Hosted ClockWork Office365 Sync – OAuth 2.0

(Formerly known as Outlook Sync)

Contents

Summary

ClockWork's Office365 Sync (Formerly known as Outlook Sync) uses OAuth 2.0 for connecting to your Exchange Online. Note that OAuth 2.0 only supports Exchange Online and will not work with on-premises Exchange Servers.

Delegate Account Mailbox

We will need a delegate mailbox, to impersonate a user's calendar. This must be a regular user mailbox, that has a calendar folder. ClockWork does not need the credentials for the account, only the email address. This account must be in the same location as the user's mailboxes.

Technical Reference:

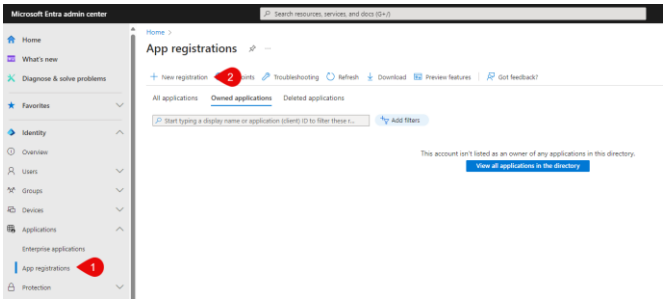
Note: The fast sync uses the delegate account for syncing, the slow sync uses the user's account for syncing.

Authenticate an EWS application by using OAuth | Microsoft Docs

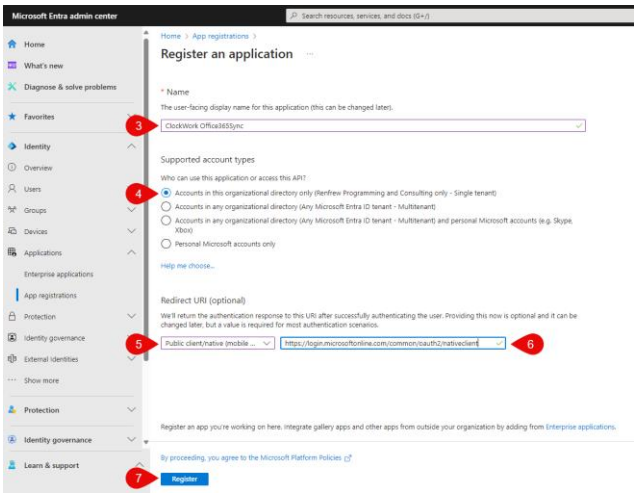
Register your ClockWork Office365 Sync App with Entra ID

Start by browsing to https://entra.microsoft.com and login

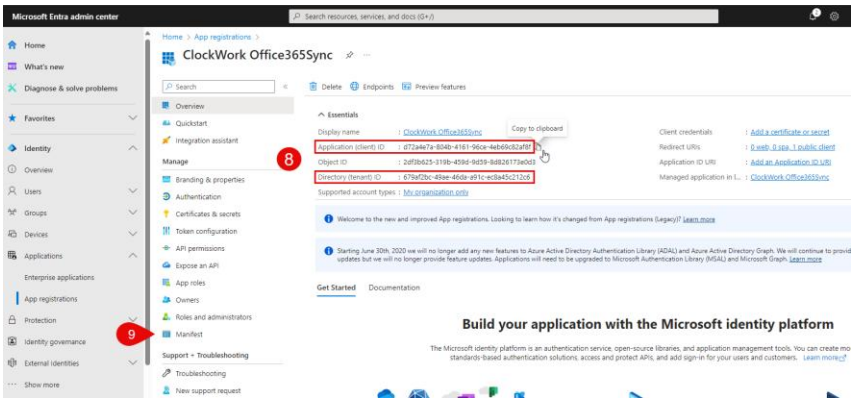
1. Click on **App registrations.**
2. Click **+ New registration**.



3. Enter the ***Name***
    a. Suggested: ClockWork Office365Sync
4. Select **Accounts in this organizational directory only (Single tenant)**
5. Set Redirect URI to: **Public client/native (mobile & desktop)**
6. Set the value for the URI to: **https://login.microsoftonline.com/common/oauth2/nativeclient**
7. Click **Register**



