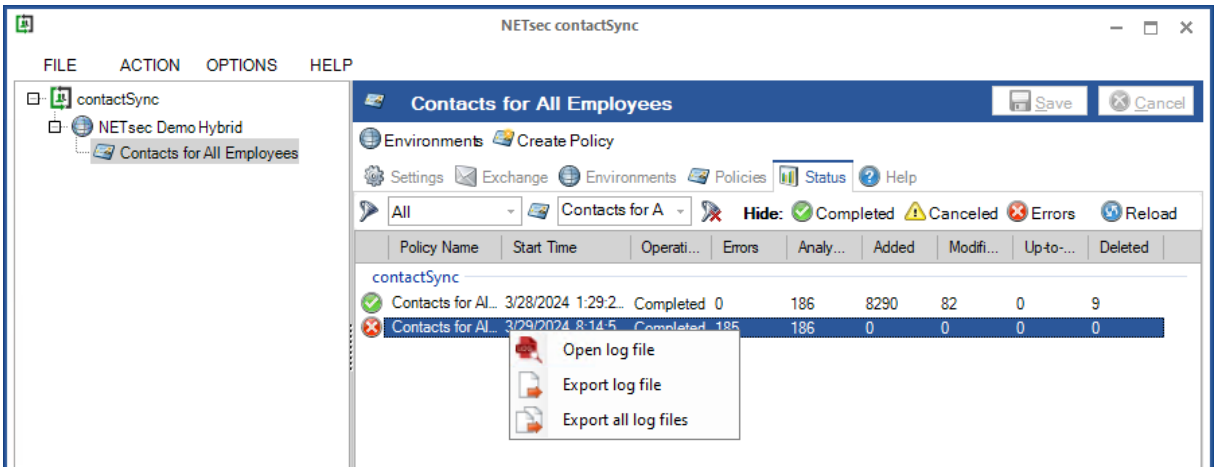
All operations have been summarized below. Further details can be obtained from the log file.



Results of synchronization shown below.



The corresponding log file can be opened by selecting the Status tab, and right-clicking the associated log and selecting **Open log file** from the context menu. This allows you to easily find the error and identify its cause.

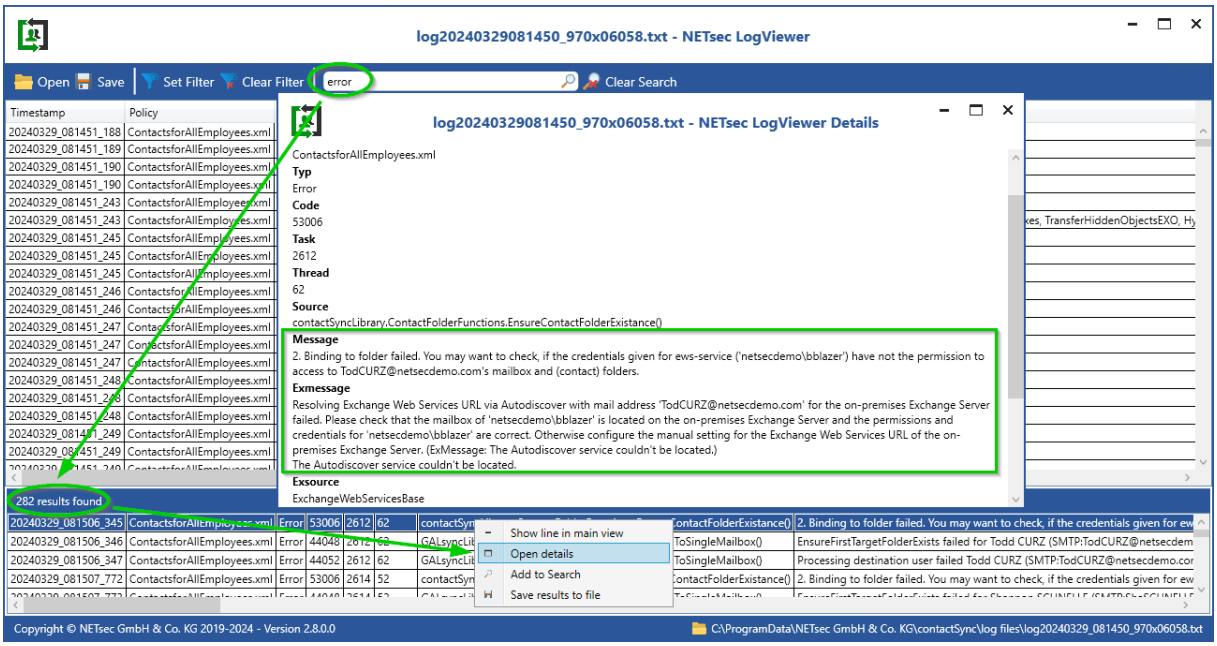


Searching for the string **error** yields 282 log entries containing this string.

Right-click any line which contains an error, then select open details.

Details of the error can be found in both the Message and Exmessage marked below.

The error indicates binding to the configured contact folder failed. Upon further review of the configuration, the dedicated users to write to this folder are lacking the Application Impersonation Role. After assigning the correction permissions, the policy run was successful

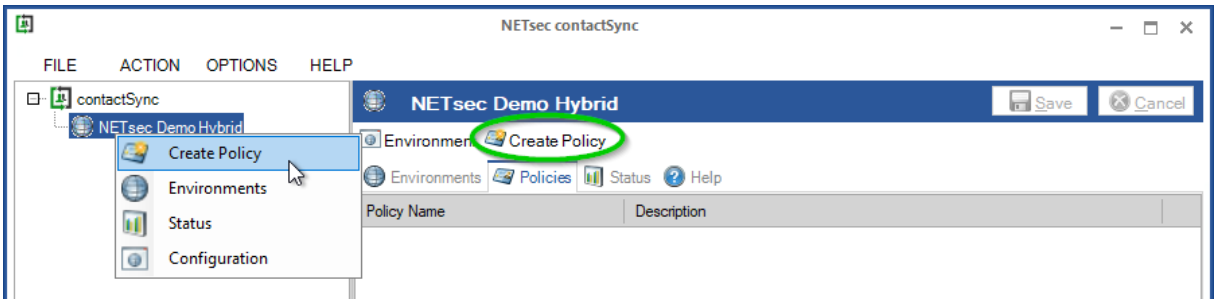


Synchronize Contacts from Exchange Online into Mailboxes

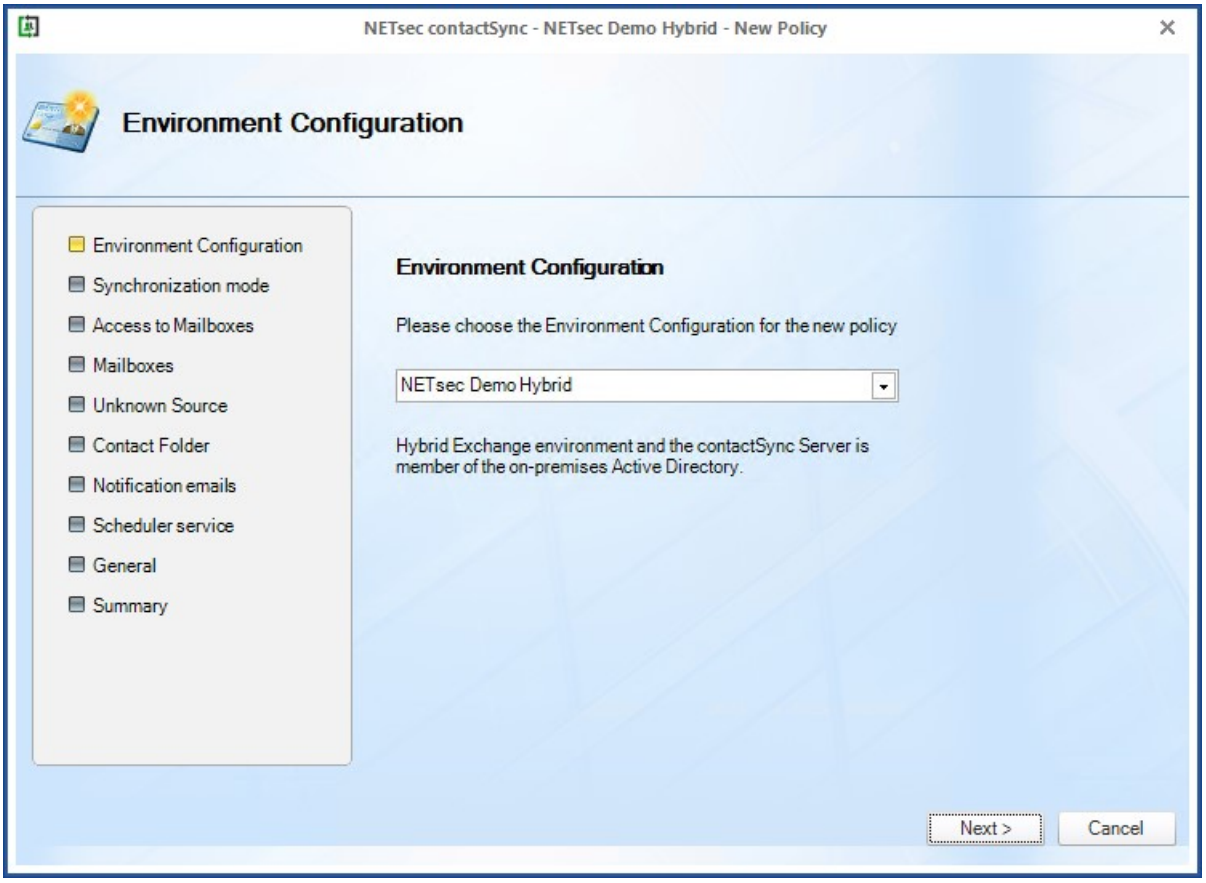
contactSync allows you to synchronize mail-enabled objects directly from Exchange Online as contacts into user mailboxes. It will connect to user mailboxes in your local Exchange Environment, whether it is in Exchange on-premises, Exchange Online or part of a hybrid Exchange environment.

Create new policy

Select the desired environment node, then click **Create Policy**.



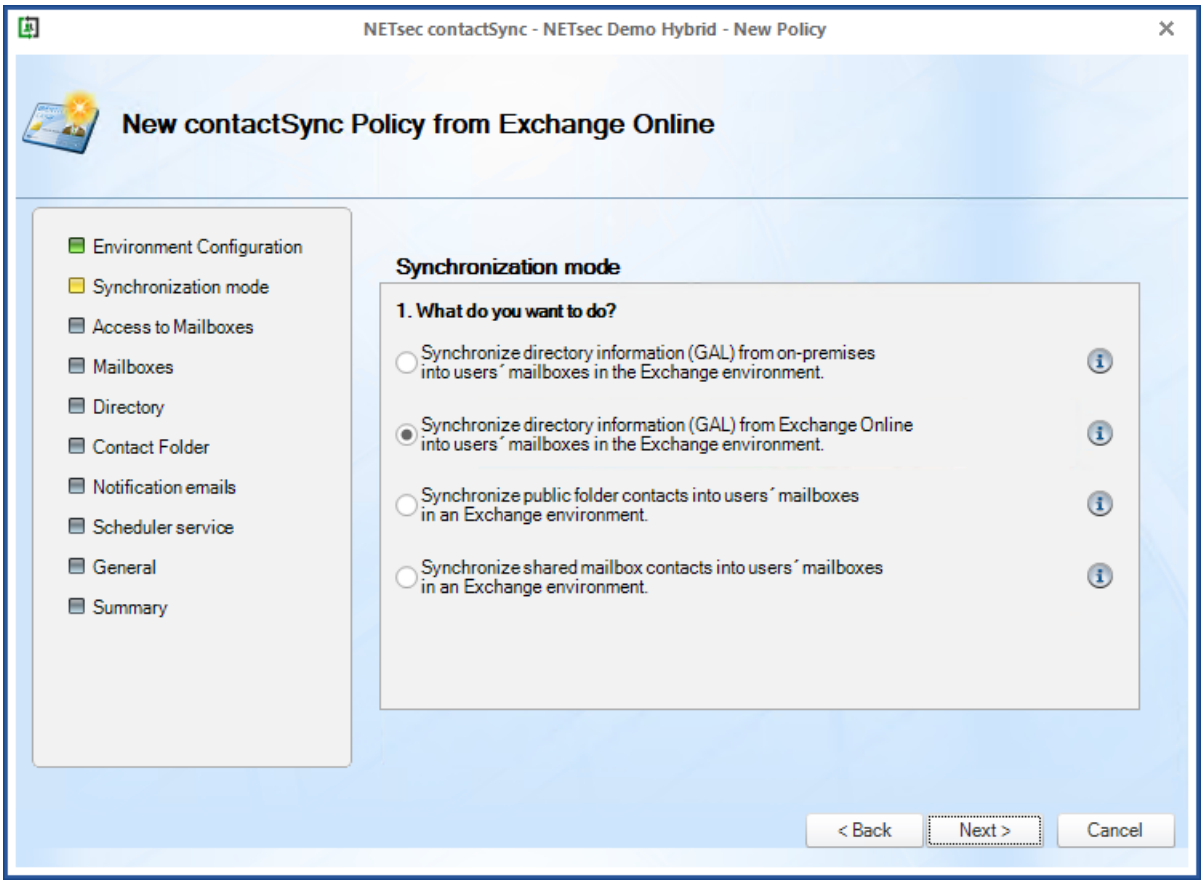
Ensure the desired environment has been selected from the dropdown.



Synchronization mode

Select **Synchronize directory information (GAL) from Exchange Online into users' mailboxes in the Exchange Environment**.

Click **Next**.

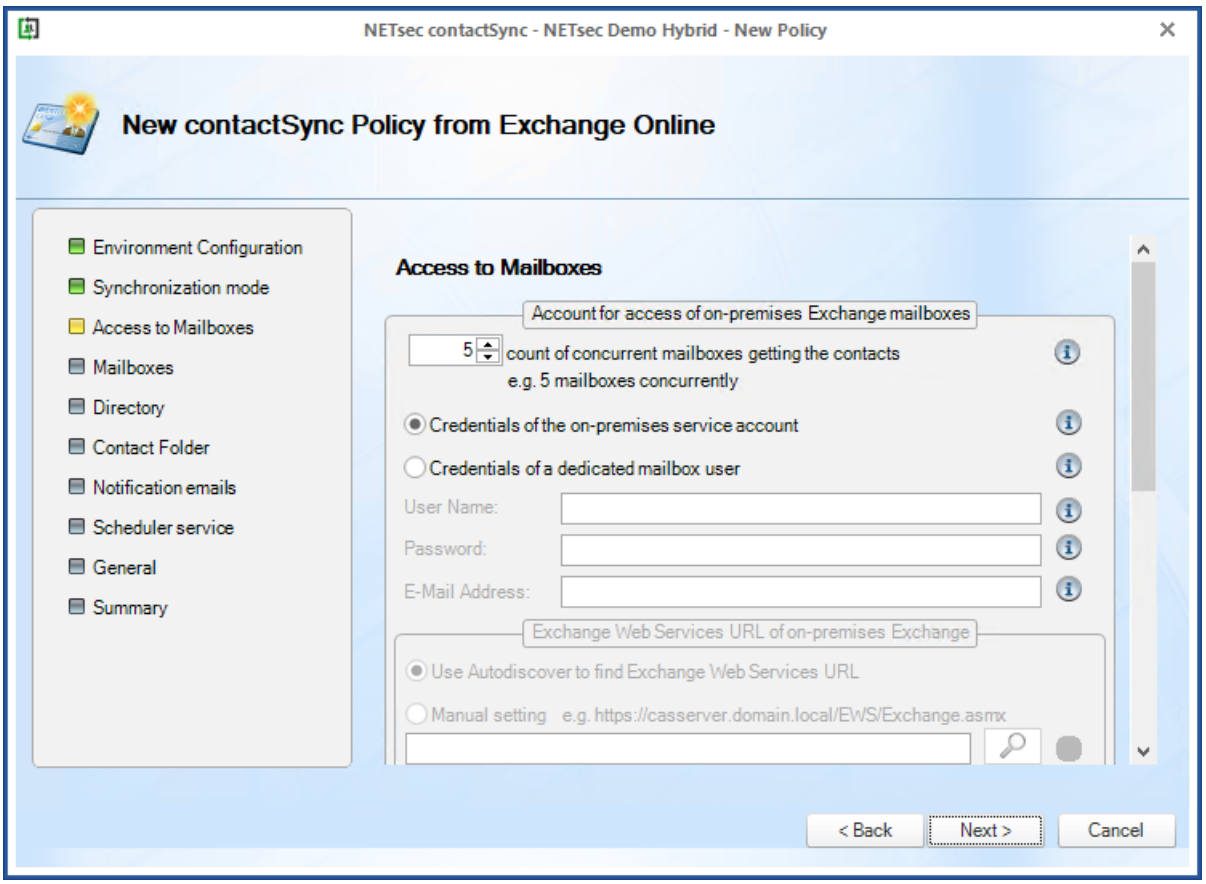


Access to Mailboxes for On-Premises Exchange

contactSync requires access to user mailboxes in order to write to their contacts folder. The **Exchange Application Impersonation** can be configured for such access, which allows up to 5 concurrent connections to user mailboxes.

By default, contactSync will use the account which has been configured in the Environment configuration.

These two roles can be split between two separate accounts by entering the credentials of a dedicated mailbox user that has the **Application Impersonation** role.



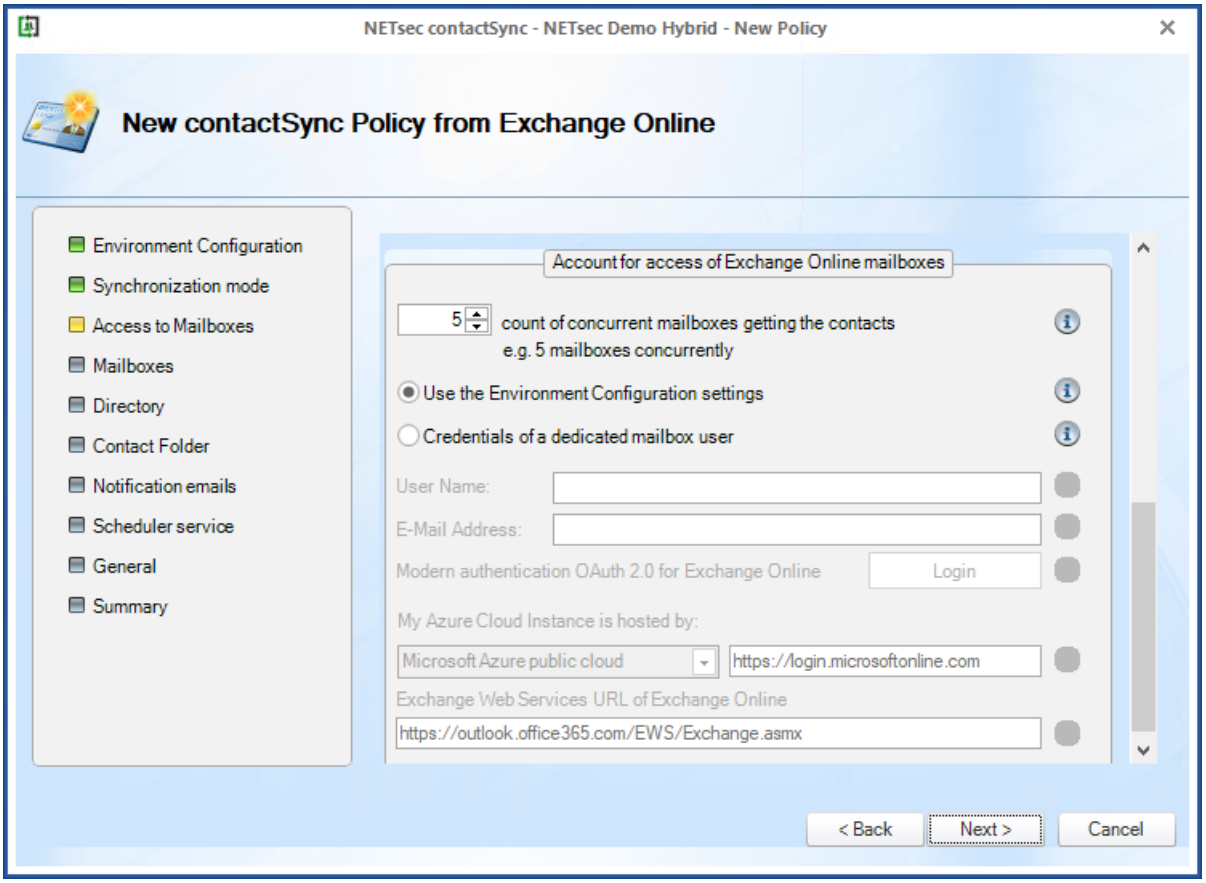
Please take a look at the chapter:

How to configure Exchange Application Impersonation

Access to Mailboxes for Exchange Online

By default, contactSync uses the Environment Configuration to access mailboxes. Application Impersonation, required for on-premises Exchange, will not be necessary when the certificate authentication via App Registration for Exchange Online is configured in the Environment Configuration.

Please take a look at the chapter
Exchange Online certificate-based authentication via App Registration

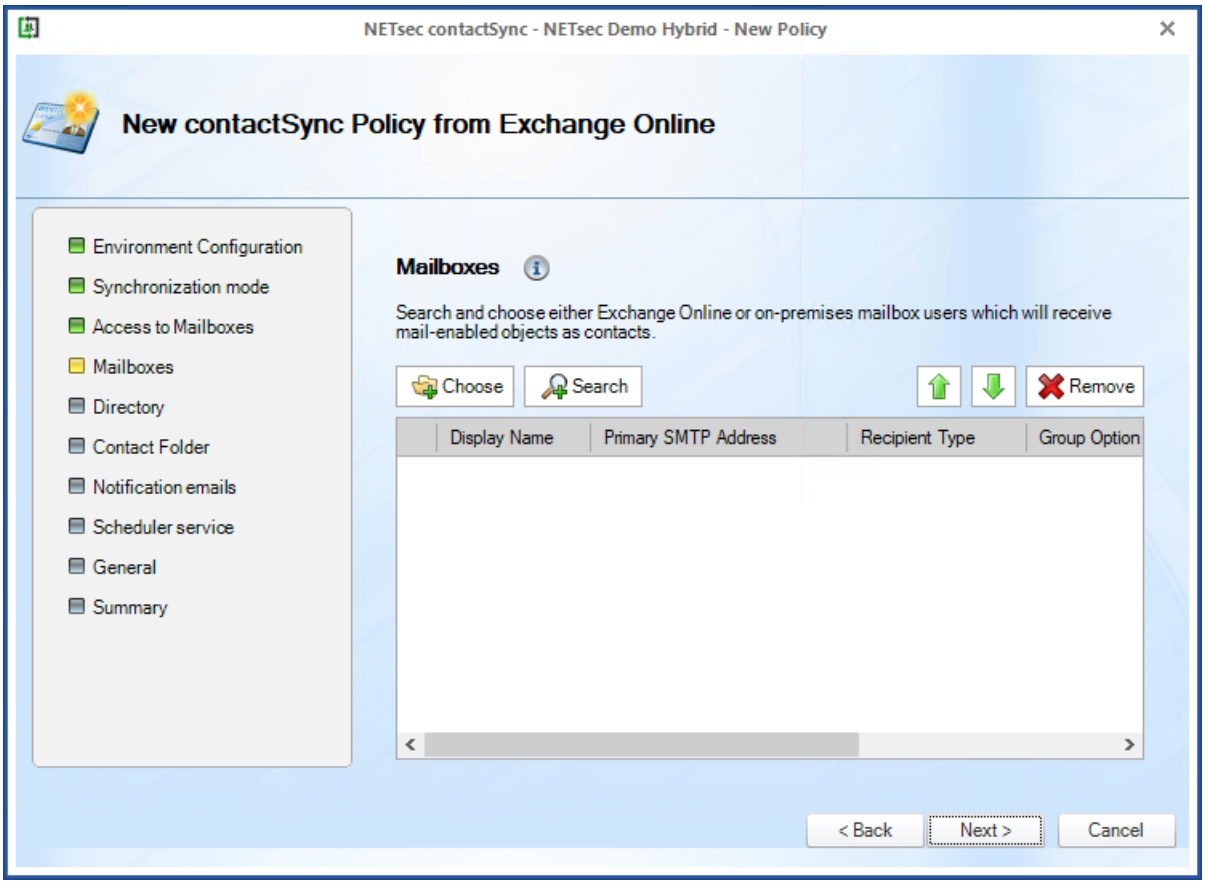


Click **Next**

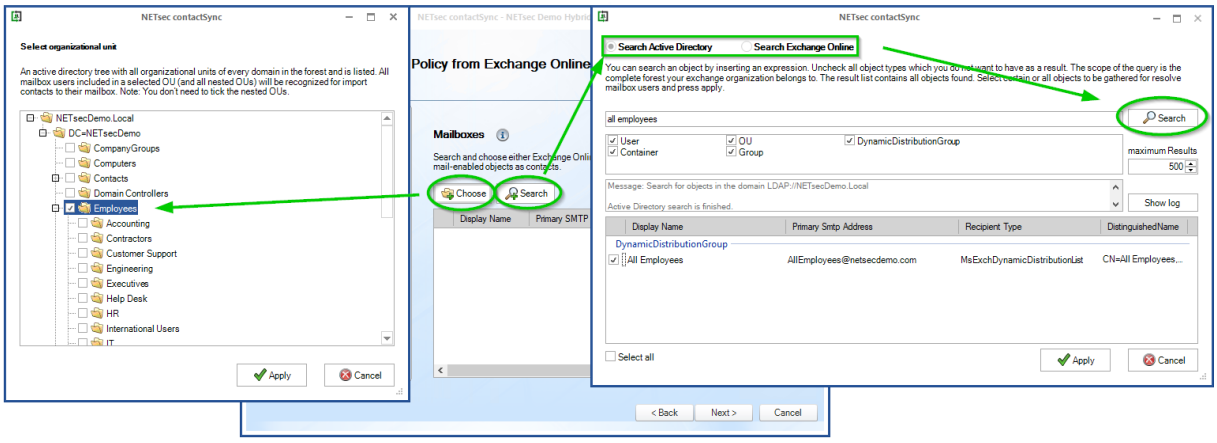
Select the Mailboxes from On-Premises Exchange

You can select Mailboxes located in an on-premises Exchange Server, which will receive contacts. It could be an on-premises Exchange environment or a part of a hybrid Exchange environment.

In the **Mailboxes** window, you are prompted to select the mailboxes which will receive the contacts. There are two ways to do make your selection.



- Click **Choose** to select mailboxes by OU where they reside in Active Directory.
- Click **Search** to open a search dialogue window from which you can search for the desired Active Directory objects. When searching Active Directory, mailboxes can be selected individually, by group membership, by container, or by OU. If you have a hybrid Exchange environment, an additional option is available to search for Exchange Online objects.

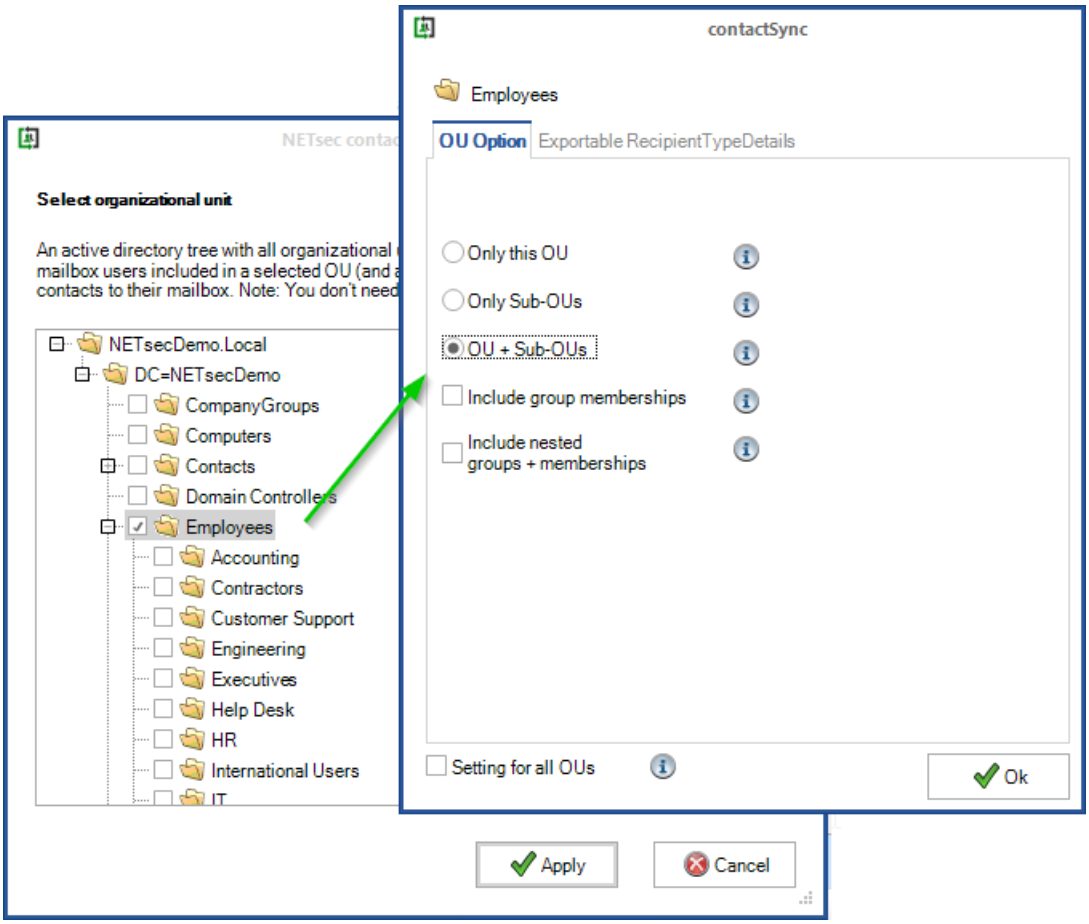


When the **Search Exchange Online** Radio Button has been selected, you can search for objects by Recipient Type, such as **UserMailbox**, **MailUniversalDistributionGroup**, **MailUniversalSecurityGroup**, **DynamicDistributionGroup**, or **Office365 Group**.

When OUs are selected, a prompt to select the OU depth is presented. If any groups are contained in the OU, contactSync will prompt the user to include mailboxes by group membership.

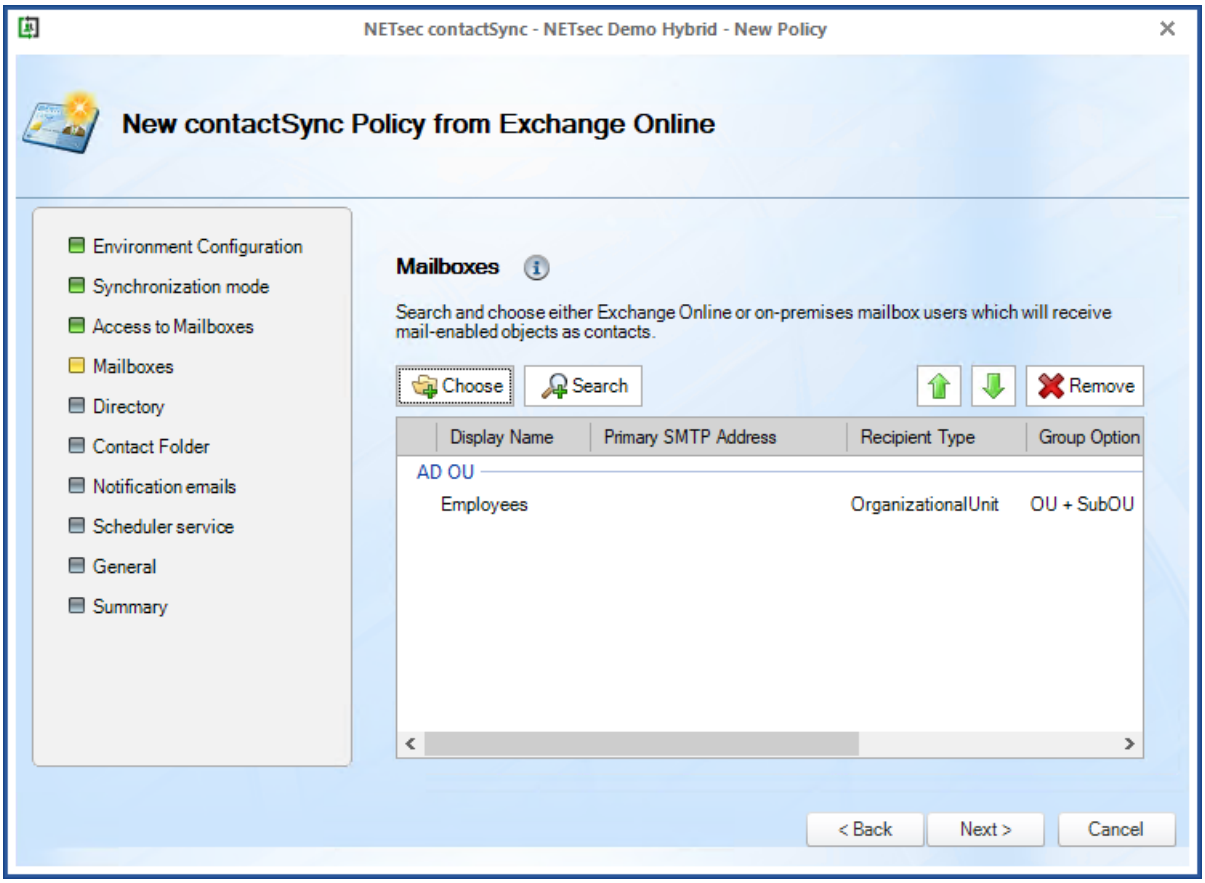
If multiple OUs have been selected, the checkbox at the bottom left will apply the settings to all selected OUs.

Click **OK**, then **Apply**.



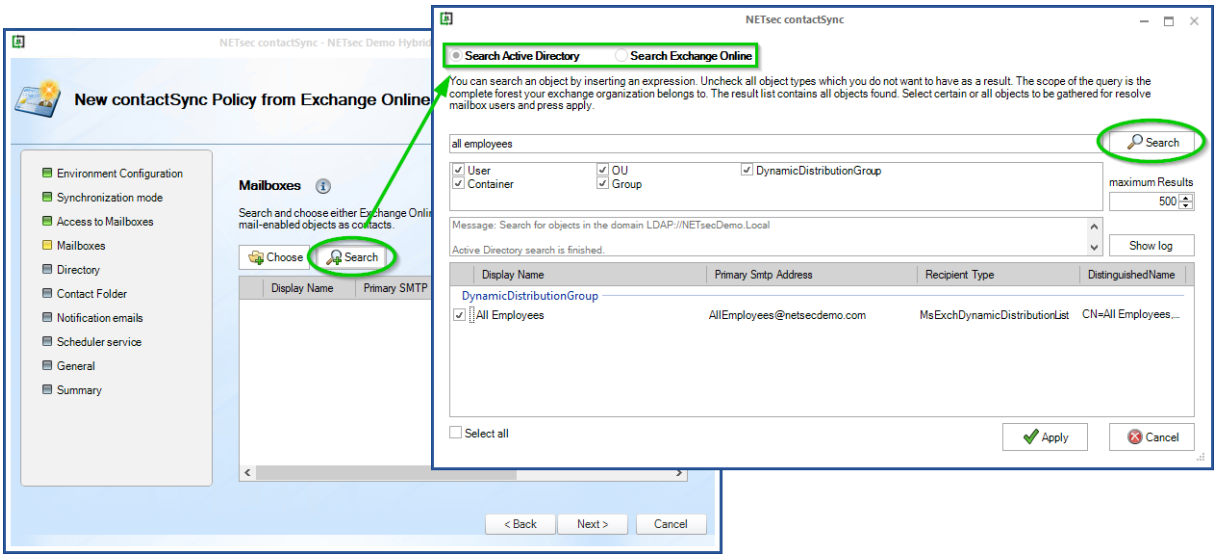
Verify the selected OUs are displayed.

Click **Apply**

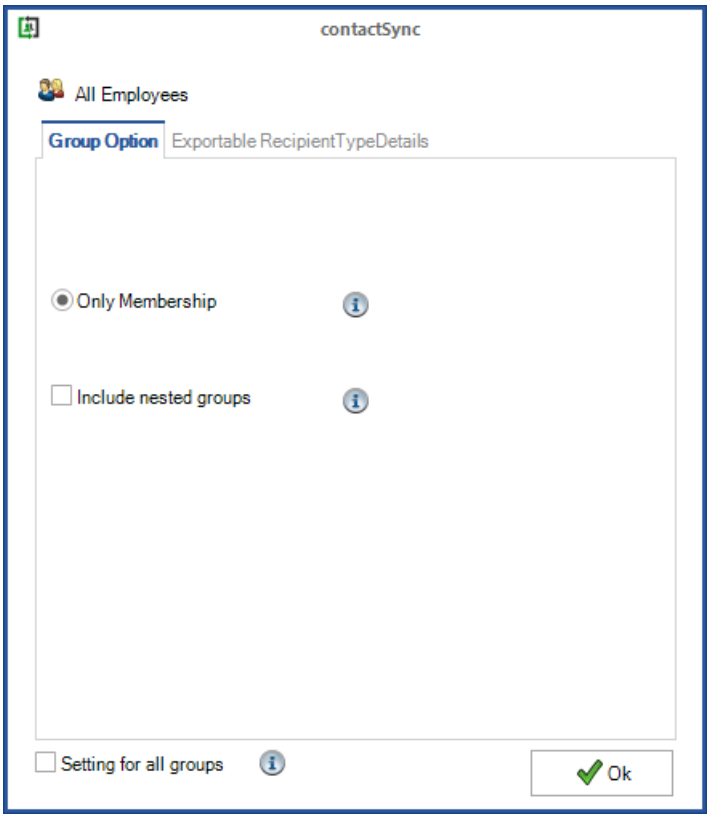


Click **Next**.

Instead of selecting OUs in Active Directory as described above, in the following example, the "All Employees" Dynamic Distribution Group has been selected from the Active Directory search.

