

## Microsoft 365 Connection Manager

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

Use the Microsoft 365 Configuration Manager to link your Microsoft 365 account to Security Awareness Training, so you can import data into a Security Awareness Training address book.

The information pulled from Microsoft 365 is users in your Microsoft 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 Microsoft 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 Microsoft 365 Administrator for updated credentials. Your Microsoft 365 Administrator can either accept or deny your request. In either case, you 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.

### Default Field Mapping

By default, there is a default mapping of standard Microsoft 365 to Security Awareness Training fields, as shown in the table below.

You can configure your own column mapping between your Microsoft 365 data and Security Awareness Training fields, described later in this article. If you choose not to customize mapping, the default values are used.

Note that if you are customizing the field mapping, you *must* map the email address field.

### Data Mapped between Microsoft 365 Data Source and Security Awareness Training Fields

| Microsoft 365 Field Name | Security Awareness Training Mapping |
|--------------------------|-------------------------------------|
| Mail                     | Email Address                       |
| GivenName                | First Name                          |
| Surname                  | Last Name                           |
| DisplayName              | Full Name                           |

|                    |                       |
|--------------------|-----------------------|
| JobTitle           | Personal Title        |
| EmployeeHireDate   | Hire Date             |
| ManagerDisplayName | Manager Name          |
| ManagerMail        | Manager Email Address |
| Department         | Organization Area     |
| EmployeeType       | Organization Level    |
| MobilePhone        | Mobile Phone          |
| MobilePhone        | Phone                 |
| CompanyName        | Company Name          |
| Country            | Country               |
| OfficeLocation     | Site/Location         |
| PreferredLanguage  | Language Code         |
| StreetAddress      | Street Address        |
| City               | City                  |
| State              | State                 |
| PostalCode         | Zip Code              |

For connectors created before the **May 9, 2022** release, the following fields are selected by default from Microsoft 365 and correspond to the following Security Awareness Training fields.

**Note** that if all field mapping rows are deleted on a connector created after the May 9, 2022 release, this default mapping will be used.

| Microsoft 365 Field Name | Security Awareness Training Mapping  |
|--------------------------|--|
| Mail                     | Email Address  |
| GivenName                | First Name   |
| Surname                  | Last Name  |
| DisplayName              | Full Name  |
| JobTitle                 | Personal Title   |
| OfficeLocation           | Site/Location  |
| MobilePhone              | Mobile Phone; Phone<br>Note that the Mobile Phone Number is used for both the <b>Mobile Phone</b> and <b>Phone</b> fields. |
| PreferredLanguage        | Language Code  |

This information is also shown in [How to Edit an Address Book](#).

---

### Creating a New Connector

---

To create a connector:

1. Navigate to **System > Microsoft 365 Connection Manager**. Then click **New**.
2. Click **Connect to Microsoft 365**. If you are not already logged into your Microsoft 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 Microsoft 365 account so you can verify that the imported data looks accurate.
5. Click **Create an Address Book** to continue the process, or click **Edit Configuration** to make changes to the connector before you create an address book. Use the **Edit Configuration** page to block specific email addresses from being retrieved from Microsoft 365 and to add or delete fields retrieved from Microsoft 365.

You can create more than one connector.

### Importing Criteria

---

Security Awareness Training 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 Security Awareness Training. (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 Microsoft 365, the imports above might include some items that you do not want to include in phishing campaigns (e.g., service accounts, conference rooms).

Before the users are imported, edit the configuration and add specific email addresses to the Email Block List.

---

## Deleting a Connector

---

### Important:

- Deleting an Microsoft 365 Connector is permanent. You cannot undo this process.
- If a connector is associated with an address book, you will not be able to update the address book using automated import.  
Within the address book, you can still add and edit entries as described in [How to Edit an Address Book](#).


To delete a connector:

1. Navigate to **System > Microsoft 365 Connection Manager**.
2. Locate the connector you want to delete. Click the delete (X) button for that row. Confirm that you want to delete that connector.  
To proceed without deleting, click the Back button on your browser.

## Mapping Microsoft 365 Fields

---

Complete the section above, [Creating a New Connector](#), before proceeding with these steps.

1. Click the **Attribute Configuration** button when viewing your new Microsoft 365 Configuration. The Attribute Configuration page displays the default mappings from the Security Awareness Training Address Fields to the Microsoft 365 Attributes.
2. **To create a new field mapping**, click **New**.
  1. Select an Address Book field and then an Microsoft 365 Attribute to create the mapping. Click **Save**.
  2. Repeat this process for each new mapping.
  3. Click **Return to the Microsoft 365 Configuration Manager** to continue.
3. **To edit a field mapping**, click the edit pencil icon  for that mapping.
  1. Select the appropriate fields to map. Click **Save**.
  2. Repeat this process for each new mapping.
  3. Click **Return to the Microsoft 365 Configuration Manager** to continue.
4. After you complete your configuration, you can create an Address Book. Refer to [How to Create an Address Book](#).

## Microsoft 365 Credentials and Permissions

---

## Keeping Your Credentials Safe

Security Awareness Training does not use – or know anything about – your Microsoft 365 password. The Microsoft 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 Security Awareness Training. 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 Microsoft 365 password at any time without affecting Security Awareness Training.

## Required Permissions/Scopes

Any Microsoft 365 account can use the Microsoft 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 Microsoft 365 Connection Manager will help you to submit a request to your organization's Microsoft 365 administrator.

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

- openid
- profile
- offline\_access
- user.read
- mailboxsettings.read
- user.readbasic.all
- user.read.all

## Figures

1. editButton.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.