netLD External Authentication
Setup Guide

Overview

netLD is able to integrate with authentication servers such as Active Directory and FreeRADIUS. When using this integration, you do not need to create the individual users in netLD.

netLD can apply specific networks and permissions to the groups sent from authentication servers.

1. Integration with a RADIUS Server

netLD will send an **Access-Request** packet to the RADIUS server and expects an **Access-Accept** packet in return. This **Access-Accept** packet will need to contain a Filter-Id containing a group name that netLD can, using **External group mappings**, map to the netLD roles and networks.

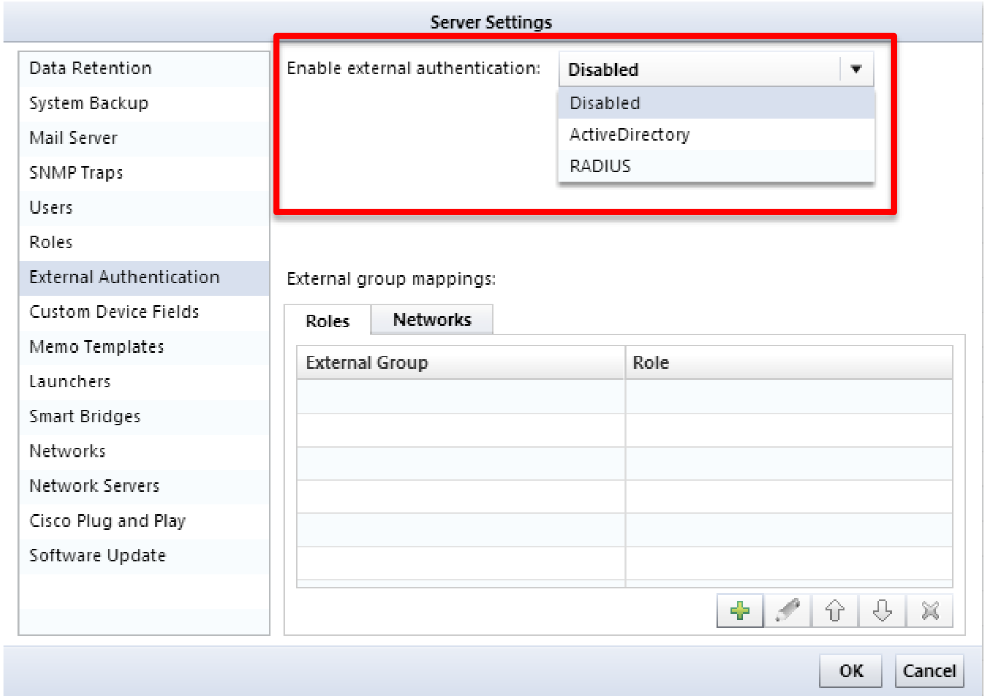
Here is an example of a user configured in FreeRADIUS:

```
LogicVein   Cleartext-Password := "password"
            Filter-Id += "GROUP",
```

In this example, when netLD sends an **Access-Request** packet including the username "LogicVein" and password "password", the RADIUS server sends back an **Access-Accept** packet which has the Filter-Id field set. The Filter-Id is used as the **External Group** in which the authenticated user will belong. Available contents are as follows.

<<Setting Procedures>>
In order to integrate with a RADIUS server, the settings can be configured in the **External authentication** page of the **Server Settings** dialog.

