LDAP credentials

# LDAP credentials#

You can use these credentials to authenticate the following nodes:

• LDAP

## Prerequisites#

Create a server directory using Lightweight Directory Access Protocol (LDAP).

Some common LDAP providers include:

• Jumpcloud

• Azure ADDS

• Okta

## Supported authentication methods#

• LDAP server details

## Related resources#

Refer to your LDAP provider's own documentation for detailed information.

For general LDAP information, refer to Basic LDAP concepts for a basic overview and The LDAP Bind Operation for information on how the bind operation and authentication work.

## Using LDAP server details#

To configure this credential, you'll need:

• The LDAP Server Address: Use the IP address or domain of your LDAP server.

• The LDAP Server Port: Use the number of the port used to connect to the LDAP server.

• The Binding DN: Use the Binding Distinguished Name (Bind DN) for your LDAP server. This is the user account the credential should log in as. If you're using Active Directory, this may look something like cn=administrator, cn=Users, dc=n8n, dc=io. Refer to your LDAP provider's documentation for more information on identifying this DN and the related password.

cn=administrator, cn=Users, dc=n8n, dc=io

• The Binding Password: Use the password for the Binding DN user.

• Select the Connection Security: Options include:  
None  
TLS  
STARTTLS

• None

None

• TLS

TLS

• STARTTLS

STARTTLS

• Optional: Enter a numeric value in seconds to set a Connection Timeout.