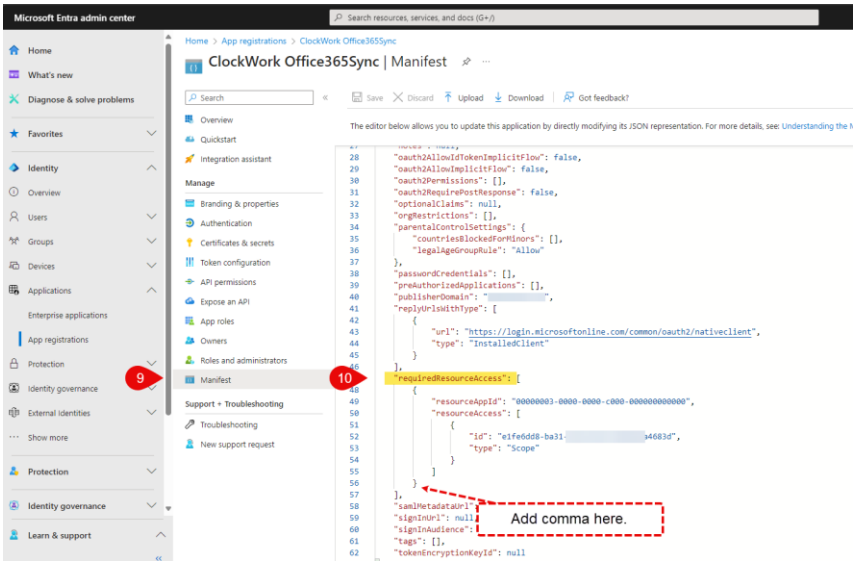
8. Copy the ***Application (client) ID***, and ***Directory (tenant) ID***, these will be needed by ClockWork.



9. Select **Manifest**
10. Locate the ***requiredResourceAccess*** property in the manifest,
11. Add a ***comma*** to the last curly brace, inside the square brackets ([])
12. Paste the following after the comma, inside the square brackets ([]).

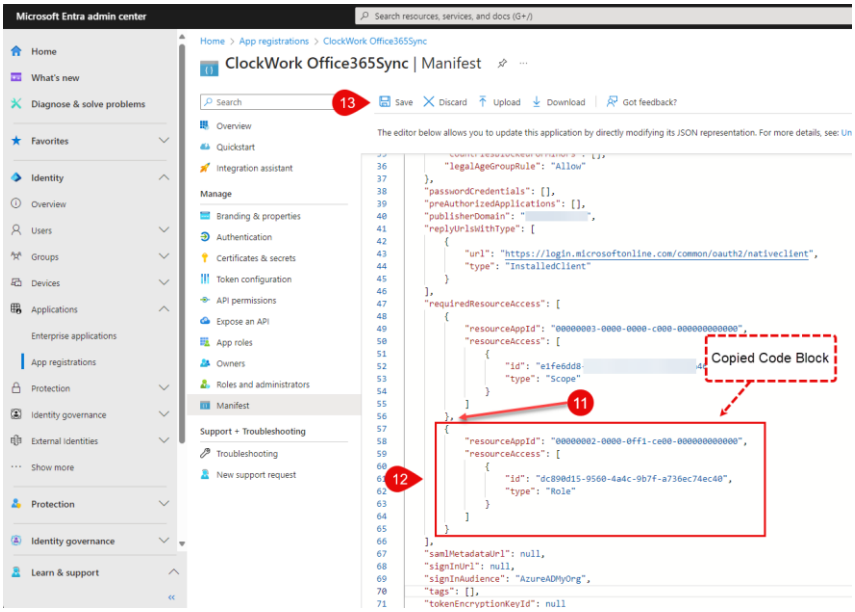
```
{
    "resourceAppId": "00000002-0000-0ff1-ce00-000000000000",
    "resourceAccess": [
        {
            "id": "dc890d15-9560-4a4c-9b7f-a736ec74ec40",
            "type": "Role"
        }
    ]
}
```

Before:



After:

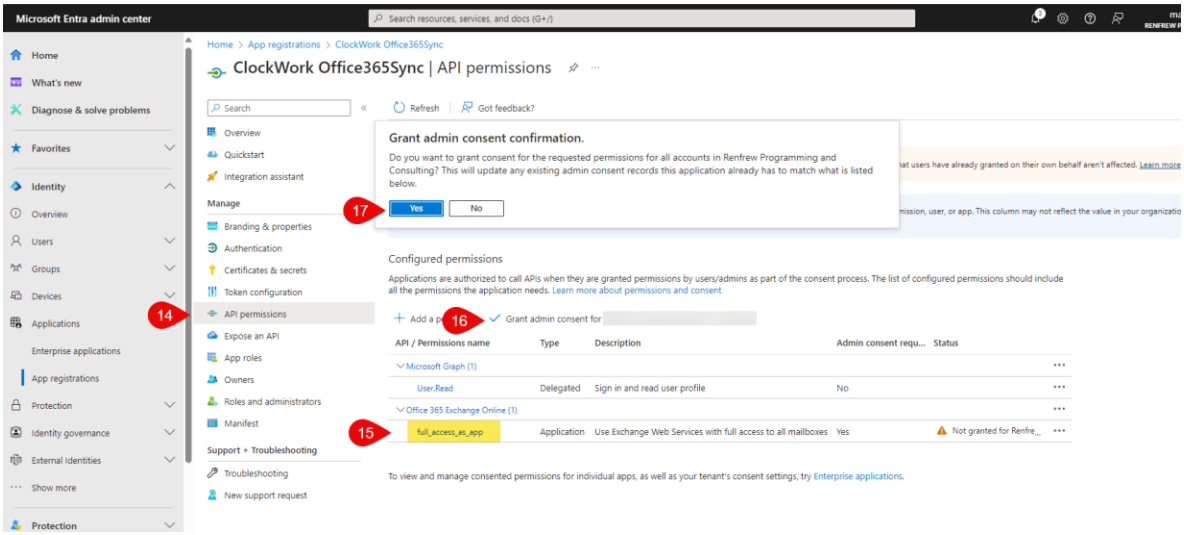
*Note: If viewing at another time, Entra ID may change the order to alphabetical, so the new entry may be at the top.



