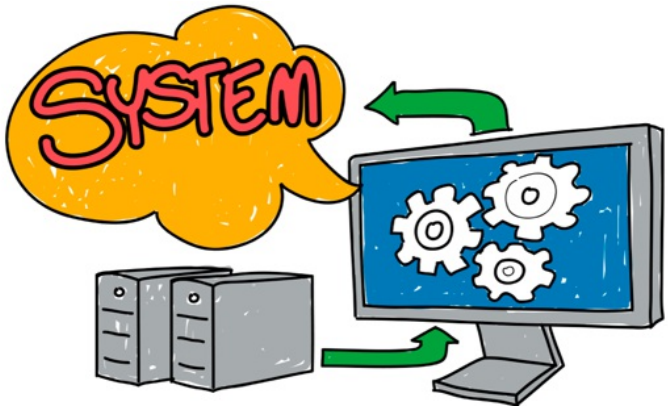
Link to article: https://discover.claromentis.com/knowledgebase/articles/543



Setting Up the LDAP tool

This article will outline how to use the LDAP tool which sits in the System 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 System 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:

NOTE: *The below fields are just an example. Please substitute accordingly to match your corporate settings.*

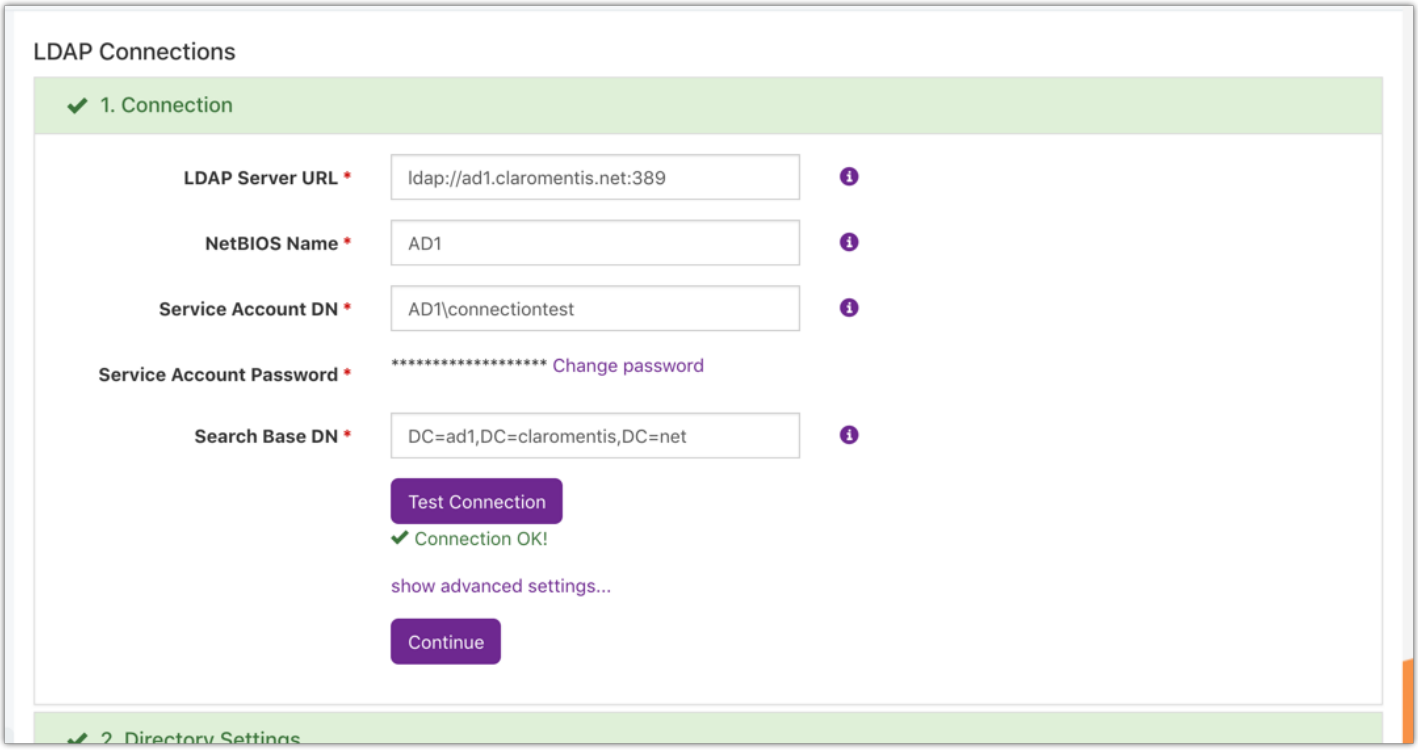


Image 1: Connection setting in the LDAP tool

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.

LDAP: ldap://ad1.claromentis.net:389

*LDAPS: ldaps://ad1.claromentis.net:636

**LDAPS will require an externally signed SSL certificate from a recognised Certificate Authority.*

Important:

SaaS Hosted: *If you are hosted by Claromentis please note that LDAPS must be used to secure traffic between your Active Directory Domain Controller & the web server.*

Client Hosted: *If you are hosted on-premise you are able to use either LDAP or LDAPS.*

NetBIOS Name: First part of FQDN that would form the Windows Login name (DOMAIN\username), 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. NT4 format.

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.

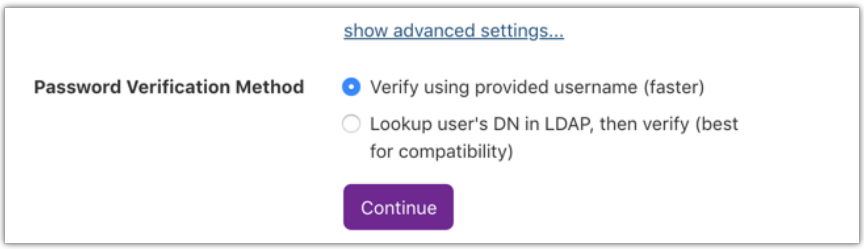


Image 2: Password verification method

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.

