Drupal LDAP/Active Directory Login / Features and Module Pricing / Active Directory / LDAP Integration SSO - NTLM & Kerberos login with Drupal site

Configure Drupal login using LDAP / Active Directory

Drupal LDAP Login module allows your LDAP / Active Directory users to login to Drupal using their LDAP / Active Directory (AD) credentials. In addition to LDAP, this module also allows you to login using NTLM and Kerberos. We provide Drupal LDAP/AD SSO login module which is compatible with Drupal 7, Drupal 8, and as well as Drupal 9.
It allows users to authenticate against various LDAP implementations like Microsoft Active Directory, OpenLDAP, OpenDS, FreeIPA, Synology, and other directory systems as well as perform authentication using NTLM and Kerberos.

If you have any doubts or queries, you can contact us at drupalsupport@xecurify.com. We will help you to configure the module. If you want, we can also schedule an online meeting to help you configure the Drupal LDAP / Active Directory integration SSO login module.

Features and Pricing

Know more about Drupal LDAP/AD integration module from here.

Pre-requisites: Download

You can download the Drupal Active Directory / LDAP integration module from here.

Setup Video LDAP integration and Active Directory (AD) integration SSO Login with Drupal site

You can refer to the steps to Configure LDAP and Active Directory SSO Login with Drupal from the Video or Documentation given below:

How to configure Active Directory/LDAP
Integration module in Drupal with your LDAP Serve
LDAP

Steps to configure LDAP integartion/Active Directory integration SSO login with Drupal website:

Step 1: Download the zip folder

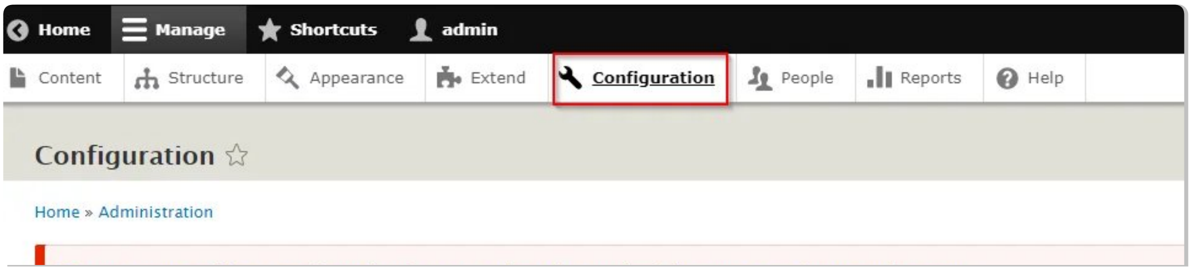
- Download the zip folder of the miniOrange AD/LDAP integration module for Drupal by clicking on the link here.

