

LDAP Settings

NetVizura provides LDAP integration so that network admins can have a central management of their user accounts.

Administrator can add, edit and delete users from their own directory (Active Directory, Open LDAP or any other implementation).



When LDAP user logs in to NetVizura for the first time, his NetVizura user account is created, and he has "read" permissions by default. Further permission change (Admin, Write, Per module) should be fine-tuned in NetVizura.

On this page:

- [Network Parameters](#)
- [Authentication](#)
- [Mapping rules](#)
- [Verifying LDAP Login](#)
- [Active Directory](#)
- [Active Directory Example](#)
- [Open LDAP Example](#)

To set LDAP integration, go to [blocked URL](#) > **Settings** > **Control Panel** > **LDAP**.

Network Parameters

- **Server address** is your LDAP server hostname or IP address
- **Port** is LDAP server port. Default port is 389 for insecure (LDAP) connections and 636 for secure (LDAPS) connections
- **Use SSL** for secure communication between LDAP server and Netvizura application

Authentication

- **Type** can be "simple" or encrypted (SASL)
- **Method** defines comma separated list of SASL mechanisms for password hashing supported by the LDAP server (e.g. DIGEST-MD5, GSSAPI, CRAM-MD5, etc.)

Mapping rules

- **Base DN** is a branch in your LDAP tree which should be used as base for LDAP user mapping. User can choose between two different LDAP implementation profiles ("Active Directory" and "Open LDAP") and load predefined settings. The third one "Custom" is used if you have some other implementation.
- **Organizational unit attribute** is used for matching specified organizational unit(s).
 Used only with Open LDAP implementation.
- **Organizational unit(s)** is a node within an LDAP directory where users are located.
 Used only with Open LDAP implementation. You can specify multiple organizational units separated by space. Order is important.
- **User attribute** is user attribute name defined on LDAP server which is used for matching authenticated user.
- **Group name** is used for relating to a specific group found on LDAP server that contains users with NetVizura privileges (eg. "Netvizura").
- **How to check groups** We can relate specified group in two ways: "User in group" (every group contains a list of users) and "Group in user" (every user has a list of groups where he or she belongs).
- **Group attribute** is used for matching specified group name.
- **Group object class** is used for fetching the list of all LDAP groups and then performs a check to see if user matches it.
 Used only with "User in group" option.
- **Member attribute** is used for matching specified group name with the user.

Verifying LDAP Login

Optionally, at the end we can verify the above connection settings by specifying username and password of the LDAP user related to Netvizura group. Username must match defined user attribute mapping rule.

You need to type only username, without domain name before it.

Active Directory

NetVizura currently supports two ways of logon to Active Directory:

1. Using **sAMAccountName** property
 - In this case user will login just with this property, without specifying domain before username (DOMAIN/username) and without specifying domain as suffix (username@domain)
 - NetVizura user account will be created with username that match **sAMAccountName** property
 - In the background, application will use this property to create username construction **sAMAccountName@baseDN** for logon to Active Directory
2. Using **UserPrincipalName** property

- In this case user will login using this property, without specifying domain before username (DOMAIN/username)
- This property is usually in the form of an email address (username@upn_suffix)
- NetVizura user account will be created with username that match **UserPrincipalName** property
- In the background, application will use this property for logon to Active Directory

i If there is a property similar to UserPrincipalName property, more precisely, if some property can be used for login to AD same as UserPrincipalName property, it also can be used in NetVizura. Rules for this property are same as for the UserPrincipalName property.

Active Directory Example

LDAP

Network parameters:

Server address: ldap.domain.com
Port: 389

Authentication:
Type: SIMPLE
Mapping rules:
Base DN: ldap.domain.com

Choose your implementation:
Active Directory
Open LDAP
Custom
User attribute: sAMAccountName
User object class: organizationalPerson
Group name: NetVizura
How to check groups:
User in group
Group in user
Group attribute: cn
Group object class: group
Member attribute: memberOf

Verify LDAP login:
Username: username
Password: *****
Verify Verification successful

Save
Cancel

Open LDAP Example

LDAP

Network parameters:

Server address: ldap.domain.com
Port: 389

Authentication:
Type: SIMPLE
Mapping rules:
Base DN: ldap.domain.com

Choose your implementation:
Active Directory
Open LDAP
Custom
Organizational unit attribute: ou
Organizational unit: users accounts
User attribute: cn
User object class: inetOrgPerson
Group name: NetVizura
How to check groups:
User in group
Group in user
Group attribute: cn
Group object class: posixGroup
Member attribute: memberUid

Verify LDAP login:
Username: username
Password: *****
Verify Verification successful

Save
Cancel