Office 365 Connection Manager

https://campus.barracuda.com/doc/94536707/

Use the Office 365 Configuration Manager to link your Office 365 account to Barracuda PhishLine, so you can import data into a Barracuda PhishLine address book.

The information pulled from Office 365 is users in your Office 365 account – which corresponds with users in your organization. This is not the same as contacts in an address book.

Required Access Level

To create the connection, you must have at least `User.Read.All` permissions, an elevated level of access, in the Office 365 account. If you do not have the adequate access, a screen from Microsoft instructs you to submit the form to ask your organization's Office 365 Administrator for updated credentials. Your Office 365 Administrator can either accept or deny your request. In either case, you will will receive an email from Microsoft. If your request was accepted while you were in the middle of the procedure described below, restart this procedure.

Creating a Connector

To create a connector:

1. Navigate to **System > Office 365 Connection Manager**. Then click **New**.
2. Click **Connect to Office 365**. If you are not already logged into your Office 365 account, you will be prompted to log in.
3. Click **Accept** to accept the permissions requested by Microsoft. If you see a notice from Microsoft about credentials, refer to the note about Required Access Level above. If you receive new credentials at this point, you must restart the process.
4. Look for the green **Success** message banner, showing that you created your connection successfully. The page displays sample data from your Office 365 account so you can verify that the imported data looks accurate.
5. Click **Create an Address Book** to continue the process.

You can create more than one connector.

Currently, you cannot edit or delete connectors.

This information is also described in How to Create an Address Book.

Importing Criteria

Barracuda PhishLine imports *all enabled user accounts* that meet the following criteria:

- Users must have a valid email address (not including @onmicrosoft.com email addresses)
- Users must have an email address that uses a domain that is authorized in Barracuda PhishLine. (See Domain Authorization.)
- The account is *not* an external or guest account.
- The account has an active, provisioned Exchange plan.

Omitting Users from Campaigns

Depending on how you have configured Office 365, the imports above might include some items that you do not want to include in phishing campaigns (e.g., service accounts, conference rooms).

After the users are imported, edit the address book to deactivate any users you do not want to include in your campaigns. Refer to How to Edit an Address Book for details.

Corresponding Fields in Office 365 and Barracuda PhishLine

The following fields are selected from Office 365 and correspond to the following Barracuda PhishLine fields:

Office 365	Barracuda PhishLine
Mail	Email Address
GivenName	First Name
Surname	Last Name
DisplayName	Full Name
JobTitle	Organization Level
OfficeLocation	Site/Location
MobilePhone	Mobile Phone; Phone Note that the Mobile Phone Number is used for both the **Mobile Phone** and **Phone** fields.
PreferredLanguage	Language Code

This information is also shown in How to Edit an Address Book.

Office 365 Credentials and Permissions

Keeping Your Credentials Safe

Barracuda PhishLine does not use – or know anything about – your Office 365 password. The Office 365 Connection Manager uses the OAuth2 specification, which is specifically designed to keep your credentials safe from third-party vendors. When you create the connection, you agree to share specific Microsoft data with Barracuda PhishLine. With OAuth2, only that data is shared – no other use of your account is allowed.

Changing Your Password

Given this connection method described above, you can change your Office 365 password at any time without affecting Barracuda PhishLine.

Required Permissions/Scopes

Any Office 365 account can use the Office 365 Connection Manager, as long as it has the required permissions (sometimes referred to as *scopes*). If your account lacks any of these permissions, the Office 365 Connection Manager will help you to submit a request to your organization's Office 365 administrator.

Office 365 permissions/scopes required to use the Office 365 Connection Manager:

- openid
- profile
- offline_access
- user.read
- mailboxsettings.read
- user.readbasic.all
- user.read.all