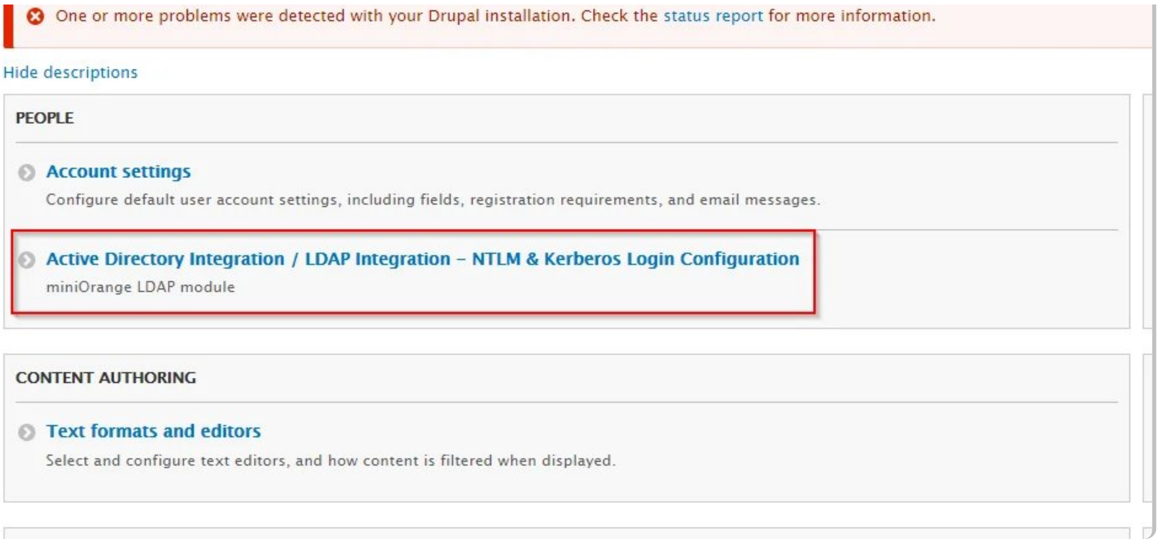
Step 2: Install New Module

- Install and enable the module on your Drupal site by clicking on the **Install New Module** button in Extends sections of your Drupal administrator console

Step 3: Drupal Active Directory / LDAP integration - NTLM & Kerberos login configuration

- Once you have enabled the module, go to the configuration and select Drupal **Active Directory / LDAP integration - NTLM & Kerberos login configuration** as shown in the below image:





One or more problems were detected with your Drupal installation. Check the status report for more information.

Hide descriptions

PEOPLE

Account settings

Configure default user account settings, including fields, registration requirements, and email messages.

Active Directory Integration / LDAP Integration – NTLM & Kerberos Login Configuration

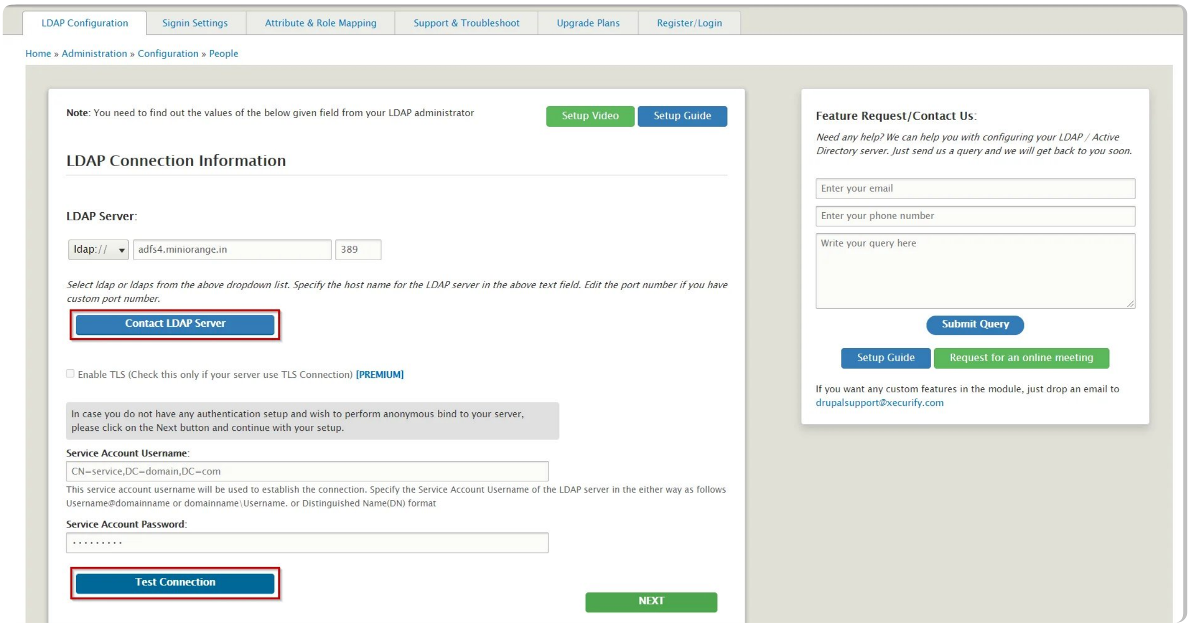
miniOrange LDAP module

CONTENT AUTHORING

Text formats and editors

Select and configure text editors, and how content is filtered when displayed.

