Est. USA 1981

www.AKCP.com

APS LDAP Manual

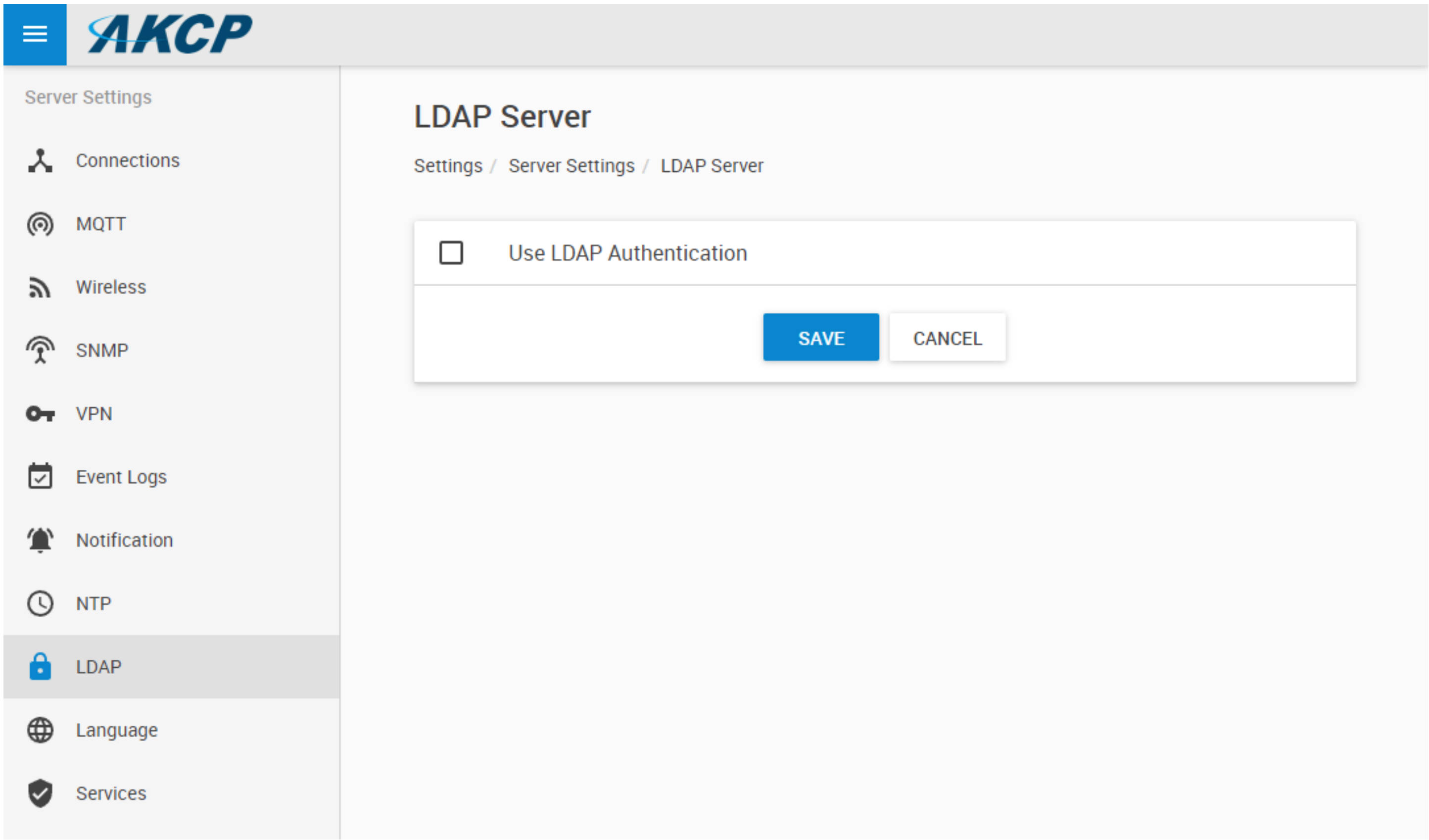
Introduction / What is Active Directory

Active Directory is Microsoft's Directory Server. It provides authentication and authorization mechanisms as well as a framework within which other related services can be deployed (AD Certificate Services, AD Federated Services, etc). It is an LDAP compliant database that contains objects. The most commonly used objects are users, computers, and groups. These objects can be organized into organizational units (OUs) by any number of logical or business needs. Group Policy Objects (GPOs) can then be linked to OUs to centralize the settings for various users or computers across an organization.