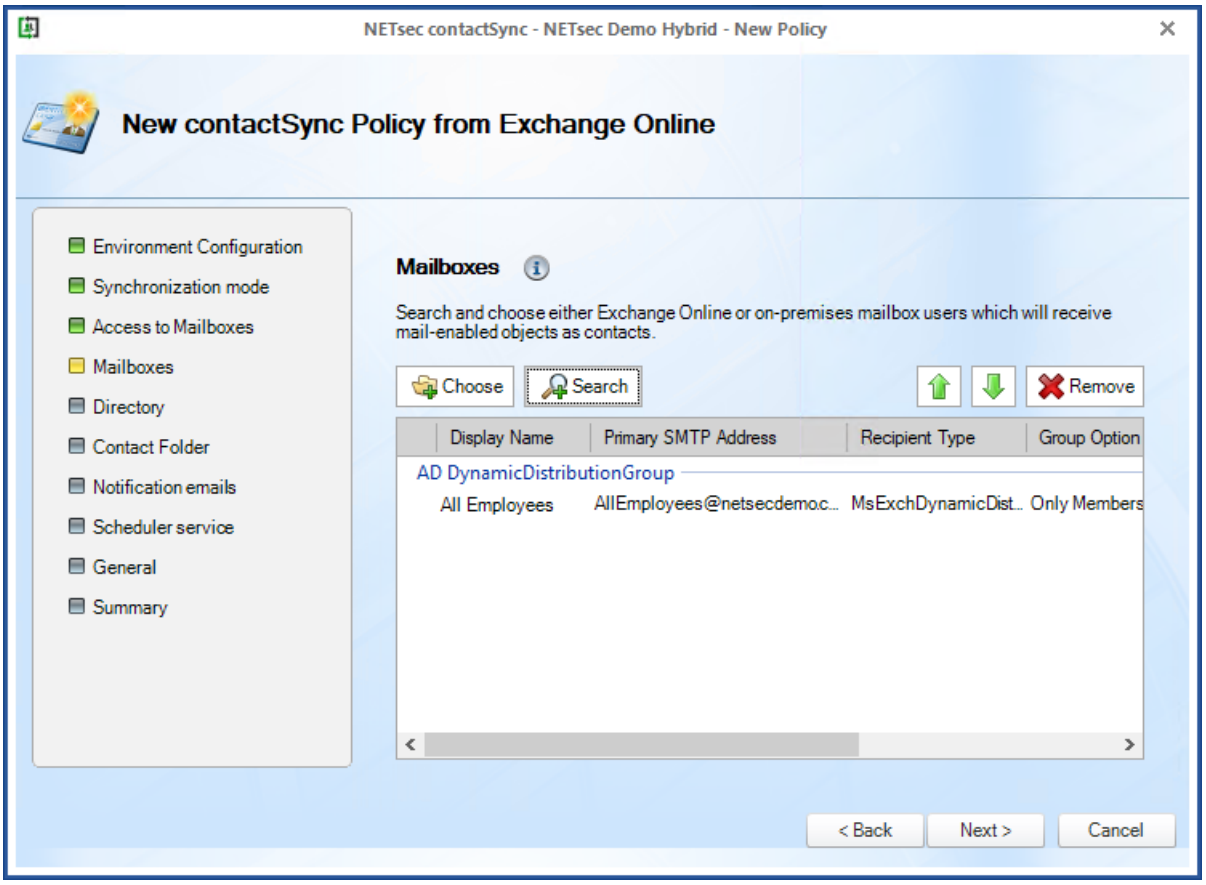


All members with a mailbox in the selected group will receive the contacts, an option is also available to include nested groups.



Click **OK**.

The selected group(s) are displayed under the appropriate heading.



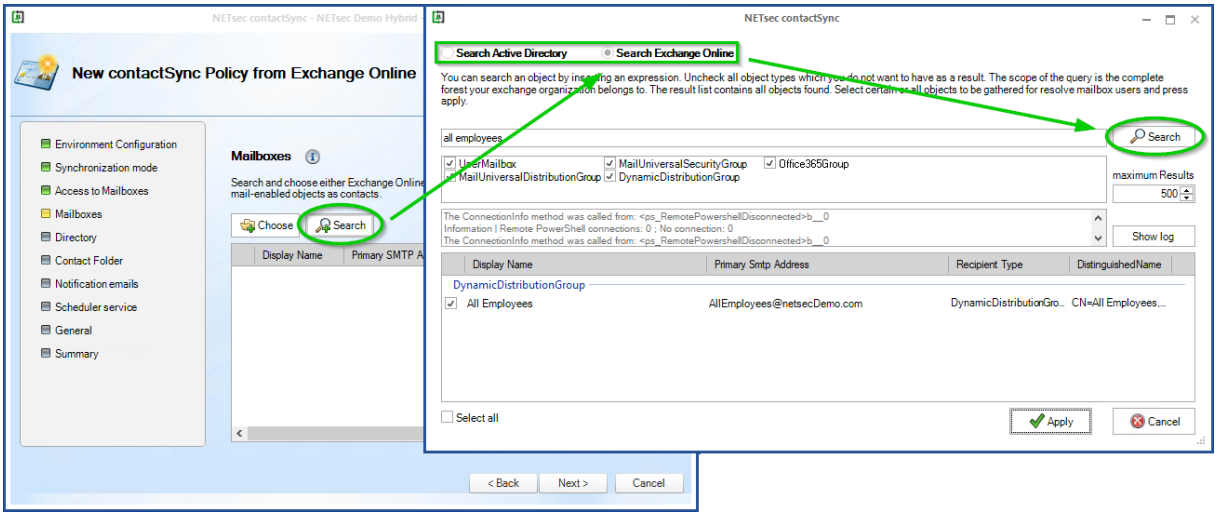
Verify the selected Group(s) is displayed.

Click **Next**.

Select the Mailboxes from Exchange Online

You can select Mailboxes located in Exchange Online which will receive the contacts. This is possible for an Exchange Online environment or a part of any hybrid Exchange environment, as shown in the screenshot below.

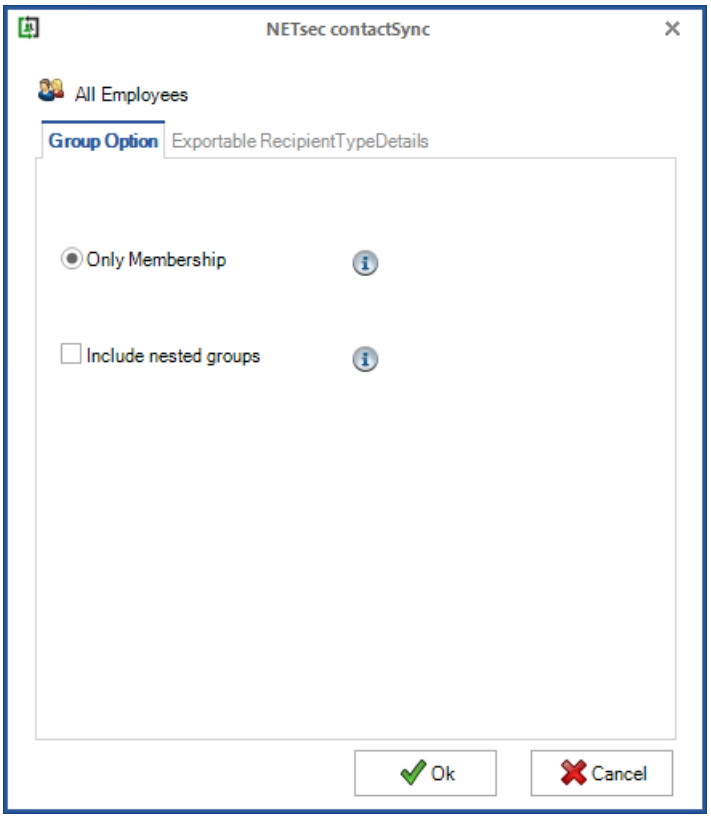
When searching for Exchange Online objects, you can search for objects by Recipient Type, such as **UserMailbox**, **MailUniversalDistributionGroup**, **MailUniversalSecurityGroup**, **DynamicDistributionGroup**, or **Office365 Group**.



In the example above, the **All Employees** Dynamic Distribution Group has been selected. You can expand your search by inserting a wild card character (*).

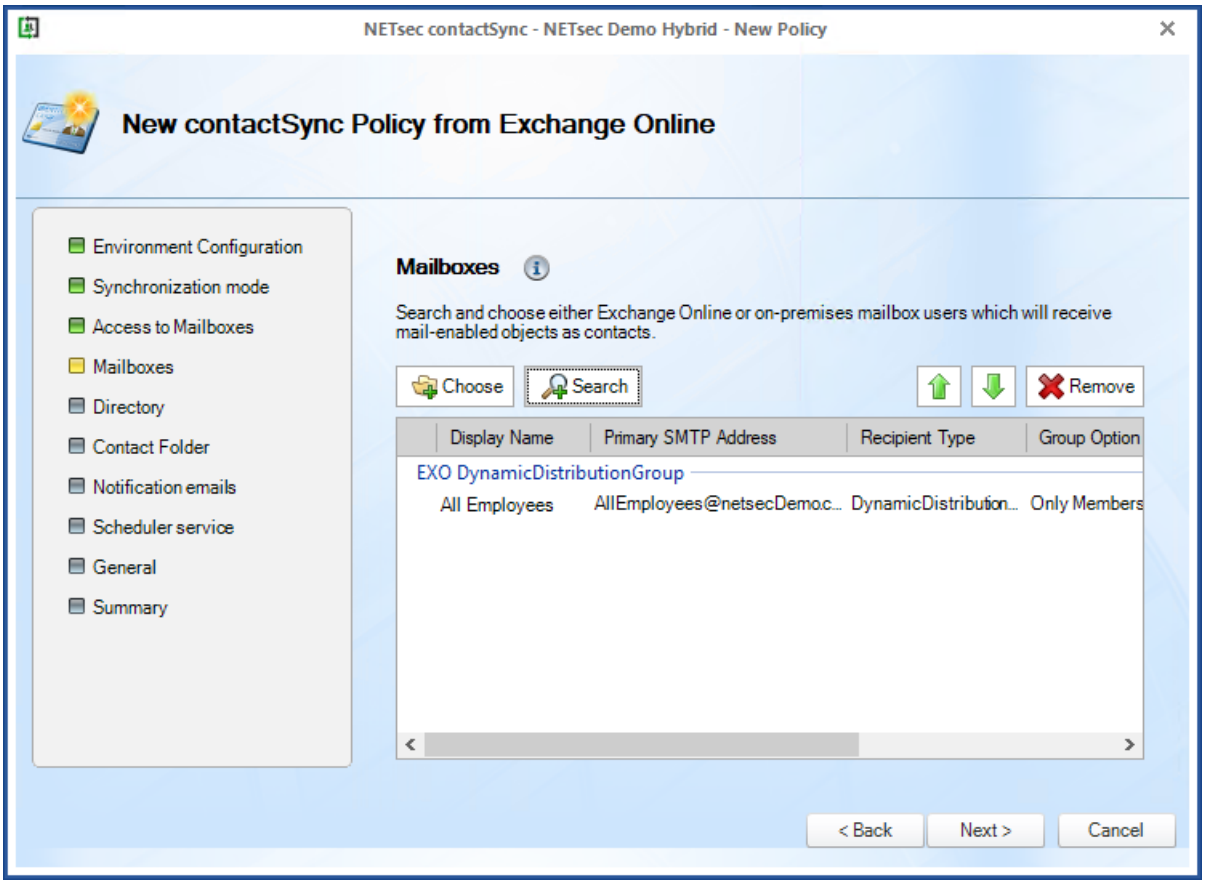
Click **Apply**.

All members with a mailbox in the selected group will receive the contacts, an option is also available to include nested groups.



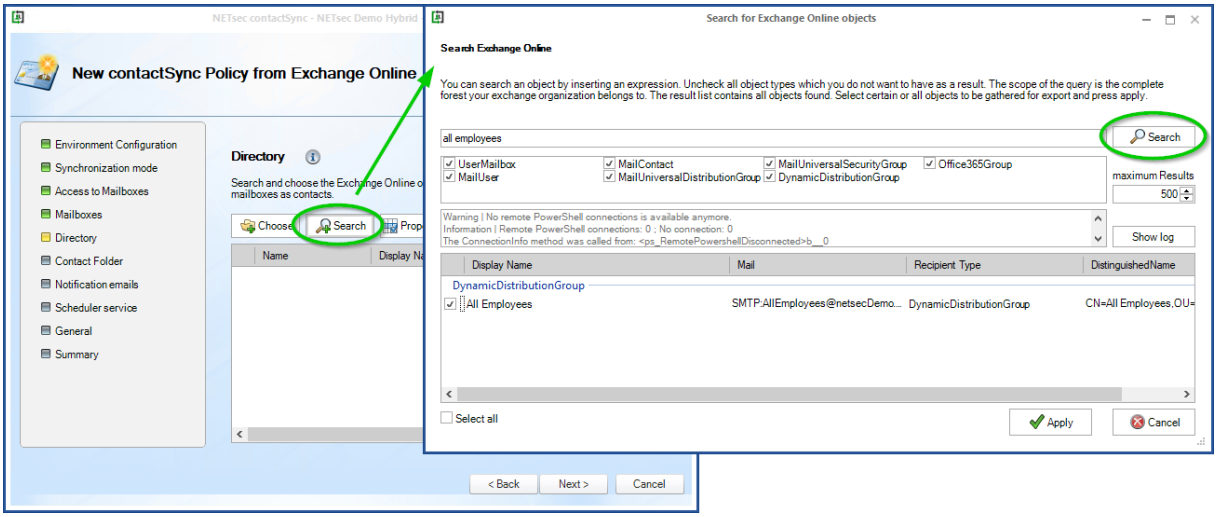
Click OK

Verify the selected group(s) are displayed. Click **Next.**



Select mail-enabled objects on the Directory tab from Exchange Online

Click **Search** to search for objects via Exchange Online PowerShell query. They can be selected individually, or by group membership (preferred method).



We recommend selecting a group which contains all the desired objects to be synchronized into the target mailboxes. This will prevent service accounts and other unnecessary objects from being synchronized into them.

When a group is selected, a prompt is presented to select how to handle its synchronization. These options include:

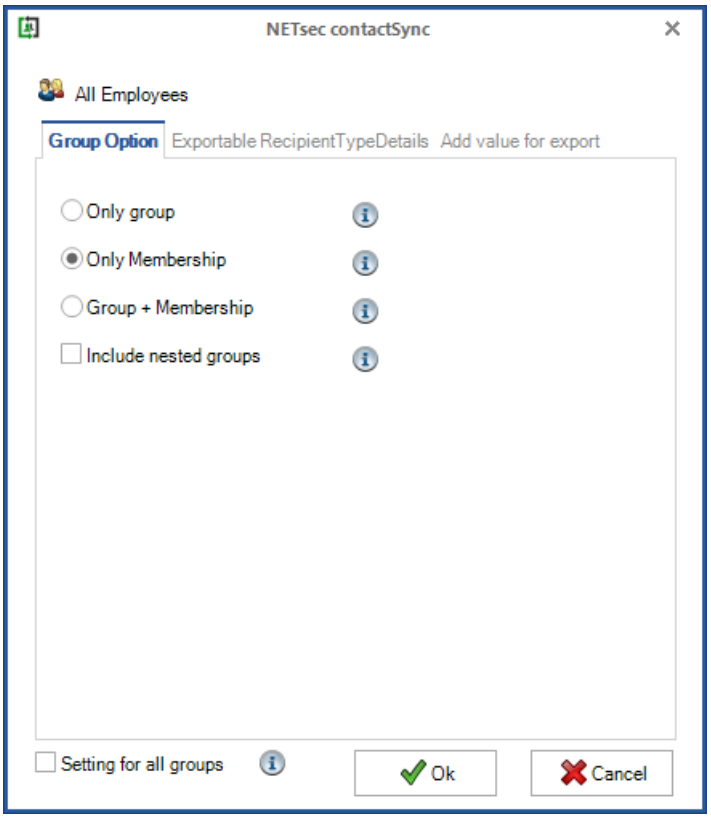
- Only group
- Only Membership
- Group + Membership

An option is also available to include nested groups.

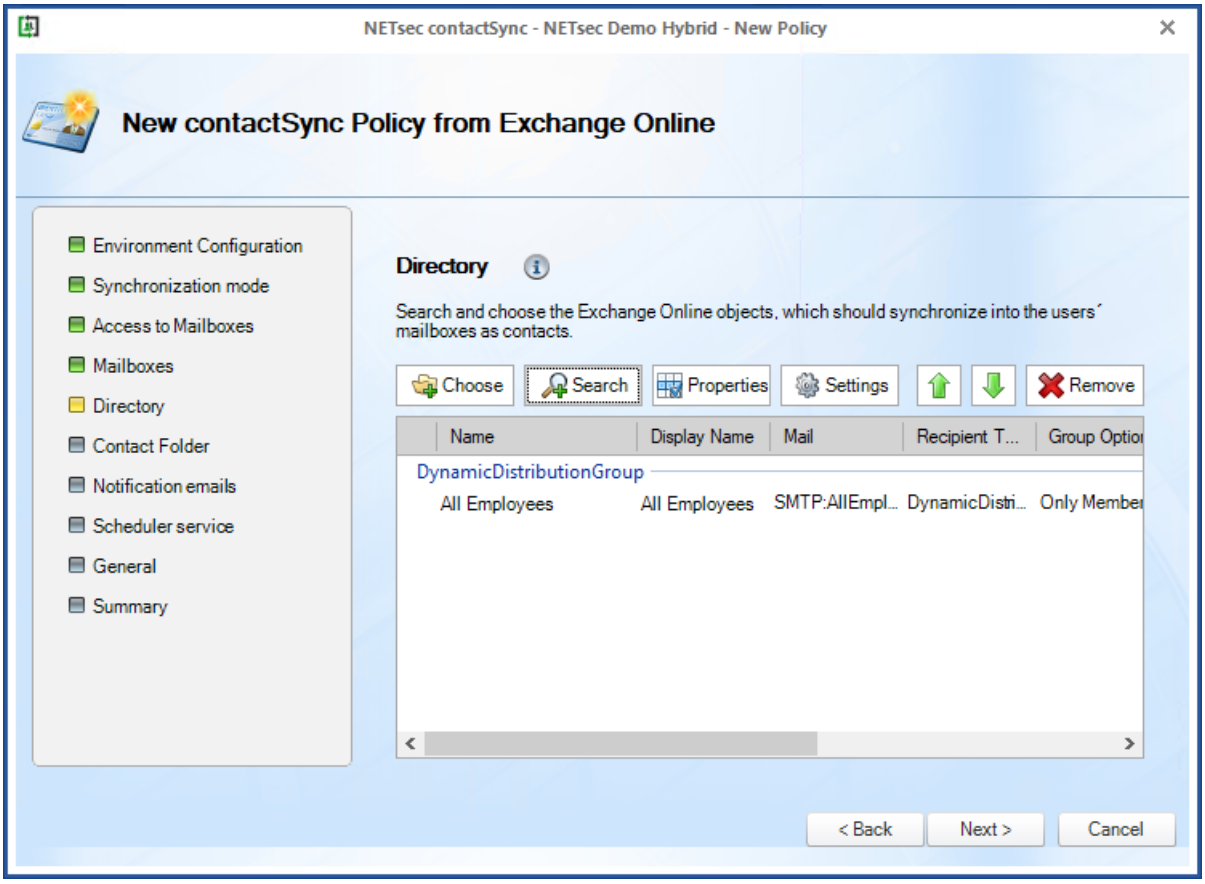
If multiple groups have been selected, the above settings can be applied individually, or checking the **Settings for All Groups** will apply the settings to all selected groups.

In the example below, only group members will be synchronized.

Click **OK**



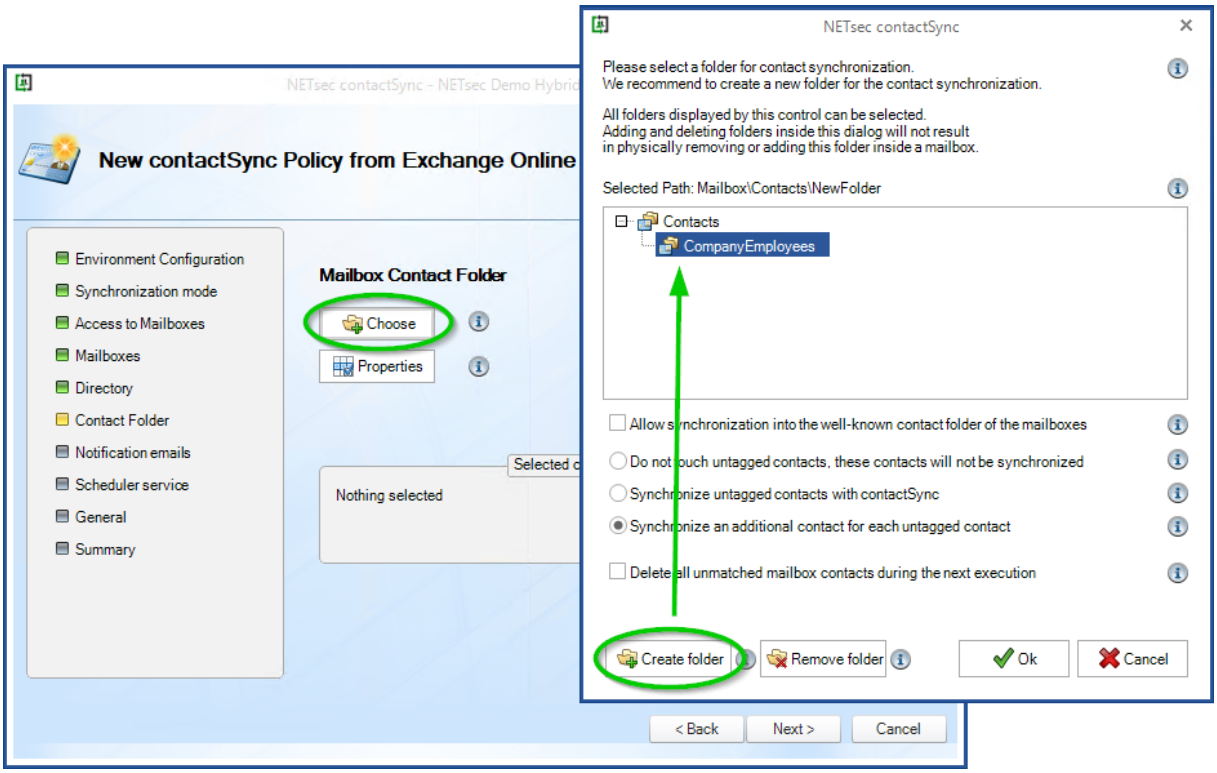
Ensure the selected group is displayed, then click **Next**.



Select the Mailbox Contact Folder

Click **Choose** to select the contacts folder where the contacts will be synchronized to.

contactSync, can be configured to import contacts directly into the top-level Contacts folder. We recommend a new folder is created, which keeps the contactSync created contacts separate from the user-created contacts.



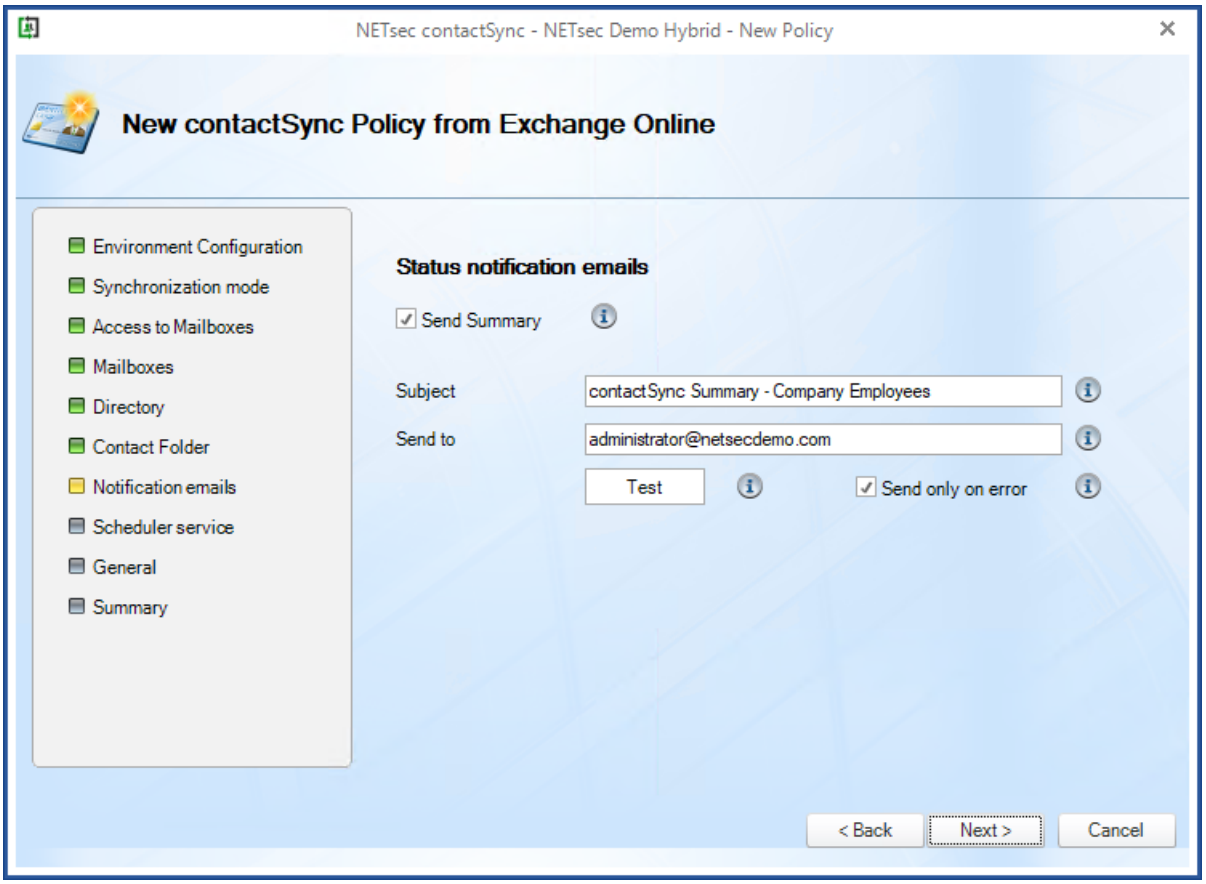
Select the top-level **Contacts** folder, then click **Create folder** to create a subfolder where the contacts will be synchronized, then give the new folder a name.

Click **OK**, then click **Next**

Status notification email

An optional status notification email can be sent to the specified recipient(s) each time the policy runs, which provides a brief summary of activity. However, if your preference is to receive one only when an error has been logged, check the **Send only on error** checkbox. Click the **Test** button to send a test email. Then verify it has been received.

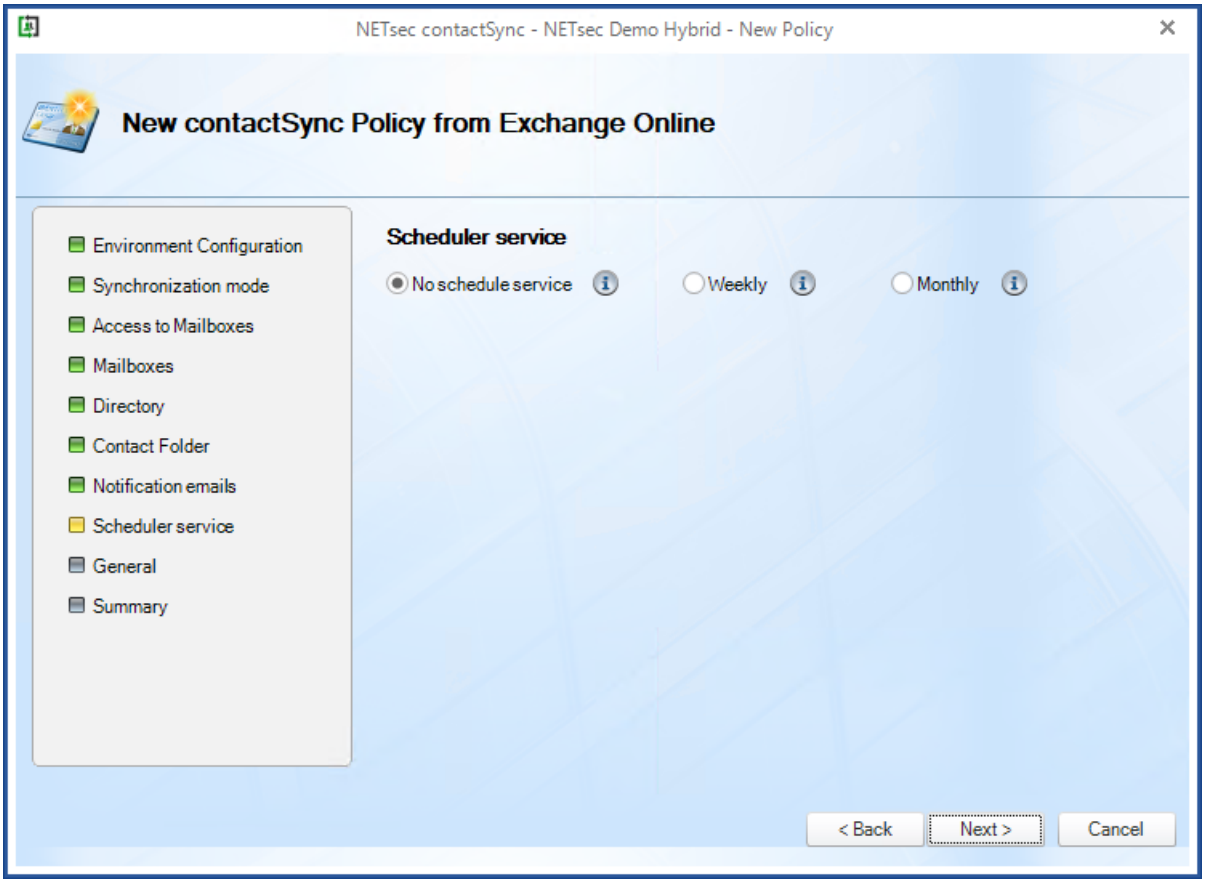
Click **Next**.



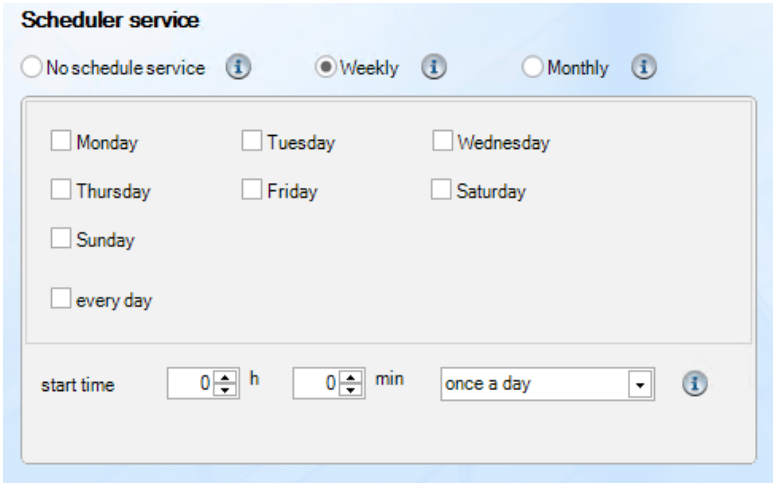
Schedule policy run

contactSync can be scheduled to run at regular intervals. We recommend the policy is manually run before any schedules are set. After the synchronization has completed successfully, you can go back and set it to run on the desired schedule.

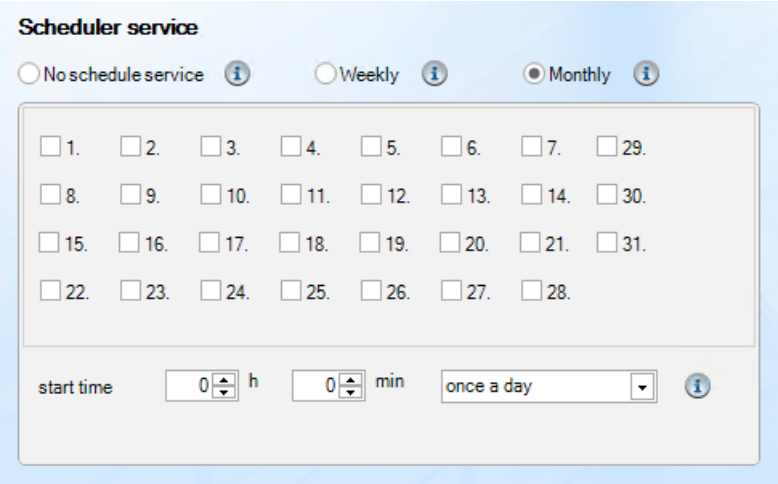
Click **Next**.



The **Weekly** schedule allows you to select which days of the week the policy runs, along with start time and frequency.

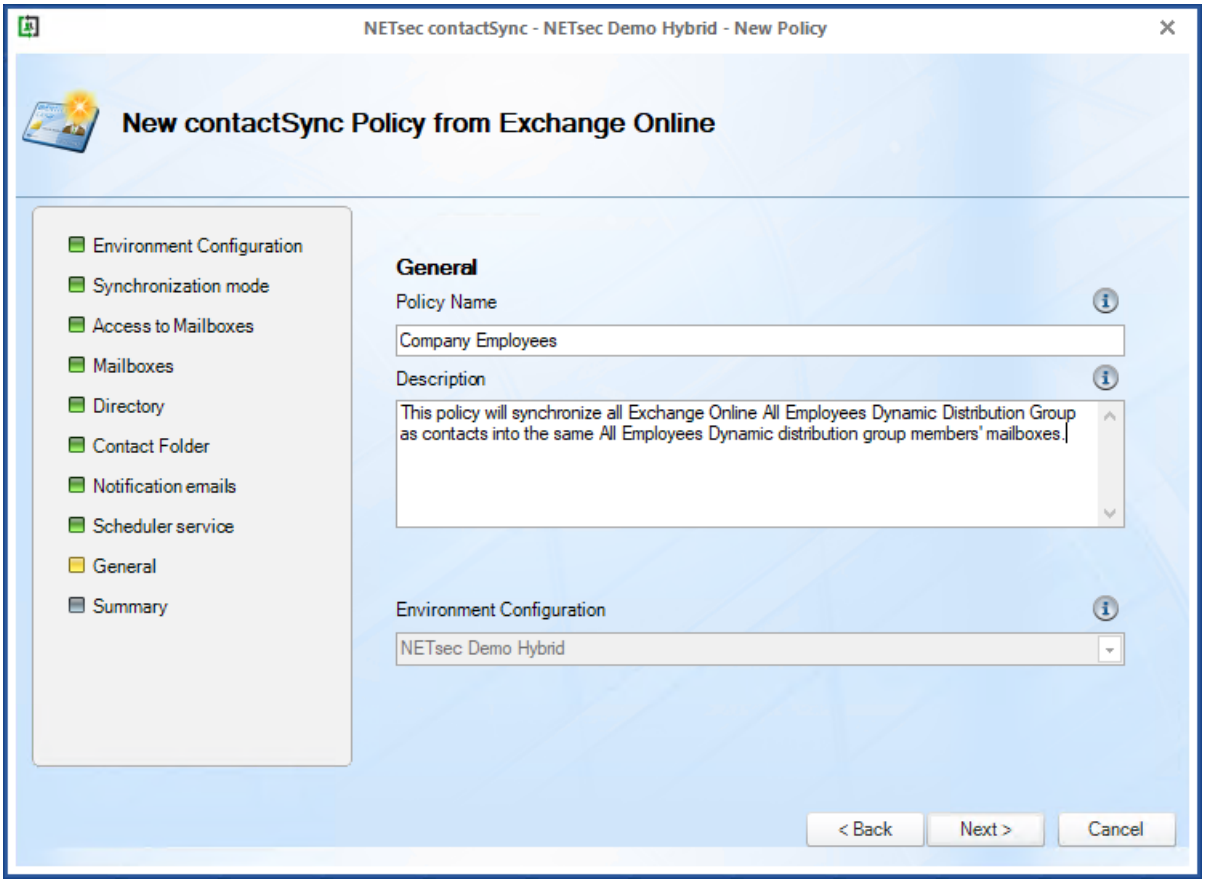


The **Monthly** schedule allows you to select which days of the month the policy runs, along with start time and frequency.



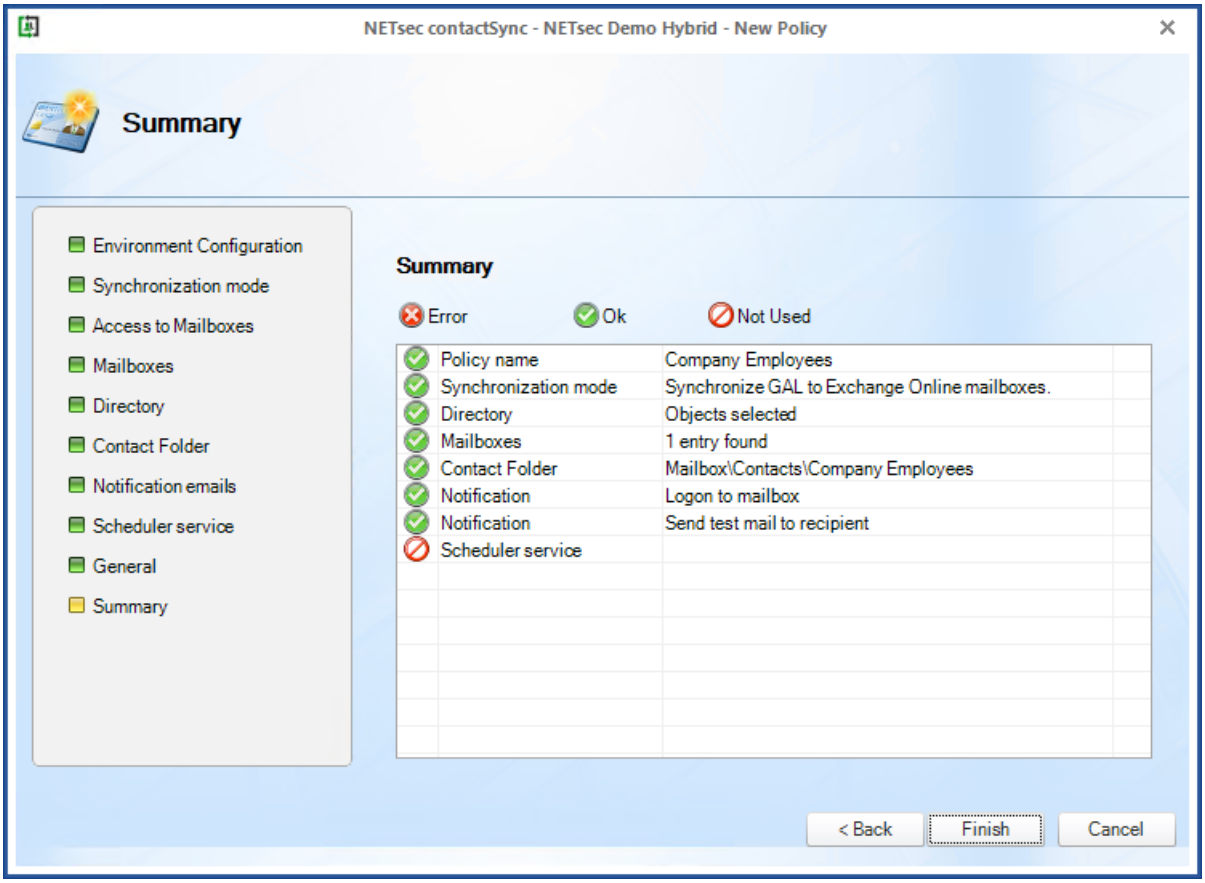
Policy name and description

Enter a policy name and an optional description, then click **Next**.