- Enter your AD Server URI and click on the **Contact LDAP** server to test your connection with your LDAP server. Then, enter the Service account username and password for your AD server and click on **Test Connection** to test the whether you are able to bind to your AD server.
- Click on the **NEXT** button to go to the next step.(refer to the image below):



Home » Administration » Configuration » People

Note: You need to find out the values of the below given field from your LDAP administrator

LDAP Connection Information

LDAP Server:

ldap:// adfs4.miniorange.in 389

Select ldap or ldaps from the above dropdown list. Specify the host name for the LDAP server in the above text field. Edit the port number if you have custom port number.

□ Enable TLS (Check this only if your server use TLS Connection) [PREMIUM]

In case you do not have any authentication setup and wish to perform anonymous bind to your server, please click on the Next button and continue with your setup.

Service Account Username:

CN=service,DC=domain,DC=com

This service account username will be used to establish the connection. Specify the Service Account Username of the LDAP server in the either way as follows Username@domainname or domainname\Username. or Distinguished Name(DN) format

Service Account Password:

·········

Feature Request/Contact Us:

Need any help? We can help you with configuring your LDAP / Active Directory server. Just send us a query and we will get back to you soon.

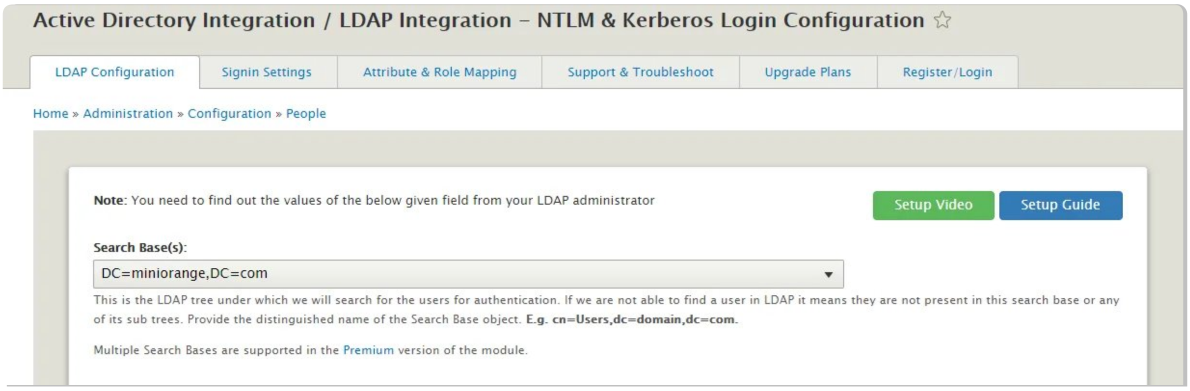
Enter your email

Enter your phone number

Write your query here

If you want any custom features in the module, just drop an email to drupalsupport@xecurify.com

- In the next screen that you see, select the Search Base and the Search Filter/Username Attribute with which your users will be searched while logging in.



Active Directory Integration / LDAP Integration – NTLM & Kerberos Login Configuration ☆