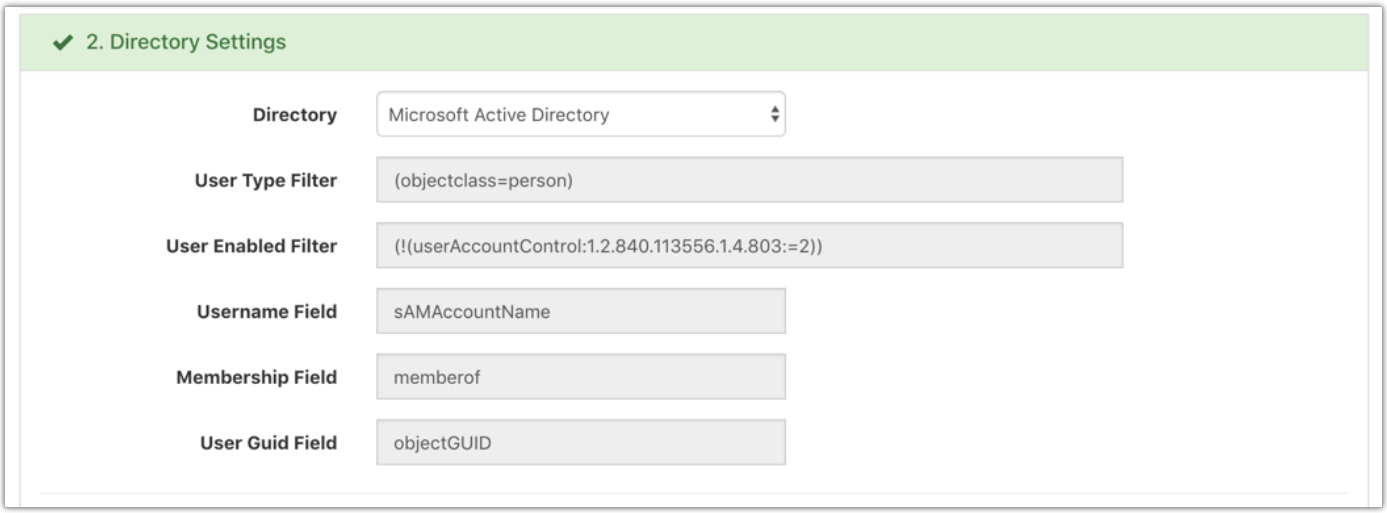


Image 3: Directory Settings

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

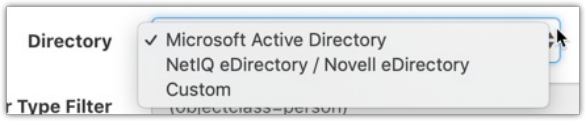


Image 4: Directory Options

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.

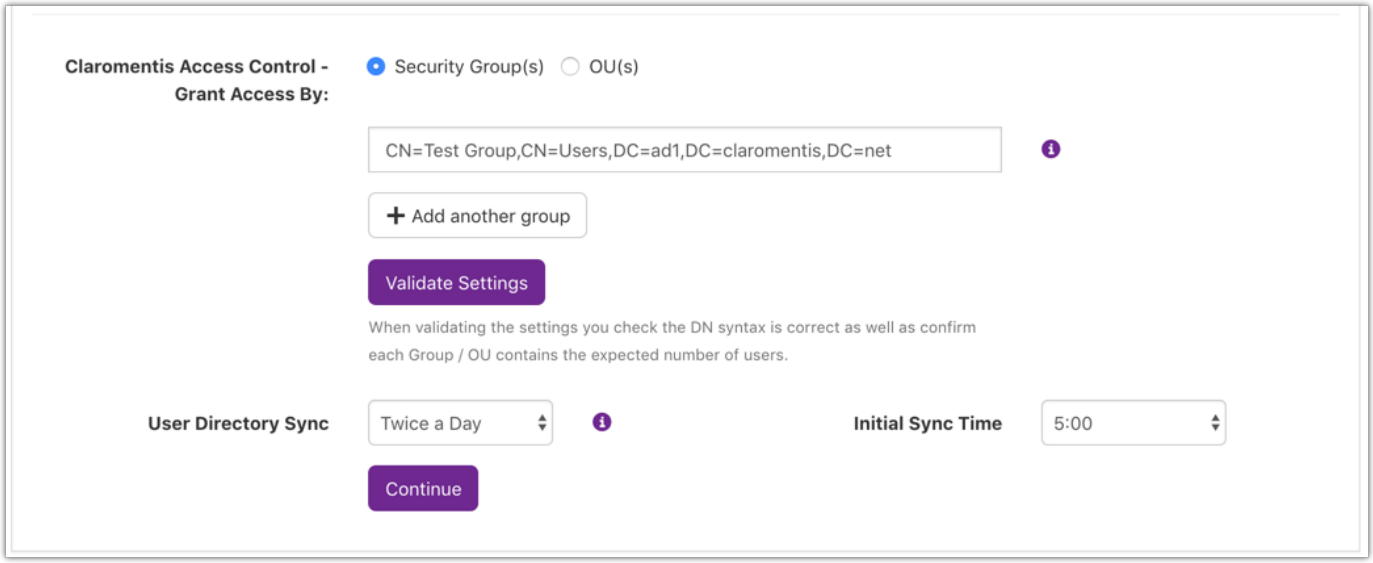


Image 5: Directory Settings cont.

You will be able to choose how Claromentis 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.

