

# Setting up the LDAP tool

This article will outline how to use the LDAP tool which sits in the Sysadmin Panel from Claromentis 8.3+

This LDAP tool means you can connect your company Active directory to sync with your Claromentis intranet without the need for a technician to get involved, meaning any time you need to change what LDAP attributes are syncing or which groups are being pulled this can be done from within the intranet itself.

The first step is to go into the Sysadmin panel and from here the LDAP tab.

If this is the first time you are setting this up you will need to select the new connection option. You will then be shown the 5 steps to set this up as outlined below.

## Connection

In step 1 'Connection' you will need to input the following information:

**LDAP Connections**

✓ 1. Connection

**LDAP Server URL \***  ⓘ

**NetBIOS Name \***  ⓘ

**Service Account DN \***  ⓘ

**Service Account Password \*** \*\*\*\*\* [Change password](#)

**Search Base DN \***  ⓘ

[Test Connection](#)

✓ Connection OK!

[show advanced settings...](#)

[Continue](#)

✓ 2. Directory Settings

Image 1: Connection setting in the LDAP tool

**LDAP Server URL:** The URL must include the protocol (LDAP or LDAPS), LDAP server address and TCP port used for communication between Claromentis and the LDAP server. Eg. - ldap://ad1.claromentis.net:389

**NetBIOS Name:** First part of FQDN, for example for ad1.claromentis.net it would be AD1. The NetBIOS name should always be in upper case (A-Z), any lowercase characters will be converted to uppercase when saving.

**Service Account DN:** We recommend setting up a Claromentis specific Service Account that can be used to run all LDAP search queries. Claromentis only requires read access to the domain and therefore, in most cases, the fact that the Service Account is part of the 'Authenticated Users' group will provide sufficient access rights.

It's also recommended not to set a password expiry policy for this Service Account given that any LDAP user on Claromentis will be unable to login if this Service Account fails to authenticate with the LDAP server

**Service Account Password:** This is not stored in the system

**Search Base DN:** The DN (Distinguished Name) of the Search Base. This is the starting point used for any LDAP search query

Once you have input all the information you should be able to test the connection and get the tick with connection ok as shown in image 1.

The final stage in the connection settings is the advanced settings.

[show advanced settings...](#)

**Password Verification Method**

Verify using provided username (faster)

Lookup user's DN in LDAP, then verify (best for compatibility)

[Continue](#)

Image 2: Password verification method

This is to set the Password verification method, you will be able to select the best option for you. Once selected select continue.

### Directory Settings

You will then be able to move onto the second step the Directory Settings.

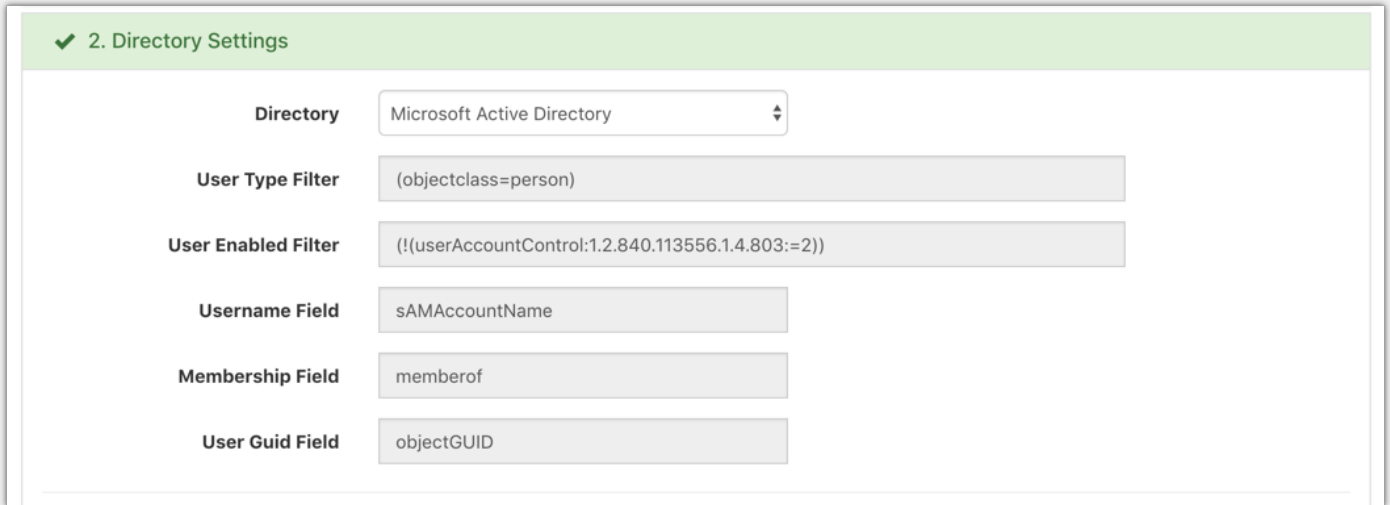


Image 3: Directory Settings

You will first need to select your directory from the drop down.