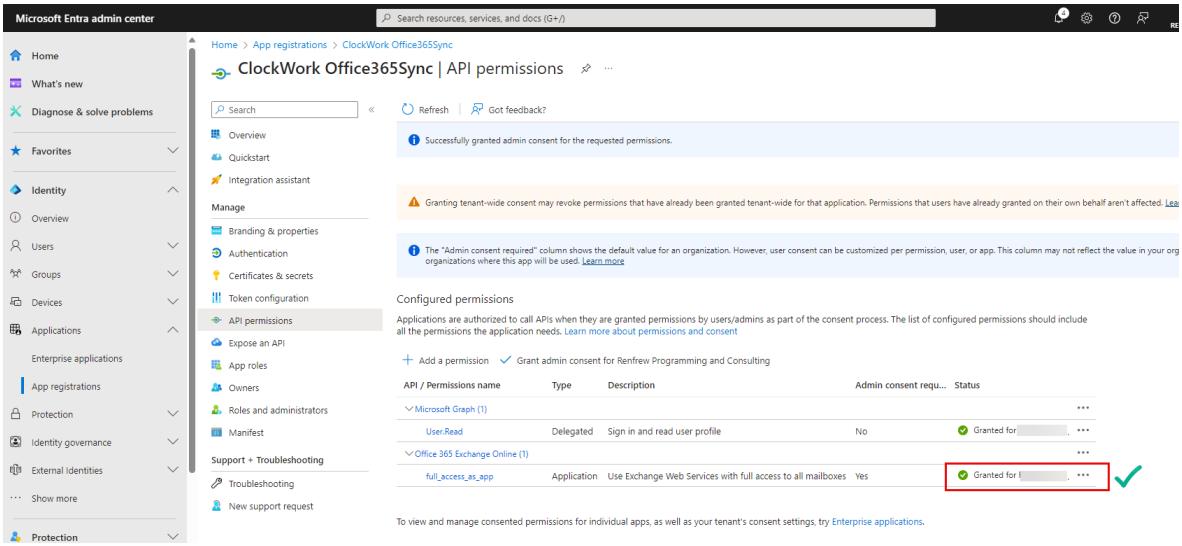
13. Click **Save**

14. Select **API permissions** under the ***Manage*** section.
15. Confirm ***full_access_as_app*** permission is listed.
16. Click **Grand admin consent for [*YourOrganizationName]***
17. Click **Yes** to grant consent.

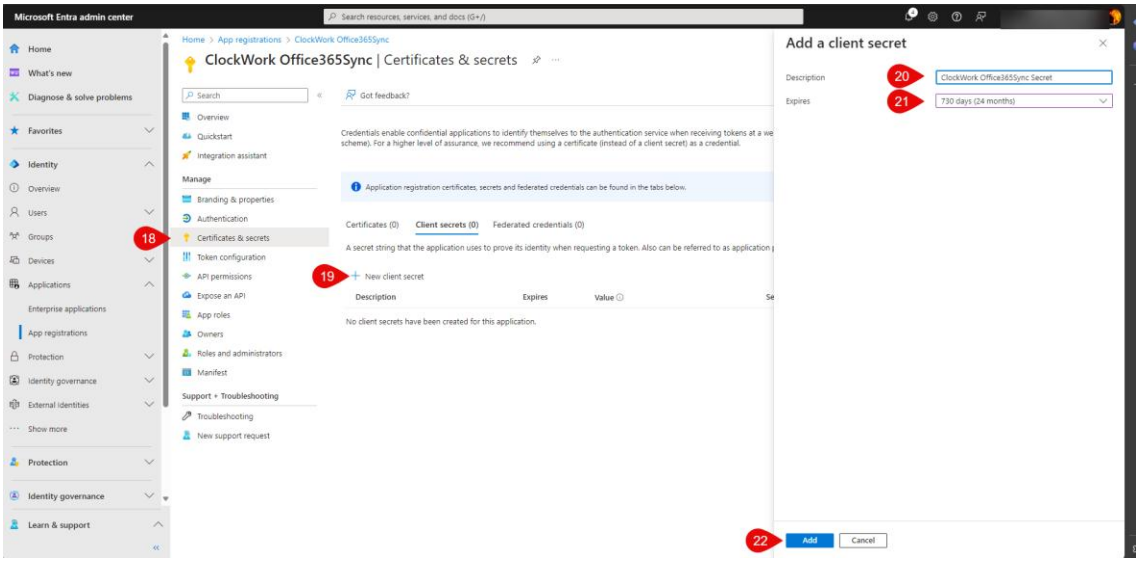
Before:



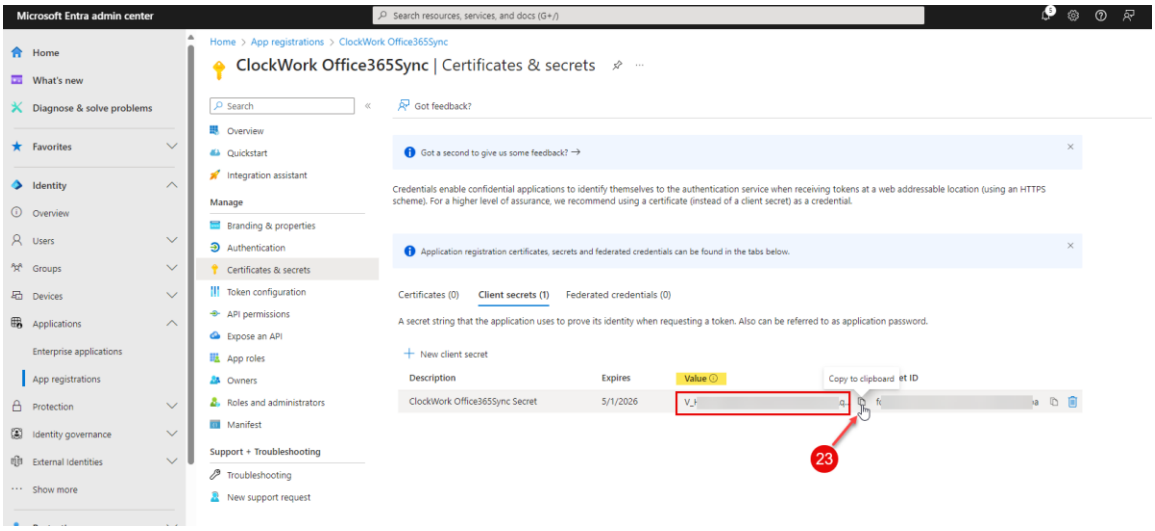
After:



18. Select **Certificates & secrets** on the left side, in the **Manage** section.
19. Click **+ New client secret**
20. Enter the description of your choosing.
    a. Suggested name: *ClockWork Office365Sync Secret*
21. Select an *expiry date*, according to your school's policies
    a. Suggested is 24 months.
    b. Important: You will need to manually create a calendar appointment as a reminder for yourself to create a new secret before this secret expires. There is no automatic reminder, and the appointments will just stop syncing.
22. Click **Add**



23. Copy the secret's ***Value***, this will be needed by ClockWork.
    a. *Note: Once you leave this screen, you will not be able to copy the secret again. You will need to create a new secret.



Restricting Application Access in Exchange Online

Summary

With support for Application Access Policies in EWS, administrators can ***optionally*** limit an AppOnly app's access to a specific set of mailboxes by specifying an inclusion or exclusion list. Exchange Administrators who want to limit a 3rd party application access to a specific set of mailboxes can use the *Application Access Policy* PowerShell cmdlets to configure access control.

Note: This is optional, and you must be an Exchange Administrator to use the PowerShell cmdlets. Any changes in Exchange Online may take up to 4 hours to replicate in Microsoft's Exchange Online environment before they will take effect.