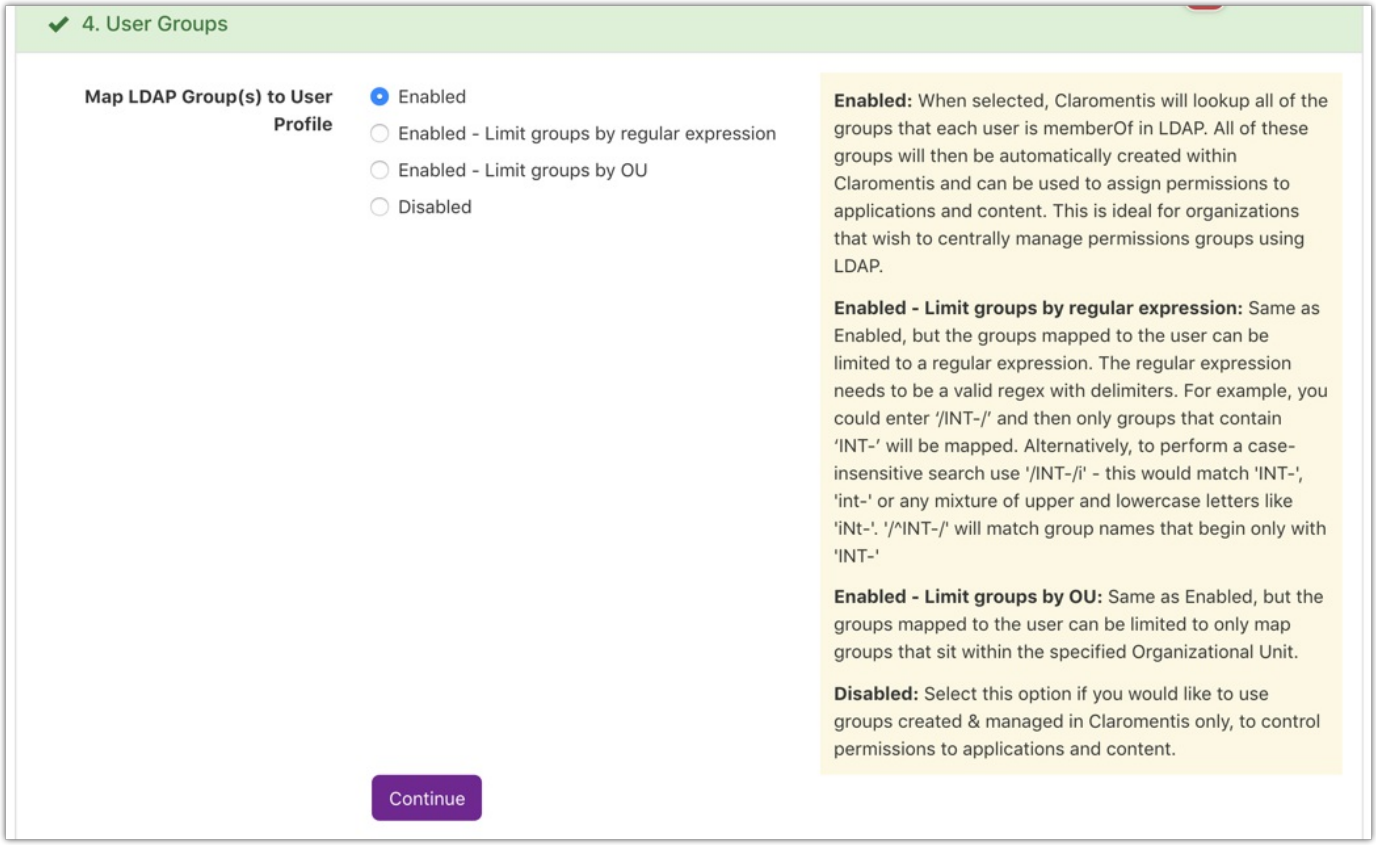


Image 6: User Groups

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

Please note: If you are syncing user groups from AD you will not be able to use local groups within your intranet as these will be overwritten when the sync runs. If you are pulling AD groups you can use Roles to manage users within the system.

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.

Multiple domains

Syncing against multiple domains is possible within the LDAP tool. You will need to create a new LDAP connection following the above for each domain you wish to sync with. These will then form individual LDAP connections, that will sync periodically according to the frequency that has been set.

Please note that it may take longer to sync users on automatic sync intervals with multiple domains configured due to the nature of querying each domain configuration.

Related Article

Microsoft DN Format

Last modified on 6 December 2023 by Hannah Door

Created on 22 March 2019 by Mhairi Hutton
Tags: active directory, intranet, ldap, people, user guide