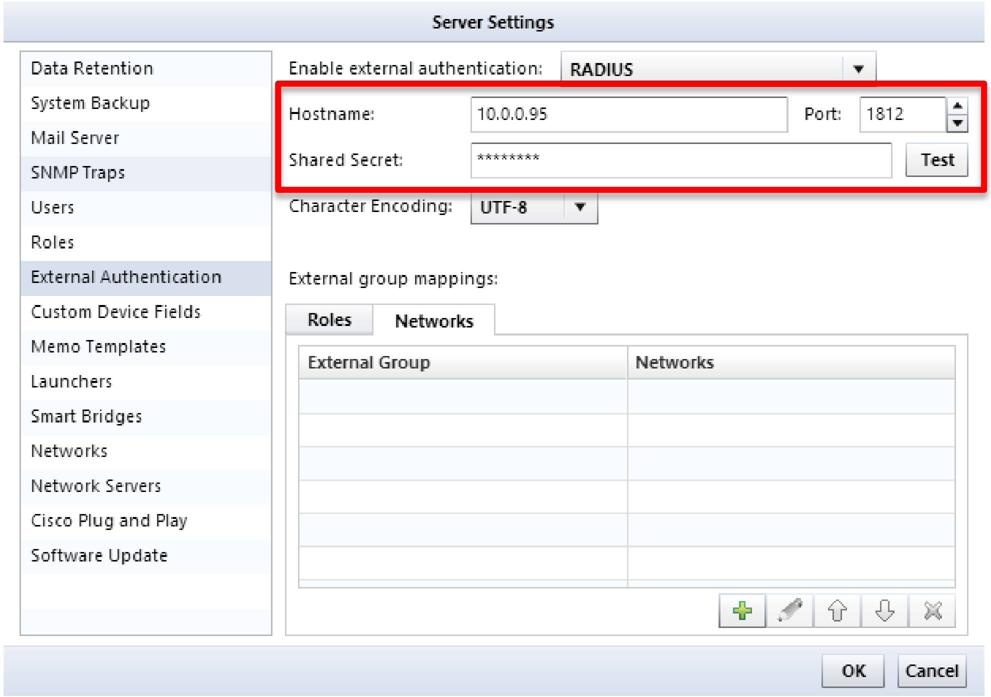
1. Select **RADIUS** for **Enable external authentication**.



Server Settings

Enable external authentication: Disabled

2. Set the IP address (or Hostname) and the Shared Secret of the RADIUS server.



Server Settings

Enable external authentication: RADIUS

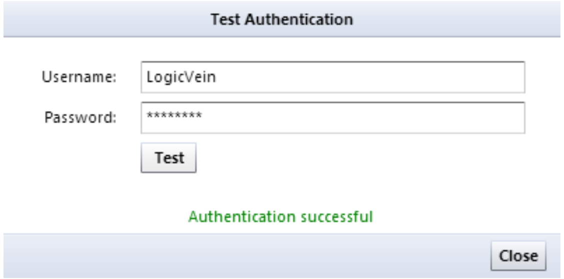
Hostname: 10.0.0.95

Port: 1812

Shared Secret: ********

Character Encoding: UTF-8

- After configuring the above settings, you can confirm the integration with the RADIUS server by clicking **Test** and providing a Username and Password. If there is no problem, the **Authentication successful** message will be shown.