Home » Administration » Configuration » People

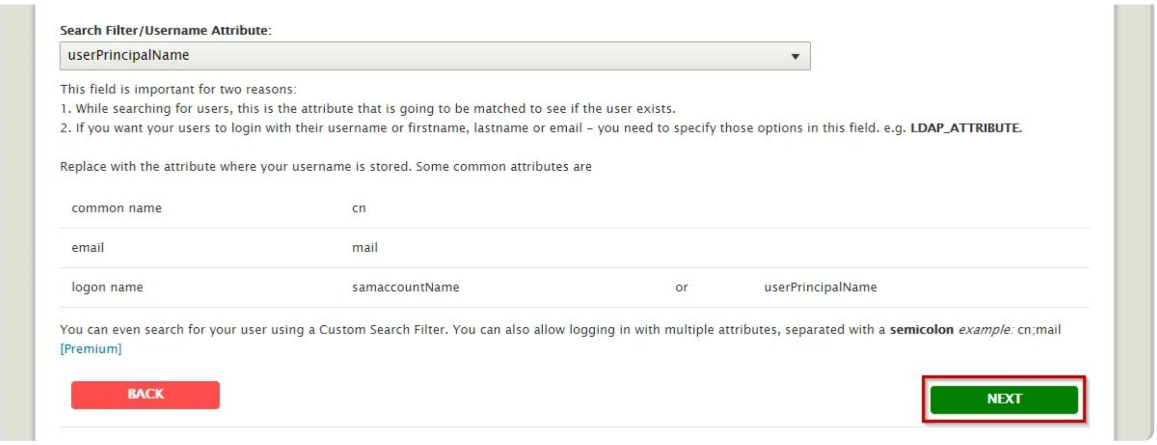
Note: You need to find out the values of the below given field from your LDAP administrator

Search Base(s):

DC=miniorange,DC=com

This is the LDAP tree under which we will search for the users for authentication. If we are not able to find a user in LDAP it means they are not present in this search base or any of its sub trees. Provide the distinguished name of the Search Base object. E.g. cn=Users,dc=domain,dc=com.

Multiple Search Bases are supported in the Premium version of the module.



Search Filter/Username Attribute:

userPrincipalName ▾

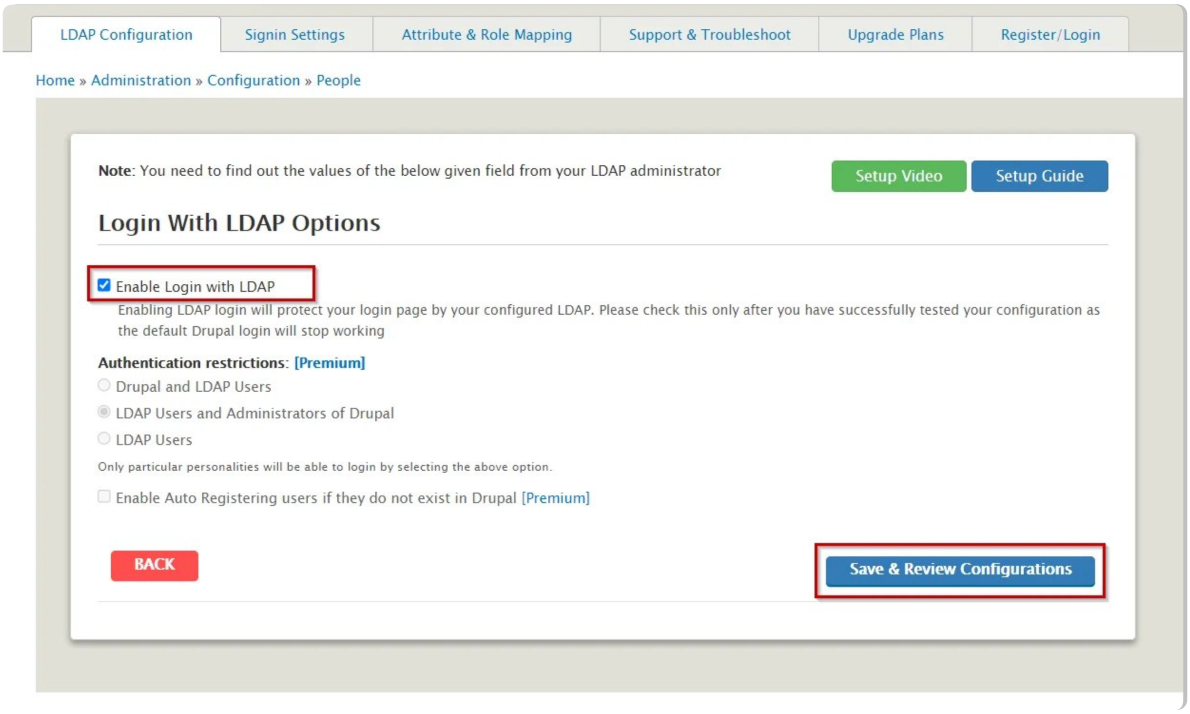
This field is important for two reasons:
1. While searching for users, this is the attribute that is going to be matched to see if the user exists.
2. If you want your users to login with their username or firstname, lastname or email – you need to specify those options in this field. e.g. **LDAP_ATTRIBUTE.**

