

LDAP Settings

In addition to the internal user management, existing corporate LDAP directories can be integrated in iDNA Applications.

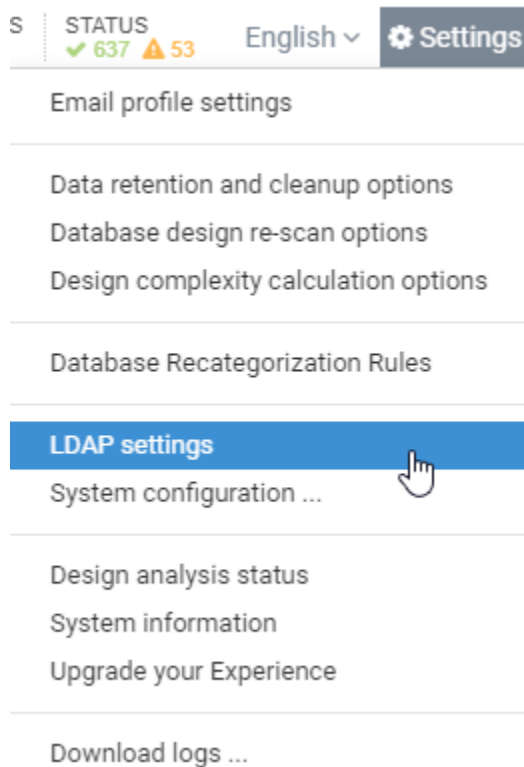
This article explains how to configure the integration with an Active Directory and Domino LDAP.




Please note that the default iDNA Applications user accounts (e.g. Config) remain active and are valid parallel to all LDAP objects.

Active Directory

- Click on *Settings - LDAP Settings*



- LDAP Settings



LDAP settings

Active ☒

Disable or enable login with LDAP

LDAP Security ☐ unsecure ☒ secure

LDAP host

Your LDAP Server hostname e.g. ldap.acme.com

LDAP port

Server port, usually 389 or 636 if SSL is used.

Bind DN

The user who is allowed to search the base DN. e.g. CN=_username,OU=Functional

Bind DN Password

The password of the user who is mentioned in the Bind DN

User Search Base

The base DN from which to search for the provided username. e.g. O=acme or OU=acme

User Filter

User lookup filter. e.g. (cn={{username}}) or (sAMAccountName={{username}}) for AD. The placeholder {{username}} will be replaced by the user supplied login

Role Mapping

Administrator	Office365Admins
User	OfficeExpertUsers

Map ldap User Groups to at least ONE panagenda user-role (comma separated list)

Test Settings

LDAP security: Select unsecure (ldap://) or secure (ldaps://), depending on your environment

LDAP host: Enter the directory URL

LDAP port: Type in the server port

Bind DN: Enter the canonical name of the bind user

Example: CN=_bindusername,OU=Functional,OU=Users,OU=acme,DC=acme,DC=local

IMPORTANT: The binduser has to see at least one of the following member attributes: memberOf, isMember, member

Bind DN Password: Enter the password of the bind user account

User Search Base: Enter the Search Base where the User Objects are located

User Filter: For Active Directory please enter the following string:

sAMAccountName={{username}}

Role Mapping (Administrators - Monitoring- Viewer)

Assign an AD Group to the respective role

Example: Office365Admins is an AD group with certain members (all these members would gain administrator access to iDNA Applications)

IMPORTANT:

- If a user is member of an Administrator group and Viewer group, then the User gets the higher permission Administrator
- If a user which is NOT member of any assigned group, tries to login, the user will not be able to login.

Domino LDAP

- LDAP Settings

The screenshot shows the 'LDAP settings' configuration page in Domino. It includes a gear icon and the title 'LDAP settings'. The settings are organized into sections: 'Active' (checked), 'LDAP Security' (secure selected), 'LDAP host' (ldap.acme.com), 'LDAP port' (636), 'Bind DN' (CN=_bindusername,O=acme), 'Bind DN Password' (masked), 'User Search Base' (O=acme), 'User Filter' (cn={{username}}), and 'Role Mapping' (Administrator: DominoAdmins, User: OfficeExpertUsers). Each field has a descriptive tooltip. At the bottom right are 'Test Settings' and 'Save' buttons.

LDAP security: Select unsecure (ldap://) or secure (ldaps://), depending on your environment

LDAP host: Enter the directory URL

LDAP port: Type in the server port

Bind DN: Enter the canonical name of the bind user

Example: CN=_bindusername,OU=Functional,OU=Users,OU=acme,DC=acme,DC=local

IMPORTANT: The bind user has to see the attribute: dominoaccessgroups

Bind DN Password: Enter the password of the bind user account

User Search Base: Enter the Search Base where the user objects are located

User Filter: for Domino LDAP please enter the following string:

cn={{username}}

Role Mapping (Administrators - Monitoring- Viewer)

Assign a Domino group to the respective role

Example: DominoAdmins is a Domino group with certain members (all these members would gain administrator access to iDNA Applications)

IMPORTANT:

- If a user is member of an Administrator group and Viewer group, then the User gets the higher permission Administrator

- If a user which is NOT member of any assigned group, tries to login, the user will not be able to login.