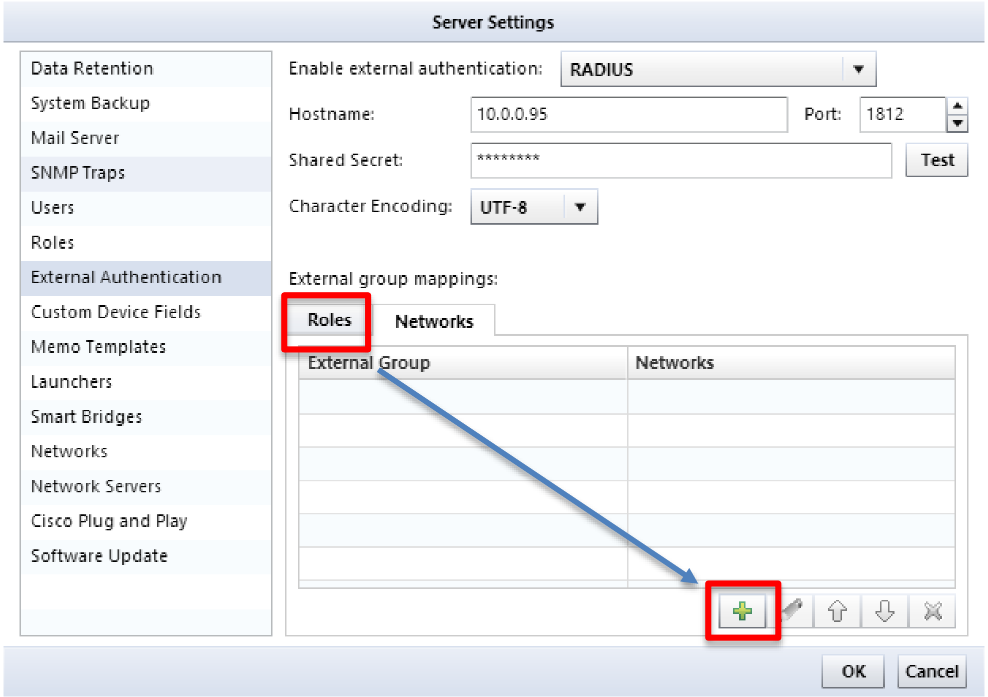
Test Authentication

Username: LogicVein

Password: ********

Authentication successful

3. Assign **Roles** using **External group mappings**. A mapping is added by clicking the [**+**] button.



Server Settings

Enable external authentication: RADIUS

Hostname: 10.0.0.95

Port: 1812

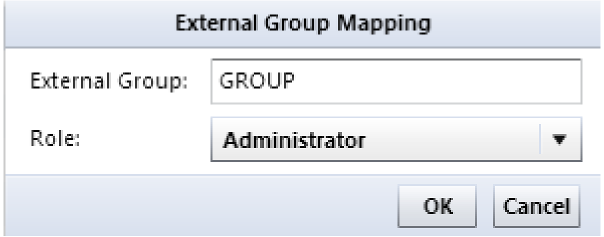
Shared Secret: ********

Character Encoding: UTF-8

External group mappings:

External Group	Networks

4. Enter the group that was set in the Filter-Id of the RADIUS server into **External Group** field and select a role to apply to the group.