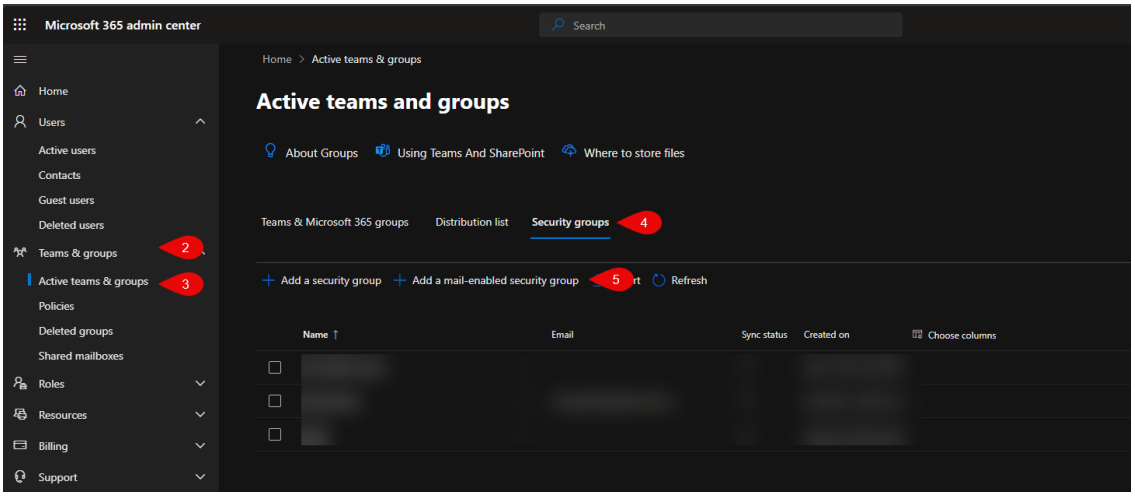
Technical References:

Limiting application permissions to specific Exchange Online mailboxes | Microsoft Docs

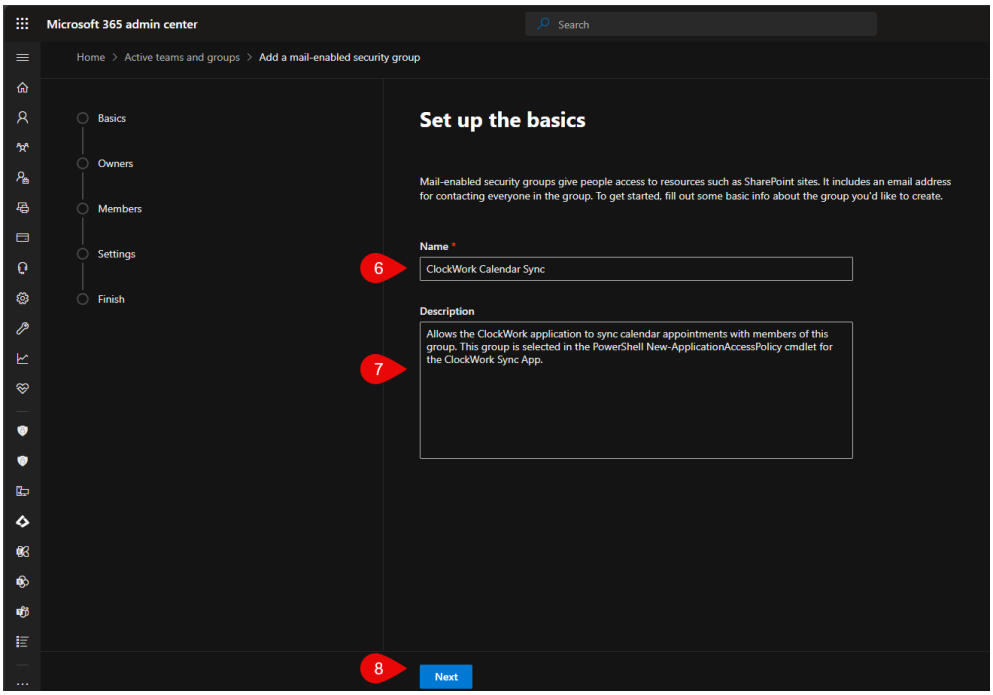
Instructions – Example

Create the Mail-Enabled Security Group

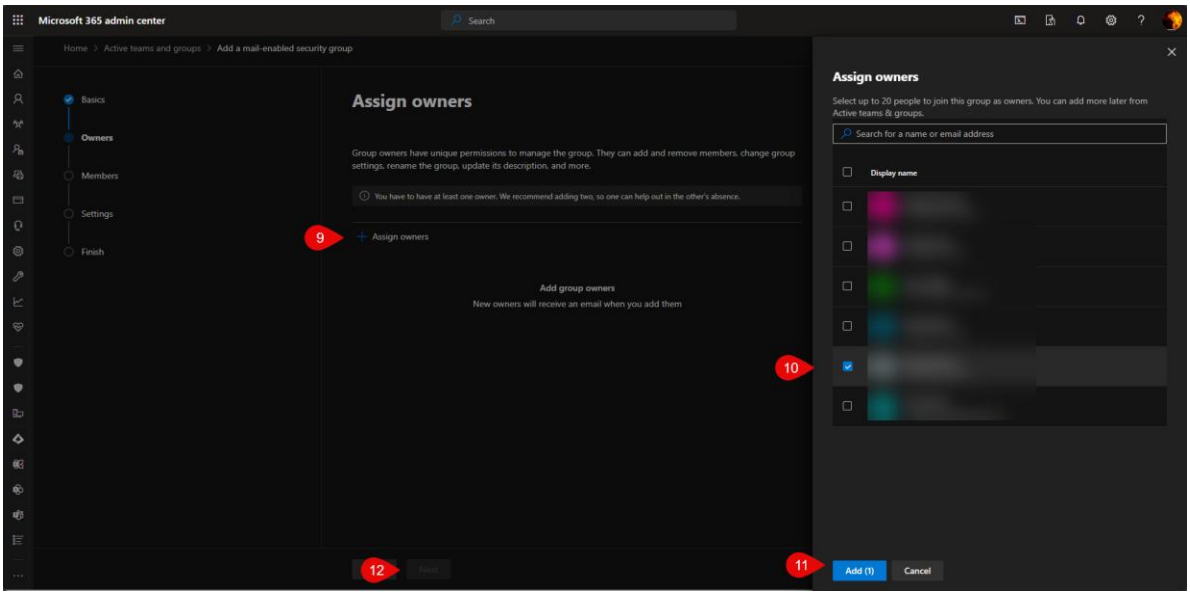
1. Login to the **Microsoft 365 admin center**
2. Click to expand **Teams & groups.**
3. Click to select **Active teams & groups.**
4. Select the ***Security groups*** tab.
5. Click **Add a mail-enabled security group.**