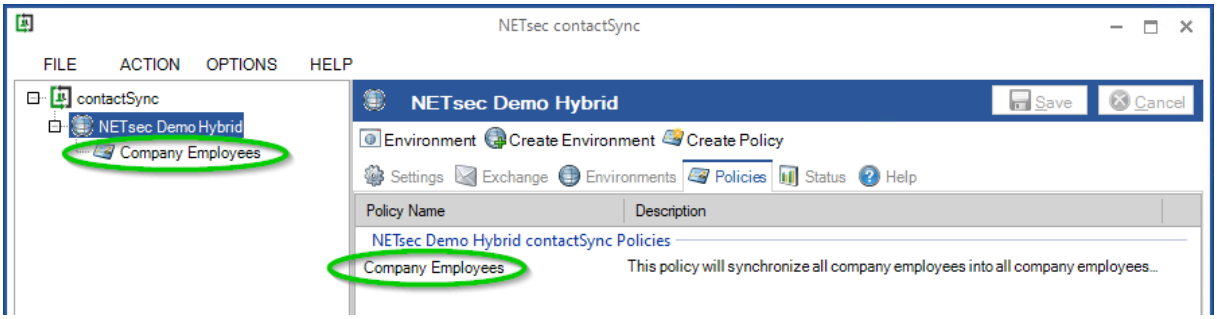
To ensure your settings have been properly configured contactSync will check your policy settings and notify you of any detected errors.

Click **Finish**.

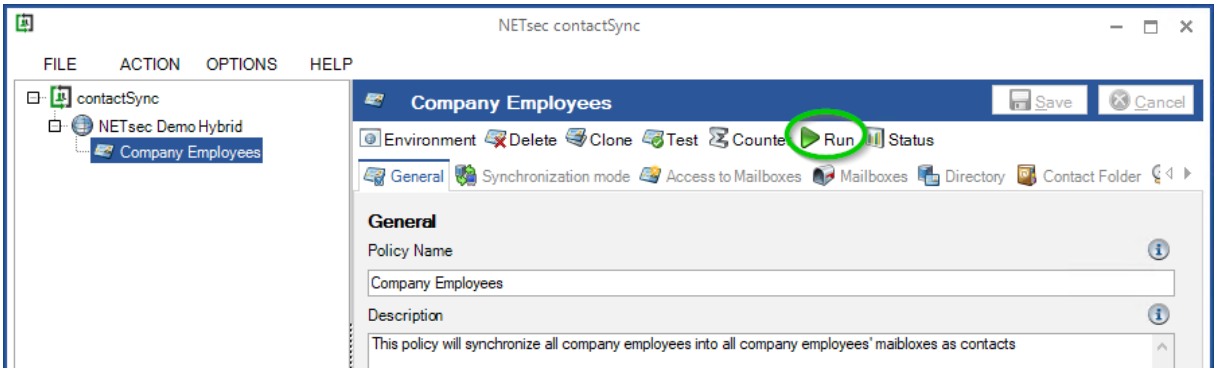


Execute policy and check log files

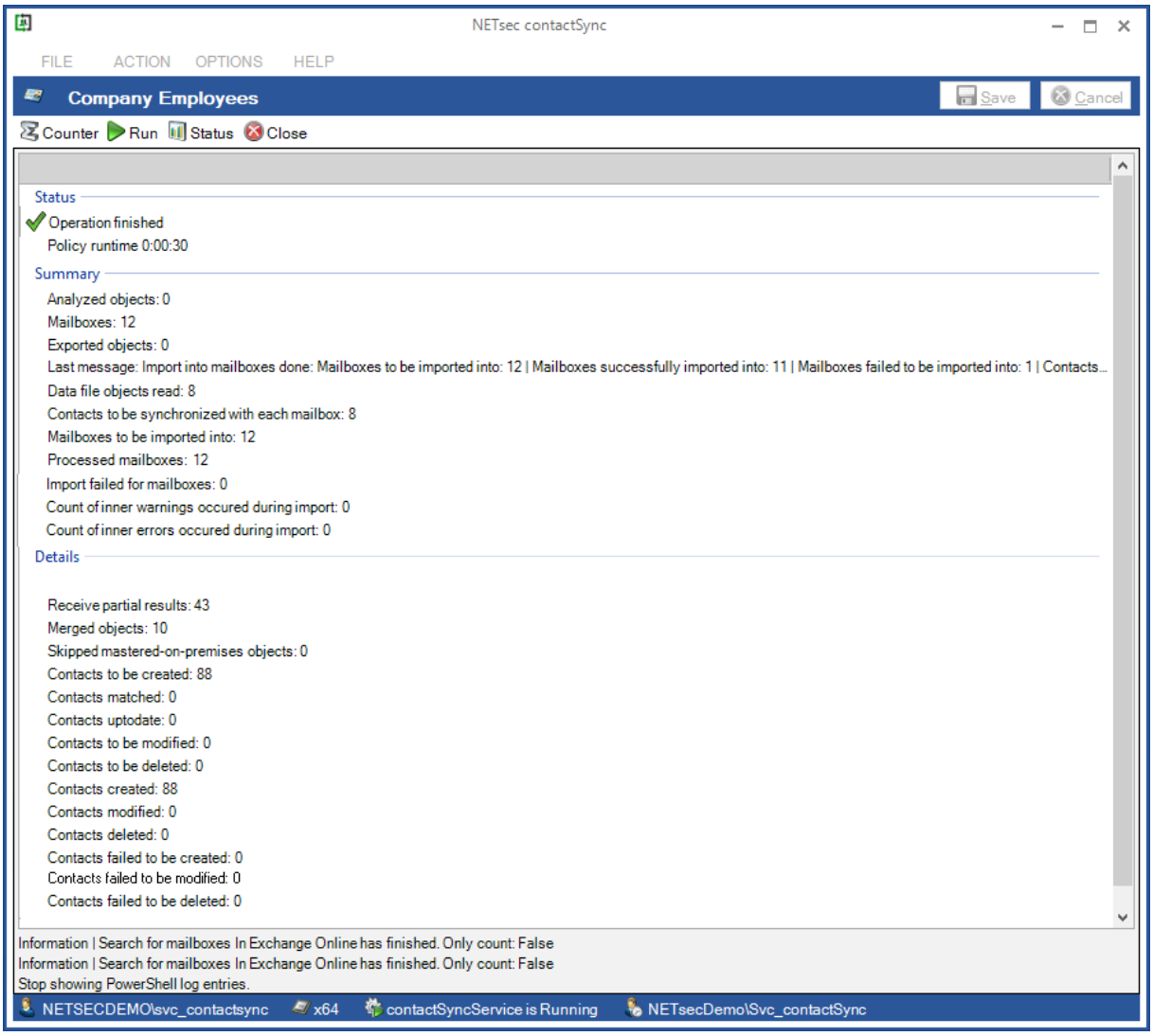
The new policy is accessible by selecting it from either link shown below. Select the policy node.



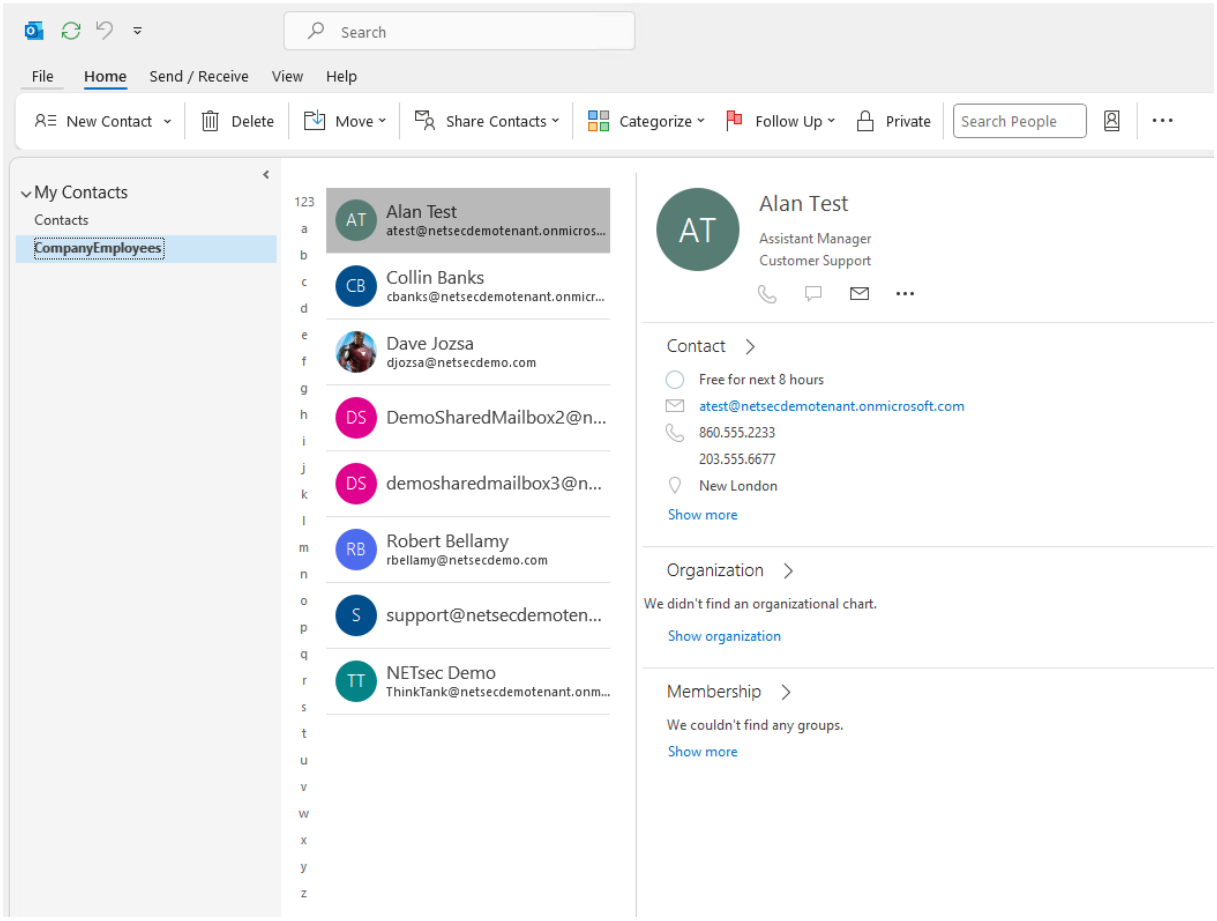
Click **Run**.



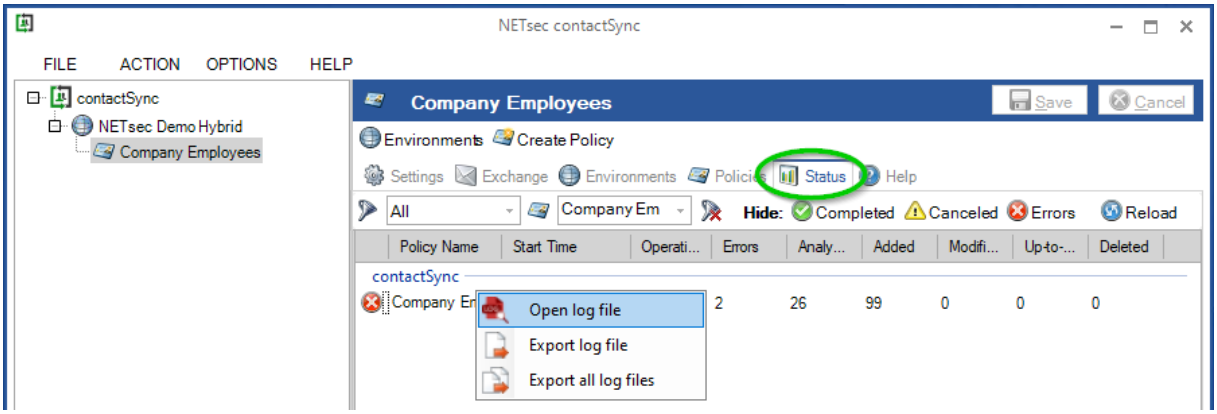
The status and a detailed summary are displayed upon completion. contactSync synchronized 7 contacts into 2 separate mailboxes.



Results of synchronization shown below.



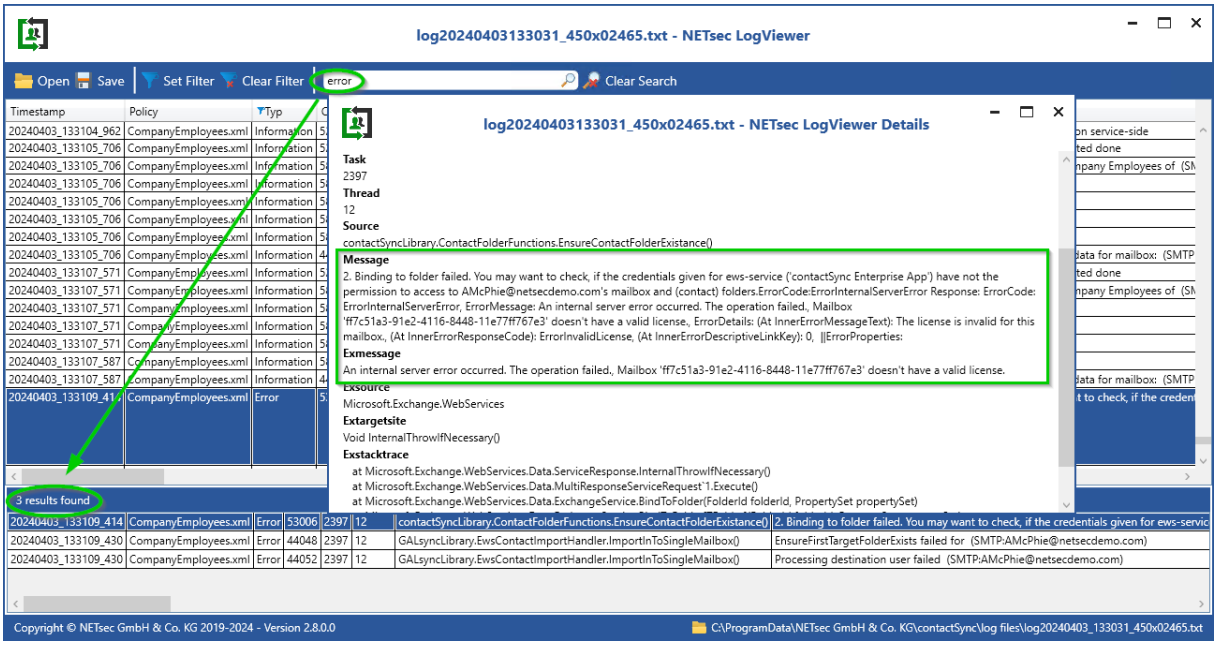
The corresponding log file can be opened by selecting the **Status** tab, and right-clicking the associated log and selecting **Open log file** from the context menu. This allows you to easily find the error and identify its cause.



Searching for the string “error” yields 3 log entries containing this string.

Double-click the line which contains the error. This will highlight the line in the log which contains the details of this log entry.

Double-click the highlighted line in the log viewer to open a new window containing the details of the error.

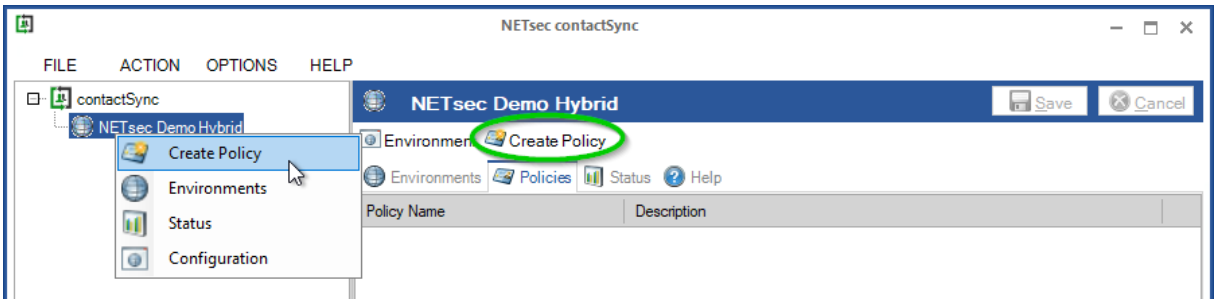


Synchronize Contacts from Public Folder

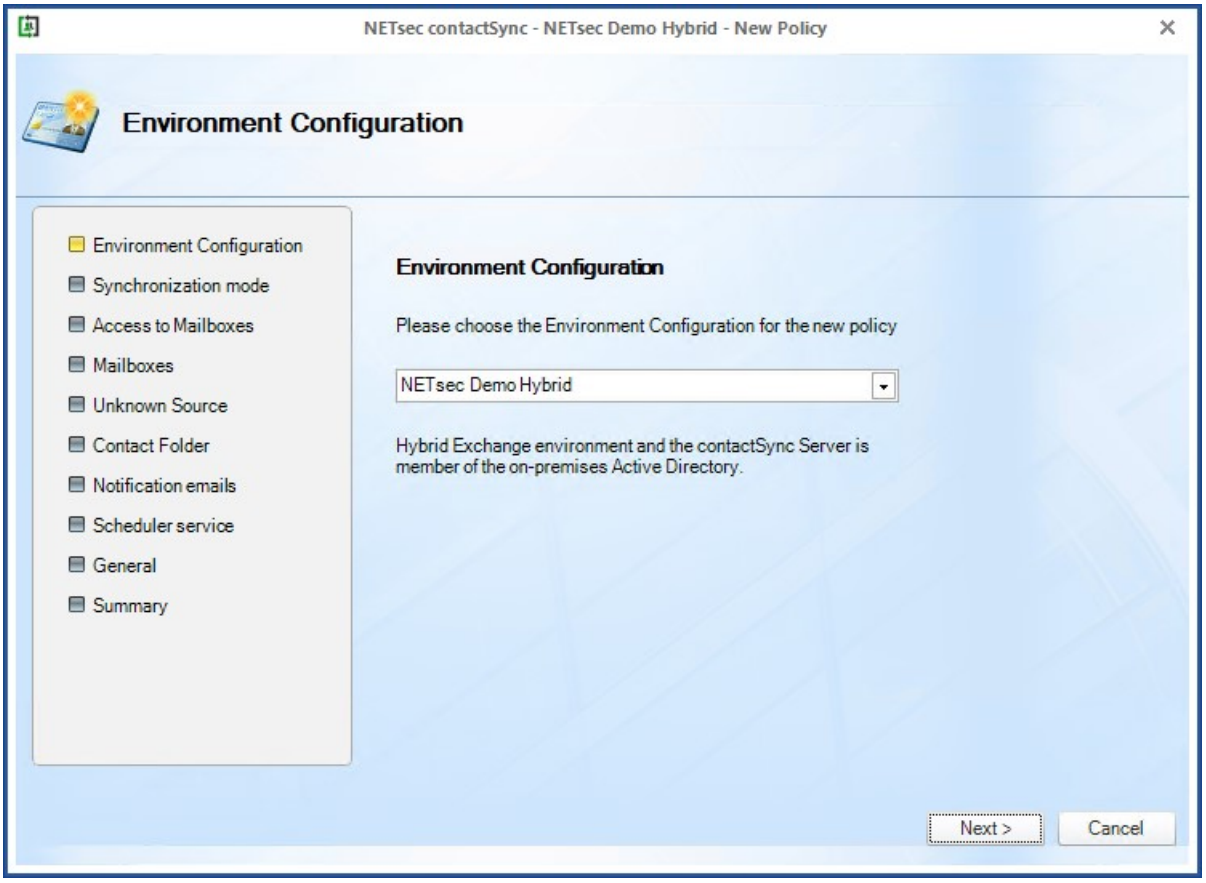
contactSync allows you to synchronize contacts directly from a public folder to user mailboxes. It will connect to public folders in your local Exchange Environment, whether it is in Exchange on-premises or Exchange Online. In Hybrid Exchange Environments contactSync can access public folders in both locations.

Create a new policy

Right click the Environment and select **Create Policy** from the context menu.



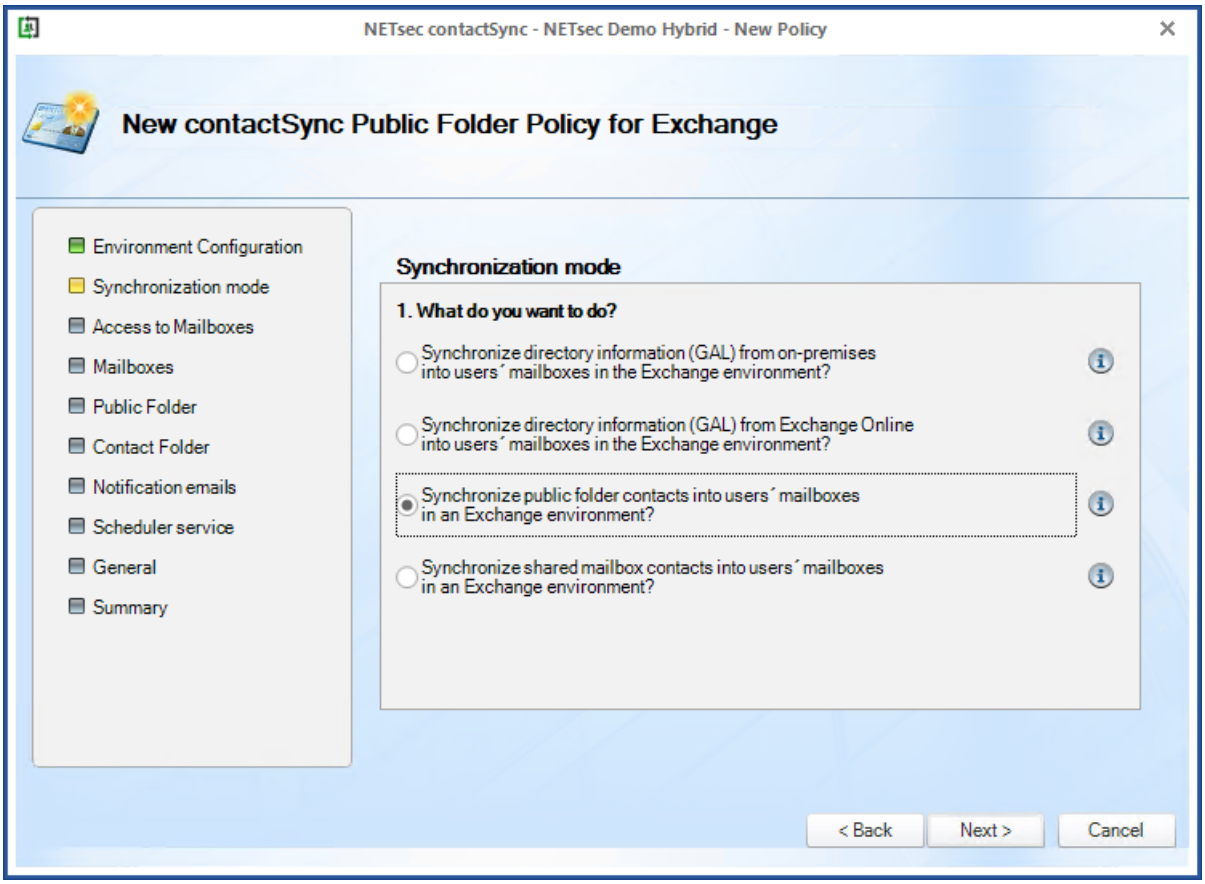
Ensure the desired environment has been selected from the dropdown.



Synchronization mode

Select **Synchronize public folder contacts into users' mailboxes in an Exchange environment**.

Click **Next**.



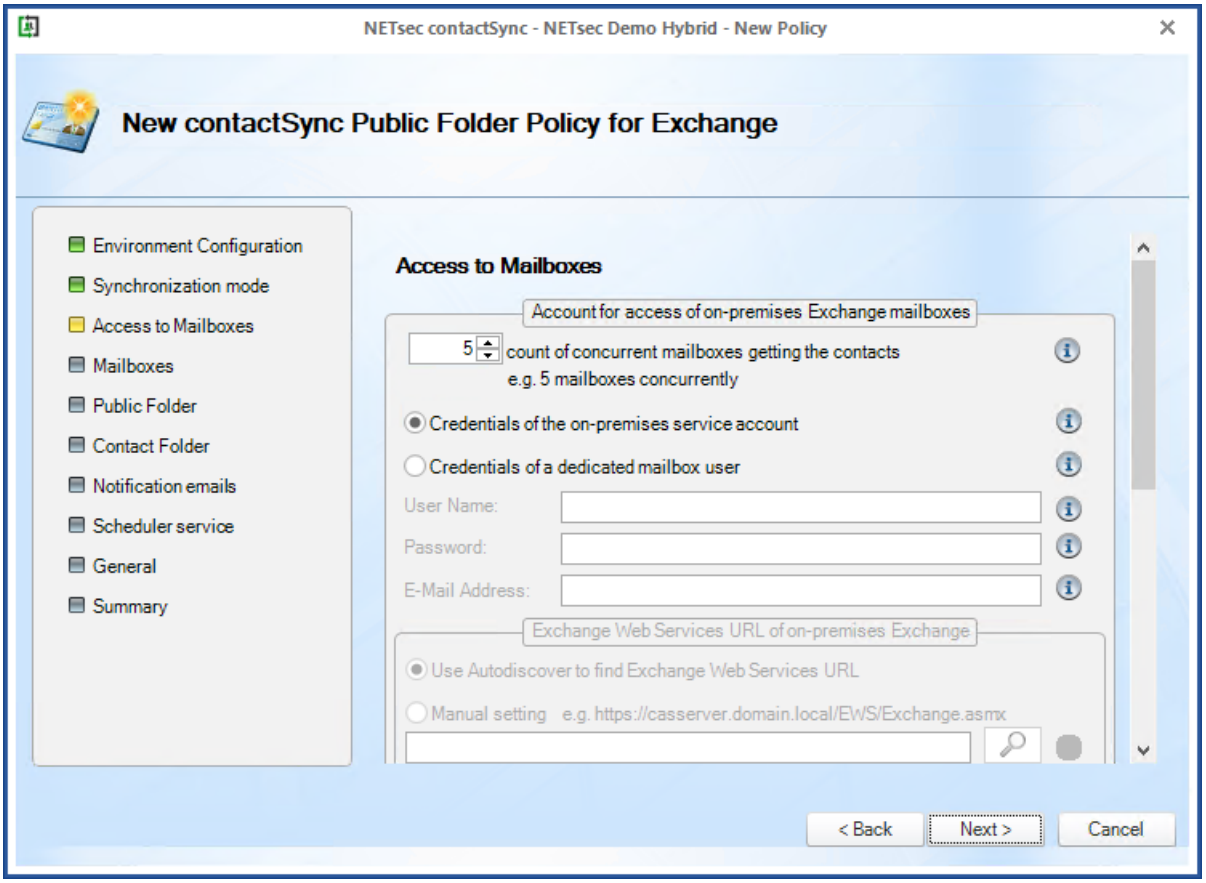
Please note, the Exchange Web Services URL is required to access Public Folders.

For on-premises Public Folder, the Exchange Web Services URL for the on-premises Exchange Server must be set manually in the configuration or the mailbox of the contactSync service account must be located on the on-premises Exchange Server. The policy is cancelled if Autodiscover cannot detect the Exchange Web Services URL for the on-premises Exchange Server.

Access to Mailboxes for on-premises Exchange

contactSync requires access to user mailboxes in order to write to their contacts folder. It will be necessary to use **Exchange Application Impersonation** for access, which allows up to 5 concurrent connections to user mailboxes.

Since the contactSync mailbox requires the **Exchange Administrator** role, you can split these two roles between two separate accounts by entering the credentials of a dedicated mailbox user that has the **Application Impersonation** role.



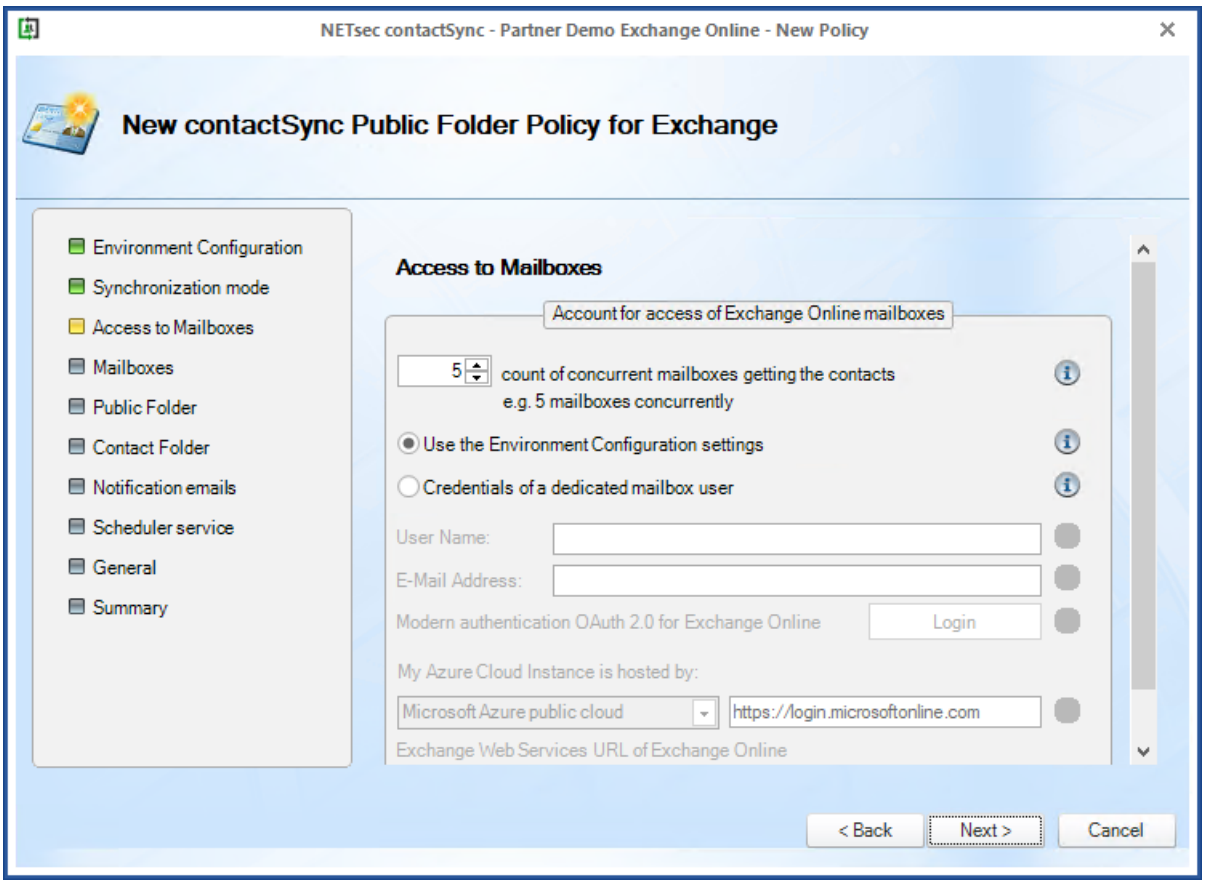
Please take a look at the chapter:

How to configure Exchange Application Impersonation

Access to Mailboxes for Exchange Online

By default, contactSync uses the Environment Configuration to access mailboxes. Application Impersonation, required for on-premises Exchange, will not be necessary when the certificate authentication via App Registration for Exchange Online is configured in the Environment Configuration.

Please take a look at the chapter
Exchange Online certificate-based authentication via App Registration

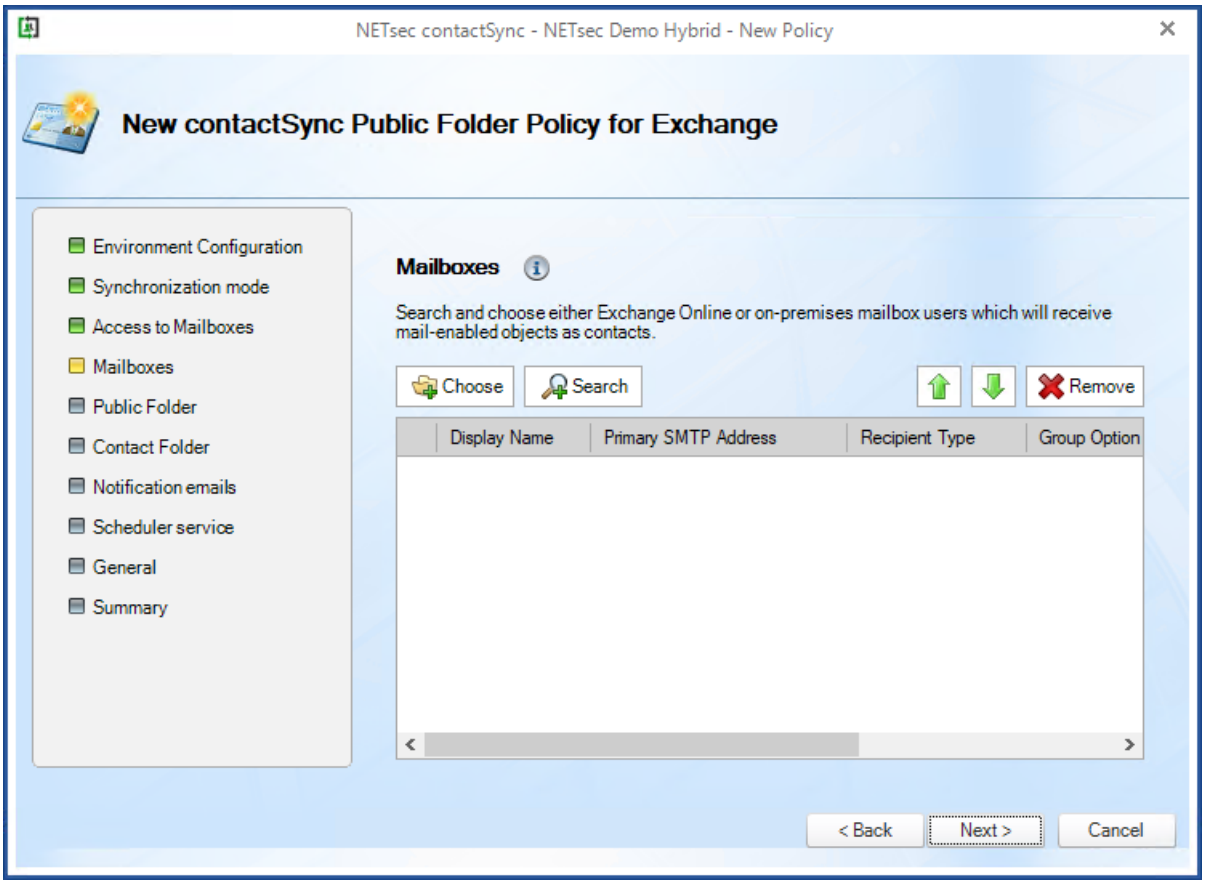


Click **Next**

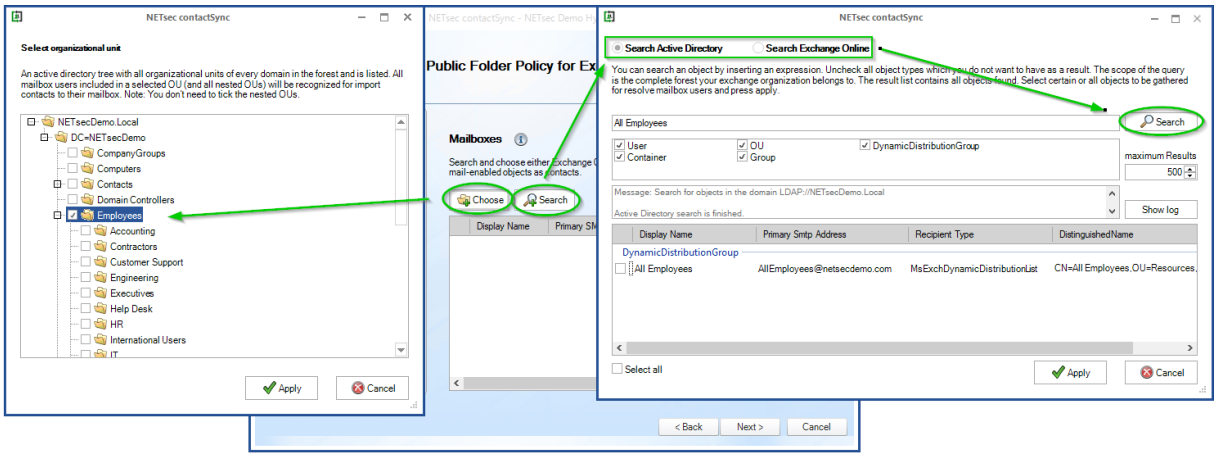
Select the Mailboxes from On-Premises Exchange

You can select Mailboxes located in an on-premises Exchange Server, which will receive contacts. It could be an on-premises Exchange environment or a part of a hybrid Exchange environment.

In the **Mailboxes** window, you are prompted to select the mailboxes which will receive the contacts. There are two ways to do make your selection.



- Click **Choose** to select mailboxes by OU where they reside in Active Directory.
- Click **Search** to open a search dialogue window from which you can search for the desired Active Directory objects. When searching Active Directory, mailboxes can be selected individually, by group membership, by container, or by OU. If you have a hybrid Exchange environment, an additional option is available to search for Exchange Online objects.