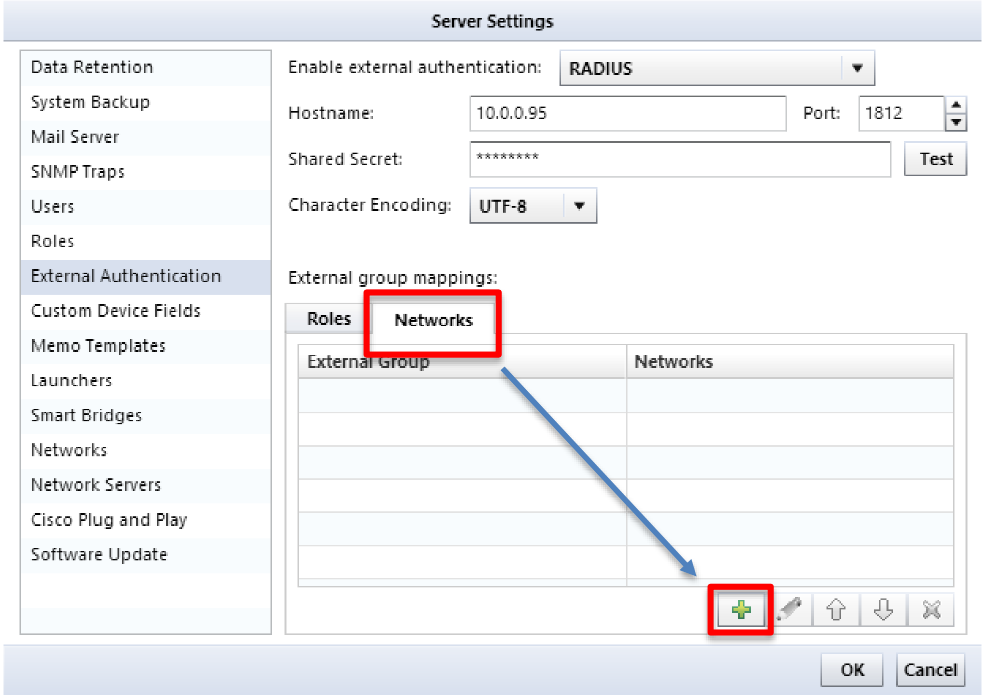


External Group Mapping

External Group: GROUP

Role: Administrator

5. Assign **Networks** using **External group mappings**. A mapping is added by clicking [**+**] button.



Server Settings

Enable external authentication: RADIUS

Hostname: 10.0.0.95

Port: 1812

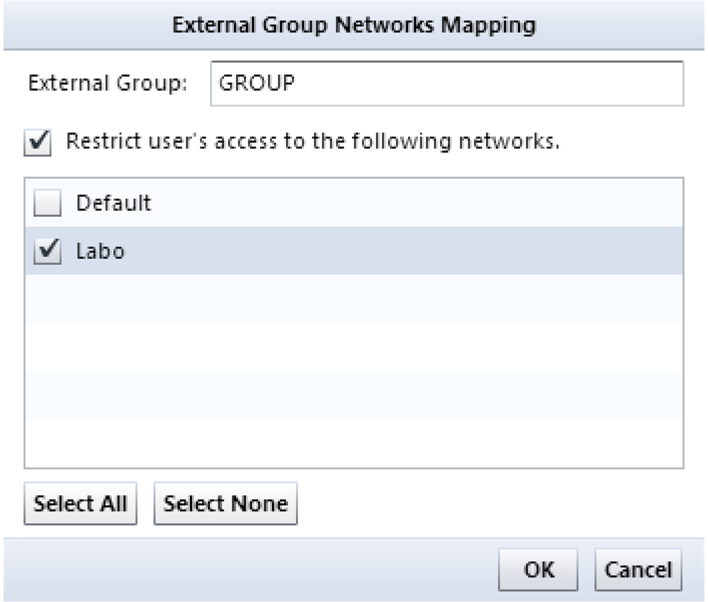
Shared Secret: ********

Character Encoding: UTF-8

External group mappings:

External Group	Networks

6. Enter the group that was set in the Filter-Id of the RADIUS server into the External Group field and select the networks that the users of the group should be able to see.



External Group Networks Mapping

External Group: GROUP

☑ Restrict user's access to the following networks.

□ Default

☑ Labo

➢ Users in this group will be given permission to see the selected networks.

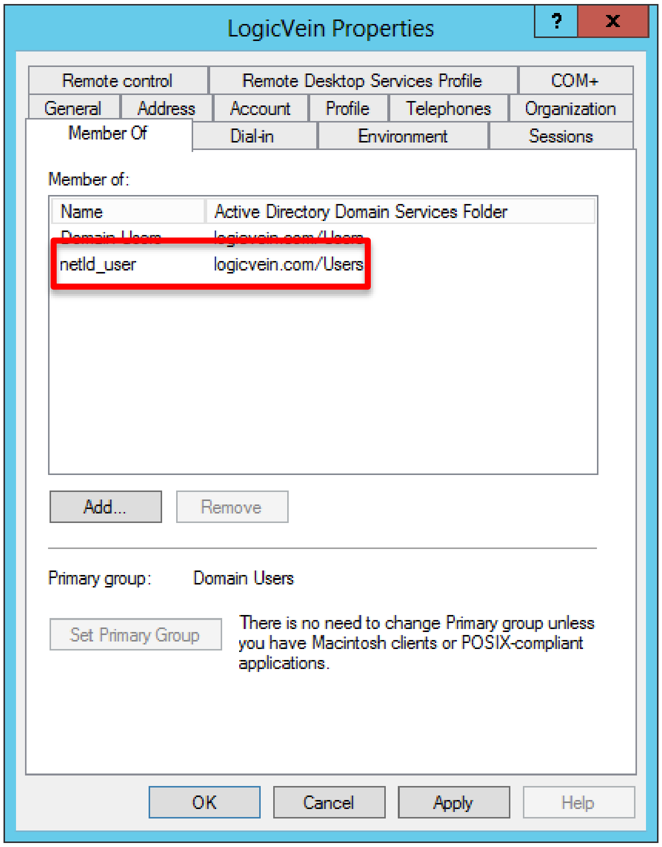
Setup is now complete. After saving the server setting by clicking **OK**, logout once and Login with the user configured in the RADIUS server.

Username: LogicVein

Password: ********

2. Integration with ActiveDirectory Server

When integrating with an ActiveDirectory server, determine netLD roles and networks by using the ActiveDirectory groups that the registered users are members of.



Member of:

Name	Active Directory Domain Services Folder
Domain Users	logicvein.com/Users
netld_user	logicvein.com/Users