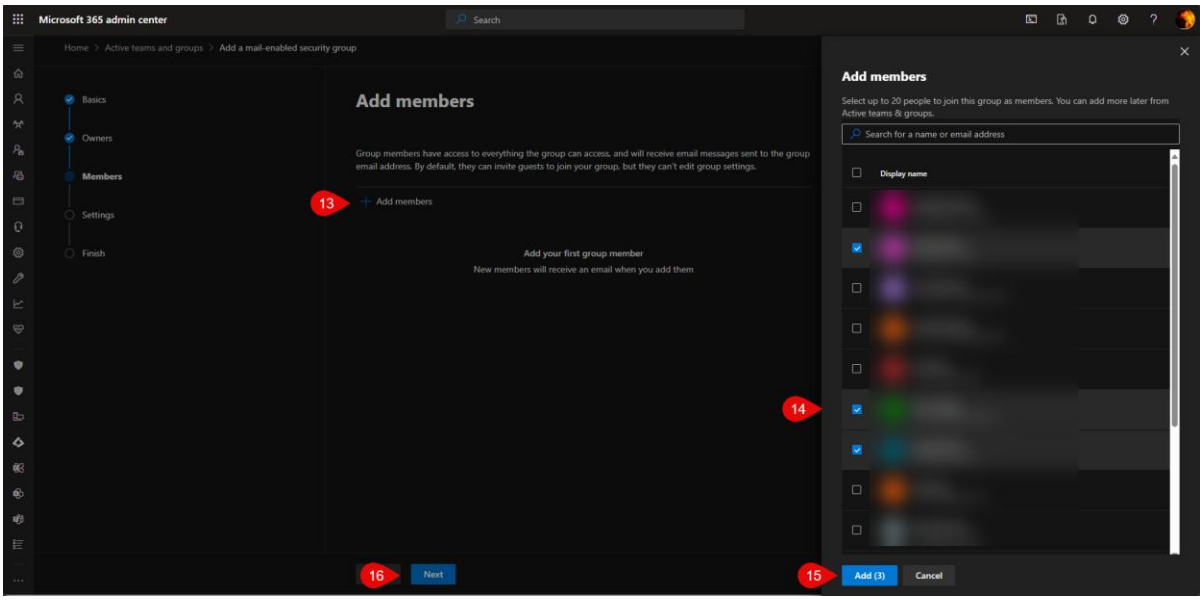
6. Enter a name for the group.
    a. Suggested: ClockWork Calendar Sync
7. Enter a description for the group.
8. Click **Next**