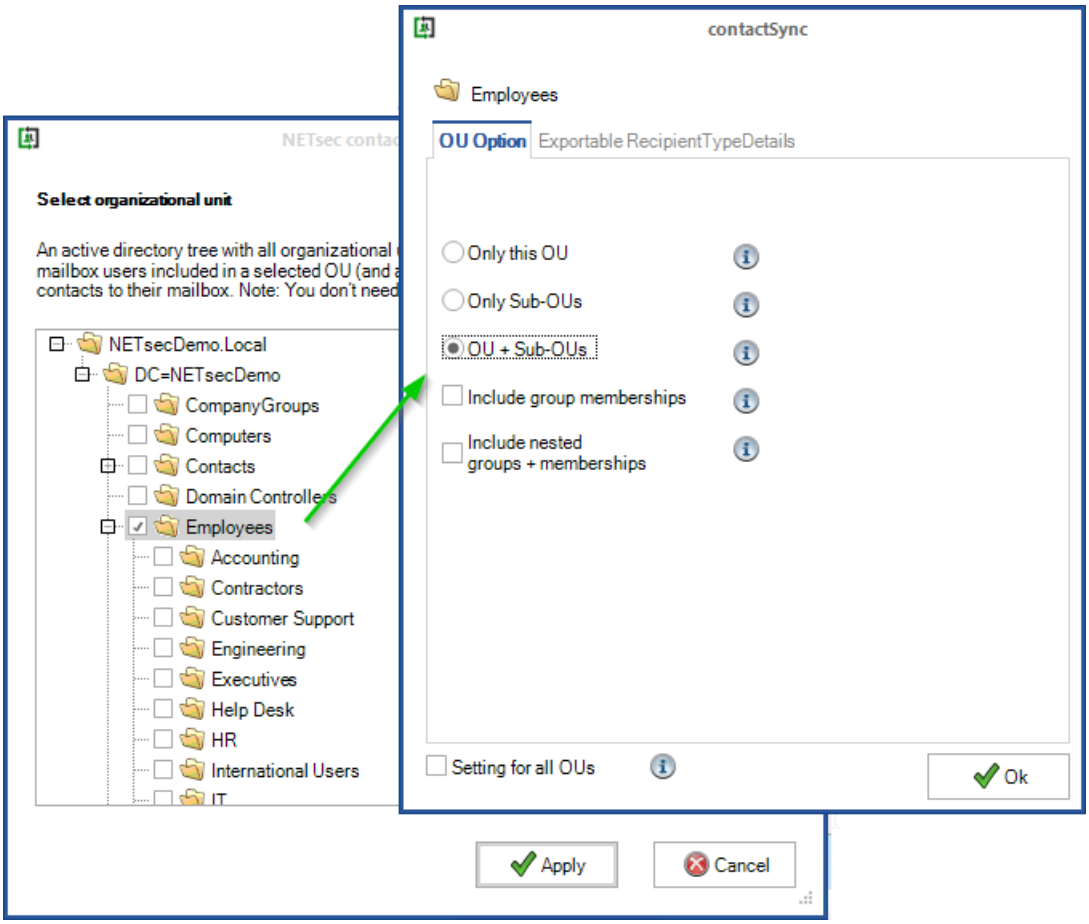


When the **Search Exchange Online** Radio Button has been selected, you can search for objects by Recipient Type, such as **UserMailbox**, **MailUniversalDistributionGroup**, **MailUniversalSecurityGroup**, **DynamicDistributionGroup**, or **Office365 Group**.

When OUs are selected, a prompt to select the OU depth is presented. If any groups are contained in the OU, contactSync will prompt the user to include mailboxes by group membership.

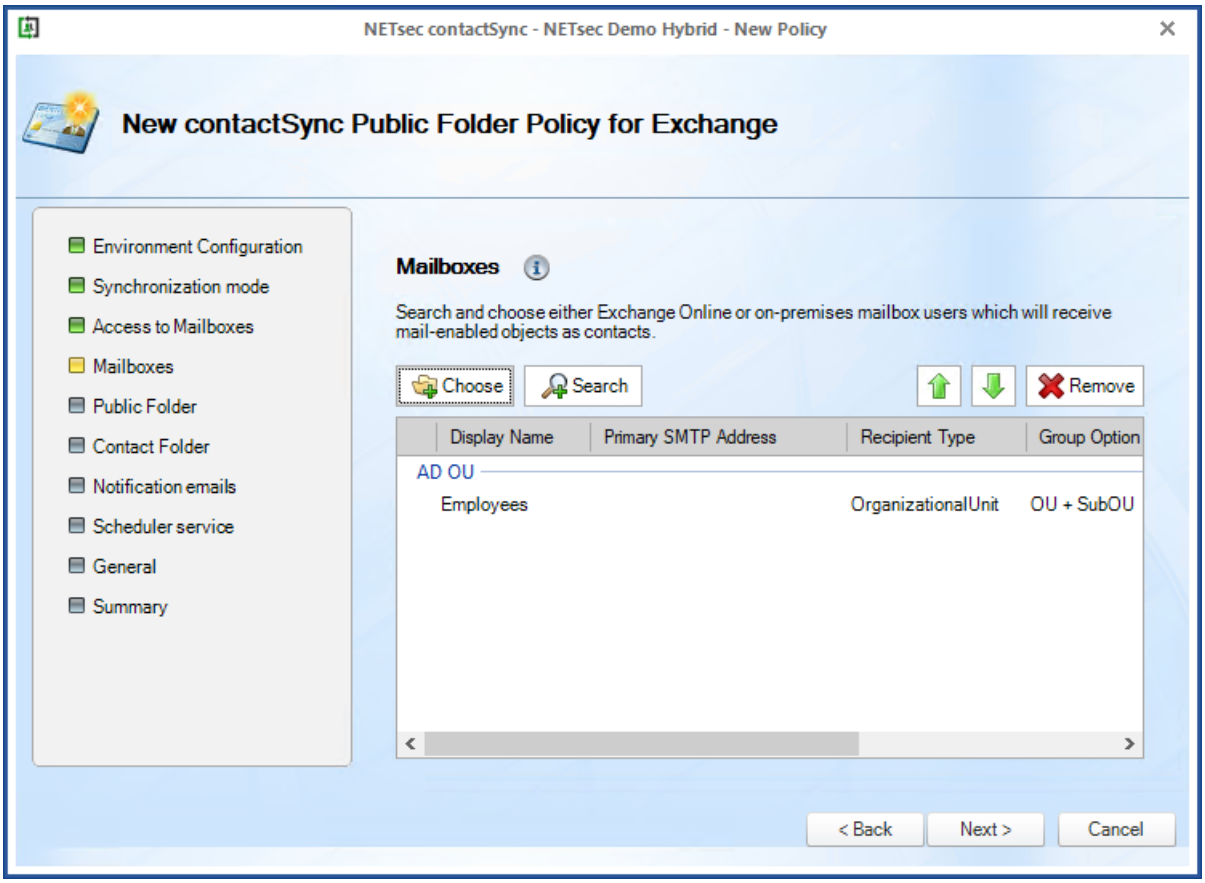
If multiple OUs have been selected, the checkbox at the bottom left will apply the settings to all selected OUs.

Click **OK**, then **Apply**.



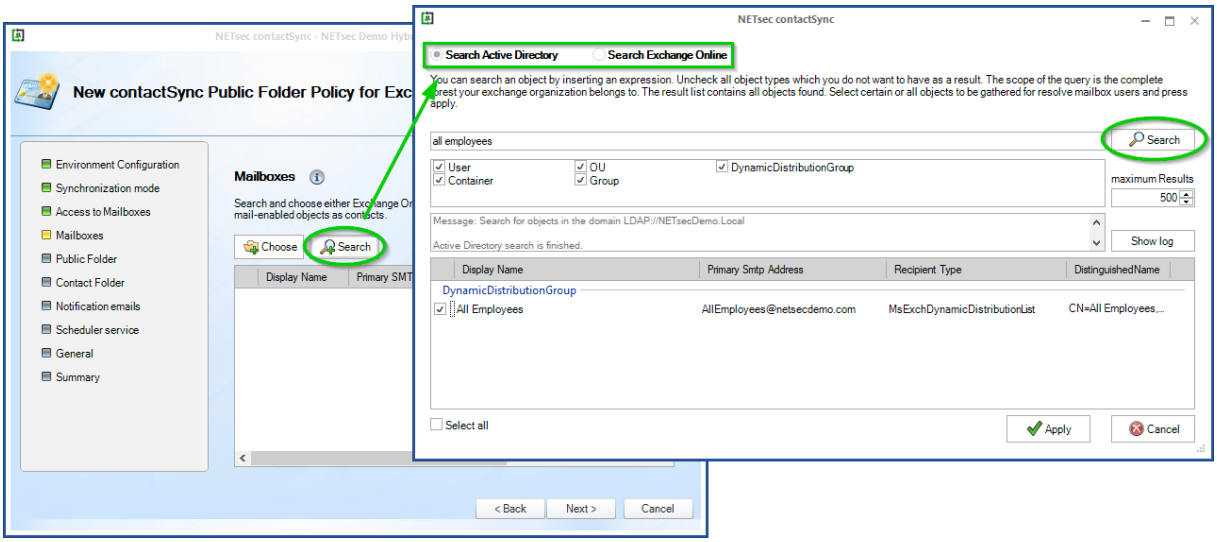
Verify the selected OUs are displayed.

Click **Apply**

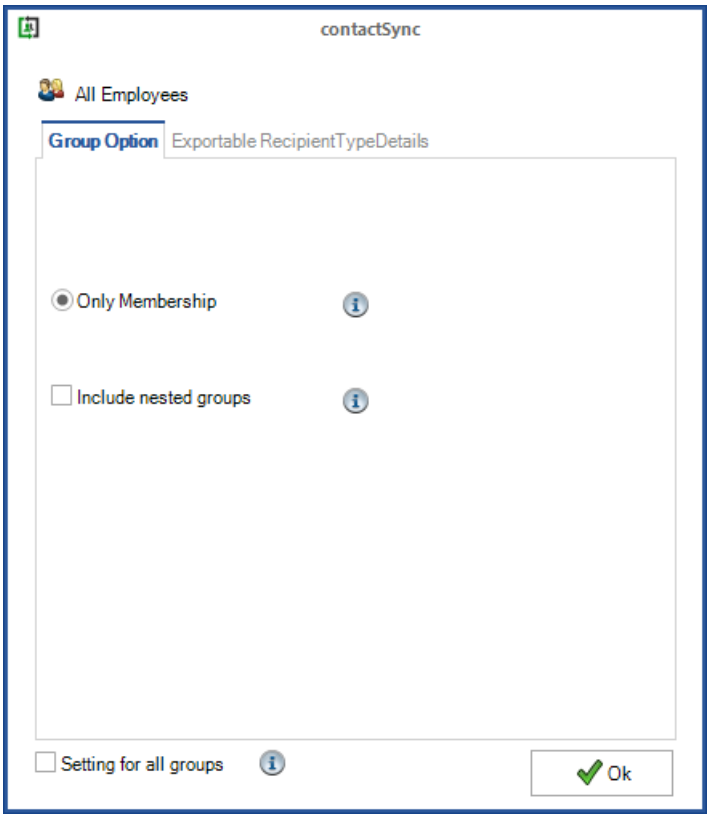


Click **Next**.

Instead of selecting OUs in Active Directory as described above, in the following example, the **All Employees** Dynamic Distribution Group has been selected from the Active Directory search.

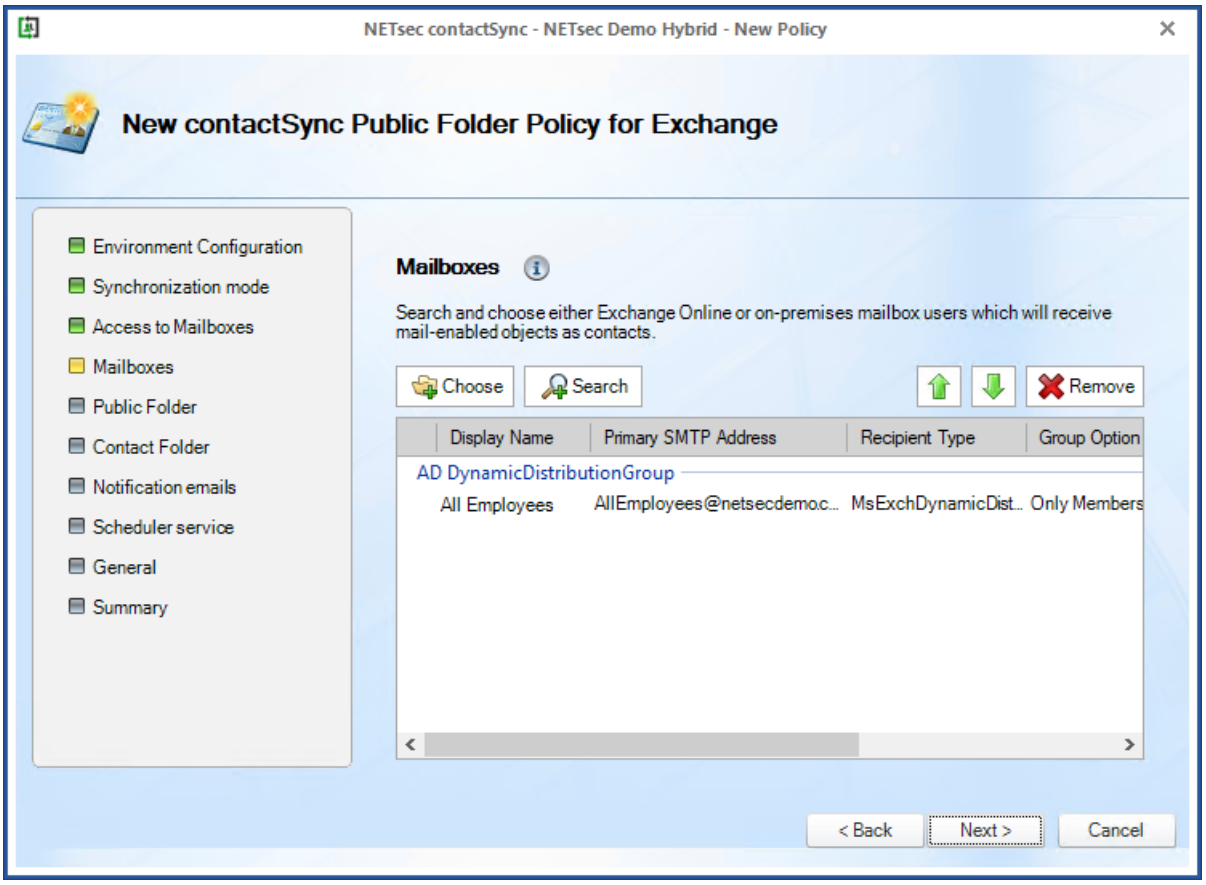


All members with a mailbox in the selected group will receive the contacts, an option is also available to include nested groups.



Click **OK**.

The selected group(s) are displayed under the appropriate heading.

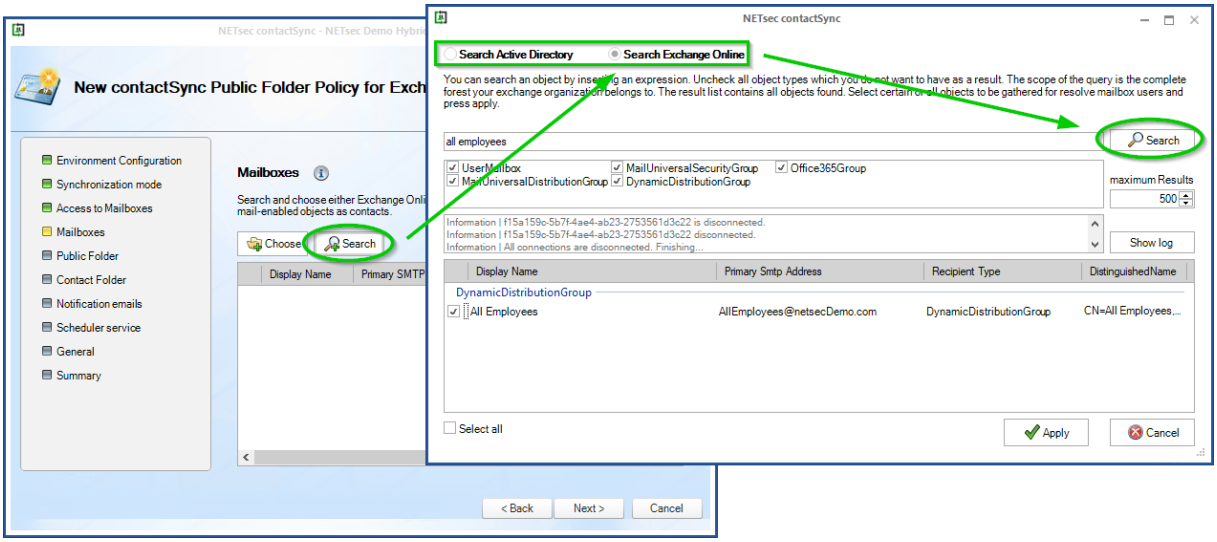


Click **Next**

Select the Mailboxes from Exchange Online

You can select Mailboxes located in Exchange Online which will receive the contacts. This is possible for an Exchange Online environment or a part of any hybrid Exchange environment, as shown in the screenshot below.

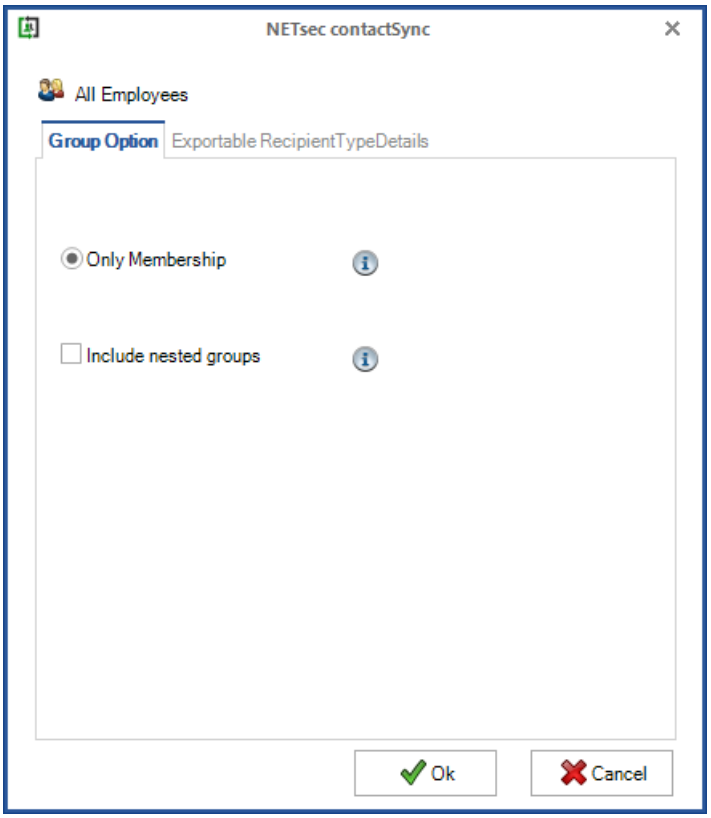
When searching for Exchange Online objects, you can search for objects by Recipient Type, such as **UserMailbox**, **MailUniversalDistributionGroup**, **MailUniversalSecurityGroup**, **DynamicDistributionGroup**, or **Office365 Group**.



In the example above, the **All Employees** Dynamic Distribution Group has been selected. You can expand your search by inserting a wild card character (*).

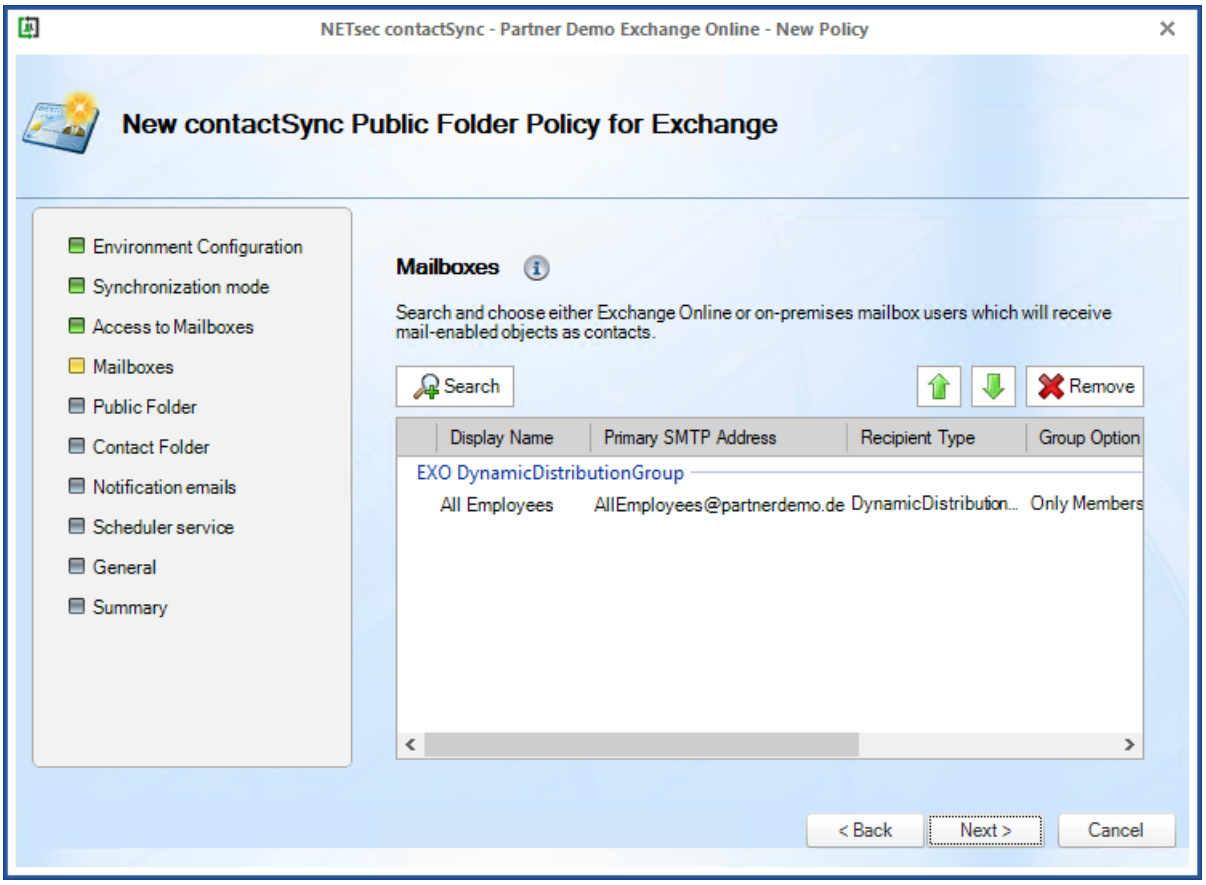
Click **Apply**.

All members with a mailbox in the selected group will receive the contacts, an option is also available to include nested groups.



Click **OK**

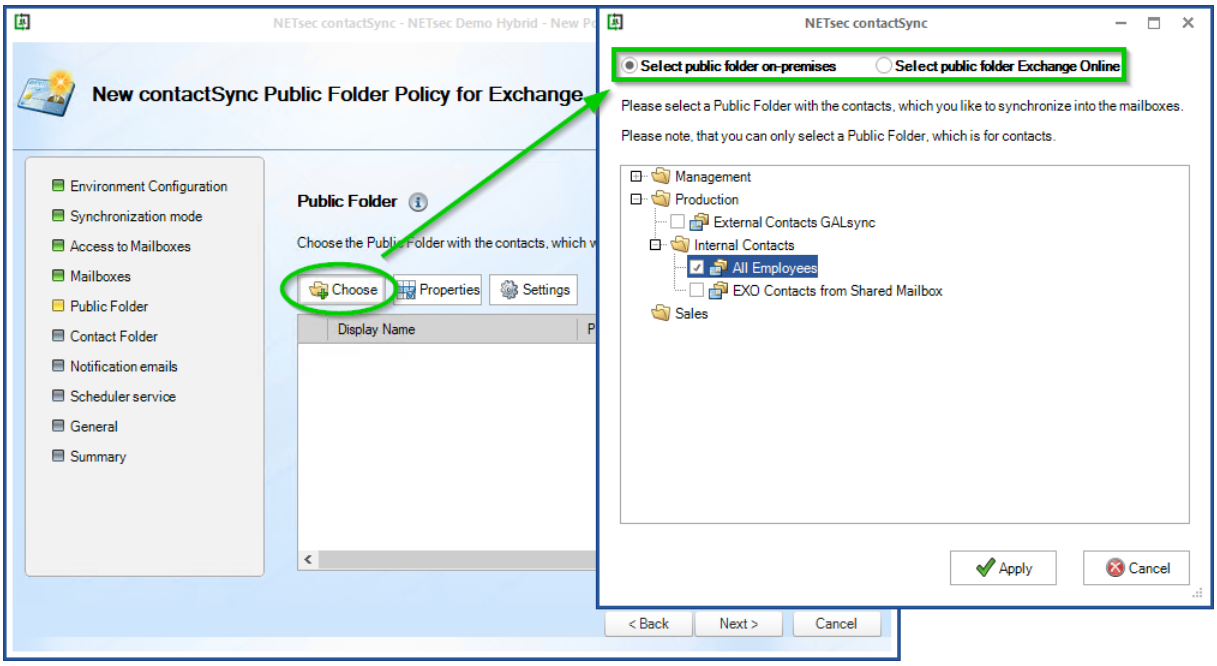
Verify the selected group(s) are displayed. Click **Next.**



Select Public Folder

Depending on the Exchange environment a Public Folder with contacts can be selected.

Click **Choose**, then select the appropriate radio button **Select public folder on-premises**, or **Select public folder Exchange Online** to open and expand the public folder tree, then select the public folder from which to synchronize contacts. Then click **Apply**.



Please note, the Exchange Web Services URL is required to access Public Folders.

For on-premises Public Folder, the Exchange Web Services URL for the on-premises Exchange Server must be set manually in the configuration or the mailbox of the contactSync service account must be located on the on-premises Exchange Server. The policy is cancelled if Autodiscover cannot detect the Exchange Web Services URL for the on-premises Exchange Server.

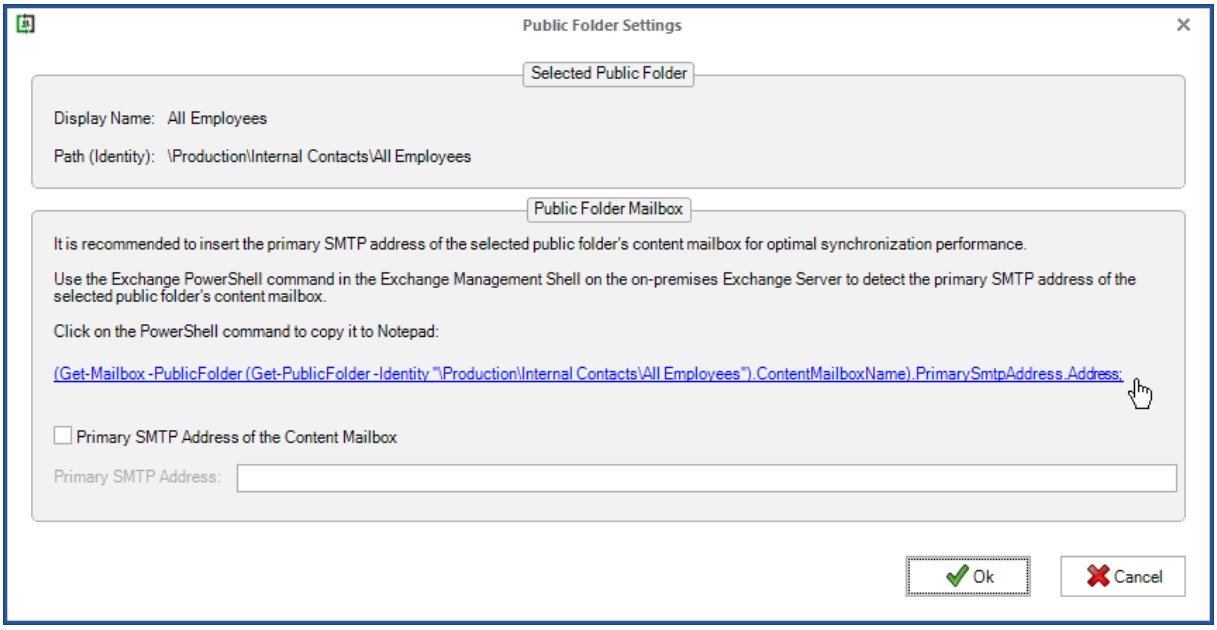
After clicking **Apply** the **Public Folder Settings** dialog will open to help to determine the primary SMTP address of the public folder. The determination procedure differs between a public folder that is located on-premises and a public folder that is located in Exchange Online.

Determine the primary SMTP address of the public folder located on-premises

Determine the primary SMTP address of the public folder located Exchange Online

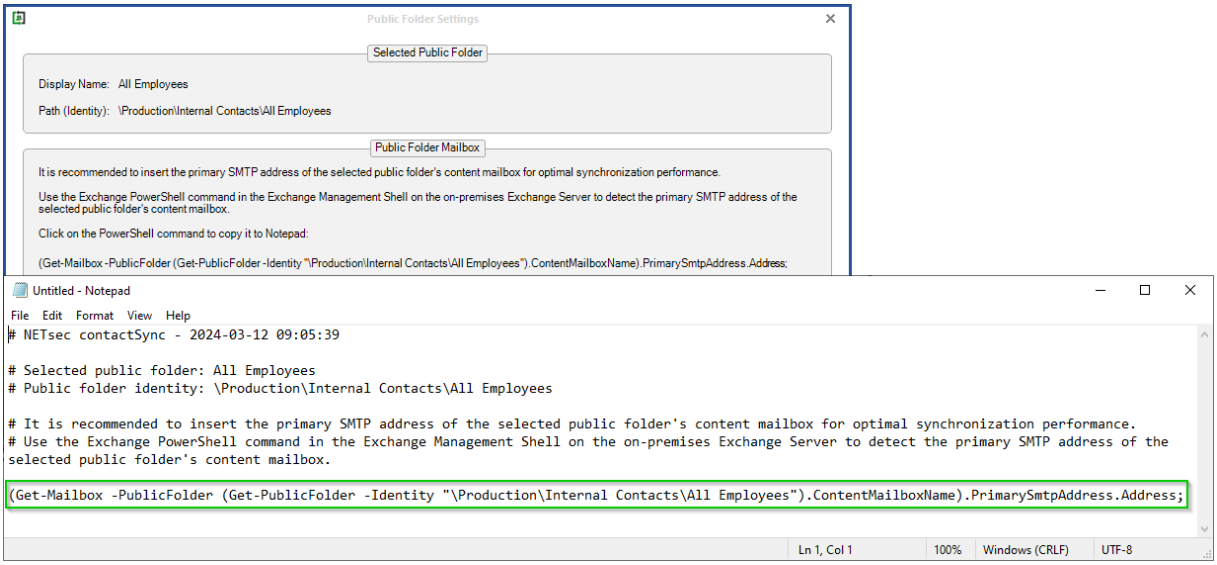
Determine the primary SMTP address of the public folder located on-premises

The **Public Folder Settings** dialog opens.



contactSync needs the primary SMTP address of the selected public folder´s content mailbox for optimal synchronization performance.

Click on the generated PowerShell command to copy it to Notepad.

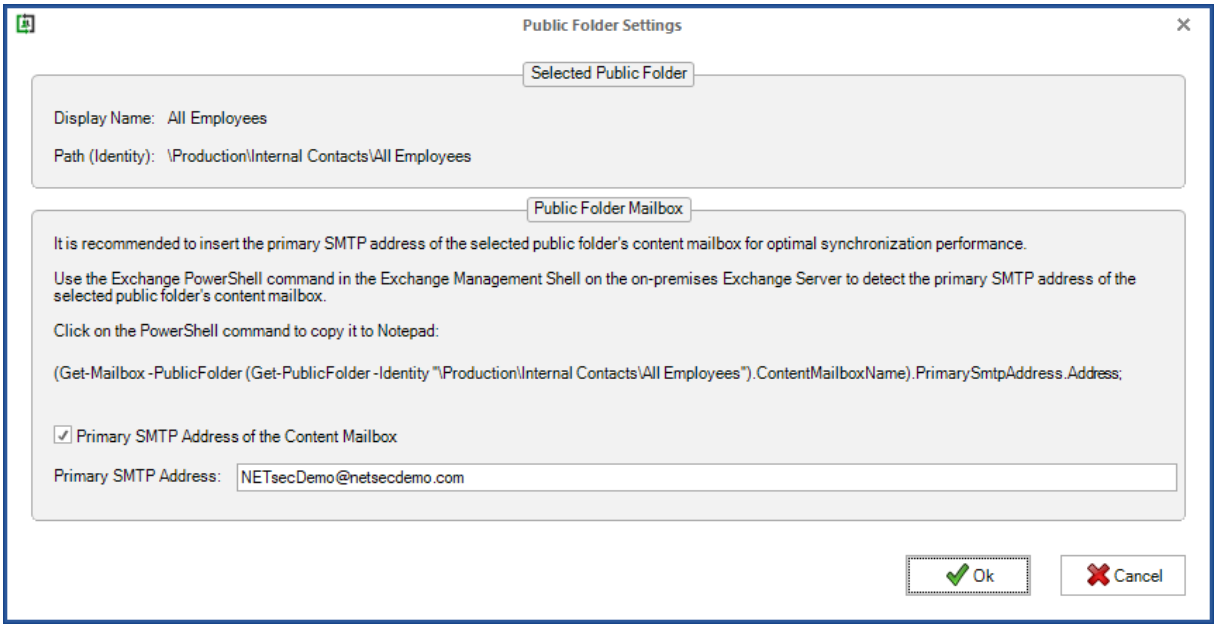


Run the PowerShell command in the **Exchange Management Shell** on the on-premises Exchange Server to retrieve the primary SMTP address of the selected public folder´s content mailbox.

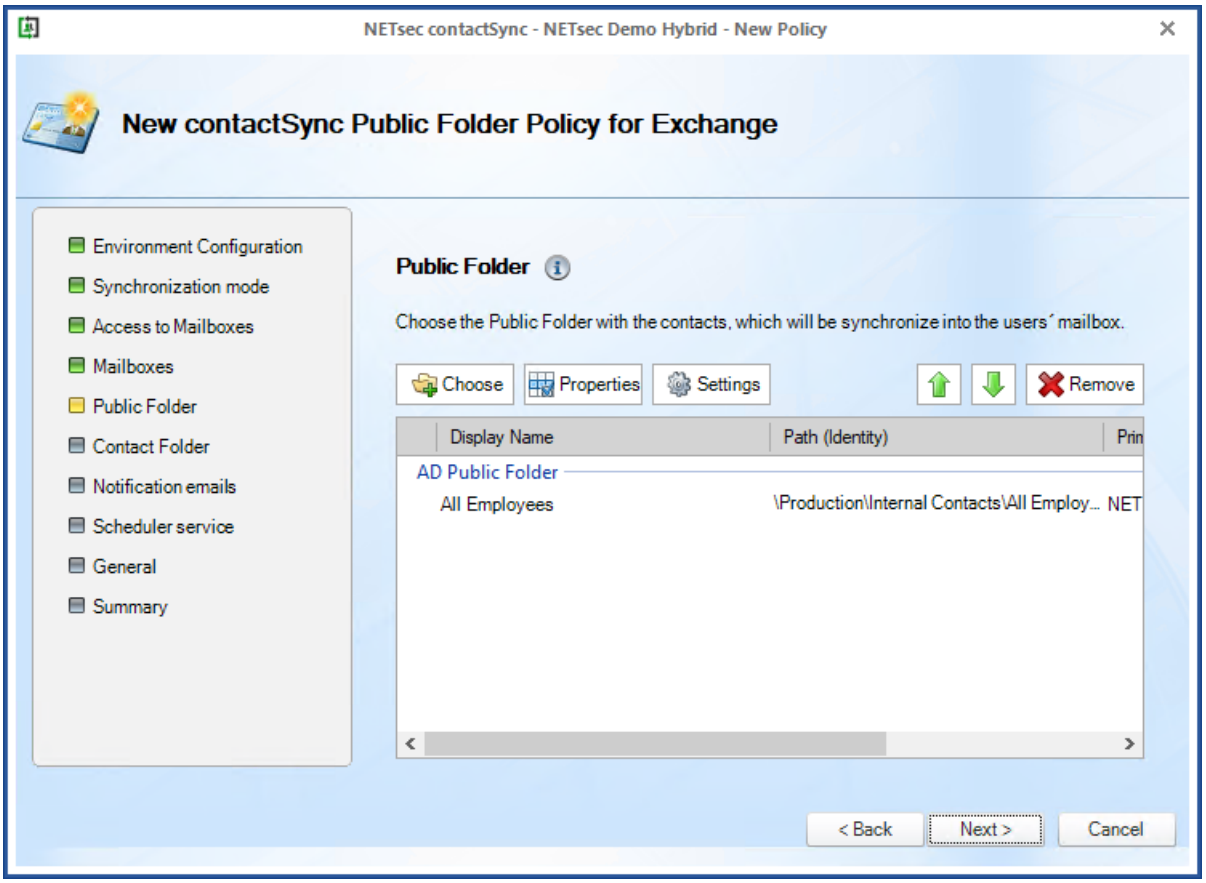
The result should be the primary SMTP address of the Public Folder mailbox.

Copy the primary SMTP address to insert it in the **Public Folder Settings** dialog.

Enable the option **Primary SMTP Address of the Content Mailbox** and insert the detected primary SMTP address of the selected public folder´s content mailbox.



Click **Ok**.

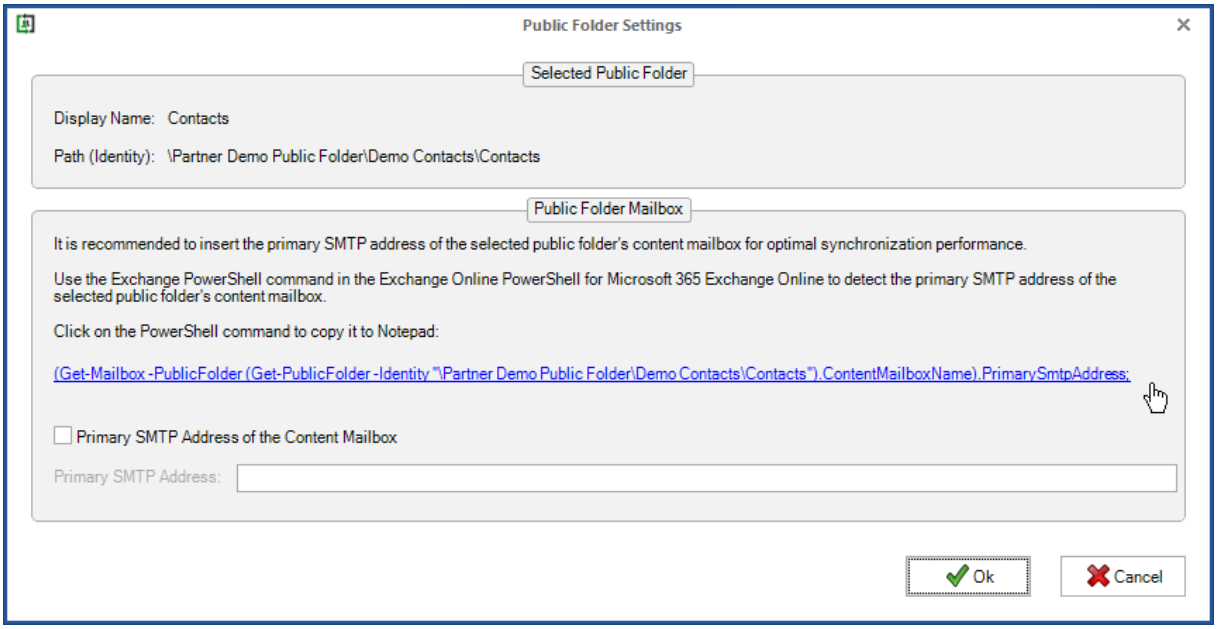


Verify the selected public folder is displayed.

Click **Next**.

