

# Multi-domain Active Directory Integration with OnPremise server

## Active Directory Integration with OnPremise server

Description:	The work is to configure a direct LDAPS user sync between Web server and client's AD server across all specified domains (not SSO)
Pre-conditions:	<ul style="list-style-type: none"><li>- Claromentis to provide web server IP address(es)</li><li>- Client to open LDAPS ports to external incoming traffic (636, 3269) from web server IP(s)</li><li>- Client to ensure that they have AD user account which can read all user LDAP attributes which they want to sync and the memberOf field</li><li>- Client to decide which security groups or OU are to be used for user authentication</li><li>- Client to ensure that there is a valid SSL cert on AD server. This can either be externally or self signed</li><li>- Client to confirm if the self-signed certificate is used</li><li>- Claromentis to configure the web server <b>prior</b> to LDAPS integration work</li></ul>
Steps to complete:	<p>Client to login using their admin account and follow the guidelines of LDAP tool in Admin &gt; System &gt; LDAP</p> <p>We estimate that given all preconditions are complete prior, this work should take no longer than 1 hour to set up.</p>
Constraints:	<ul style="list-style-type: none"><li>- No proxy servers, direct connection only</li><li>- Only <a href="#">LDAPS method</a> is supported for the purposes of user sync</li></ul>
Troubleshooting:	If there are issues with setting up the LDAPS connection, please contact your Claromentis project manager to seek assistance
Downtime:	none
Resources required:	Client tech resource, Claromentis tech resource if self-signed cert is used.

Last modified on 5 May 2022 by [Hannah Door](#)

Created on 26 May 2018 by [Stas Dreiling](#)

Tags: [work package](#)