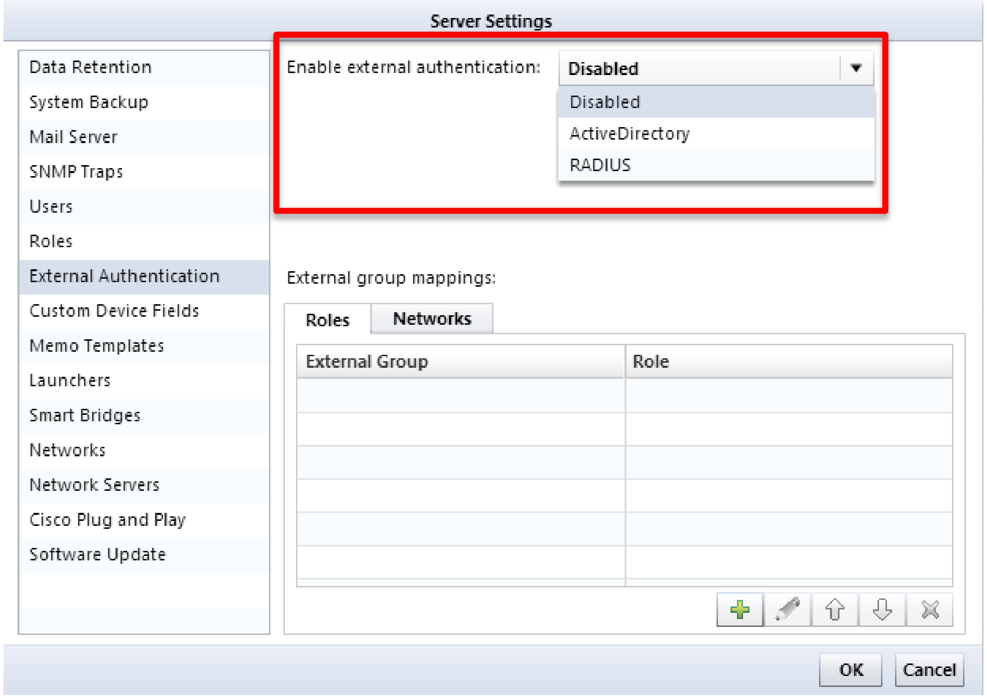
Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

<<Setting Procedures>>

In order to integrate with ActiveDirectory server, the settings can be configured in the **External authentication** page of the **Server Settings** dialog.

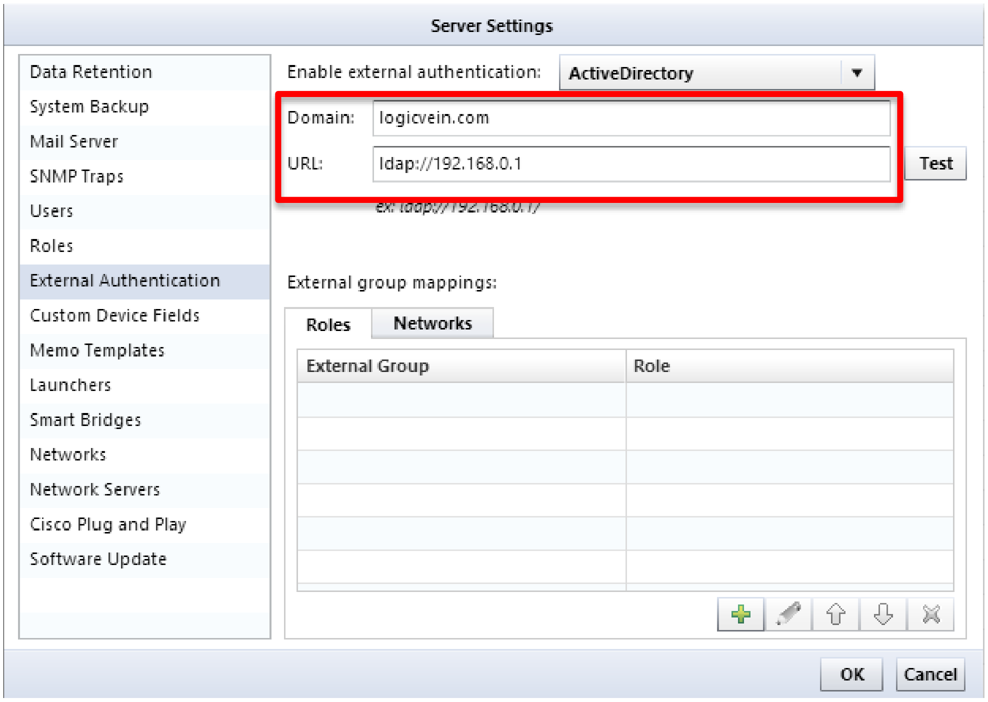
1. Select **ActiveDirectory** for **Enable external authentication**.



Server Settings

Enable external authentication: Disabled

2. Set the domain name and IP address (or Hostname) of the ActiveDirectory server.



Server Settings

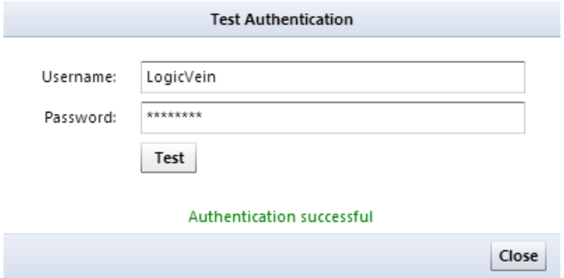
Enable external authentication: ActiveDirectory

Domain: logicvein.com

URL: ldap://192.168.0.1

ex: ldap://192.168.0.1/

- After setting the above, you can confirm the integration with ActiveDirectory server by clicking **Test** and providing a Username and Password. If there is no problem, the **Authentication successful** message will be shown.