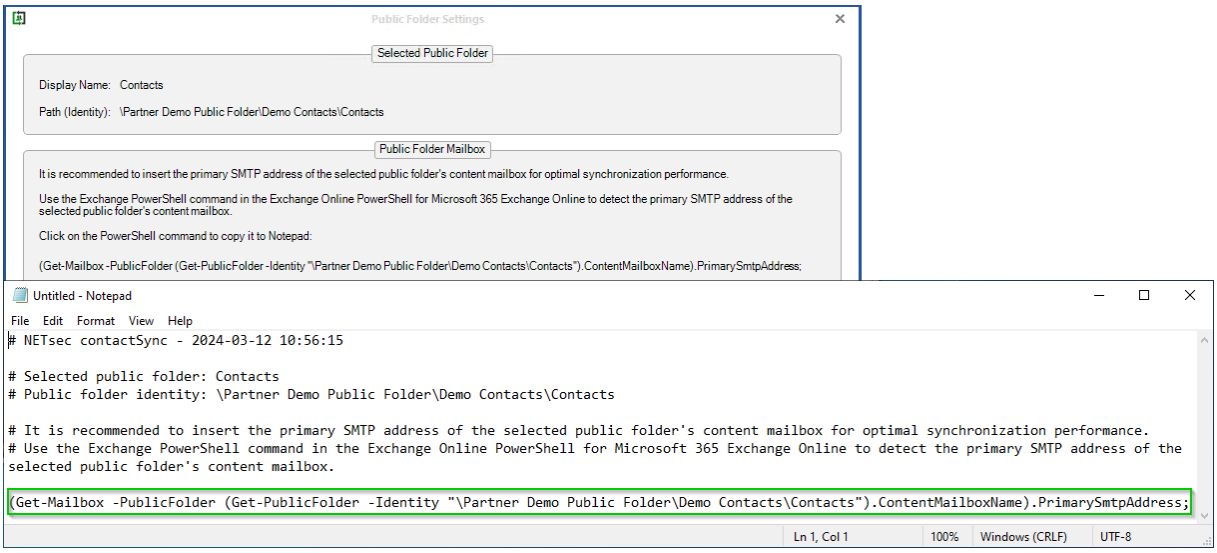
Determine the primary SMTP address of the public folder located Exchange Online

The **Public Folder Settings** dialog opens.



contactSync needs the primary SMTP address of the selected public folder´s content mailbox for optimal synchronization performance.

Click on the generated PowerShell command to copy it to Notepad.

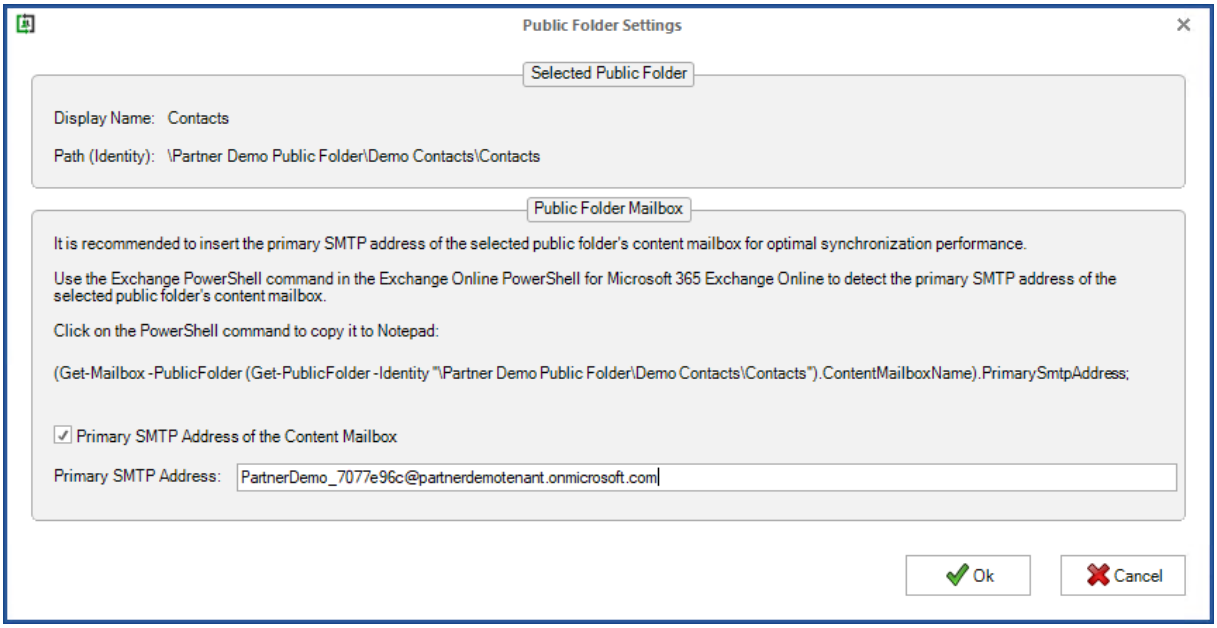


Run the PowerShell command in the **Exchange Online Management Module** for PowerShell to retrieve the primary SMTP address of the selected public folder´s content mailbox.

The result should be the primary SMTP address of the Public Folder mailbox.

Copy the primary SMTP address to insert it in the **Public Folder Settings** dialog.

Enable the option **Primary SMTP Address of the Content Mailbox** and insert the detected primary SMTP address of the selected public folder´s content mailbox.

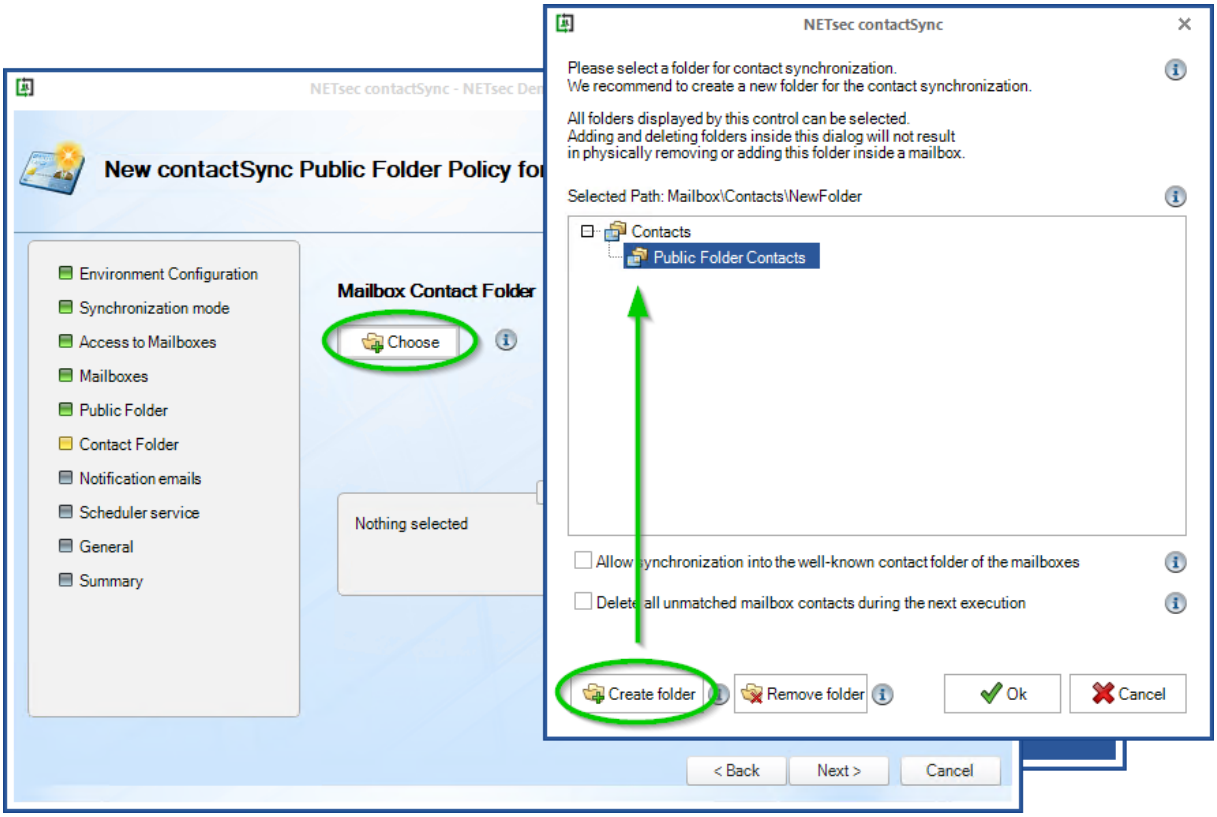


Click **OK**

Select the Mailbox Contact Folder

Click **Choose** to select the contacts folder where the contacts will be synchronized to.

contactSync, can be configured to import contacts directly into the top-level Contacts folder. We recommend a new folder is created, which keeps the contactSync created contacts separate from the user-created contacts.



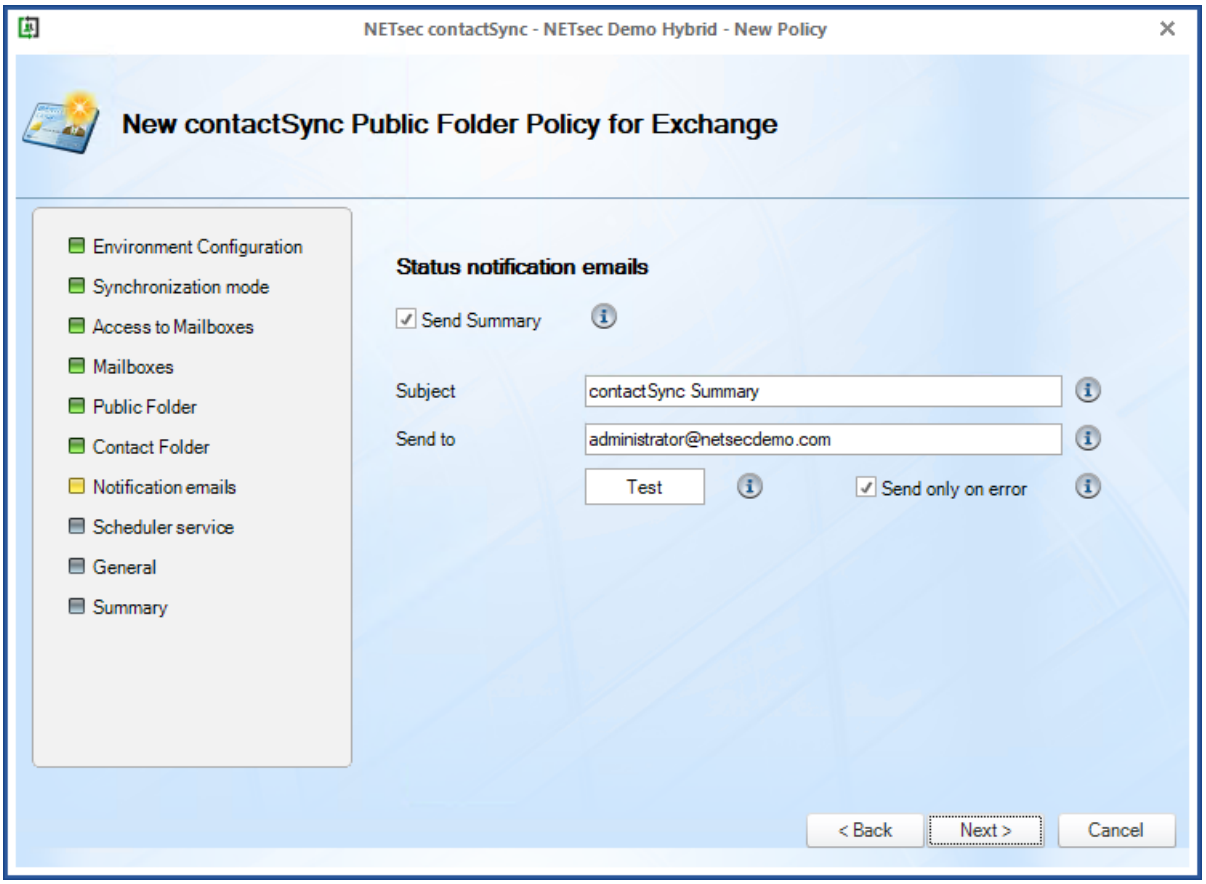
Select the top-level **Contacts** folder, then click **Create folder** to create a subfolder where the contacts will be synchronized, then give the new folder a name.

Click OK, then click **Next**.

Status notification email

An optional status notification email can be sent to the specified recipient(s) each time the policy runs, which provides a brief summary of activity. However, if your preference is to receive one only when an error has been logged, check the **Send only on error** checkbox. Click the **Test** button to send a test email. Then verify it has been received.

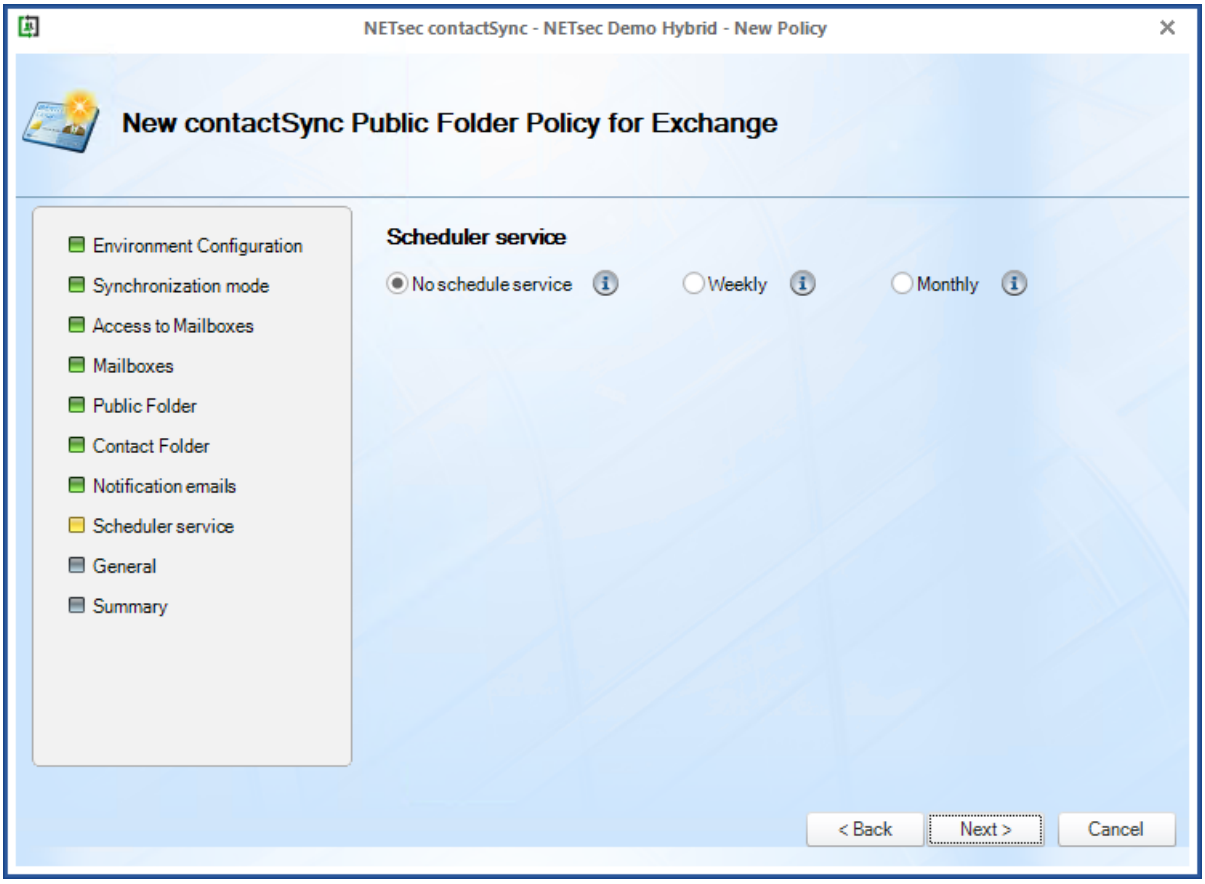
Click **Next**.



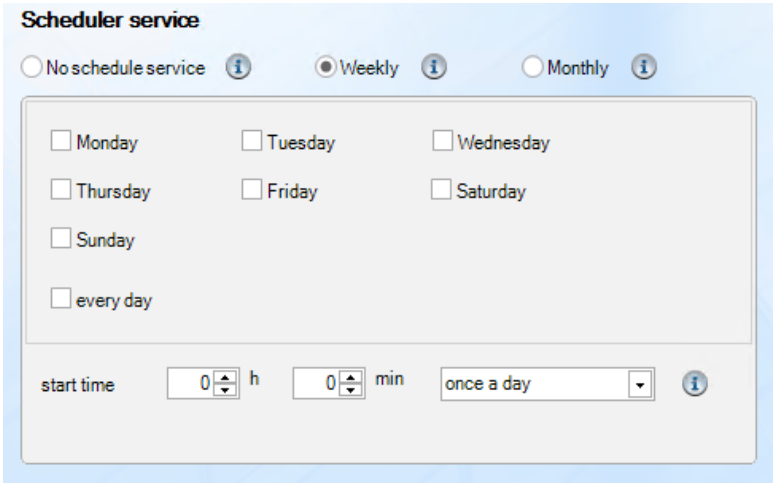
Schedule policy run

contactSync can be scheduled to run at regular intervals. We recommend the policy is manually run before any schedules are set. After the synchronization has completed successfully, you can go back and set it to run on the desired schedule.

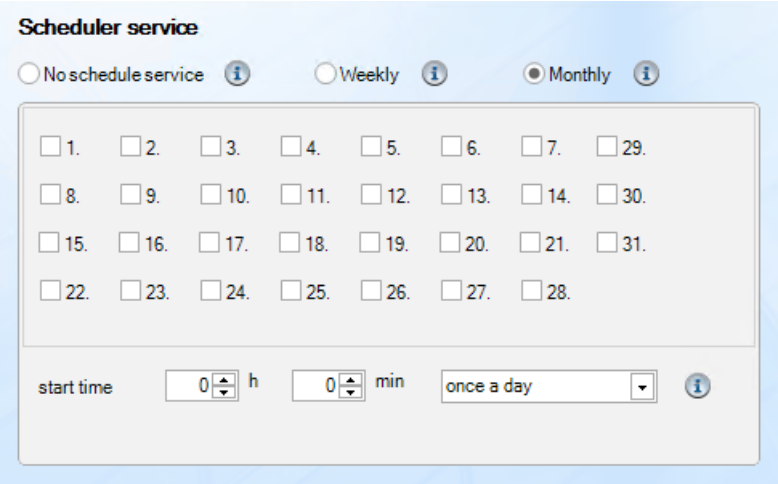
Click **Next**.



The **Weekly** schedule allows you to select which days of the week the policy runs, along with start time and frequency.

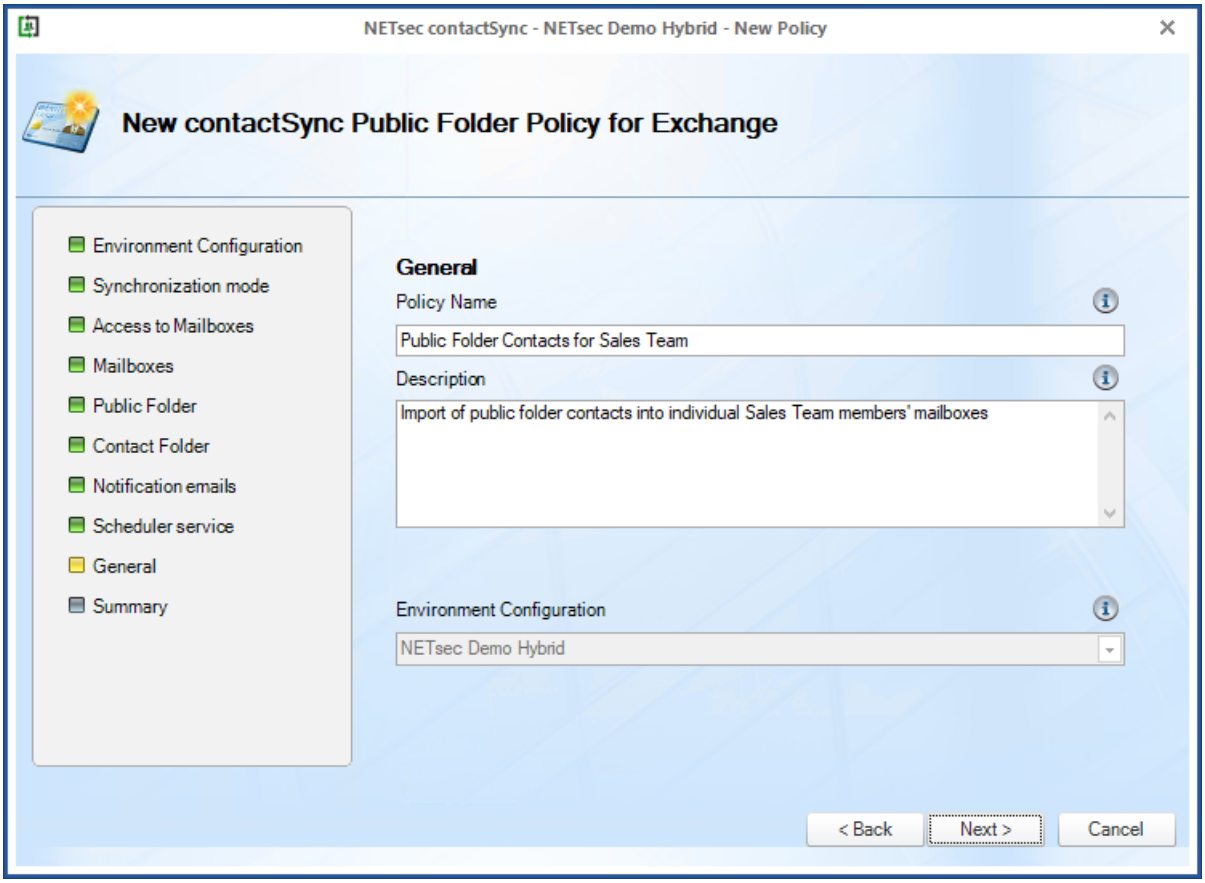


The **Monthly** schedule allows you to select which days of the month the policy runs, along with start time and frequency.



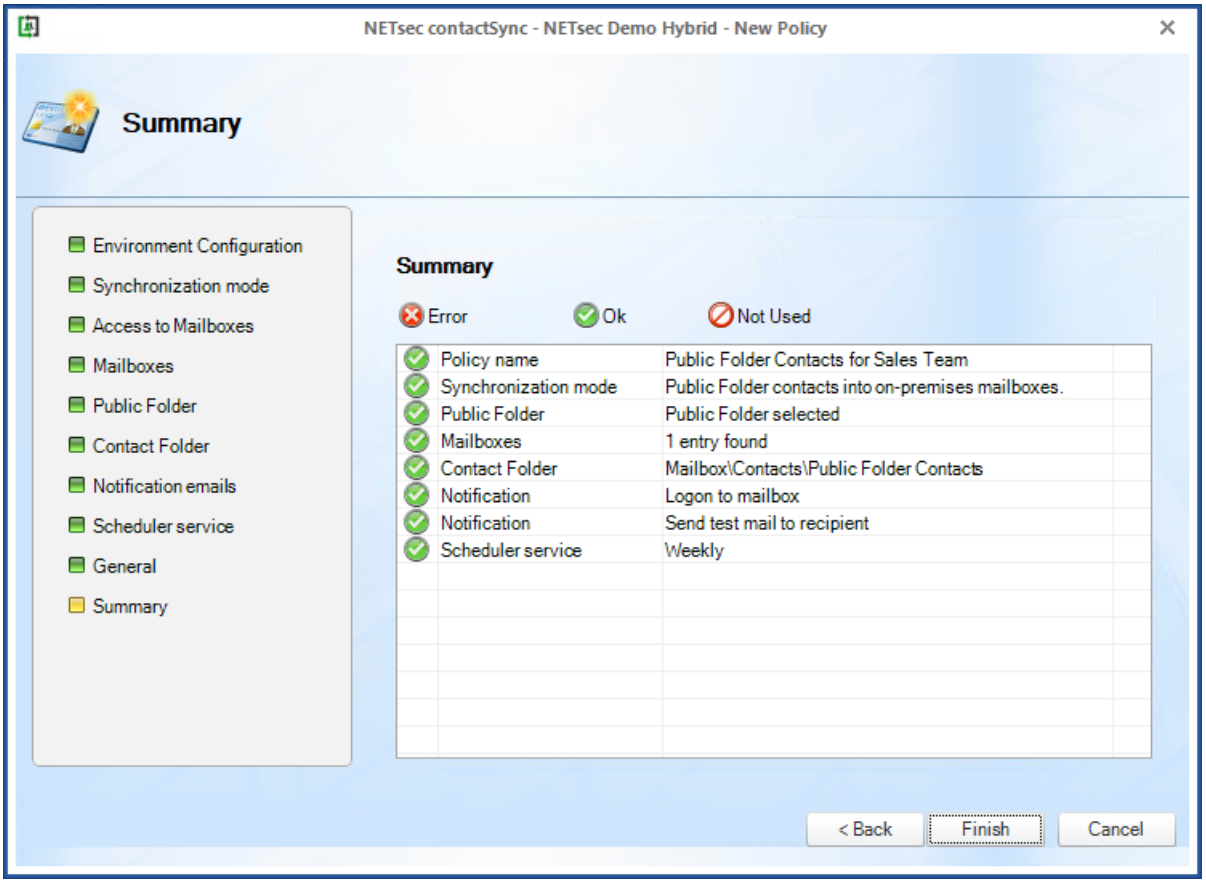
Policy name and description

Enter a policy name and an optional description, then click **Next**.



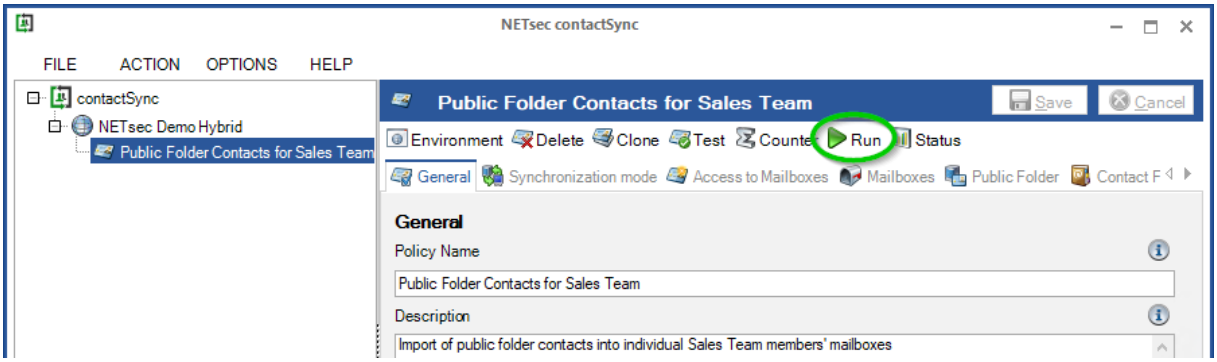
To ensure your settings have been properly configured contactSync will check your policy settings and notify you of any detected errors.

Click **Finish**.

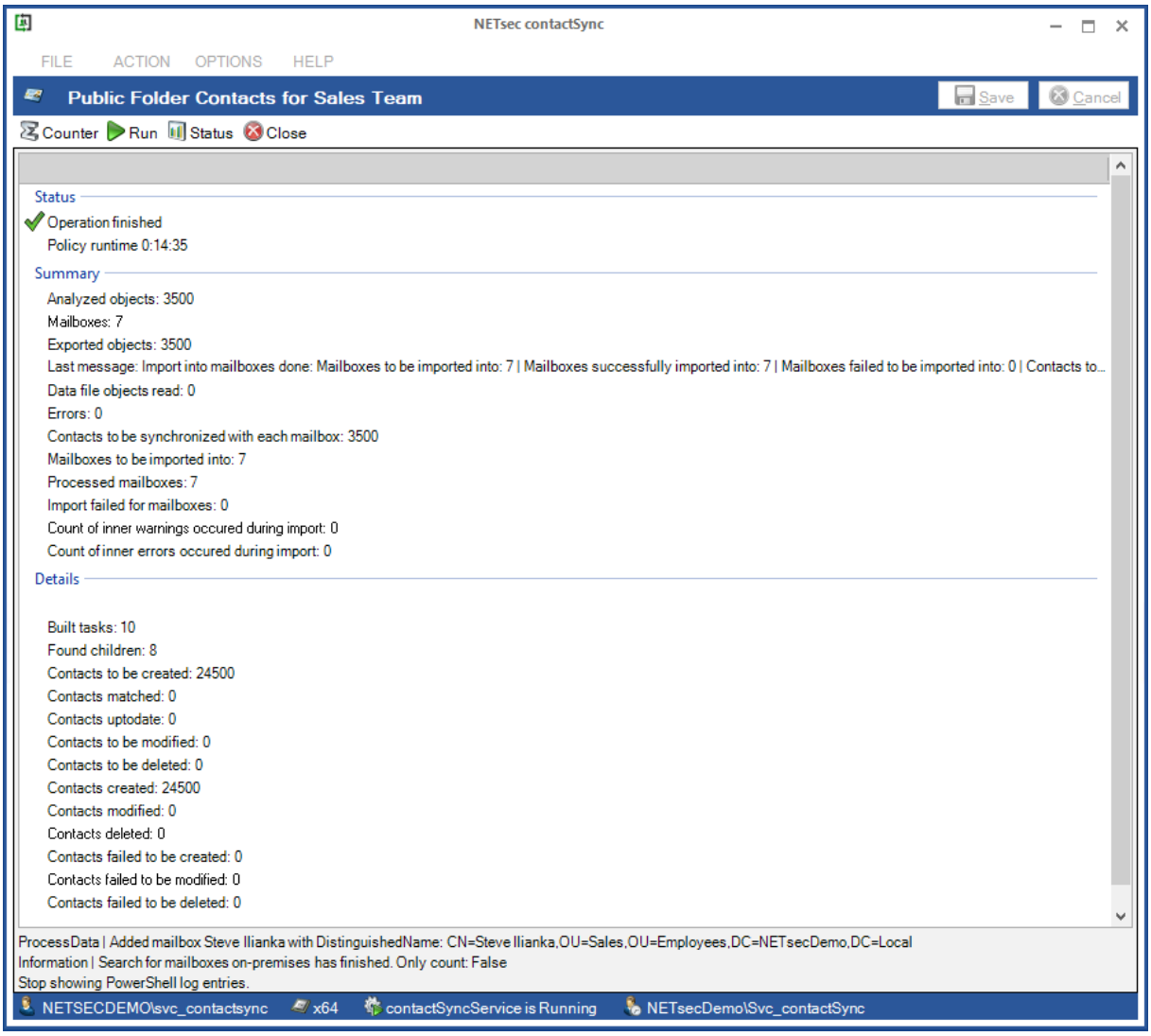


Execute policy and check log files

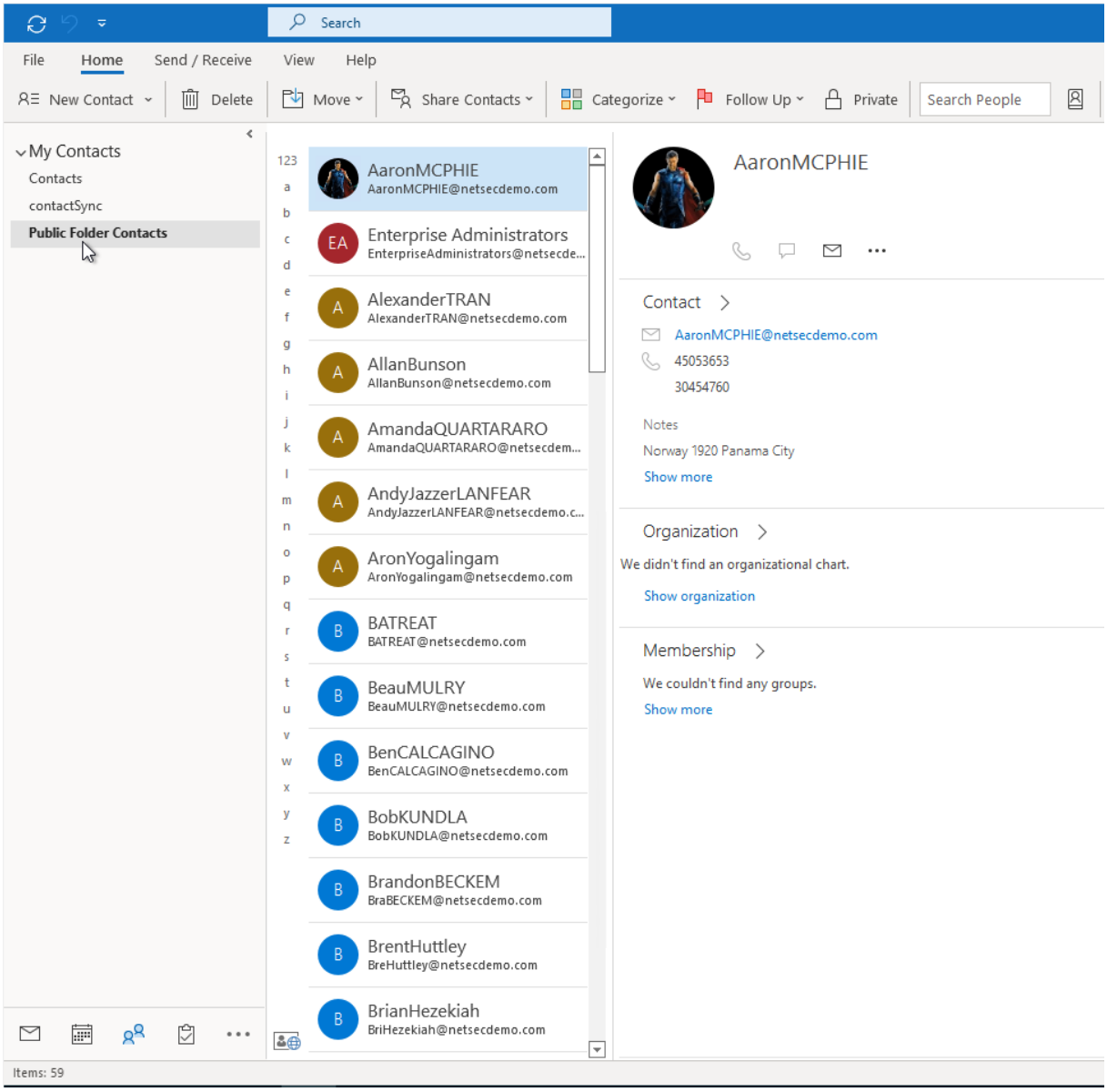
Select the policy node and click **Run**.



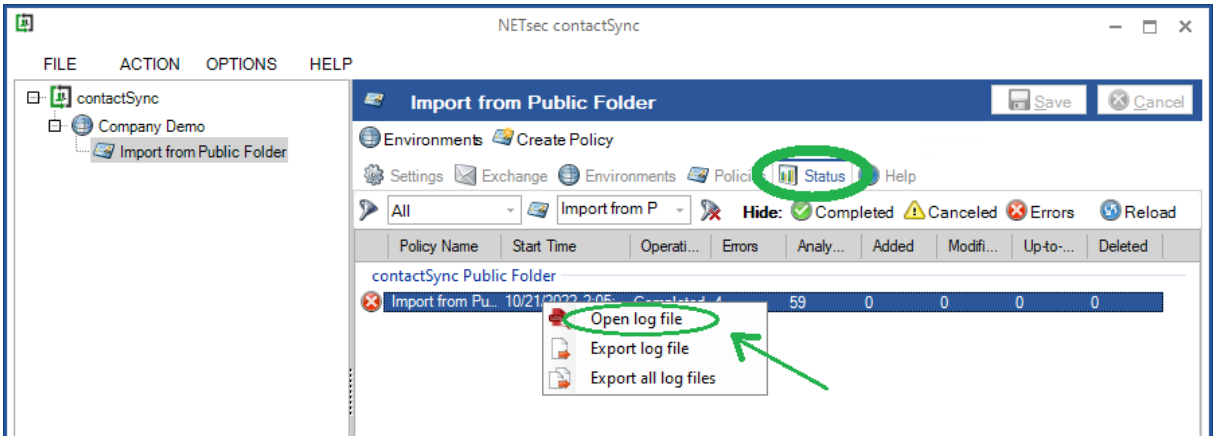
The status and a detailed summary are displayed upon completion.
contactSync synchronized 3500 contacts into 7 separate mailboxes



Results of synchronization shown below:



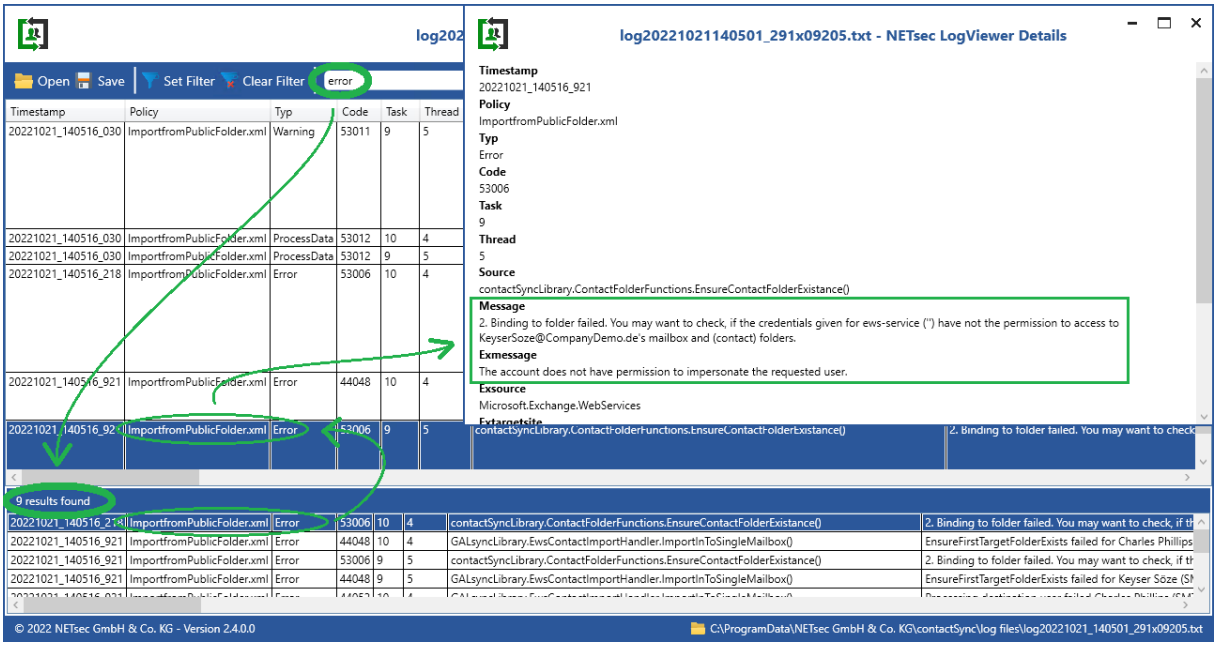
The corresponding log file can be opened by selecting the **Status** tab, and right-clicking the associated log and selecting **Open log file** from the context menu. This allows you to easily find the error and identify its cause.