Replace with the attribute where your username is stored. Some common attributes are

common name	cn		
email	mail		
logon name	samaccountName	or	userPrincipalName

You can even search for your user using a Custom Search Filter. You can also allow logging in with multiple attributes, separated with a **semicolon** *example:* cn;mail [Premium]

- **Search Base:** This is the LDAP hierarchy under which your users will be searched.
- **Username Attribute:** While logging in Drupal, your users will be searched by this attribute in your AD.
- Click on the NEXT button to enable **Login using LDAP** and **Auto creating of users in Drupal if not present.**



Home » Administration » Configuration » People

Note: You need to find out the values of the below given field from your LDAP administrator

Login With LDAP Options

☑ Enable Login with LDAP

Enabling LDAP login will protect your login page by your configured LDAP. Please check this only after you have successfully tested your configuration as the default Drupal login will stop working

Authentication restrictions: **[Premium]**

○ Drupal and LDAP Users

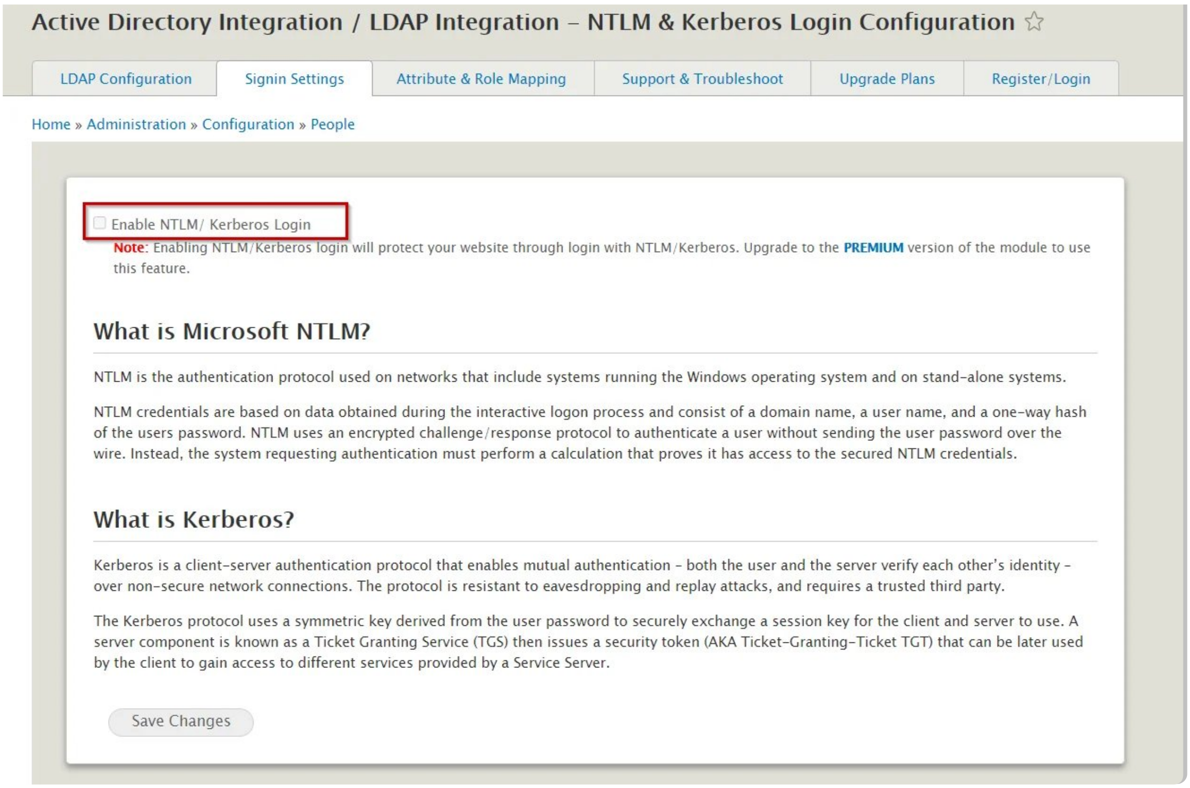
● LDAP Users and Administrators of Drupal

○ LDAP Users

Only particular personalities will be able to login by selecting the above option.