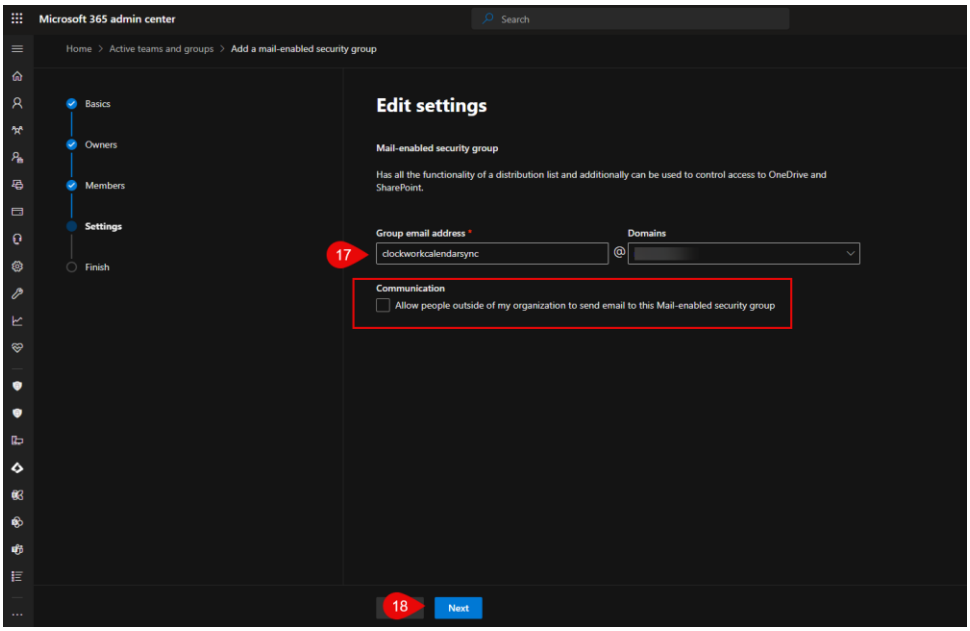
9. Click **+ Assign owners.**
10. Select the owners, who will be managing this group.
11. Click **Add**
12. Click **Next**



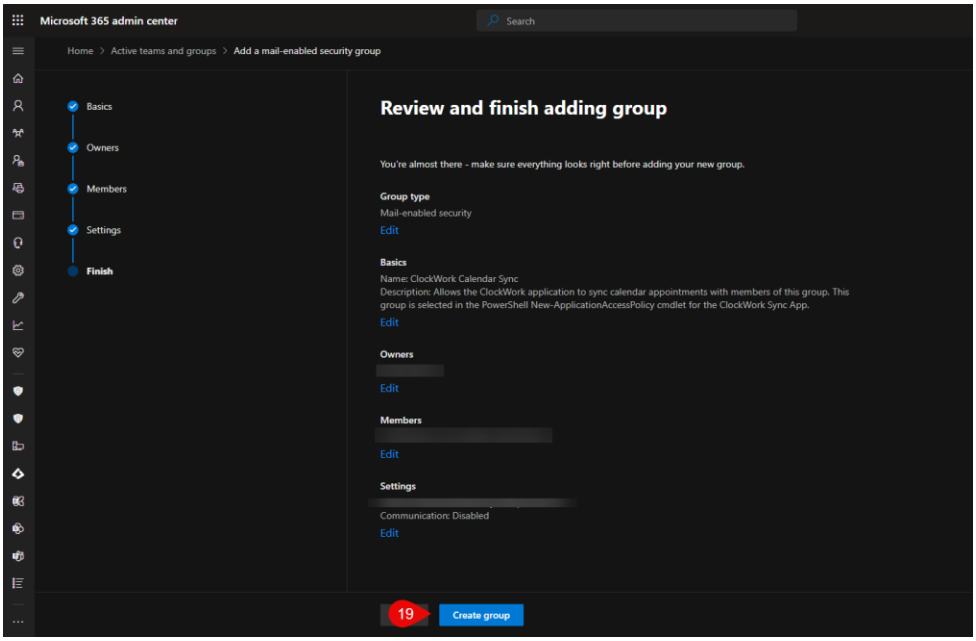
13. Click **+ Add members.**
14. Select all the ClockWork staff accounts that need to sync their ClockWork calendars.
    a. NOTE: The delegate mailbox must also be a member of this group
15. Click **Add**
16. Click **Next**



17. Enter the email address for this group.
    a. You normally should NOT allow people outside of your organization to send emails to this group.
18. Click **Next**



19. Review the information, if it is correct click **Create Group**



Run the PowerShell Cmdlet

You need to be assigned permissions before you can run these cmdlets. Although this topic lists only some parameters for the cmdlets, you may not have access to the parameters if they're not included in the permissions assigned to you. To find the permissions required to run any cmdlet or parameter in your organization, see Find the permissions required to run any Exchange cmdlet.

Note: Do NOT include the angle brackets in the parameters below (< >)

1. **Microsoft officially only supports Exchange PowerShell modules running on PowerShell 7 or higher**.
   a. Install PowerShell 7 Reference: Installing PowerShell on Windows - PowerShell | Microsoft Learn
2. Make sure *ExchangeOnlineManagement* PowerShell module is installed on the computer:
   a. Reference: Install the Exchange Online Management PowerShell Module | Microsoft Learn
3. Import the Exchange Online PowerShell Module

   Cmdlet:

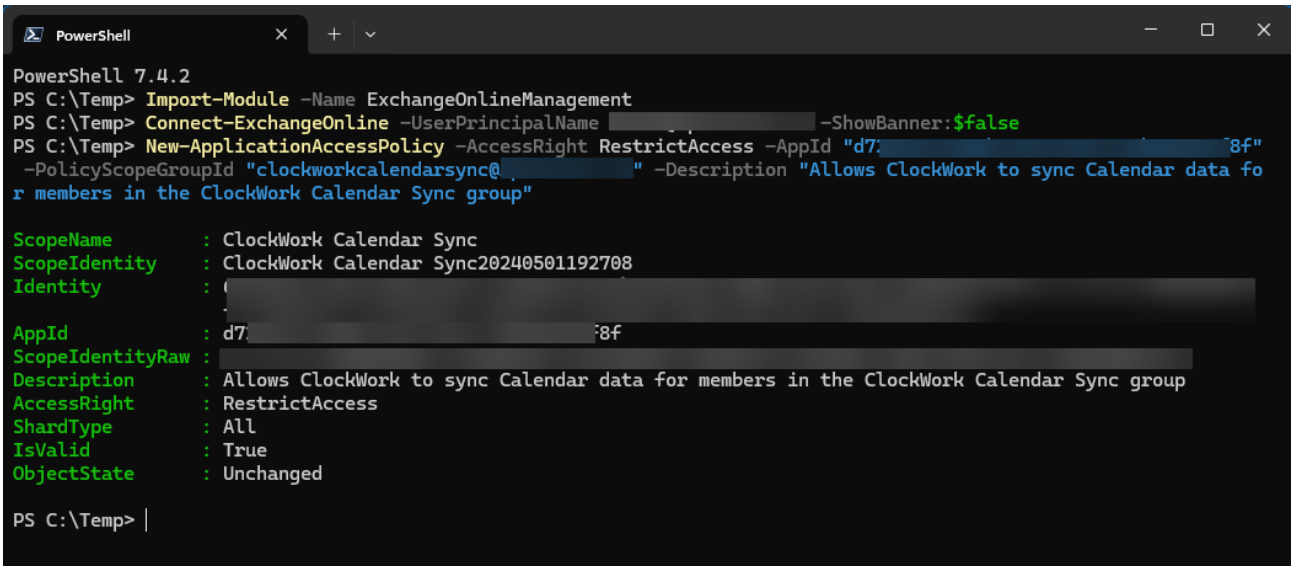
   ```
   Import-Module -Name ExchangeOnlineManagement
   ```

4. Connect to your Exchange Online
   a. Cmdlet:

   ```
   Connect-ExchangeOnline -UserPrincipalName "<your email address>"
   ```

5. Run the **New-ApplicationAccessPolicy** cmdlet:
   a. **Note:** The command below is using the PowerShell *ExchangeOnlineManagement* module version 3.4.0 with PowerShell 7.4.2

   ```
   New-ApplicationAccessPolicy -AccessRight RestrictAccess -AppId "<your Application (client) Id from above>"
   -PolicyScopeGroupId "<your mail-enabled security group email address>" -Description "Allows ClockWork to
   sync Calendar data for members in the ClockWork Calendar Sync group"
   ```



References:

- Connect to Exchange Online PowerShell | Microsoft Learn
- New-ApplicationAccessPolicy (ExchangePowerShell) | Microsoft Docs

Troubleshooting PowerShell Cmdlets

Application PowerShell Commands

Get-ApplicationAccessPolicy

This will show all the Application Access Policies you have on your Exchange Server.

Get-ApplicationAccessPolicy -Identity <Your ***Identity*** from above>

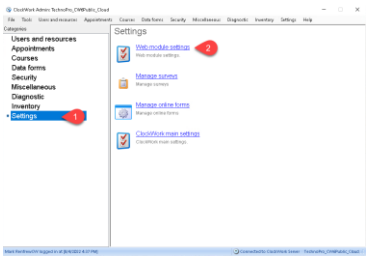
This will show the Application Access Policy you have created above.

Summary of Information Needed for ClockWork

1. Application (client) ID (on page 4)
2. Directory (tenant) ID (on page 4)
3. App secret's value (on page 7)
4. Delegate email address

ClockWork Admin Settings

1. Click Settings
2. Click Web module settings



3. **Application Sync Version:** Exchange2013_SP1
4. **Authentication type:** Office365OAuth2
    a. **Note:** ***Application Sync Version*** is not used for OAuth2 and can be ignored.
    b. **Note:** If using basic authentication, for on-premises Exchange, then set to: LegacyBasicAuthentication
5. **Sync Service Url:** https://outlook.office365.com/EWS/Exchange.asmx
6. Under Exchange Legacy Authentication settings:
    a. **Application Sync Legacy Authentication Delegate Username:** Delegate email address
7. Under the Office365 Authentication settings:
    a. **Office 365 Authentication Application Id:** *Application (client) ID (on page 4)*
    b. Office 365 Authentication Client Secret: *App secret's value (on page 7)*
    c. Office 365 Authentication Tenant Id: *Directory (tenant) ID (on page 4)*
8. Set the **ClockWork users to sync** as normal.