Searching for the string **error** yields 9 log entries containing this string.

Double-click the line which contains the error. This will highlight the line in the log which contains the details of this log entry.

Double-click the highlighted line in the log viewer to open a new window containing the details of the error.

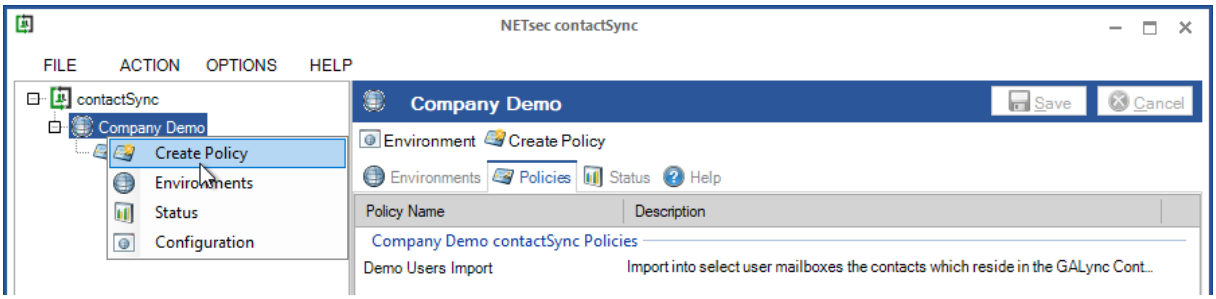


Synchronize Contacts from Shared Mailbox

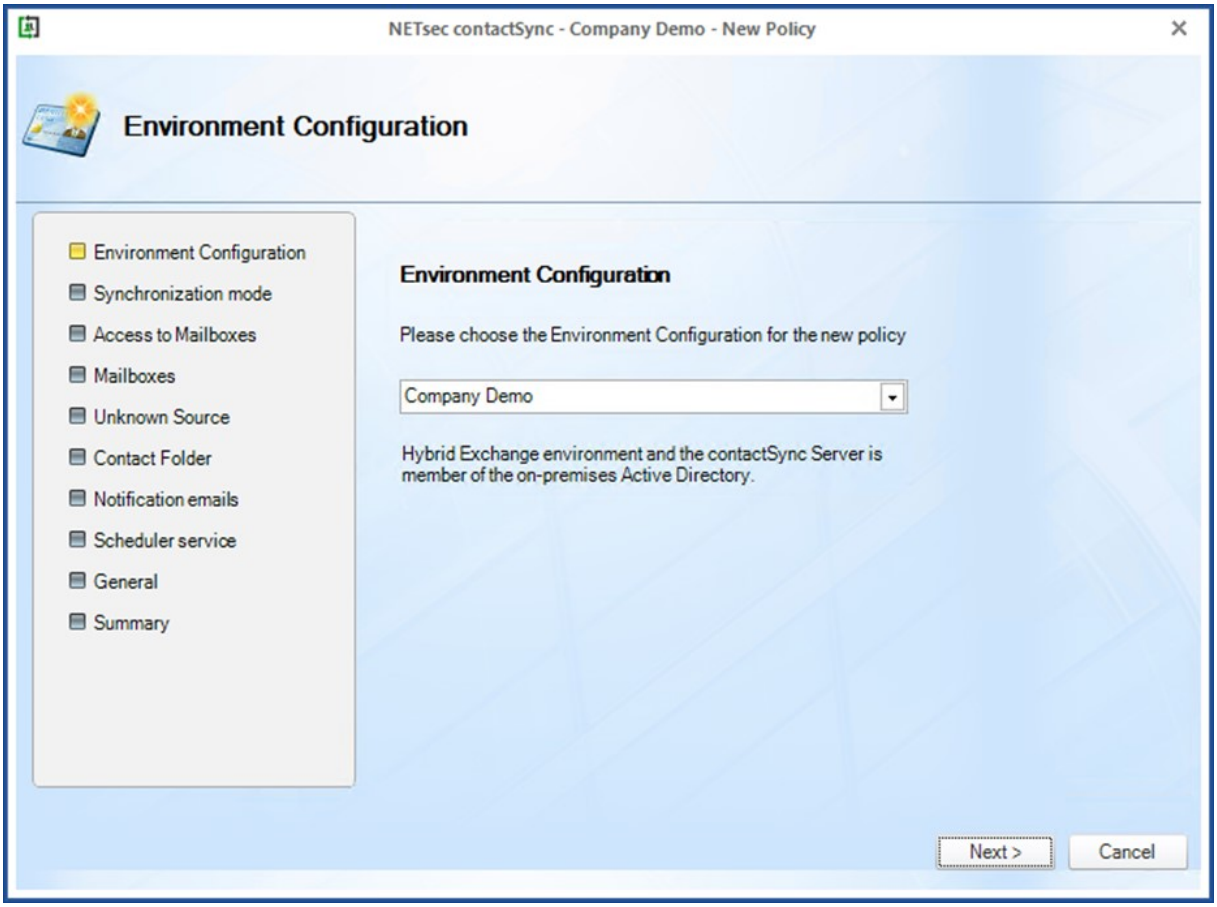
contactSync allows you to synchronize contacts directly from a shared mailbox to user mailboxes. It will connect to a Shared Mailbox in your local Exchange Environment, whether it is in Exchange on-premises or Exchange Online. In Hybrid Exchange Environments contactSync can access the shared mailbox in both locations.

Create new policy

Right click the Environment and select **Create Policy** from the context menu.



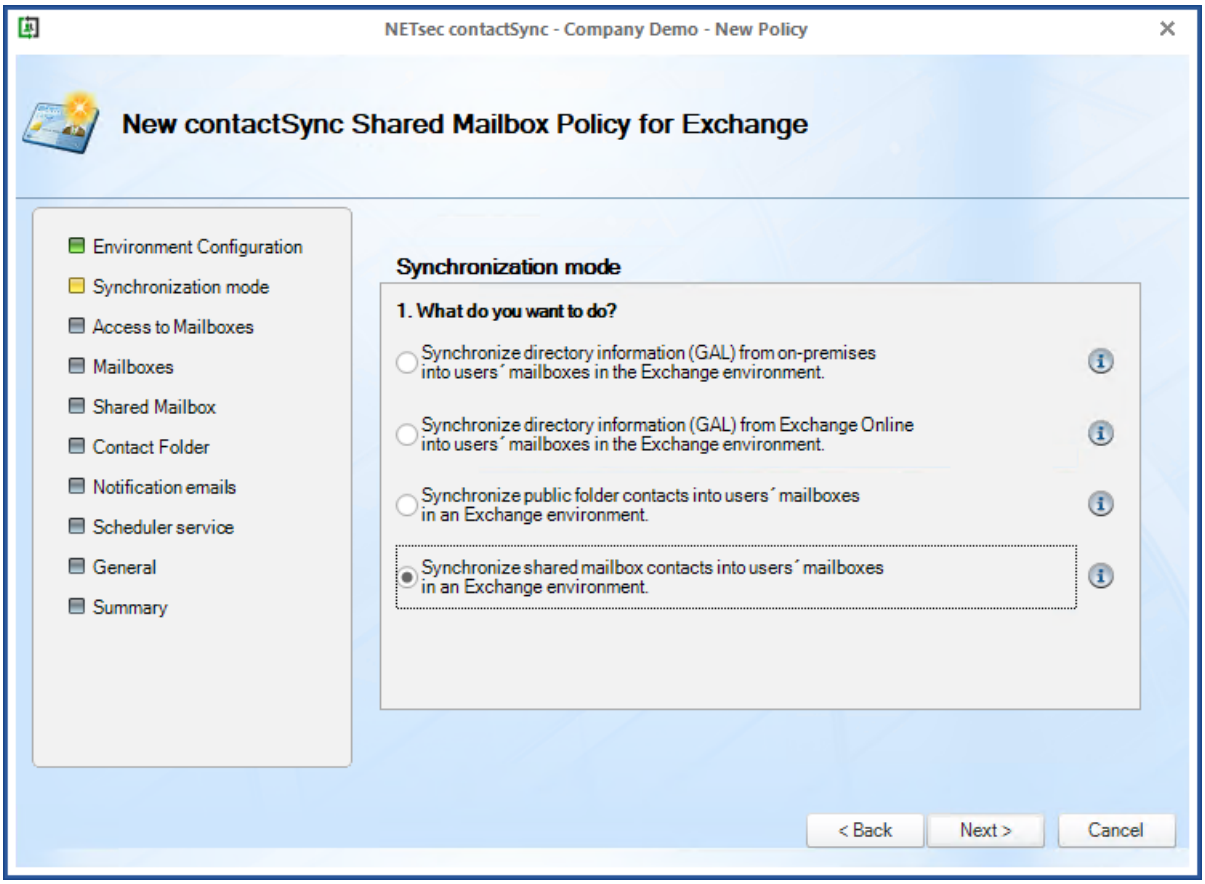
Ensure the desired environment has been selected from the dropdown.



Synchronization mode

Select **Synchronize shared mailbox contacts into users' mailboxes in an Exchange environment**.

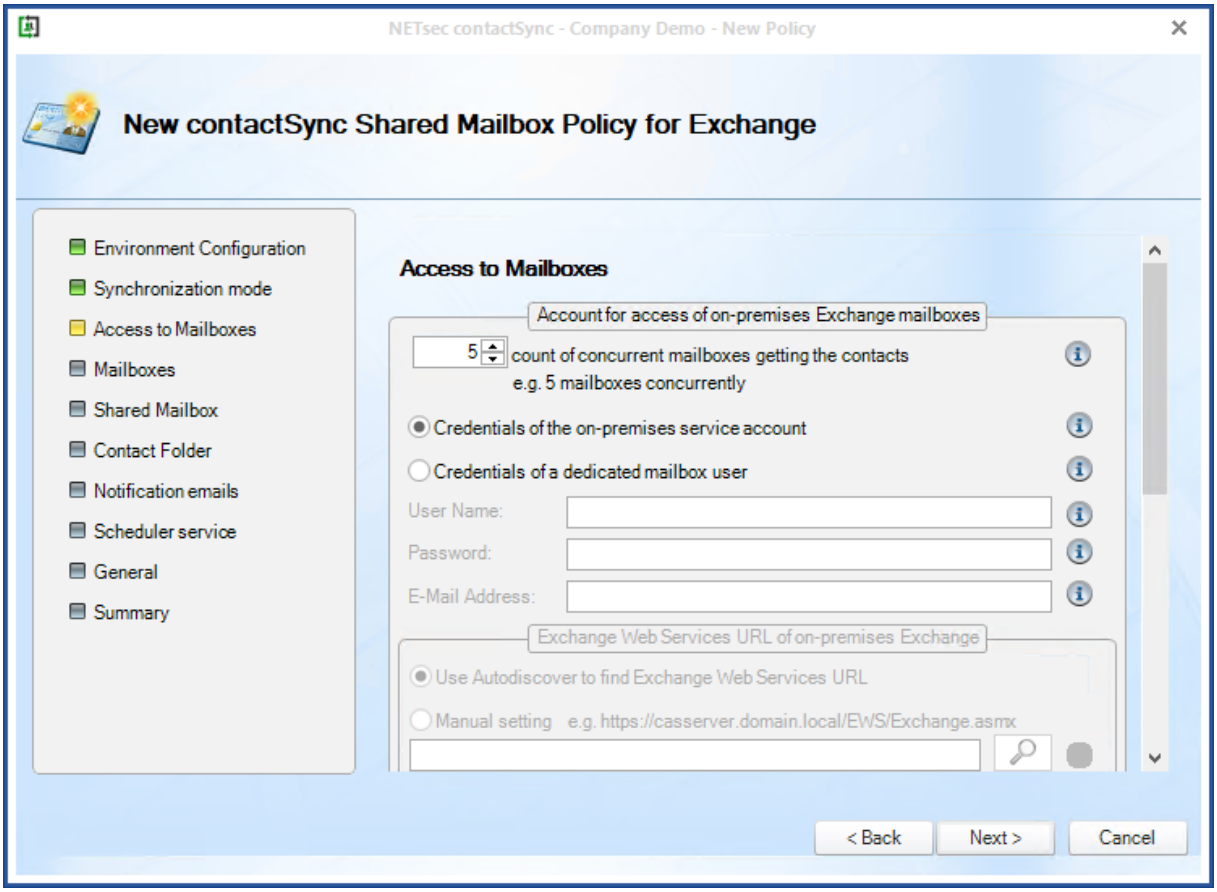
Click **Next**.



Access to Mailboxes for on-premises Exchange

contactSync requires access to user mailboxes in order to write to their contacts folder. It will be necessary to use **Exchange Application Impersonation** for access, which allows up to 5 concurrent connections to user mailboxes.

Since the contactSync mailbox requires the **Exchange Administrator** role, you can split these two roles between two separate accounts by entering the credentials of a dedicated mailbox user that has the **Application Impersonation** role.



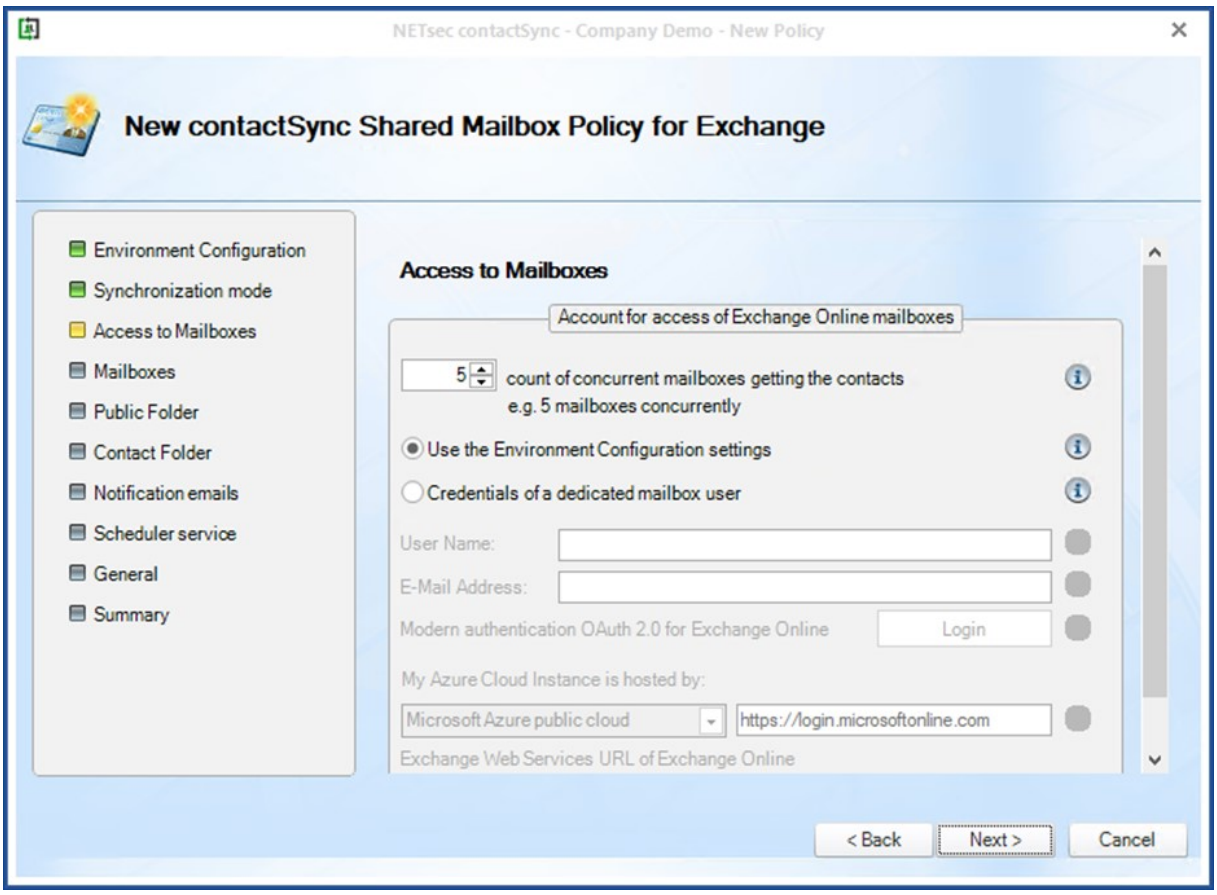
Please take a look at the chapter:

How to configure Exchange Application Impersonation

Access to Mailboxes for Exchange Online

By default, contactSync uses the Environment Configuration to access mailboxes. Application Impersonation, required for on-premises Exchange, will not be necessary when the certificate authentication via App Registration for Exchange Online is configured in the Environment Configuration.

Please take a look at the chapter
Exchange Online certificate-based authentication via App Registration

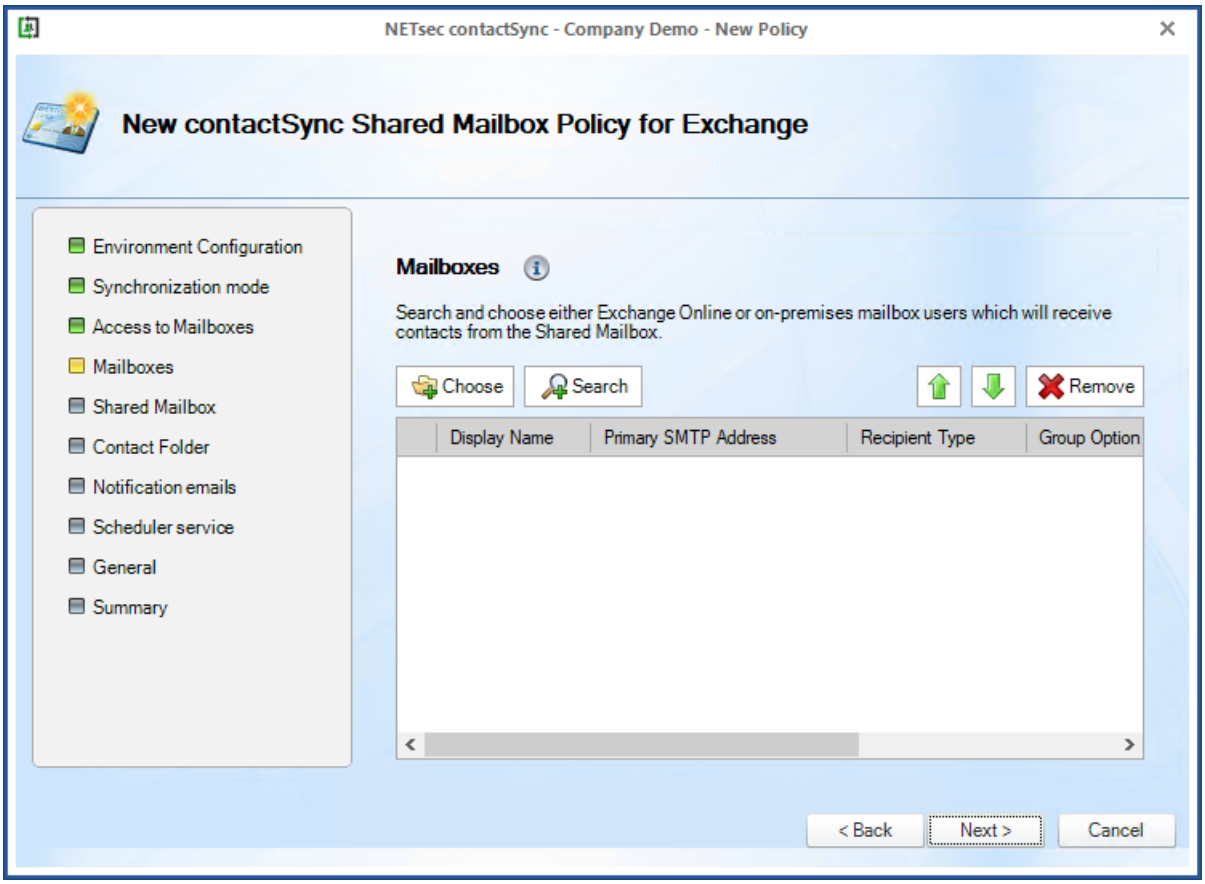


Click **Next**

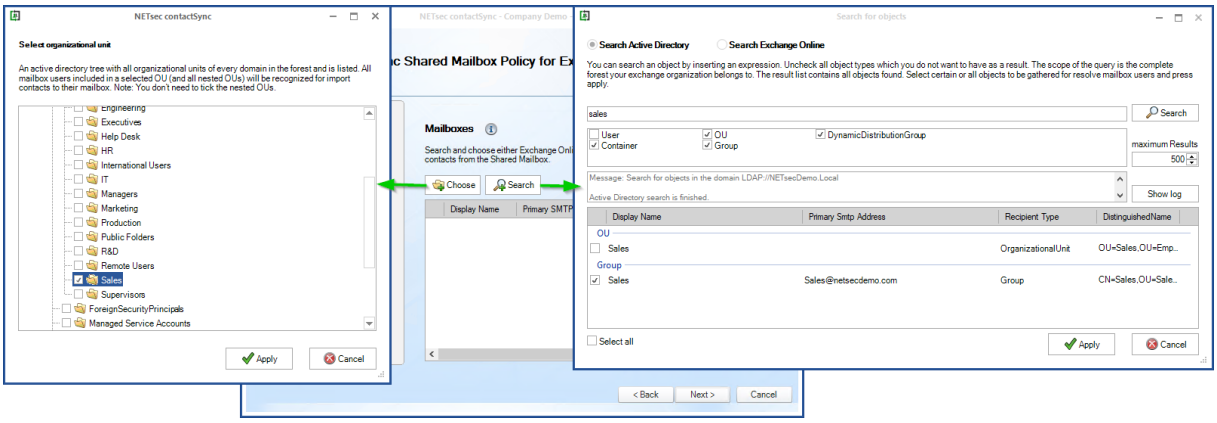
Select the Mailboxes from On-Premises Exchange

You can select Mailboxes located in an on-premises Exchange Server, which will receive contacts. It could be an on-premises Exchange environment or a part of a hybrid Exchange environment.

In the **Mailboxes** window, you are prompted to select the mailboxes which will receive the contacts. There are two ways to do make your selection.



- Click **Choose** to select mailboxes by OU where they reside in Active Directory.
- Click **Search** to open a search dialogue window from which you can search for the desired Active Directory objects. When searching Active Directory, mailboxes can be selected individually, by group membership, by container, or by OU. If you have a hybrid Exchange environment, an additional option is available to search for Exchange Online objects.

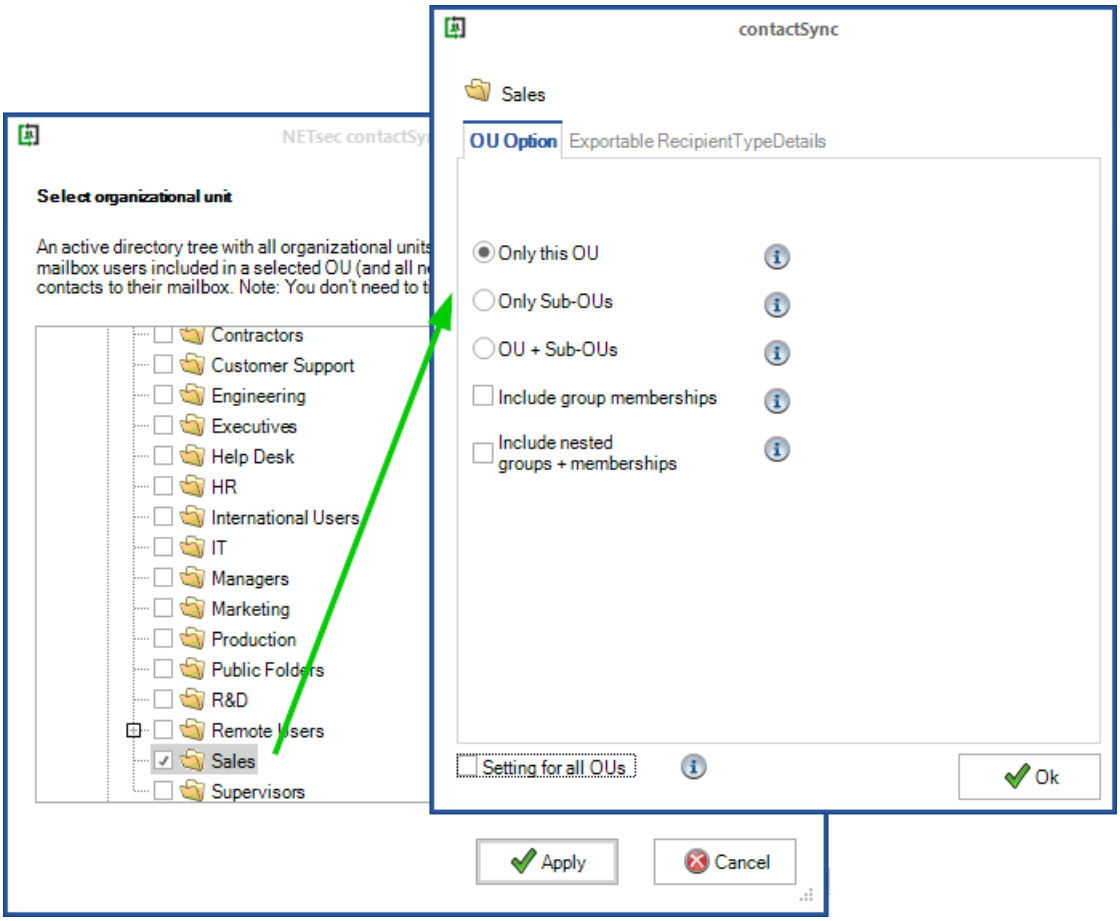


When the **Search Exchange Online** Radio Button has been selected, you can search for objects by Recipient Type, such as **UserMailbox**, **MailUniversalDistributionGroup**, **MailUniversalSecurityGroup**, **DynamicDistributionGroup**, or **Office365 Group**.

When OUs are selected, a prompt to select the OU depth is presented. If any groups are contained in the OU, contactSync will prompt the user to include mailboxes by group membership.

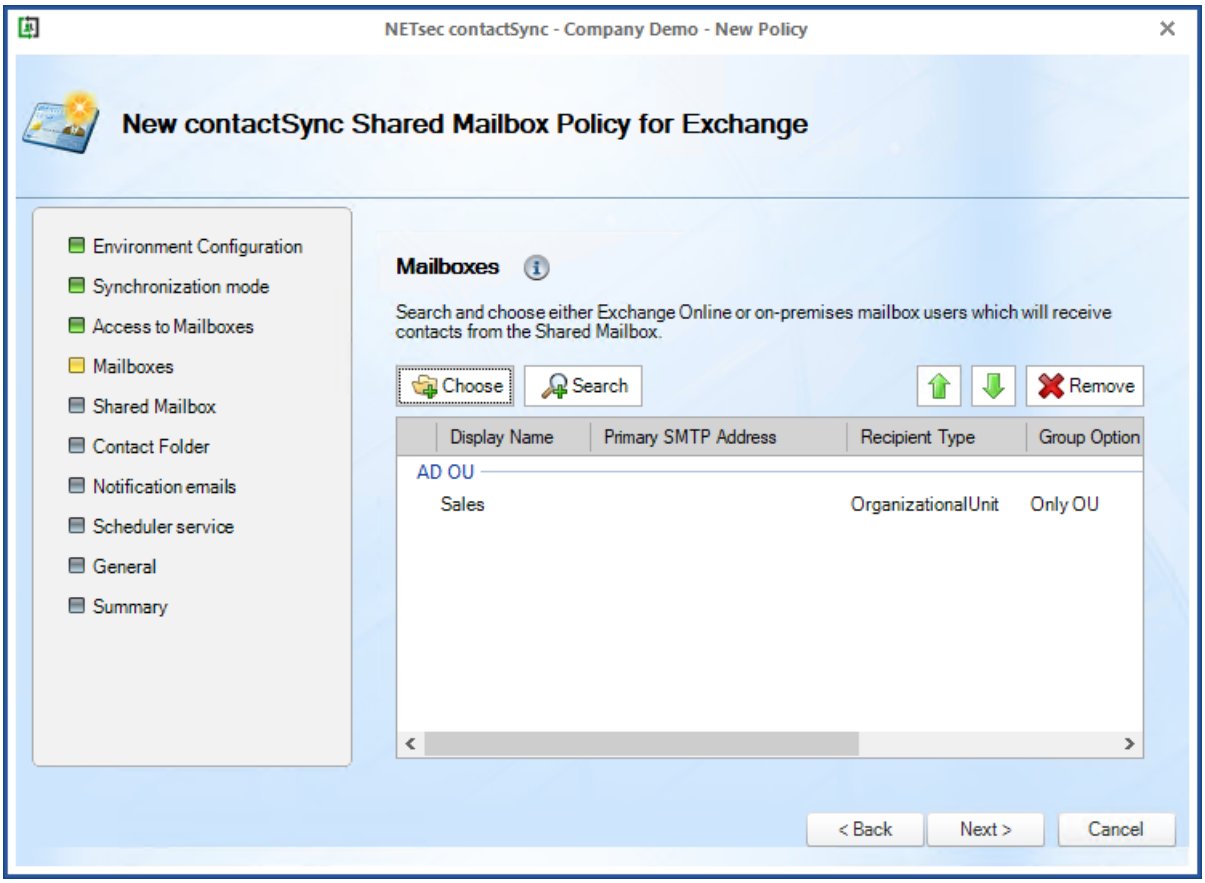
If multiple OUs have been selected, the checkbox at the bottom left will apply the settings to all selected OUs.

Click **OK**, then **Apply**.

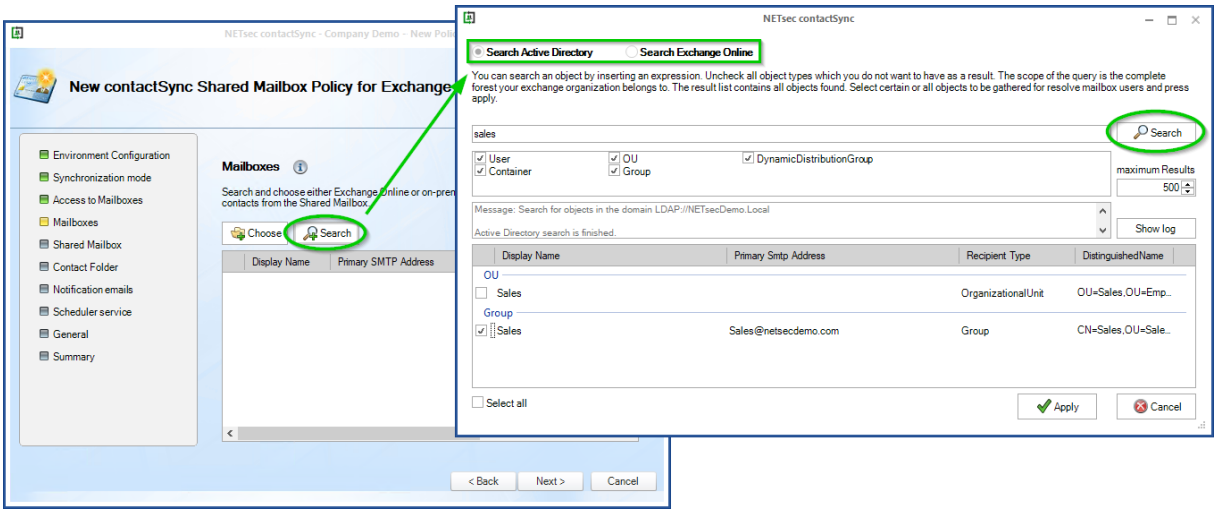


Verify the selected OUs are displayed.

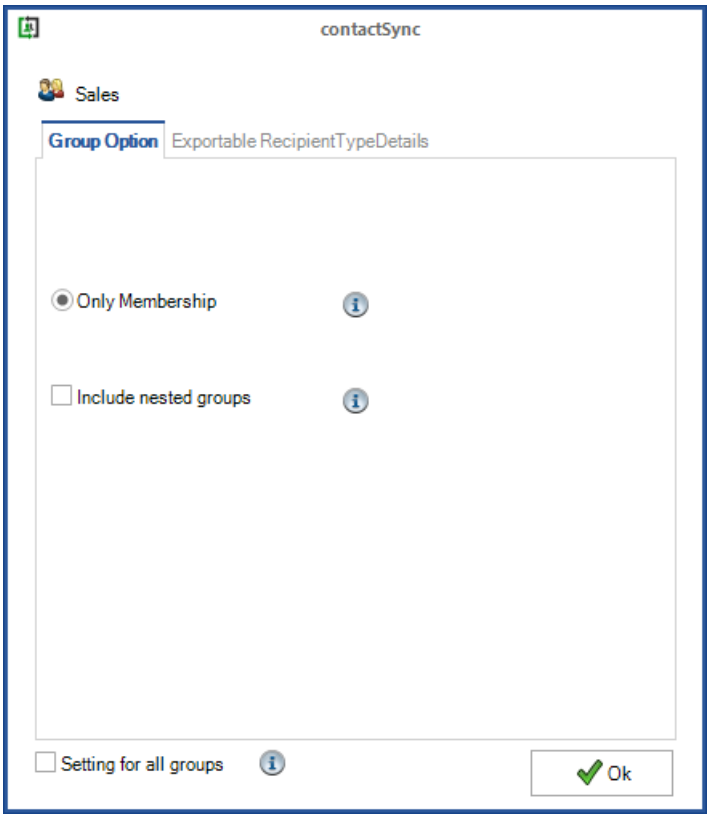
Click **Next**



Instead of selecting OUs in Active Directory as described above, in the following example, the **Sales** Distribution Group has been selected from the Active Directory search.

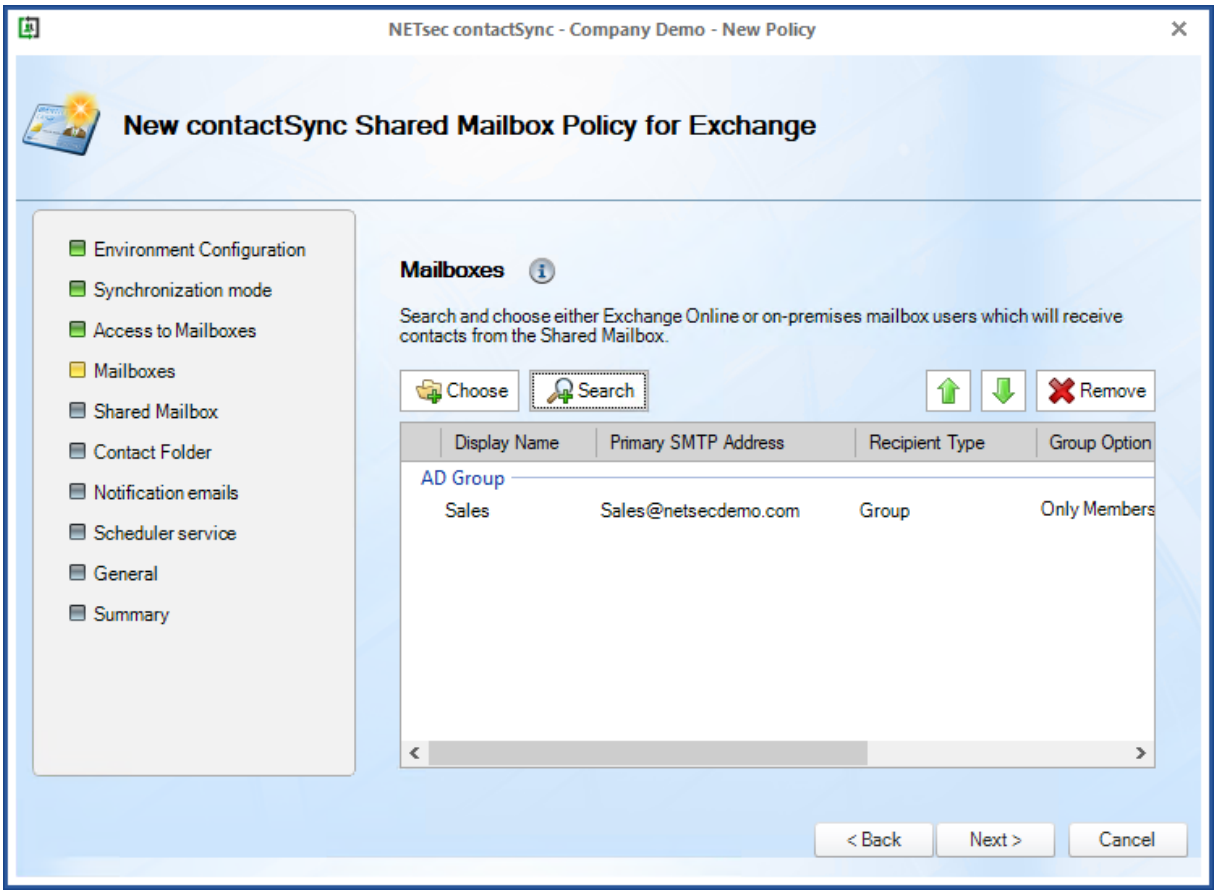


All members with a mailbox in the selected group will receive the contacts, an option is also available to include nested groups.



Click **OK**.

The selected group(s) are displayed under the appropriate heading.

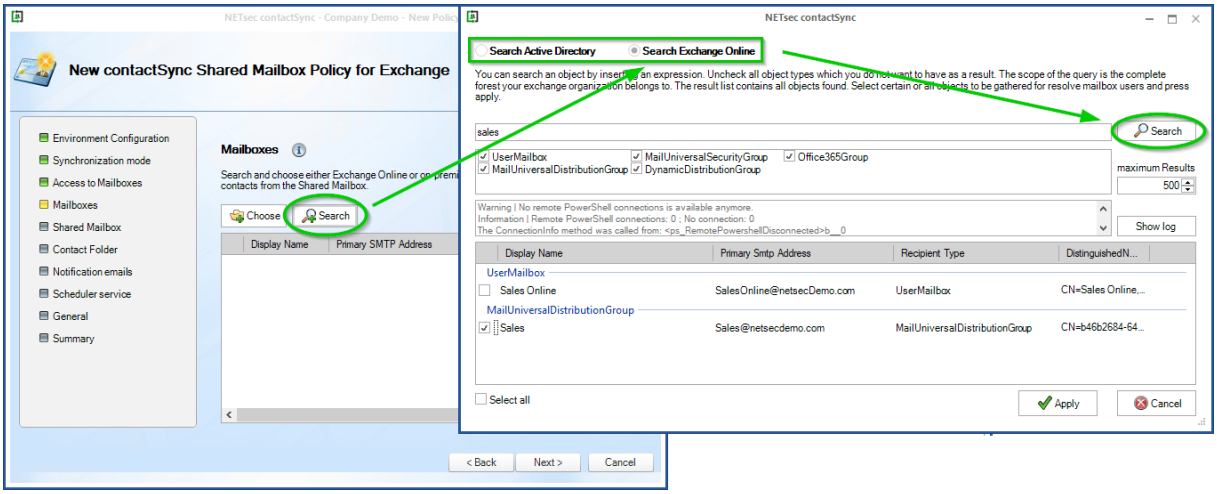


Click **Next**

Select the Mailboxes from Exchange Online

You can select Mailboxes located in Exchange Online which will receive the contacts. This is possible for an Exchange Online environment or a part of any hybrid Exchange environment, as shown in the screenshot below.