□ Enable Auto Registering users if they do not exist in Drupal [Premium]

- Click on Save & Review Configurations to view all the configurations you have made so far.
- That's it!, you have configured the module successfully. Now, please go to the login page of your Drupal site and login using your AD credentials.
- Also, if you want to enable NTLM or Kerberos login, please go to the Sign In setting tab and select the below-highlighted checkbox and click on the Save button to save your Configurations:


Active Directory Integration / LDAP Integration – NTLM & Kerberos Login Configuration ☆
LDAP Configuration
Signin Settings
Attribute & Role Mapping
Support & Troubleshoot
Upgrade Plans
Register/Login
Home » Administration » Configuration » People
Save Changes

□ Enable NTLM/ Kerberos Login

Note: Enabling NTLM/Kerberos login will protect your website through login with NTLM/Kerberos. Upgrade to the **PREMIUM** version of the module to use this feature.

What is Microsoft NTLM?

NTLM is the authentication protocol used on networks that include systems running the Windows operating system and on stand-alone systems.

NTLM credentials are based on data obtained during the interactive logon process and consist of a domain name, a user name, and a one-way hash of the users password. NTLM uses an encrypted challenge/response protocol to authenticate a user without sending the user password over the wire. Instead, the system requesting authentication must perform a calculation that proves it has access to the secured NTLM credentials.

What is Kerberos?

Kerberos is a client-server authentication protocol that enables mutual authentication – both the user and the server verify each other's identity – over non-secure network connections. The protocol is resistant to eavesdropping and replay attacks, and requires a trusted third party.

The Kerberos protocol uses a symmetric key derived from the user password to securely exchange a session key for the client and server to use. A server component is known as a Ticket Granting Service (TGS) then issues a security token (AKA Ticket-Granting-Ticket TGT) that can be later used by the client to gain access to different services provided by a Service Server.

Advanced features [In Premium module]

You can also configure other features like Attribute Mapping i.e. mapping the user attributes coming from your AD to the Drupal user attributes, Role Mapping i.e. mapping your Roles from AD to your Drupal site and many more.

24*7 Active Support:

If you have any questions regarding the guide or in case you are facing any issues configuring the module, please feel free to reach out to us at drupalsupport@xecurify.com or through the Support block on each of the tabs.

In case you want some additional features to be included in the module, please get in touch with us, and we can get that custom-made for you. Also, If you want, we can also schedule an online meeting to help you configure the Drupal Active Directory/LDAP SSO login integration module.
If you don't find what you are looking for, please contact us at **info@xecurify.com** or call us at **+1 978 658 9387**.

Our Other modules:

SAML SP | SAML IDP | 2FA | OAuth/OIDC Client | LDAP/AD Login | OAuth Server | OTP Verification | Website Security | Rest API Authentication | SCIM User Provisioning

miniOrange

☎ +1 978 658 9387 (US)
+91 97178 45846 (India)

✉ info@xecurify.com

STAY CONNECTED

SIGN UP FREE

Product

- Single Sign On
- Identity Brokering
- OAuth / OpenID Connect Server
- Multi Factor Authentication
- Adaptive Authentication
- User Provisioning
- Directory Services

Solutions

- SAML Solutions
- OAuth Solutions
- 2FA Solutions
- Mobile Solutions

Directory Integrations

Federation Integrations

Windows Solutions

SSO Connectors

Secure Browser SSO

View All

Why miniorange

Our Success Stories

Content Library

Videos

FAQs

Forum

Company

Overview

News

Partners

Customers

Contact Us