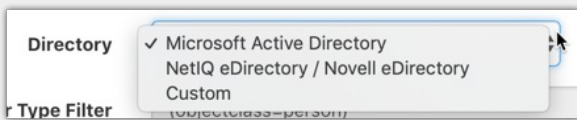


Image 4: Directory Options

After this fill in the fields from your AD settings included in Image 3.

The second part of the Directory settings is the access control and setting up the sync as shown in image 4.

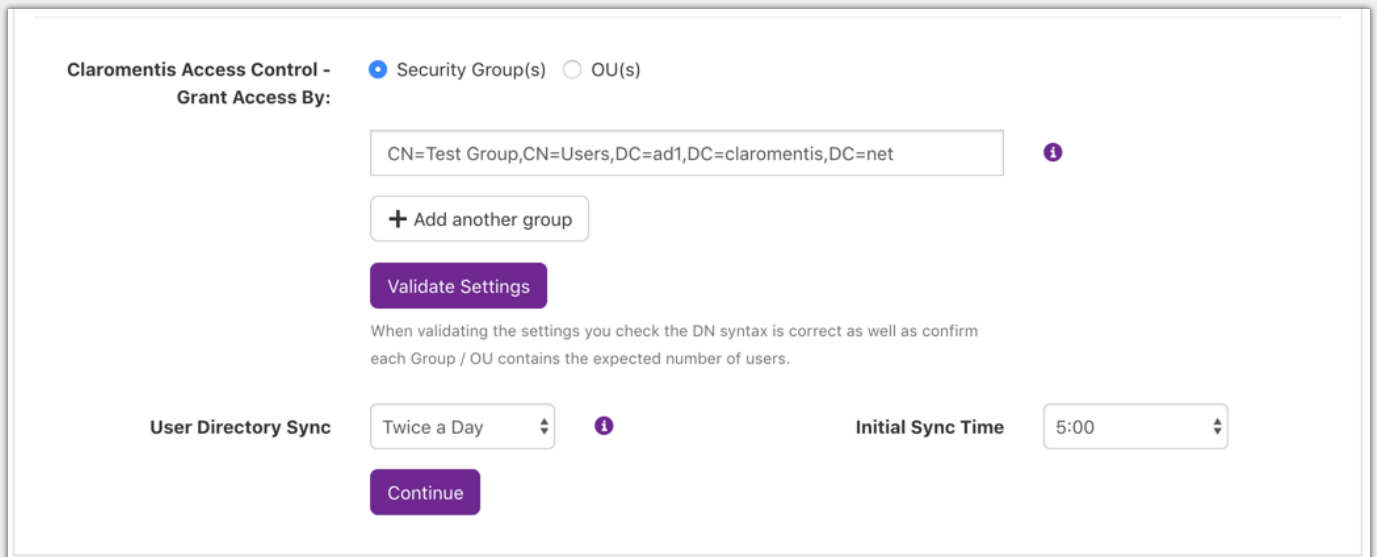


Image 5: Directory Settings cont.

You will be able to choose how Claramentis is given access and specify the OU using the DN format. Your user directory sync can be set up as a specific time and how often. The following options are given.

- Disabled
- Every Hour
- Twice a day
- Daily (Recommended)
- Weekly

Depending on what option you select you will be able to specify the initial sync time. Once complete select continue to move on to syncing the LDAP attributes which is outlined in this article - LDAP attributes article.

### User Groups

After you have synced the LDAP attributes you can move on to the group set up.

### ✓ 4. User Groups

**Map LDAP Group(s) to User Profile**

Enabled

Enabled - Limit groups by regular expression

Enabled - Limit groups by OU

Disabled

**Enabled:** When selected, Claromentis will lookup all of the groups that each user is memberOf in LDAP. All of these groups will then be automatically created within Claromentis and can be used to assign permissions to applications and content. This is ideal for organizations that wish to centrally manage permissions groups using LDAP.

**Enabled - Limit groups by regular expression:** Same as Enabled, but the groups mapped to the user can be limited to a regular expression. The regular expression needs to be a valid regex with delimiters. For example, you could enter '/INT-/' and then only groups that contain 'INT-' will be mapped. Alternatively, to perform a case-insensitive search use '/INT-/i' - this would match 'INT-', 'int-' or any mixture of upper and lowercase letters like 'iNt-'. '/^INT-/' will match group names that begin only with 'INT-'

**Enabled - Limit groups by OU:** Same as Enabled, but the groups mapped to the user can be limited to only map groups that sit within the specified Organizational Unit.

**Disabled:** Select this option if you would like to use groups created & managed in Claromentis only, to control permissions to applications and content.

[Continue](#)

Image 6: User Groups

There are 4 options you have with the user sync, please read each option thoroughly to decide what syn will work best for you.

### Status

The final step in the LDAP tool configuration is to select the status this is weather you need to enable or disable the LDAP connection, this can be disable but the details remain if needed.

Once you have set everything correctly please click save in the bottom right hand corner to complete the setup.