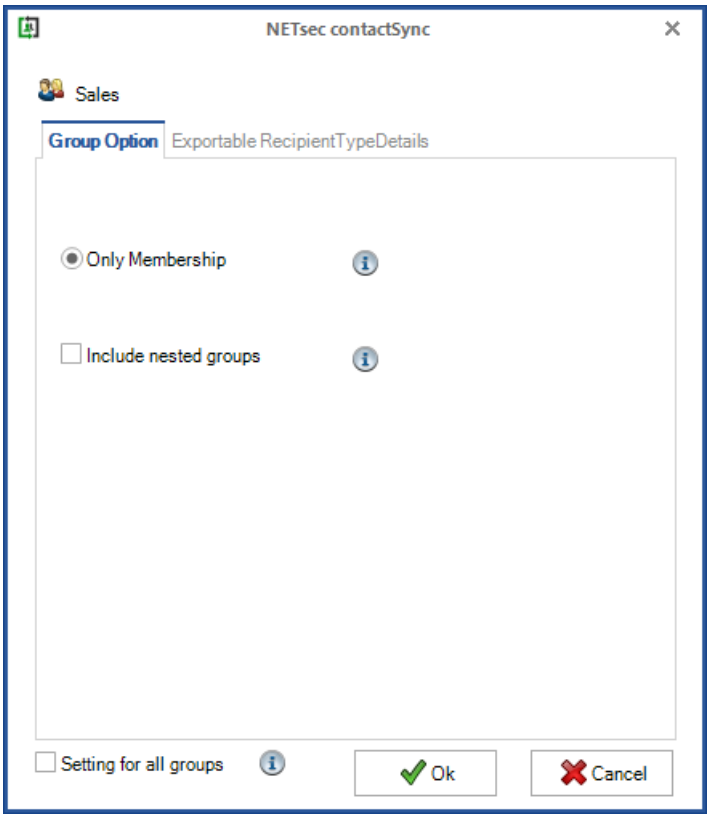
When searching for Exchange Online objects, you can search for objects by Recipient Type, such as **UserMailbox**, **MailUniversalDistributionGroup**, **MailUniversalSecurityGroup**, **DynamicDistributionGroup**, or **Office365 Group**.



In the example above, the **Sales** Distribution Group has been selected. You can expand your search by inserting a wild card character (*).

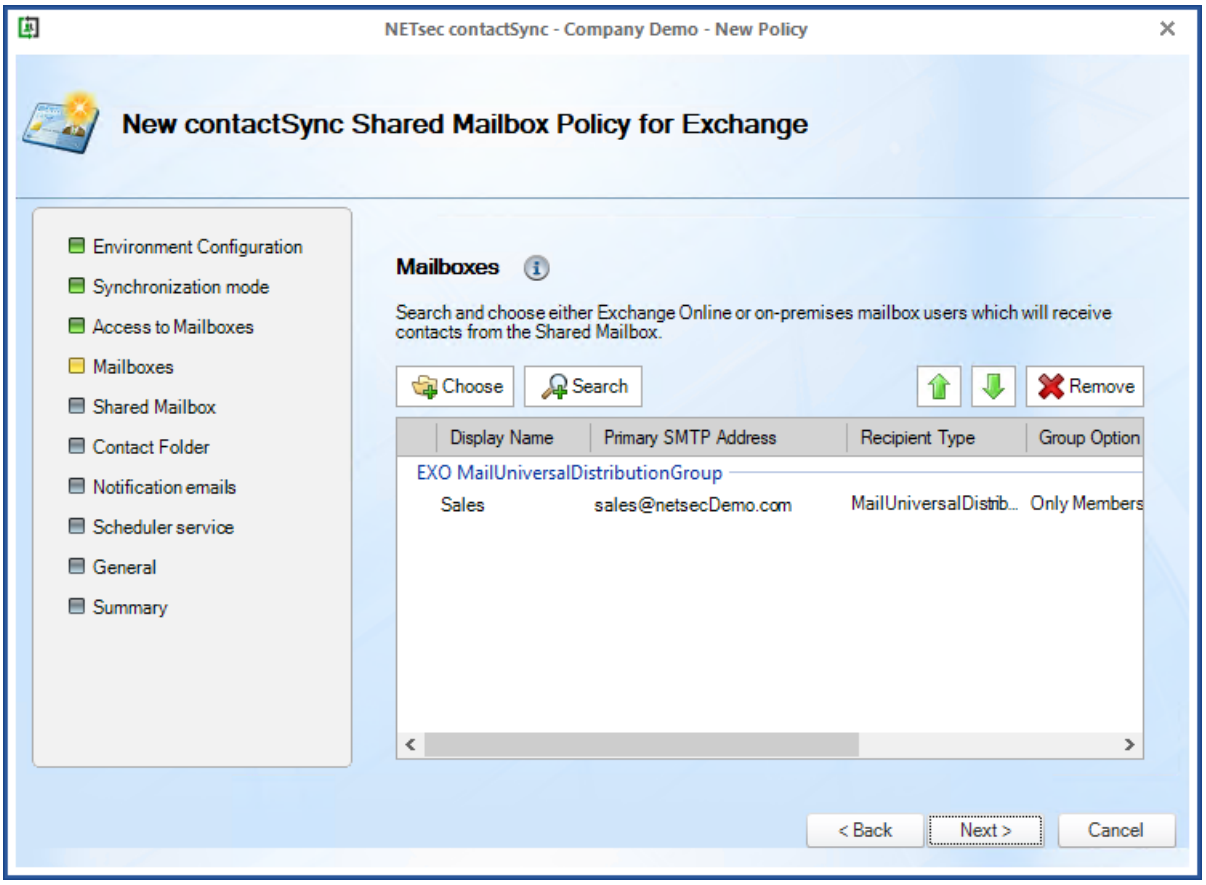
Click **Apply**.

All members with a mailbox in the selected group will receive the contacts, an option is also available to include nested groups.



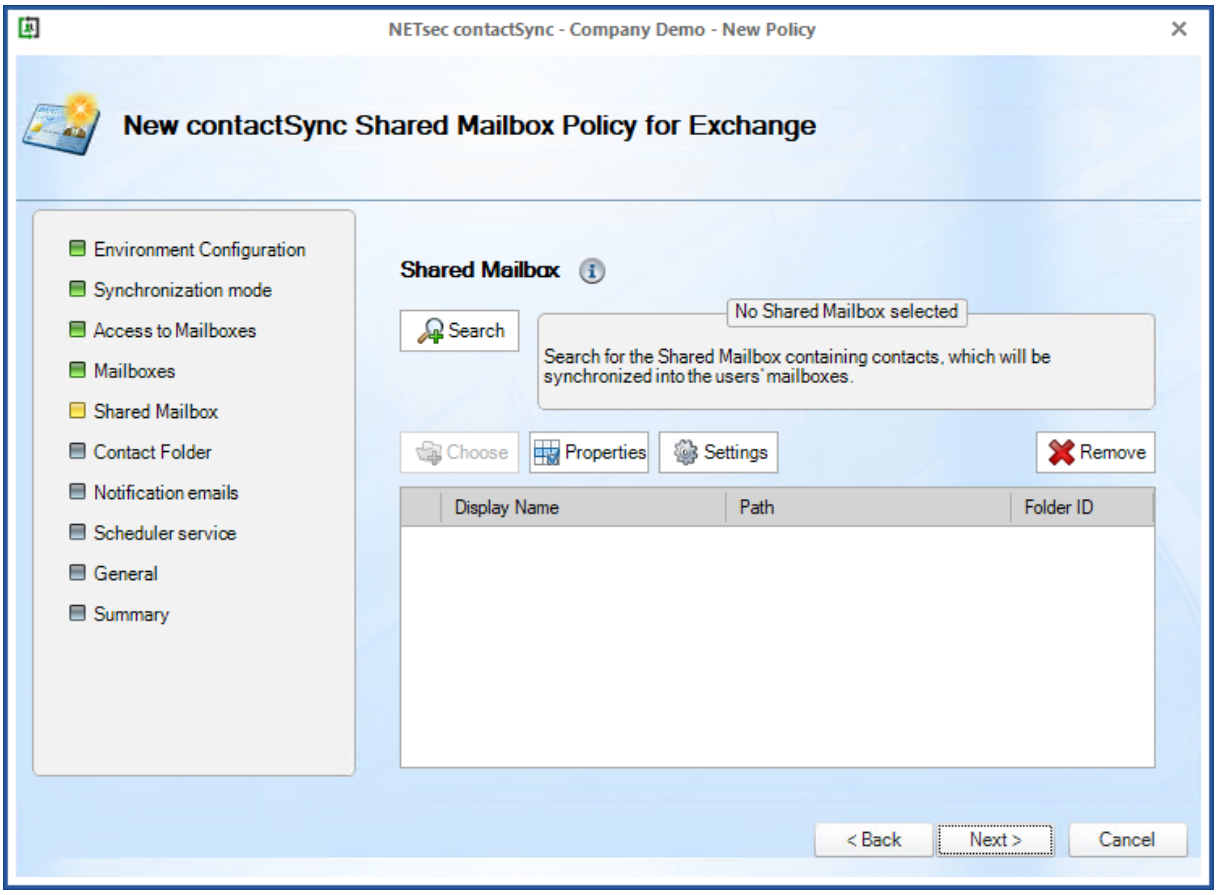
Click **OK**

Verify the selected group(s) are displayed. Click **Next.**

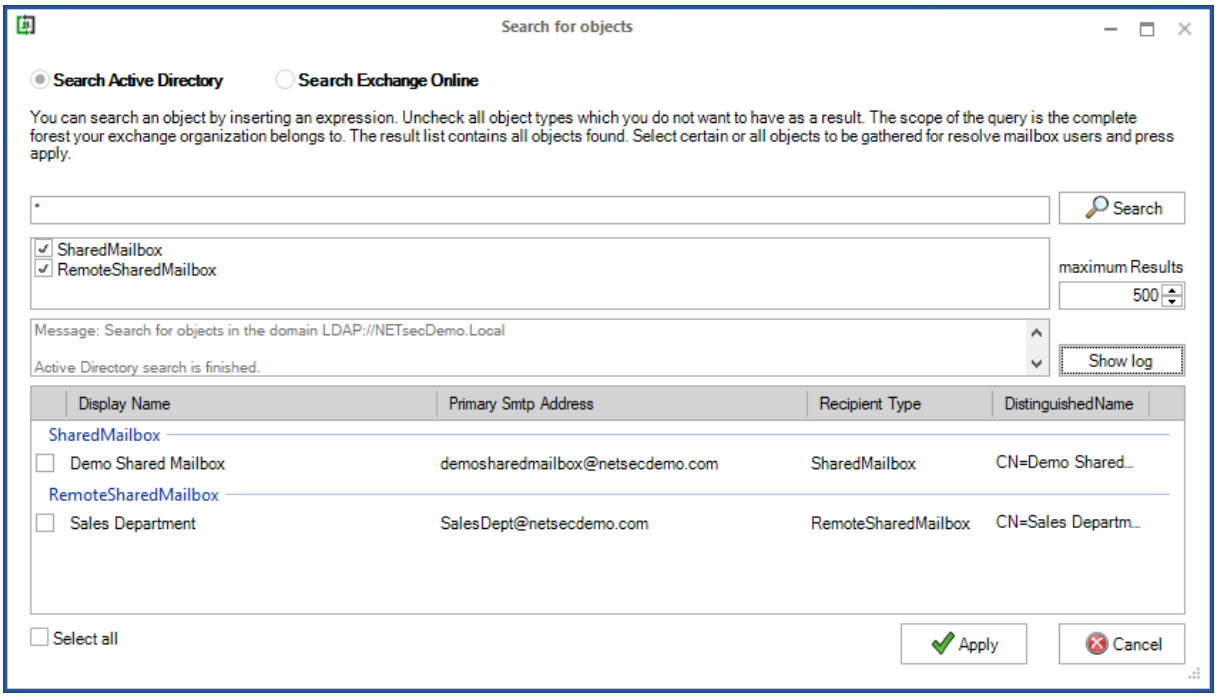


Select Shared Mailbox

The Shared Mailbox page is displayed below.



Click **Search** to open the **Search for objects** dialog window.



Select where you want to search in a hybrid Exchange environment. Search in the on-premises **Active Directory** or search in **Exchange Online** for a Shared Mailbox.

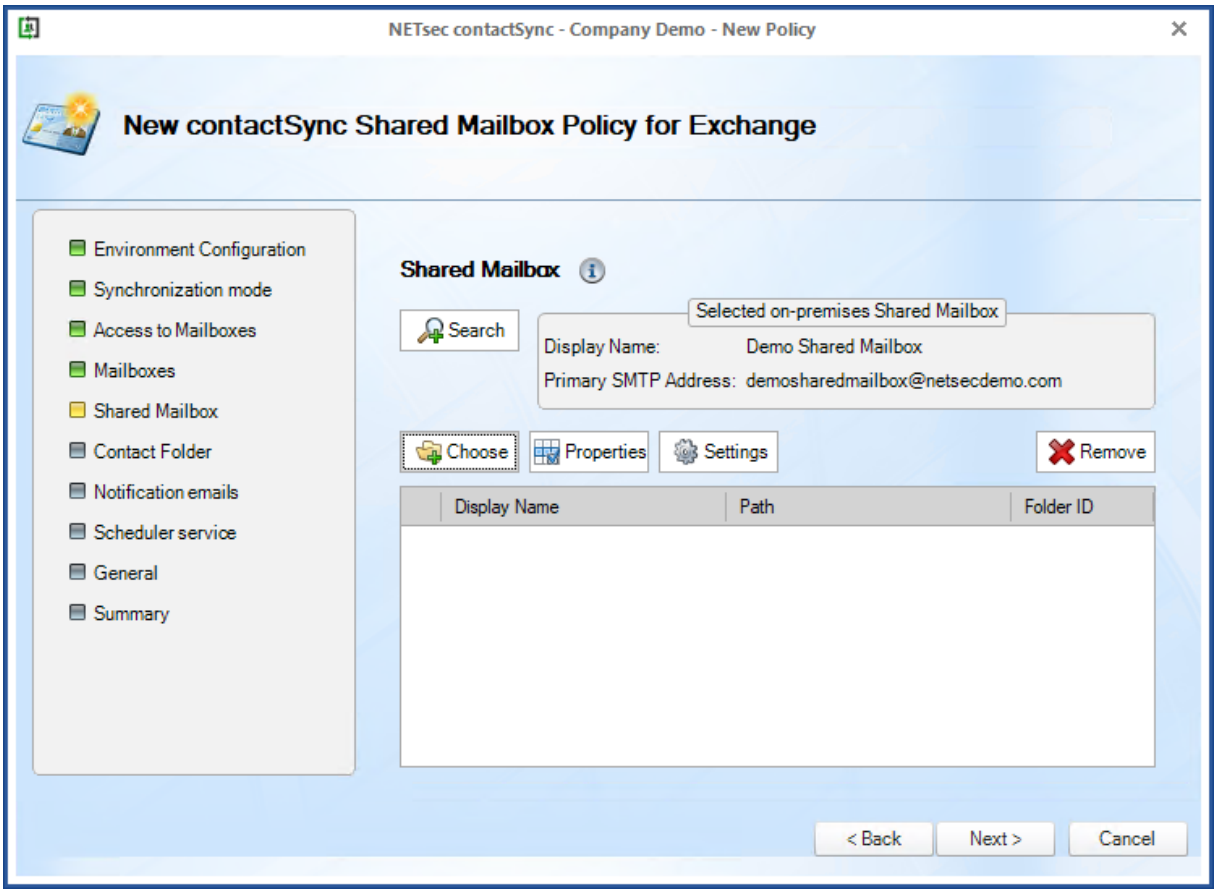
Then search for and select the desired Shared Mailbox which contains the contacts to be synchronized into user mailboxes.

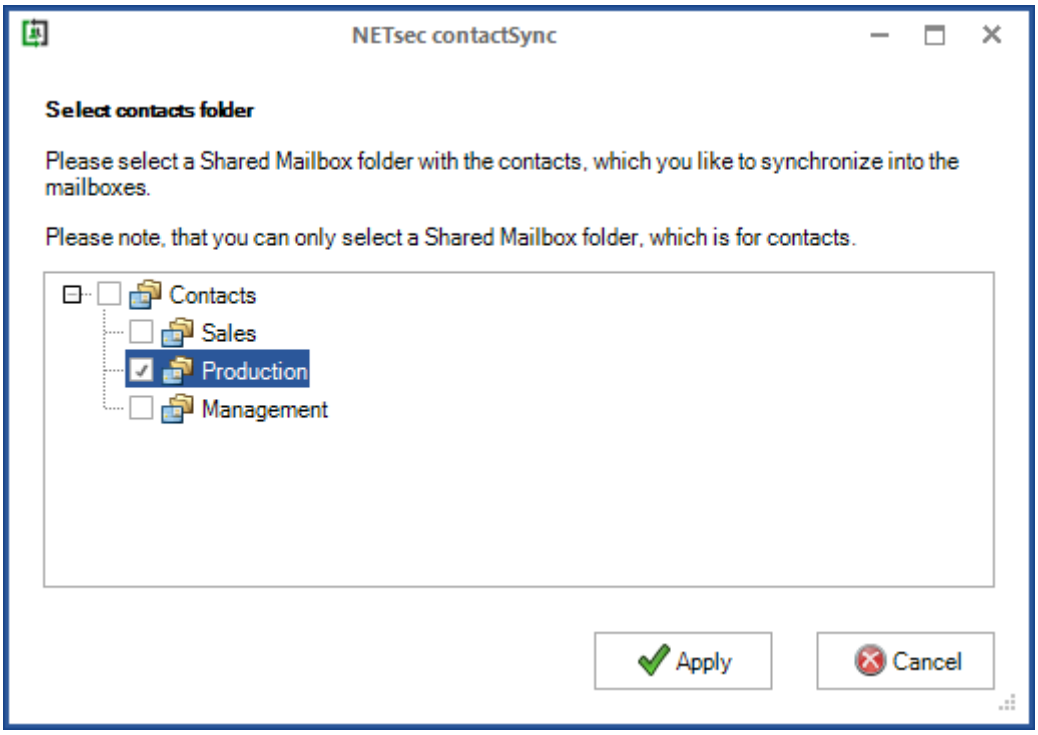
Here you may pick either all objects or specify a filter by ticking recipient types you want to choose. With a wildcard * you can widen your search criteria, and broaden the results.

Next select the desired shared mailbox and click **Apply**.

Select Contact Folder in the Shared Mailbox

After a shared mailbox is selected, click **Choose** to select the contact folder with contacts you want to synchronize into the mailboxes.

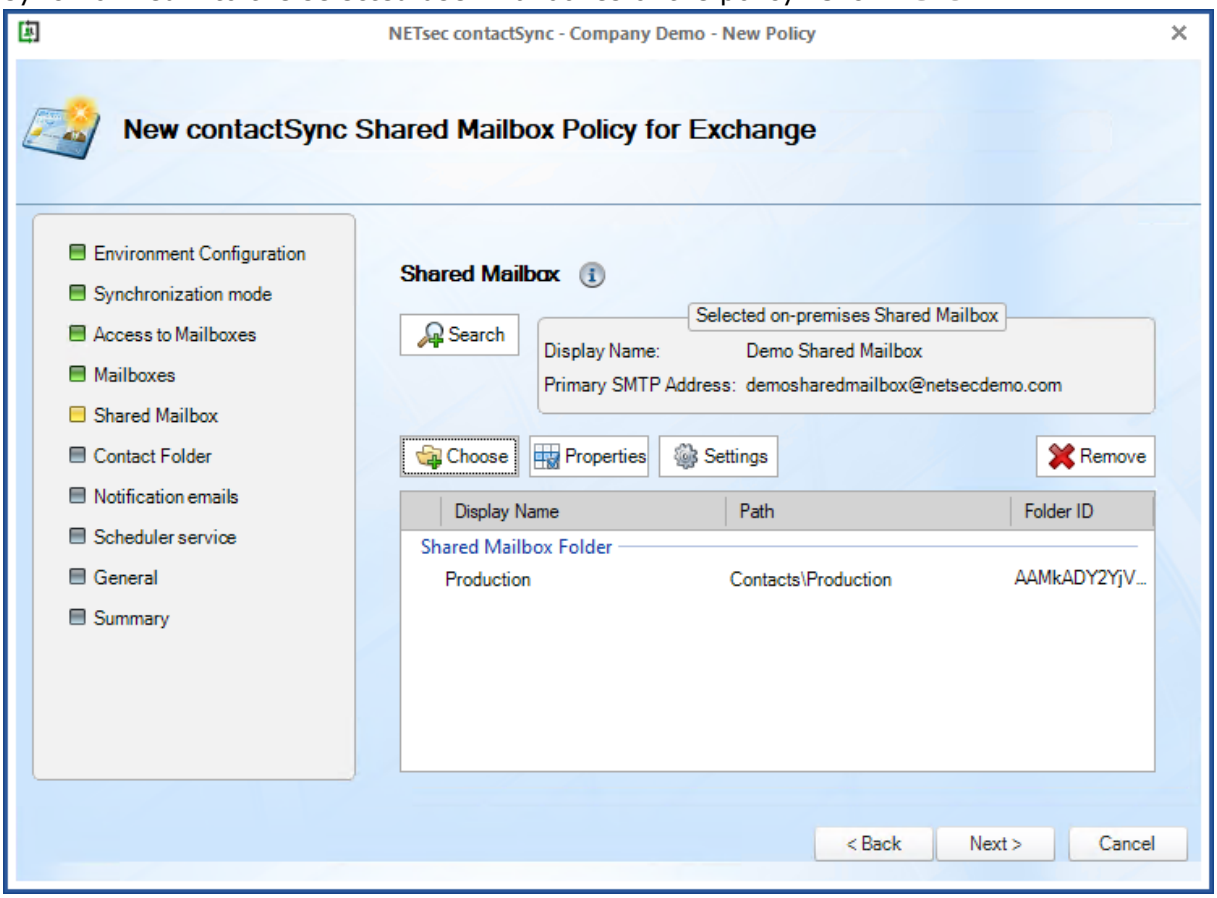




Here, a shared mailbox with all contact folders will be displayed. You may tick a contact folder in the tree, but only a contact folder dedicated for contacts can be selected.

Afterwards click **Apply**, the selected contact folder is listed on the **Shared Mailbox** tab.

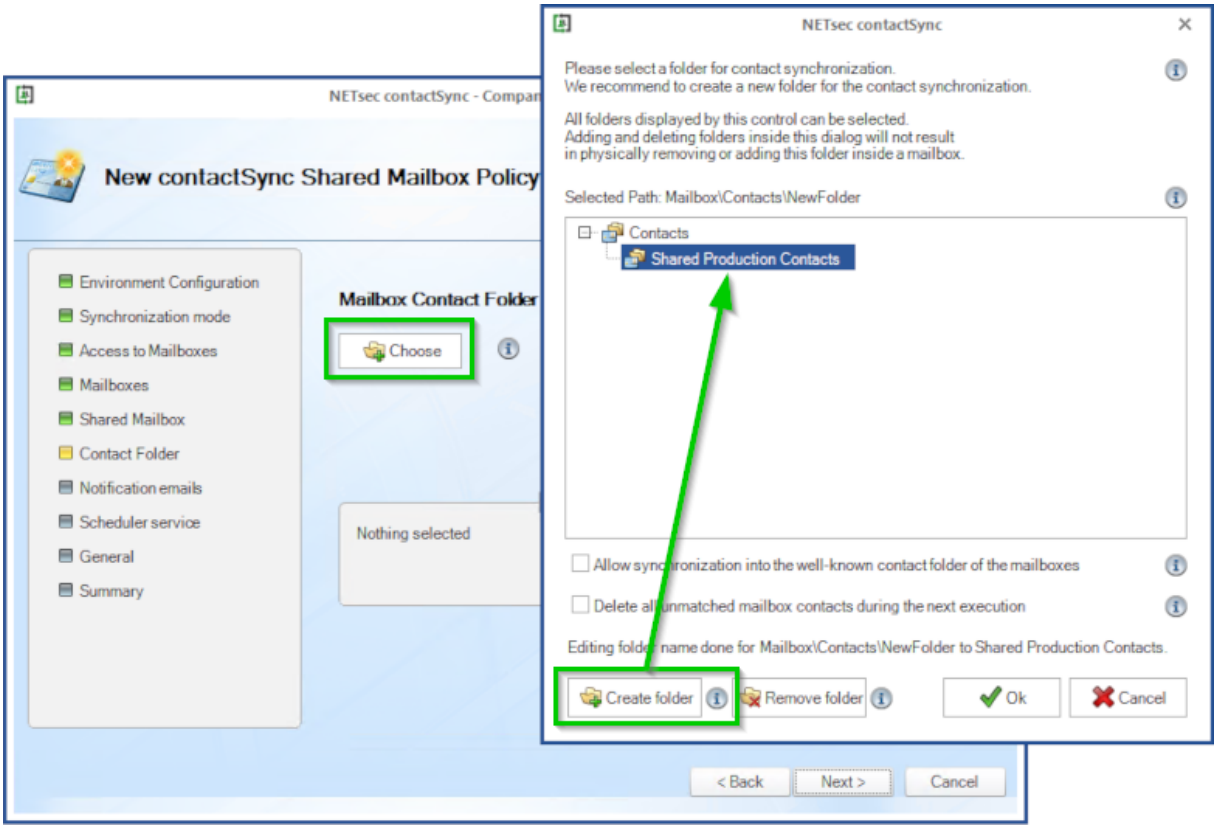
In this example the **Production** folder contacts in the **Demo Shared Mailbox** will be synchronized into the selected user mailboxes of the policy. Click **Next**.



Select the Mailbox Contact Folder

Click **Choose** to select the contacts folder where the contacts will be synchronized to.

contactSync, can be configured to import contacts directly into the top-level Contacts folder. We recommend a new folder is created, which keeps the contactSync created contacts separate from the user-created contacts.



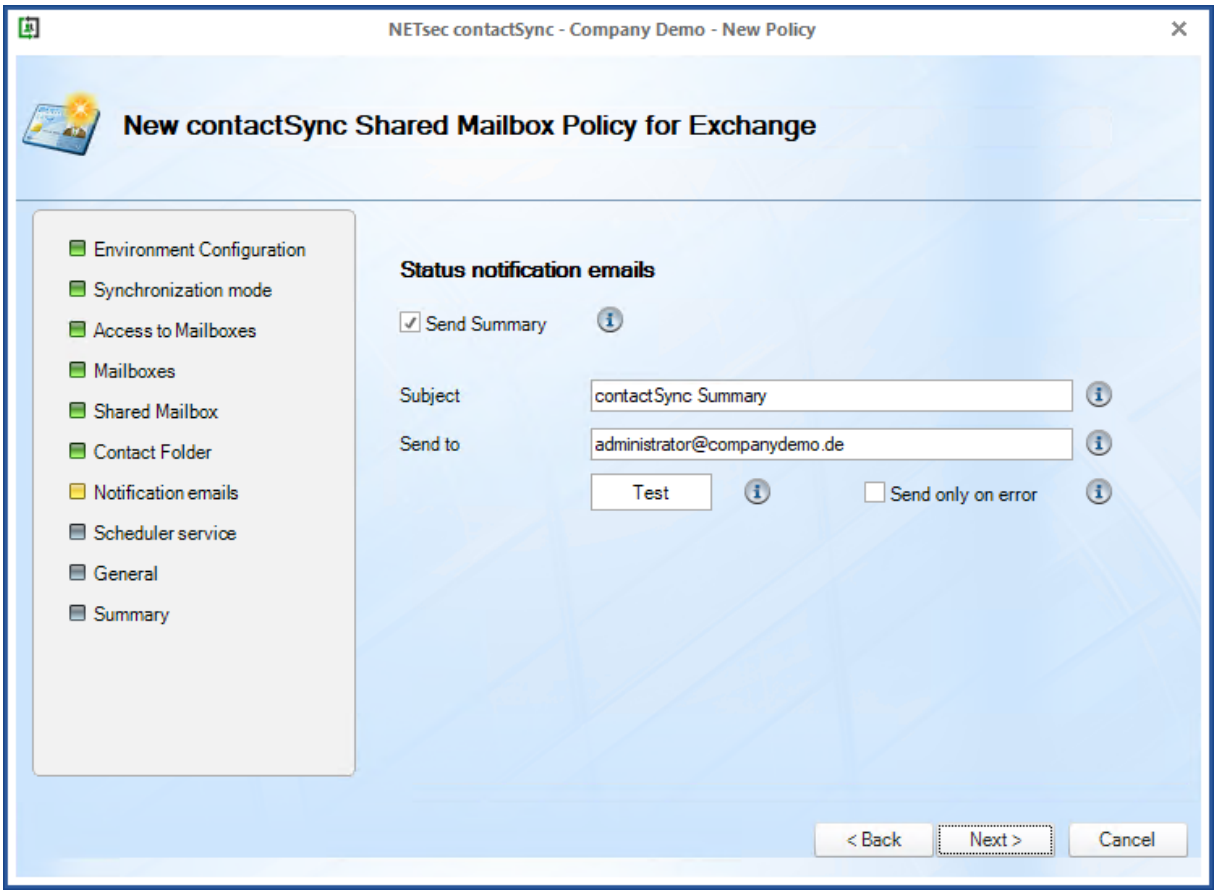
Select the top-level **Contacts** folder, then click **Create folder** to create a subfolder where the contacts will be synchronized, then give the new folder a name.

Click OK, then click **Next**.

Status notification email

An optional status notification email can be sent to the specified recipient(s) each time the policy runs, which provides a brief summary of activity. However, if your preference is to receive one only when an error has been logged, check the **Send only on error** checkbox. Click the **Test** button to send a test email. Then verify it has been received.

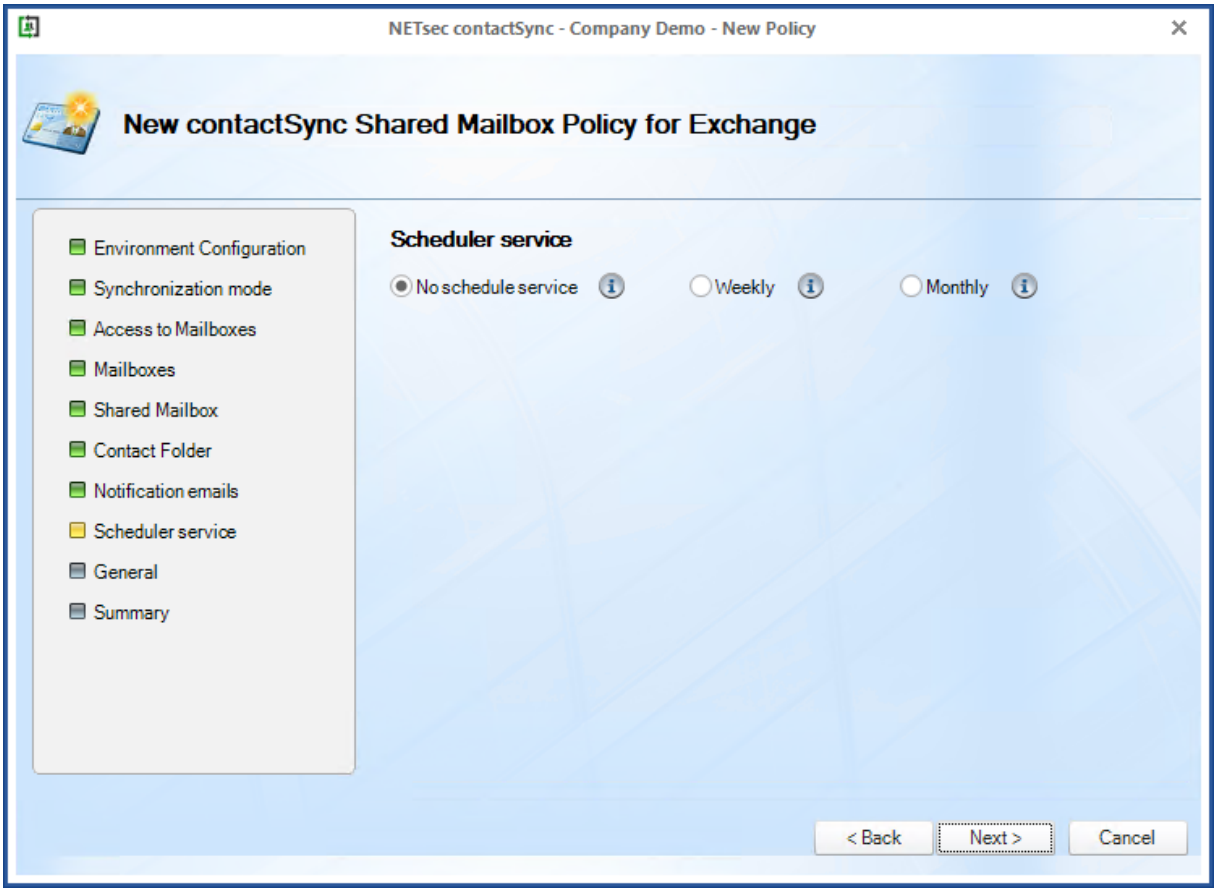
Click **Next**.



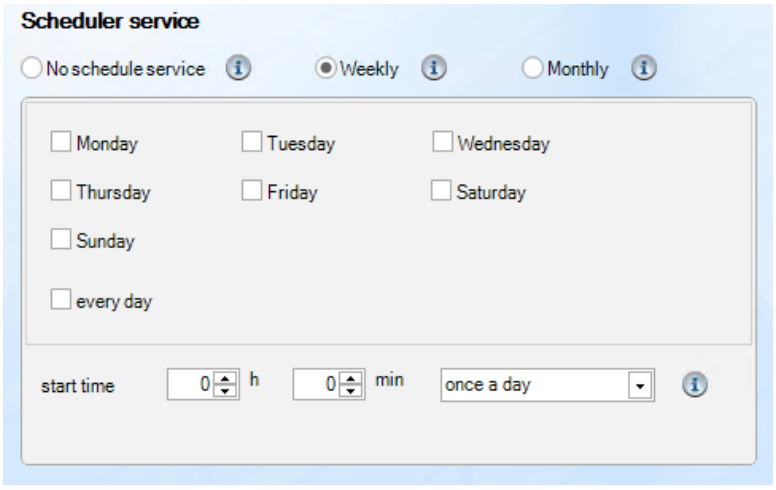
Schedule policy run

contactSync can be scheduled to run at regular intervals. We recommend the policy is manually run before any schedules are set. After the synchronization has completed successfully, you can go back and set it to run on the desired schedule.

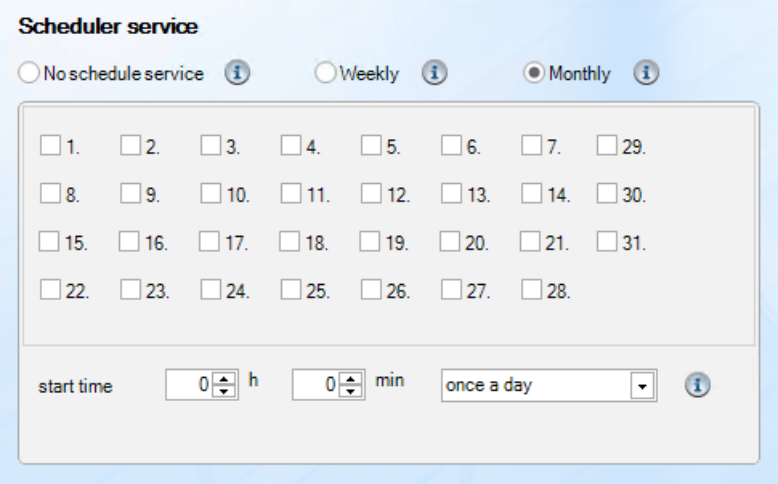
Click **Next**.



The **Weekly** schedule allows you to select which days of the week the policy runs, along with start time and frequency.

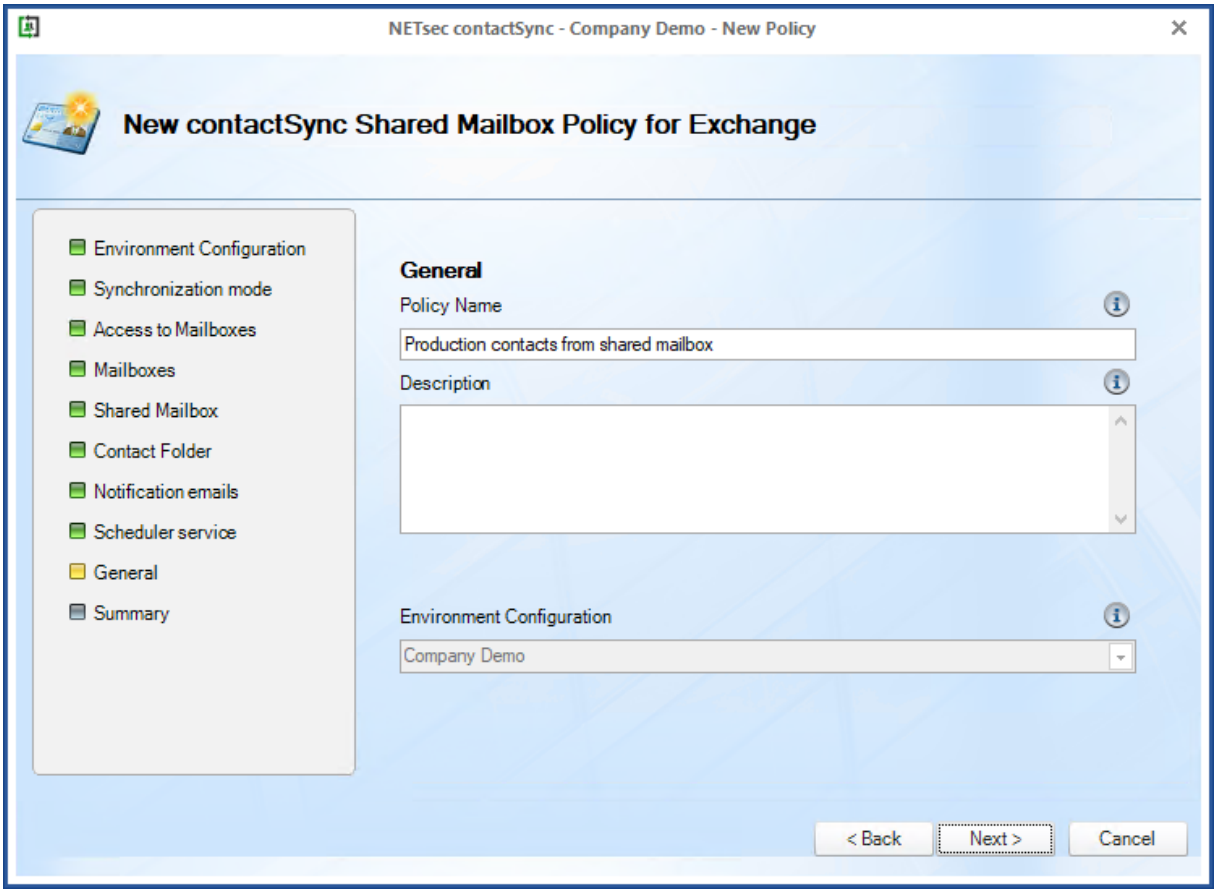


The **Monthly** schedule allows you to select which days of the month the policy runs, along with start time and frequency.



