LDAP/AD Configuration Manager

https://campus.barracuda.com/doc/79465243/

Use the LDAP Configuration Manager to customize your LDAP or Active Directory data import into a Security Awareness Training address book.

Using this tool is optional. It is not required for importing data into a Security Awareness Training address book. Refer to How to Create an Address Book for:

- basic information on importing address book data
- a standard list of LDAP column attributes pulled for import

Note for Azure AD Users

The instructions in this article are for *on-premises* Active Directory.

To set up Security Awareness Training using Azure Directory, you must configure Azure AD Domain Services. Refer to the following links for details:

- https://docs.microsoft.com/en-us/azure/active-directory-domain-services/configure-ldaps
- https://docs.microsoft.com/en-us/azure/active-directory-domain-services/active-directory-ds-admin-guide-configure-secure-ldap-enable-ldaps

Default Field Mapping

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

You can configure your own column mapping between your LDAP 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 LDAP Data Source and Security Awareness Training Fields

LDAP Field Name	Basic Description	Security Awareness Training Mapping
mail	email address	Email Address
sn	surname/last name	Last Name
givenname	given name/first name	First Name
displayname	usually first name + last name; alternatively, a nickname	Full Name
title	professional title	Personal Title
physicaldeliveryofficename	physical address of the office for this individual	Site
st	state	State
l	locale, like city	City
co	country	Country
department	department, like sales or marketing	Organization Area
company	company name	Company
division	a section or business unit of an organization	Organization Level

Creating a New Configuration

To use LDAP/AD Configuration Manager:

1. From the **System** menu, select **LDAP/AD Configuration Manager**.
2. Click **New**.
3. Enter the **Configuration Name** for the data source.
4. Specify the **User Name**. If you do not know the full User Name, use a tool like *dsquery* to find it.
5. The password for your LDAP user. It is not displayed here for security reasons. If you are not changing the password, leave this field empty. To change the password, enter the new password here. When you click **Save**, if a password has been entered, it will update in your LDAP/AD configuration record.
6. Specify the address of the LDAP server in the form shown in this example: `ldap.barracuda.com`
7. Specify the **Port**. The port is usually 636, unless you have permission to use a different port. See more about this port below in the "Configuring Access to your Firewall" section.
8. Specify the **Method**. Choose the more secure **LDAPS**, unless you have a specific need to use the less secure **LDAP**.
9. Specify the **Distinguished Name**, separating the standard sections with commas, as shown in this example: `ou=Users,ou=longnamehere,dc=barracuda,dc=com`
10. To select only certain parts of your data source to import, select an option in the **Search Filter**

Options menu. Its corresponding code is automatically entered in the **Search Filter** box below. You can only alter the filter code if you choose the **Other** option.

- **All Active Users (Microsoft Active Directory Only)** – Selects only the active users from your LDAP source.
- **All Users (Microsoft Active Directory Only)** – Selects all users from your LDAP source, regardless of their active/inactive status.
- **Everything** – Selects all data from the LDAP source you specify. Does not use the Microsoft-specific classifiers found in the other filter choices.
- **Other - Enter below** – Use this selection to create your own customized filter. Enter your filter code in the Search Filter box below. Note that your syntax must be exactly correct. See the section below for additional information about search filters.

11. In the **Email Block List**, specify any emails you know you will never be a part of a campaign. For example, you might enter emails for the head of your organization, your support center email, or other.
12. After you complete all of the fields, click **Test Configuration**.
    - If your test completes successfully, the LDAP attributes detected are stored, and basic configurations such a email, name fields, and address data will be mapped by default.
    - If there is an error, follow the instructions in the error message to update the appropriate information. Click **Save** then click **Test Configuration** again.
13. Optionally complete the section below if you want to change the default mapping.
    If you are satisfied with the default mapping, proceed to How to Create an Address Book to create an address book.

Mapping LDAP Fields

Complete the section above, **Creating a New Configuration**, before proceeding with these steps.

1. After you test your configuration from the last section, click **LDAP Attribute Configuration** in the middle of the page.
   The LDAP Attribute Configuration page displays the default mappings from the Security Awareness Training Address Fields to the LDAP Attributes.

   > If you do not see any available LDAP attributes on the right side, repeat the **Test Configuration** step above.

2. **To create a new field mapping** , click **New** .
   1. Select an Address Book field and then an LDAP Attribute to create the mapping. Click **Save**.
   2. Repeat this process for each new mapping.
   3. Click **Return to the LDAP/AD 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 LDAP/AD Configuration Manager** to continue.
4. After you complete your configuration, you can create an Address Book. Refer to How to Create an Address Book.

Editing an Existing Configuration

To edit an existing LDAP configuration:

1. From the **System** menu, select **LDAP/AD Configuration Manager**.
2. Locate the configuration you want to change and click the edit pencil icon ✎. Continue with the steps described above.

Importing the Data

After you have created your configuration, import the data into a Security Awareness Training address book. Refer to How to Create an Address Book for details – including a standard list of LDAP column attributes pulled for import.

Configuring Access to your Firewall

Configure your firewall to allow access from the following IP address range to the port you specified in the LDAP/AD Configuration Manager, described above in Step 7.

- 3.145.232.16/28

Search Filters

Search Filters help you locate just the records you want to import.

This section describes how to create your own custom filter. Note that your syntax must be exactly correct. An easier option is to choose a pre-configured search filter, described in Step 10 above.

The following example can help you to consider the factors involved in creating a Search Filter.

```
(&(|(mail=*yourcompany.com)(mail=*yourothercompanydomain.com))(objectCategory
=person)(objectclass=User)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))
```

The Search Filter above returns records that:

- Have EITHER an email address from @yourcompany.com OR @yourothercompanydomain.com.
- AND the record is classified a Person (as opposed to a group, list, etc.)

- AND the record is classified as a User
- AND the userAccountControl number indicates the account is not disabled.

This article from Microsoft is a helpful resource for creating Search Filters.

Figures