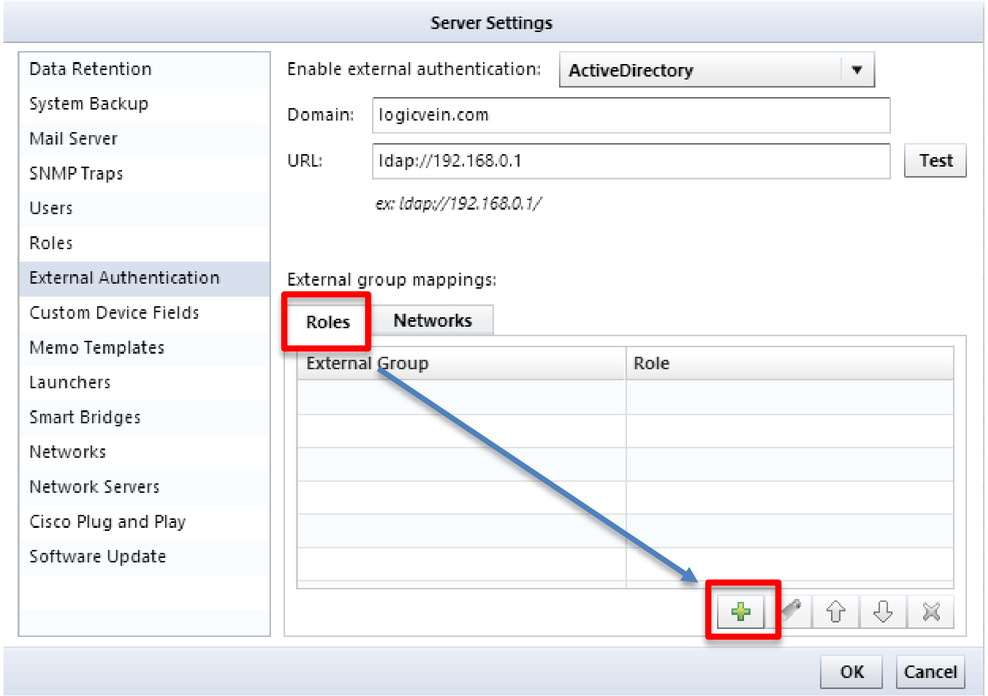

Test Authentication

Username: LogicVein

Password: ********

Authentication successful

3. Assign **Roles** using **External group mappings**. A mapping is added by clicking the [**+**] button.


Server Settings

Enable external authentication: ActiveDirectory

Domain: logicvein.com

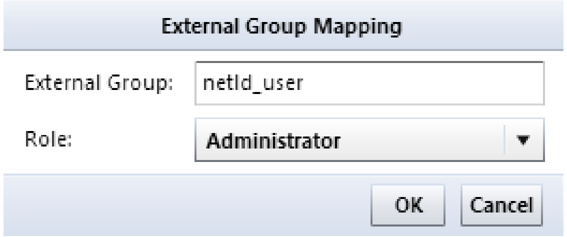
URL: ldap://192.168.0.1

ex: ldap://192.168.0.1/

External group mappings:

External Group	Role

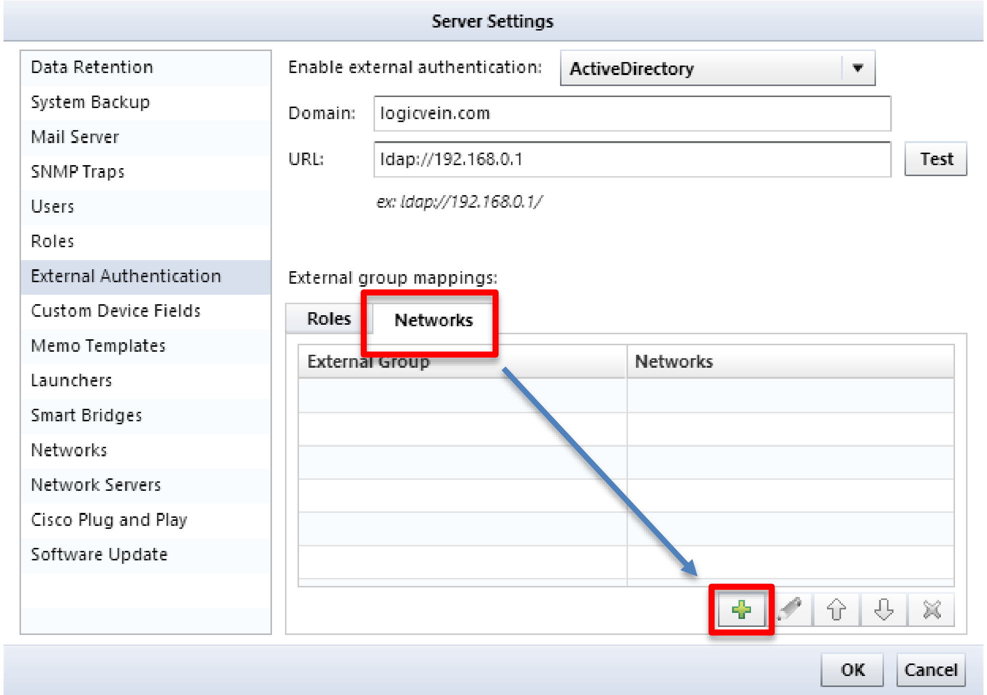
4. Enter an ActiveDirectory group that the user belongs to in the **External Group** field and select a netLD role to apply to the group.


External Group Mapping

External Group: netld_user

Role: Administrator

5. Assign **Networks** using **External group mappings**. A mapping is added by clicking the [**+**] button.



Enable external authentication: ActiveDirectory

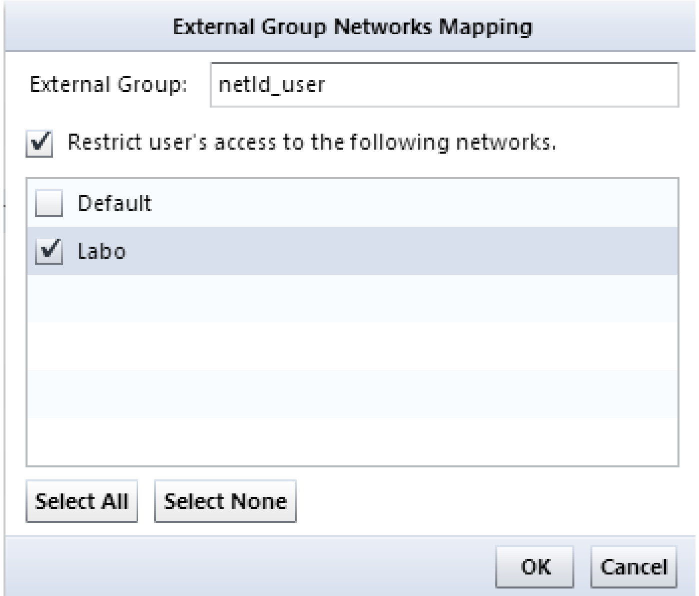
Domain: logicvein.com

URL: ldap://192.168.0.1

ex: ldap://192.168.0.1/

External group mappings:

6. Enter an ActiveDirectory group that the user belongs to in the **External Group** field and select the netLD networks that users of the group can see.



External Group: netld_user

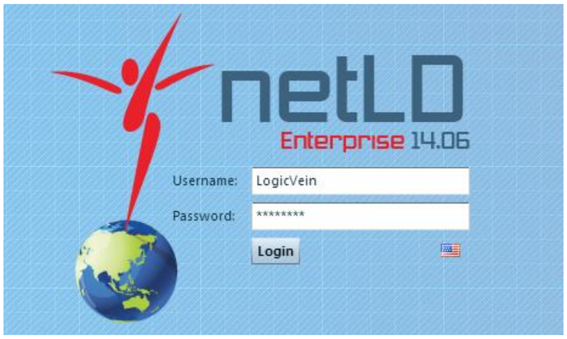
☑ Restrict user's access to the following networks.

☐ Default

☑ Labo

- Users in this group will be given permission to see the selected networks.

Setup is now complete. After saving the server settings by clicking **OK**, logout and Login with a user configured in the ActiveDirectory server.



Username: LogicVein
Password: ********