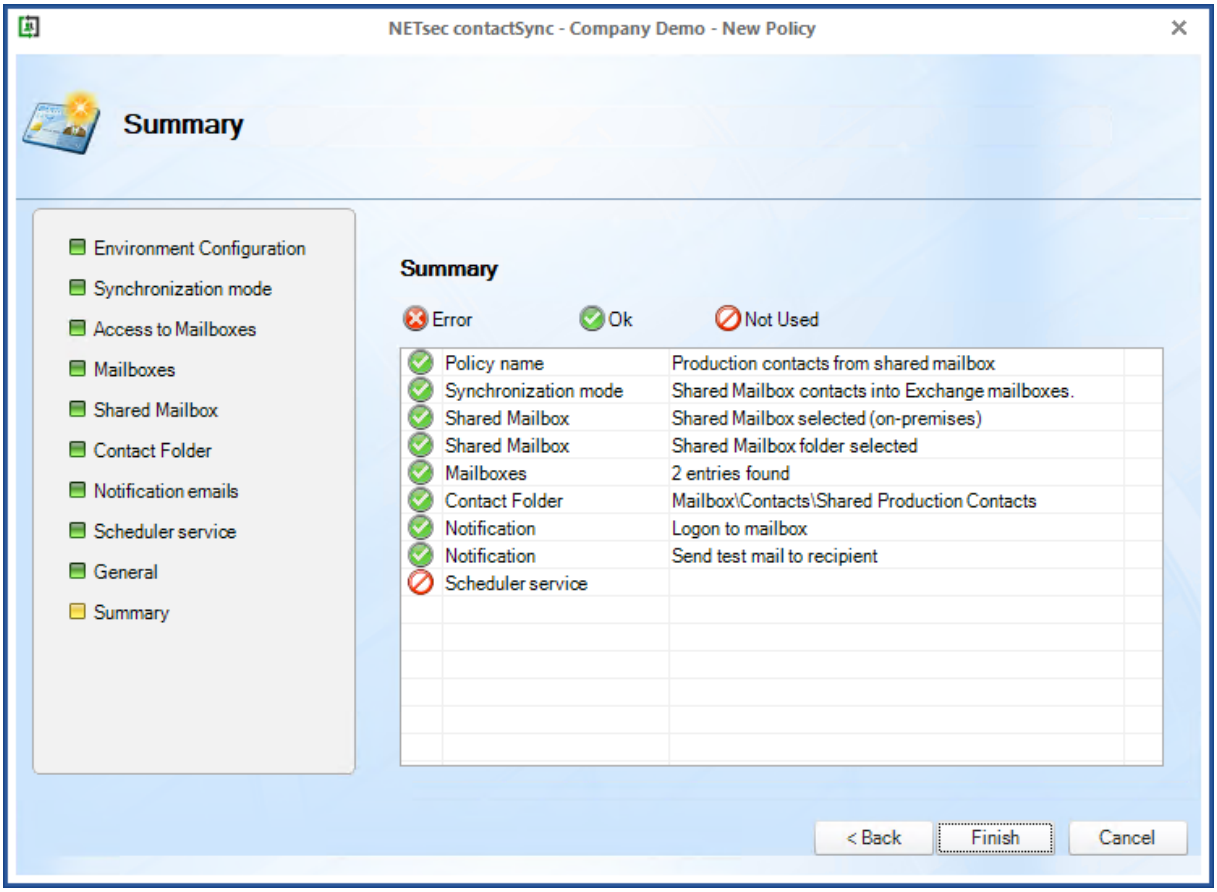
Policy name and description

Enter a policy name and an optional description, then click **Next**.



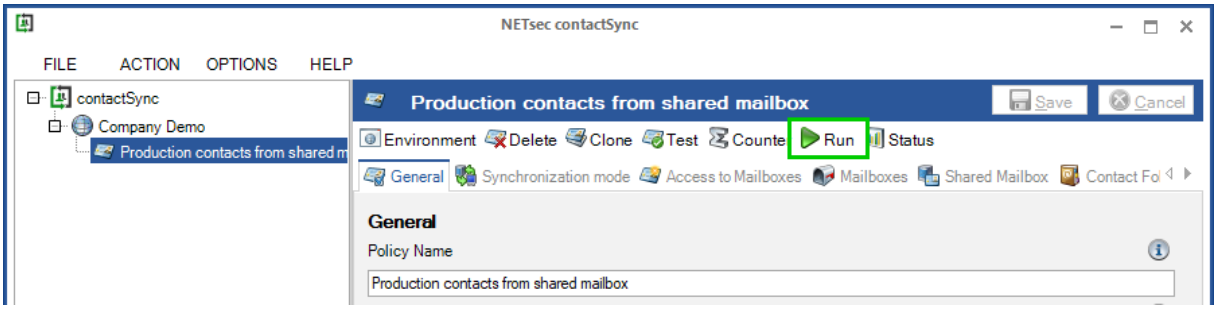
To ensure your settings have been properly configured contactSync will check your policy settings and notify you of any detected errors.

Click **Finish**.

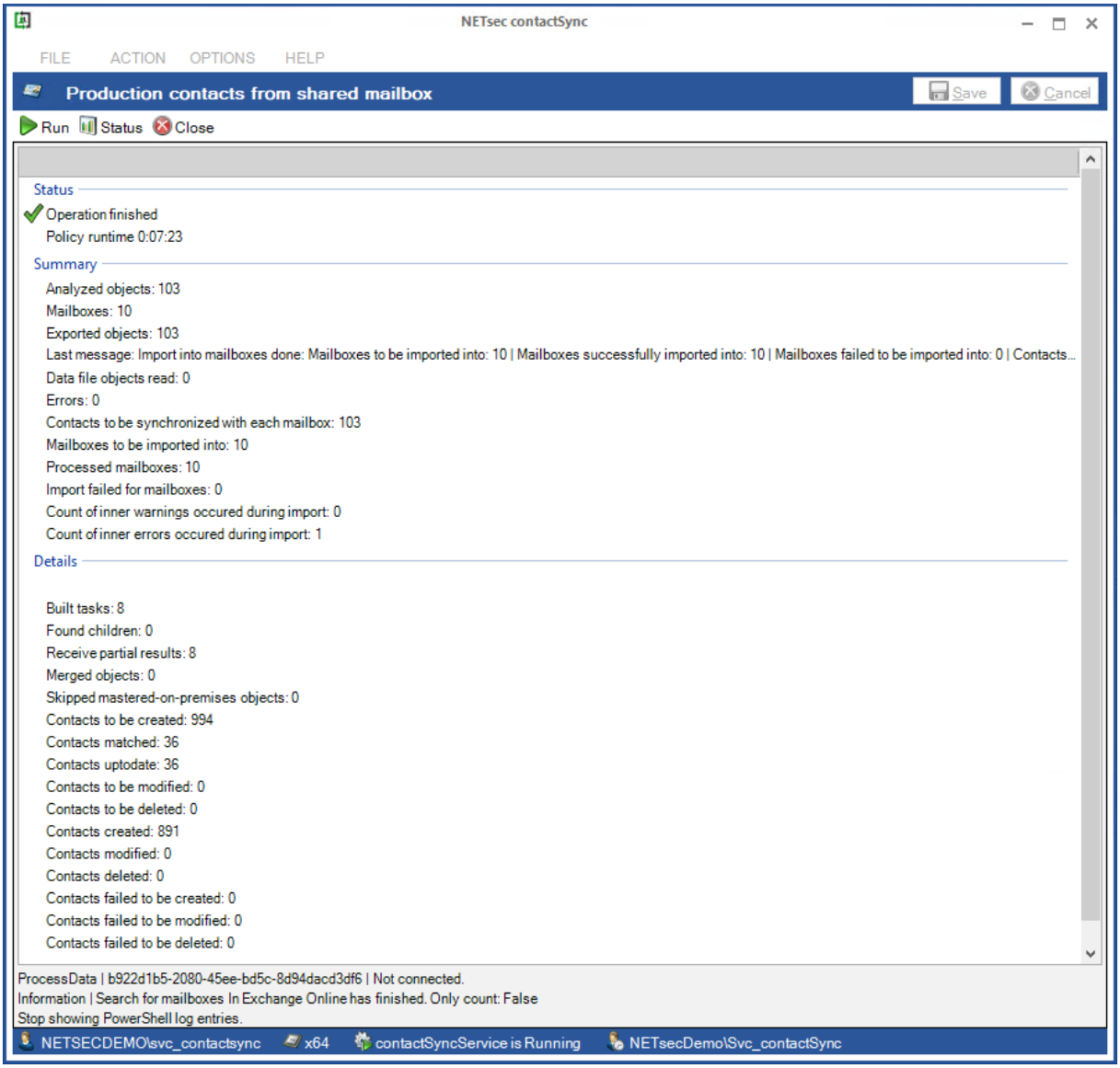


Execute policy and check log files

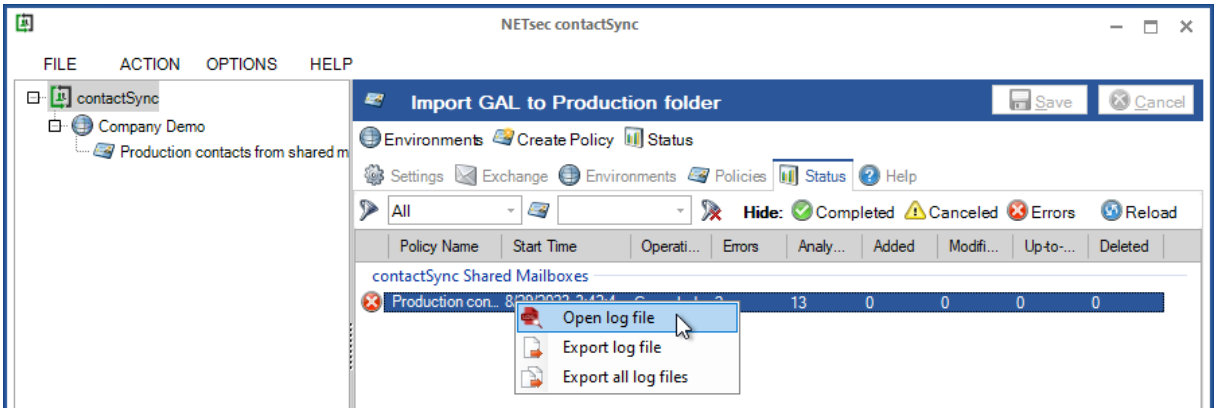
Select the policy node and click **Run**.



The status and a detailed summary are displayed upon completion.
contactSync synchronized 103 contacts into 10 separate mailboxes



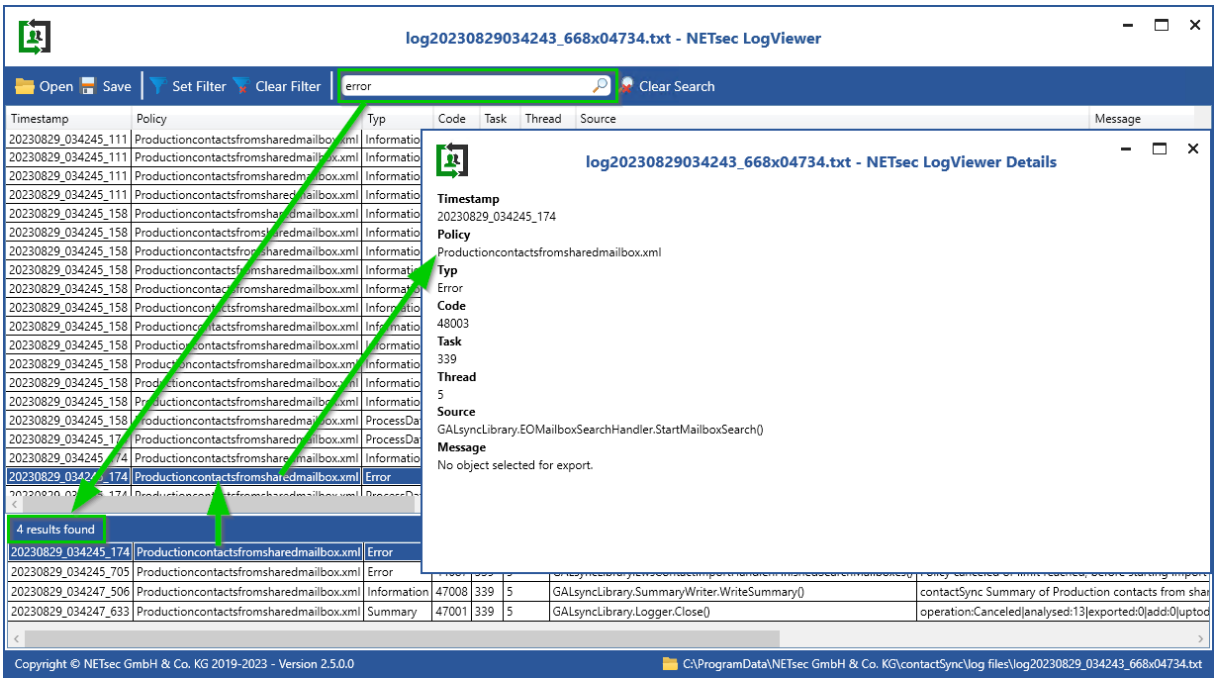
The corresponding log file can be opened by selecting the **Status** tab, and right-clicking the associated log and selecting **Open log file** from the context menu. This allows you to easily find the error and identify its cause.



Searching for the string "error" yields 4 log entries containing this string.

Double-click the line which contains the error. This will highlight the line in the log which contains the details of this log entry.

Double-click the highlighted line in the log viewer to open a new window containing the details of the error.



How to

How to configure Exchange Application Impersonation

contactSync requires a service account with the Exchange Application Impersonation role on the on-premises Exchange Server to access on-premises Exchange mailboxes.

If the user credentials of a service account are used for Exchange Online, contactSync requires the Exchange Application Impersonation role on Exchange Online for this service account to access Exchange Online mailboxes.

Exchange Application Impersonation enables a caller to impersonate a given user account. This enables the caller to perform operations by using the permissions that are associated with the impersonated account, instead of the permissions that are associated with the caller's account.

For more information, please have look at the following Microsoft Docs:

Impersonation and EWS in Exchange

https://docs.microsoft.com/en-us/exchange/client-developer/exchange-web-services/impersonation-and-ews-in-exchange

MSDN Library - Configuring Exchange Impersonation

https://docs.microsoft.com/en-us/previous-versions/office/developer/exchange-server-2010/bb204095(v=exchg.140)?redirectedfrom=MSDN

Exchange Impersonation in Exchange 2013, 2016, 2019 and Exchange Online

How can you check existing management role for Exchange Application Impersonation and how you can create a management role for Exchange Application Impersonation?

For on-premises Exchange:

Please log in on the on-premises Exchange Server with an Exchange Administrator account and open the Exchange Management Shell.

For Microsoft 365 Exchange Online:

Please connect via Exchange Online PowerShell to the Microsoft 365 tenant with an Exchange Administrator account.

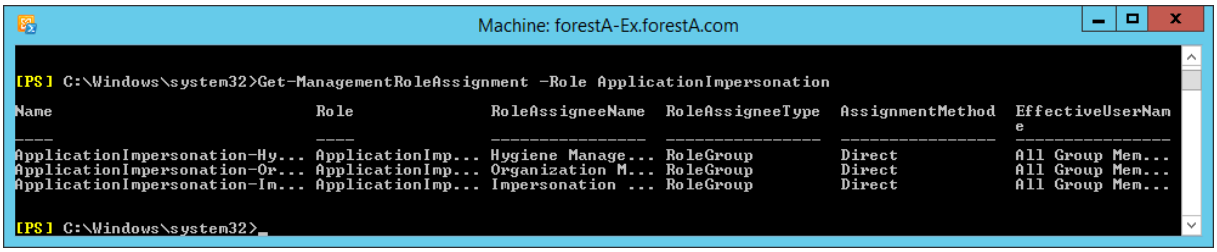
Check existing Exchange Impersonation:

Please verify whether a **Role Group** for **ApplicationImpersonation** exists.

You can check the existing Exchange Impersonation via PowerShell:

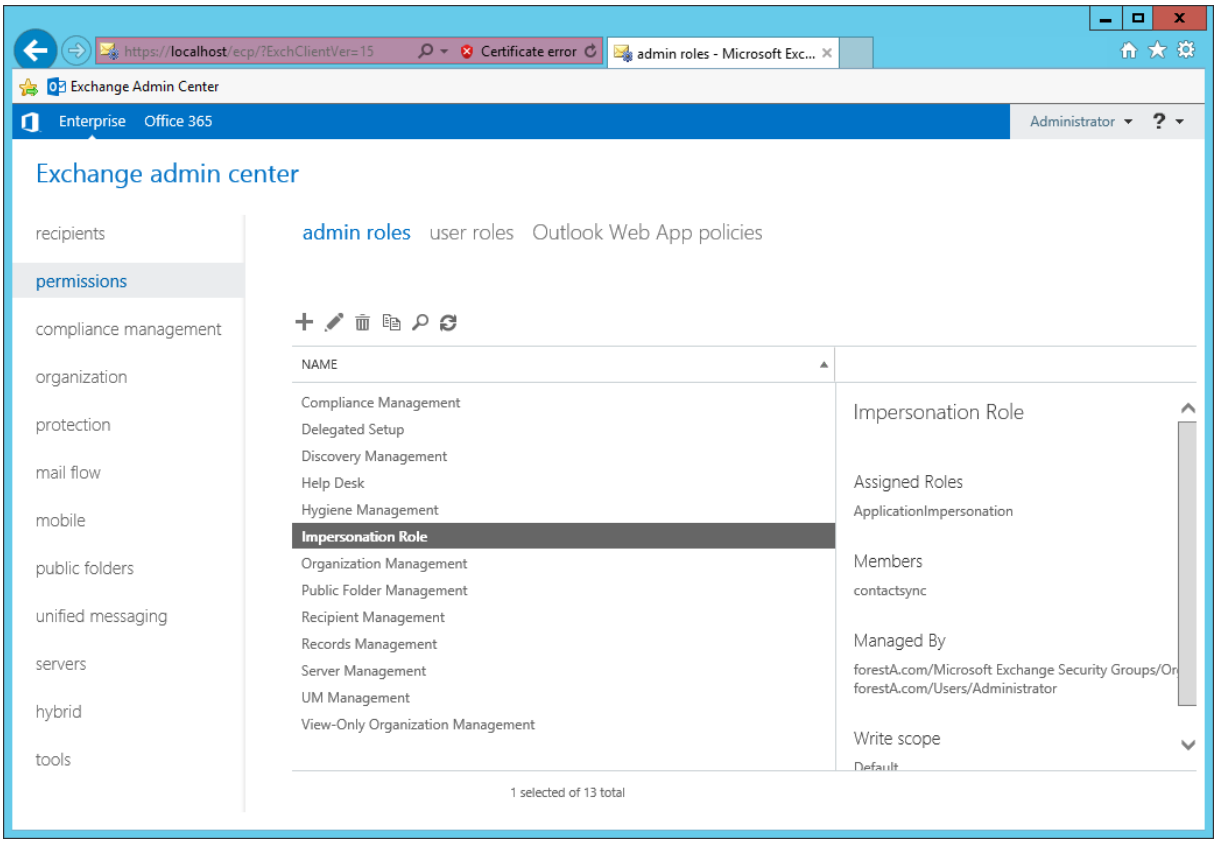
```
Get-ManagementRoleAssignment -Role ApplicationImpersonation
```

```
[PS] C:\Windows\system32>Get-ManagementRoleAssignment -Role ApplicationImpersonation
```



You can find an existing **Role Group** in the **Exchange Admin Center** under **Permissions** as **Admin Roles**.

E.g., the Impersonation Role to manage the **ApplicationImpersonation**

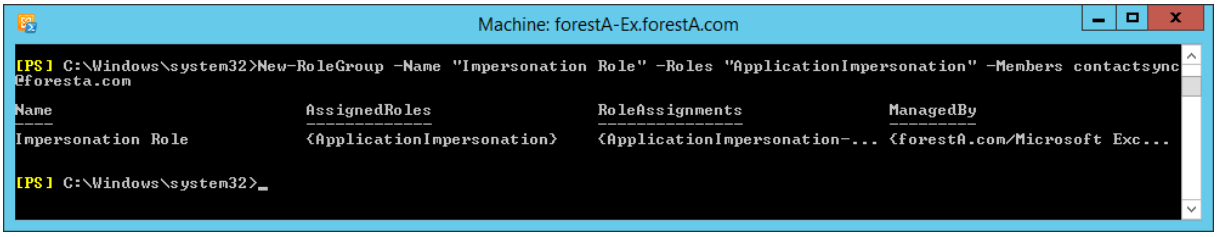


Create an Impersonation Role Group for ApplicationImpersonation via PowerShell

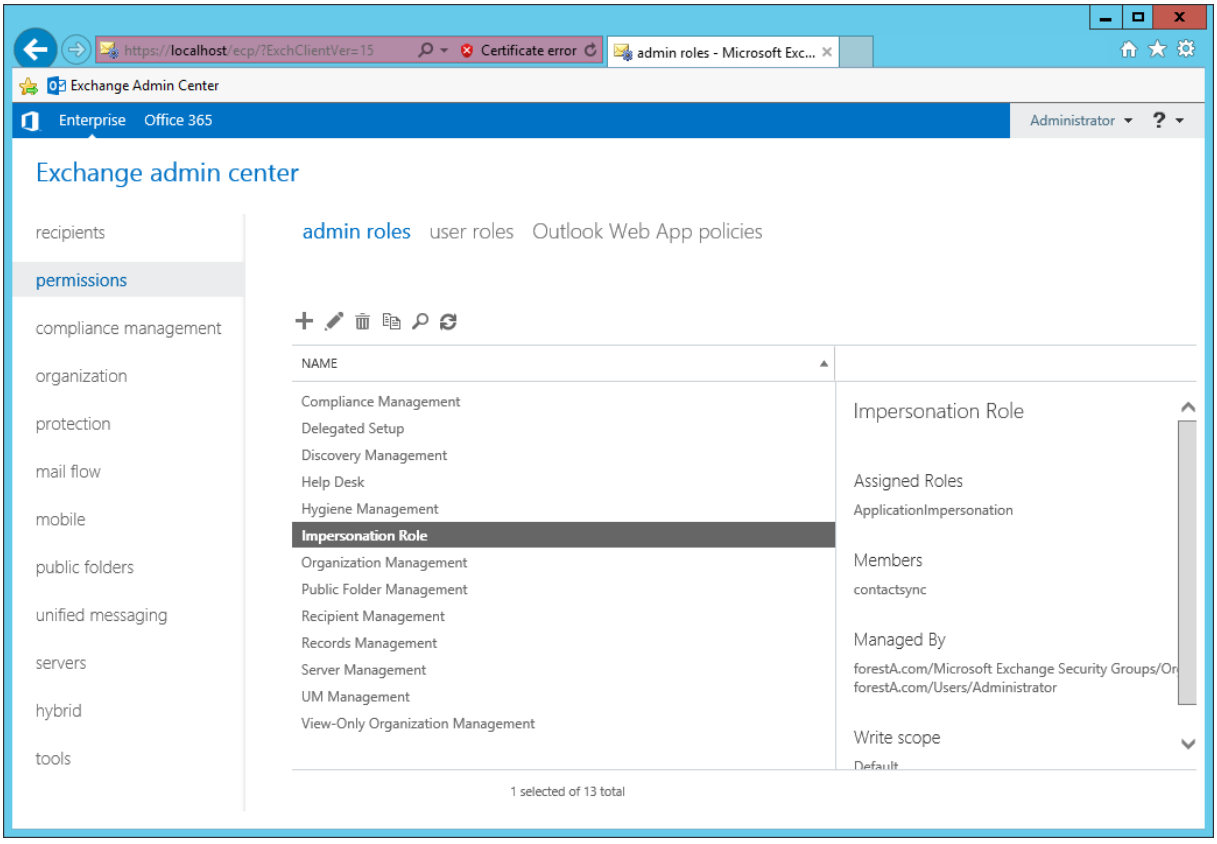
You can create a new Role Group to manage the **ApplicationImpersonation** and add your contactSync service account as member of the **Role Group**.

This example creates a **Role Group** called **Impersonation Role**:

```
New-RoleGroup -Name "Impersonation Role" -Roles "ApplicationImpersonation" -Members contactsync@foresta.com
```



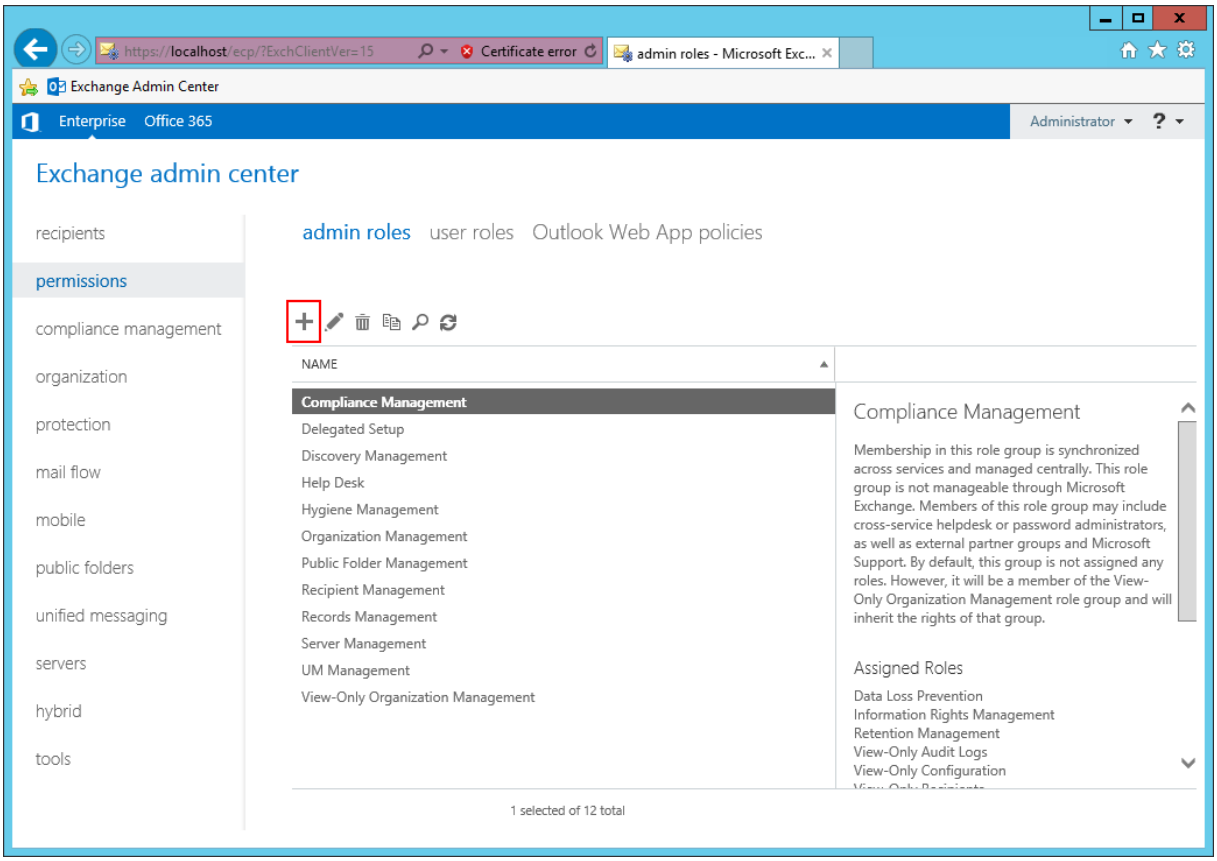
The **Impersonation Role** is also available in the **Exchange Admin Center** under **Permissions** as **Admin Roles**.



Create an Impersonation Role for ApplicationImpersonation via Exchange Admin Center

You can create a new **Role Group** in the **Exchange Admin Center** under **Permissions** as **Admin Roles**.

Add new admin role:

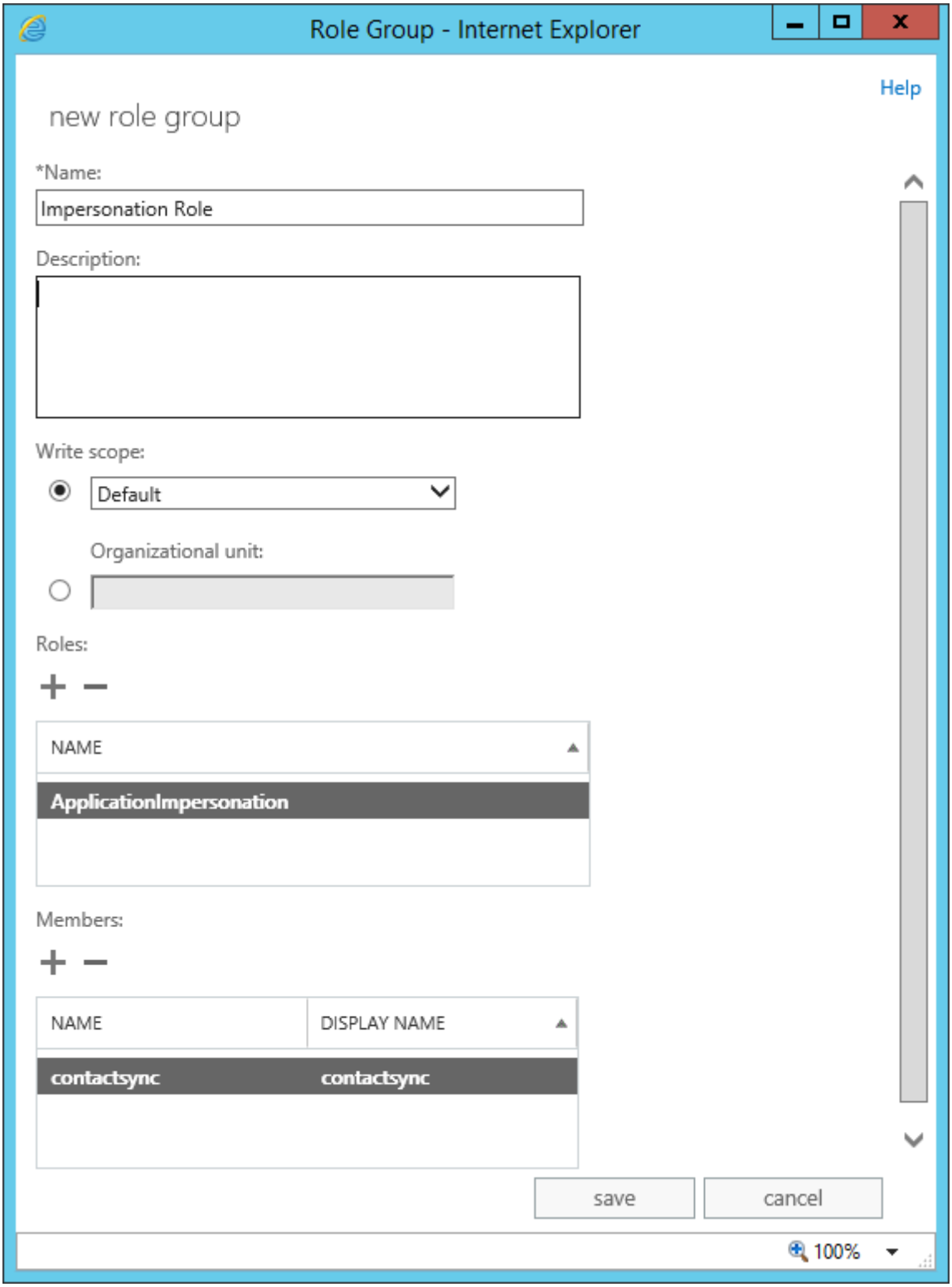


The **new role group** dialog:

Add the name **Impersonation Role**

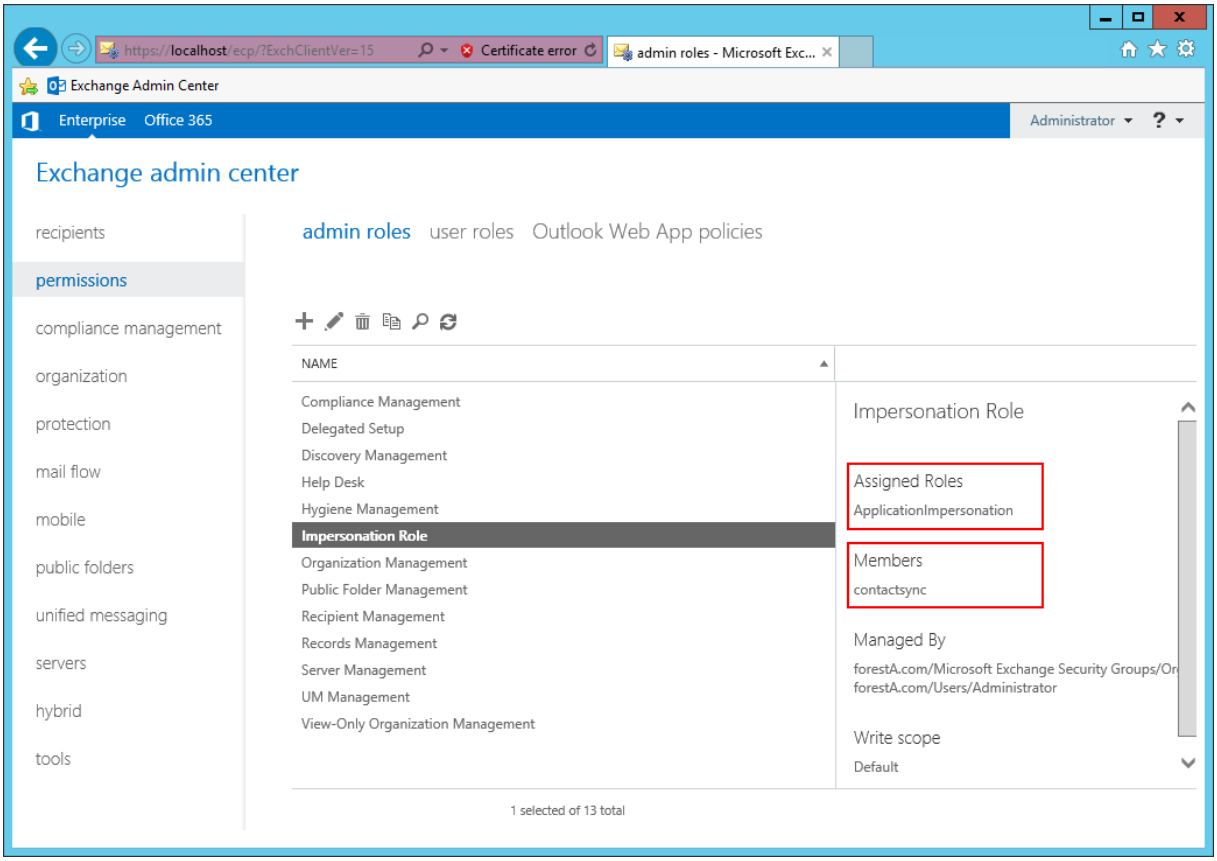
Add **ApplicationImpersonation** to the **Roles**

Add your **contactSync service account** to the **Members**



Afterwards the new **Impersonation Role** is available as **Admin Role**.

You can check the **Assigned Roles** and the **Members** of the **Impersonation Role**.



Support: What to do when I notice an error / bug?

We always try to provide a very responsive, solution orientated and effective support. Should you encounter any issue, bug or inconvenience please do not hesitate to contact us.

Please email us at support@netsec.de.

To enable us providing you the best quality support possible, please provide us with the following information:

Environment Overview

- Which Exchange version do you use?
- Which contactSync version do you use?
- Does the contactSync service account have an Exchange mailbox and where it is located?

Description of the issue

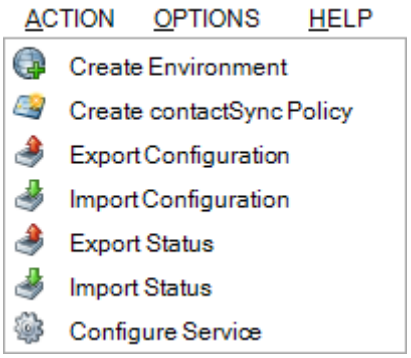
Please describe your issue/bug/inconvenience thoroughly, in detail, what you wanted to achieve and what you were doing as it occurred.
A screenshot of the issue often helps us to understand.

Configuration and log files

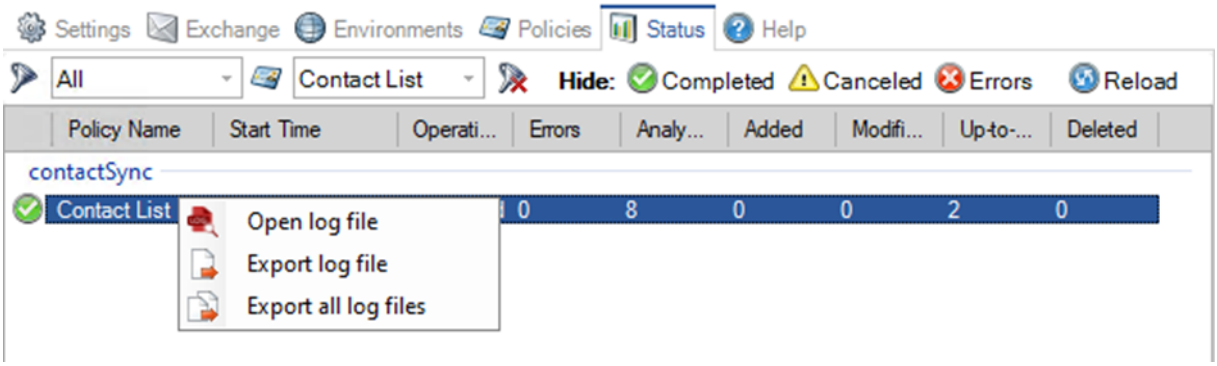
We also require the configuration and the logs, preferably zipped.

In menu **Action** -> **Export Configuration** you can zip the policies.

In menu **Action** -> **Export Status** you can zip the log files.



The log files of a policy can be also compressed on the **Status** tab:



Please send an email to support@netsec.de with a description of the issue and attach the compressed file with the configuration and the compressed file with the log files.

Alternatively, you could also upload the compressed files for us at the
NETsec Support Dropzone

https://transfer.netsec.de/dropzone/support

Do you have more questions or need further support? Please do not hesitate to contact the contactSync Support Team.

contactSync Support Team

By phone +49 2421 998 78 16 or via e-mail support@netsec.de