AKCPro Server (APS) supports LDAP authentication as an additional external user database, in conjunction with the internal users/groups database. The local user authentication method will remain available even when you have configured LDAP authentication.

APS LDAP Configuration

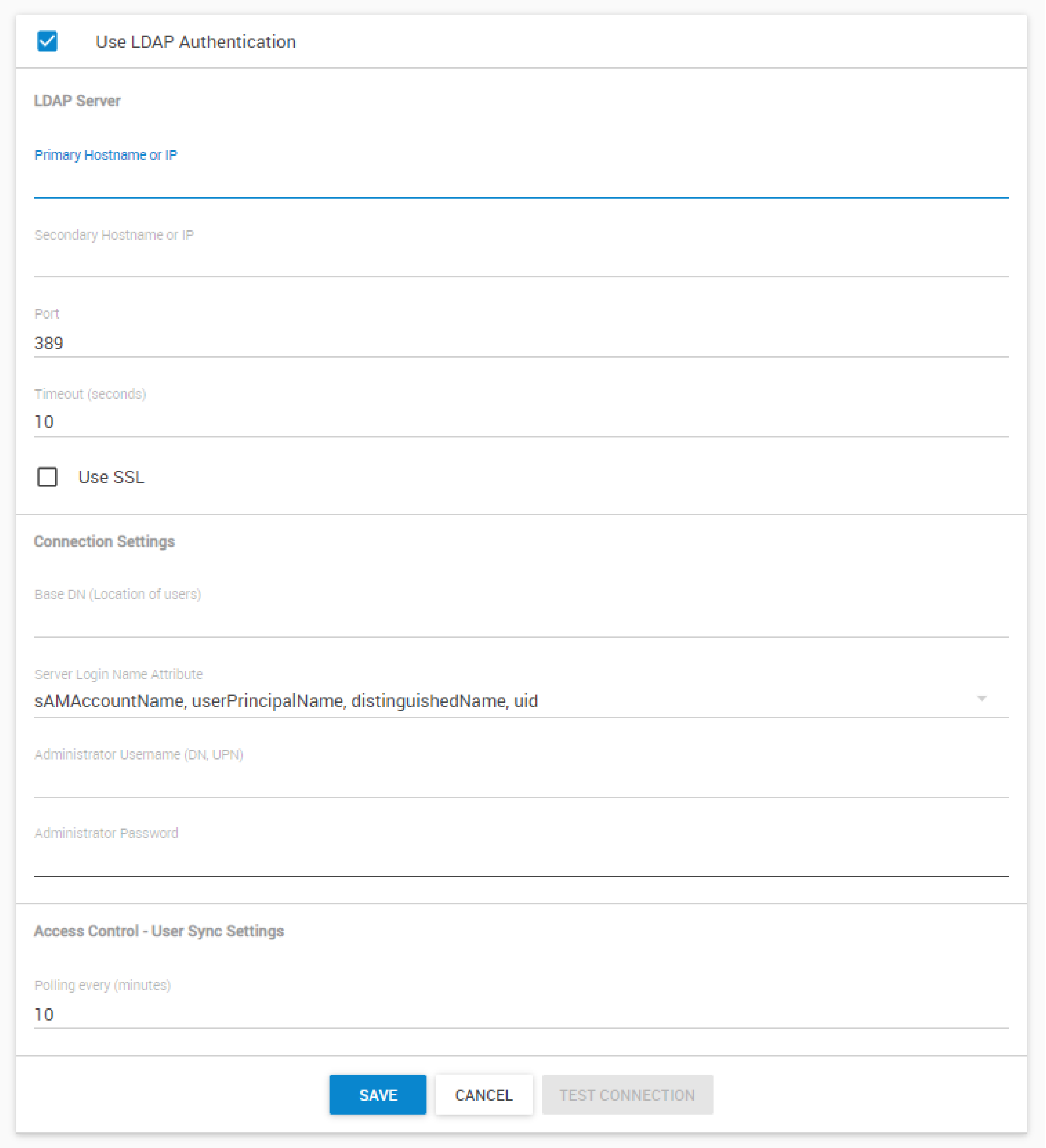
You will need to turn on LDAP support in the **Server Settings** page as shown on the screenshot below.



LDAP Server

Settings / Server Settings / LDAP Server

☐ Use LDAP Authentication



☑ Use LDAP Authentication

LDAP Server

Primary Hostname or IP

Secondary Hostname or IP

Port
389

Timeout (seconds)
10

□ Use SSL

Connection Settings

Base DN (Location of users)

Server Login Name Attribute
sAMAccountName, userPrincipalName, distinguishedName, uid

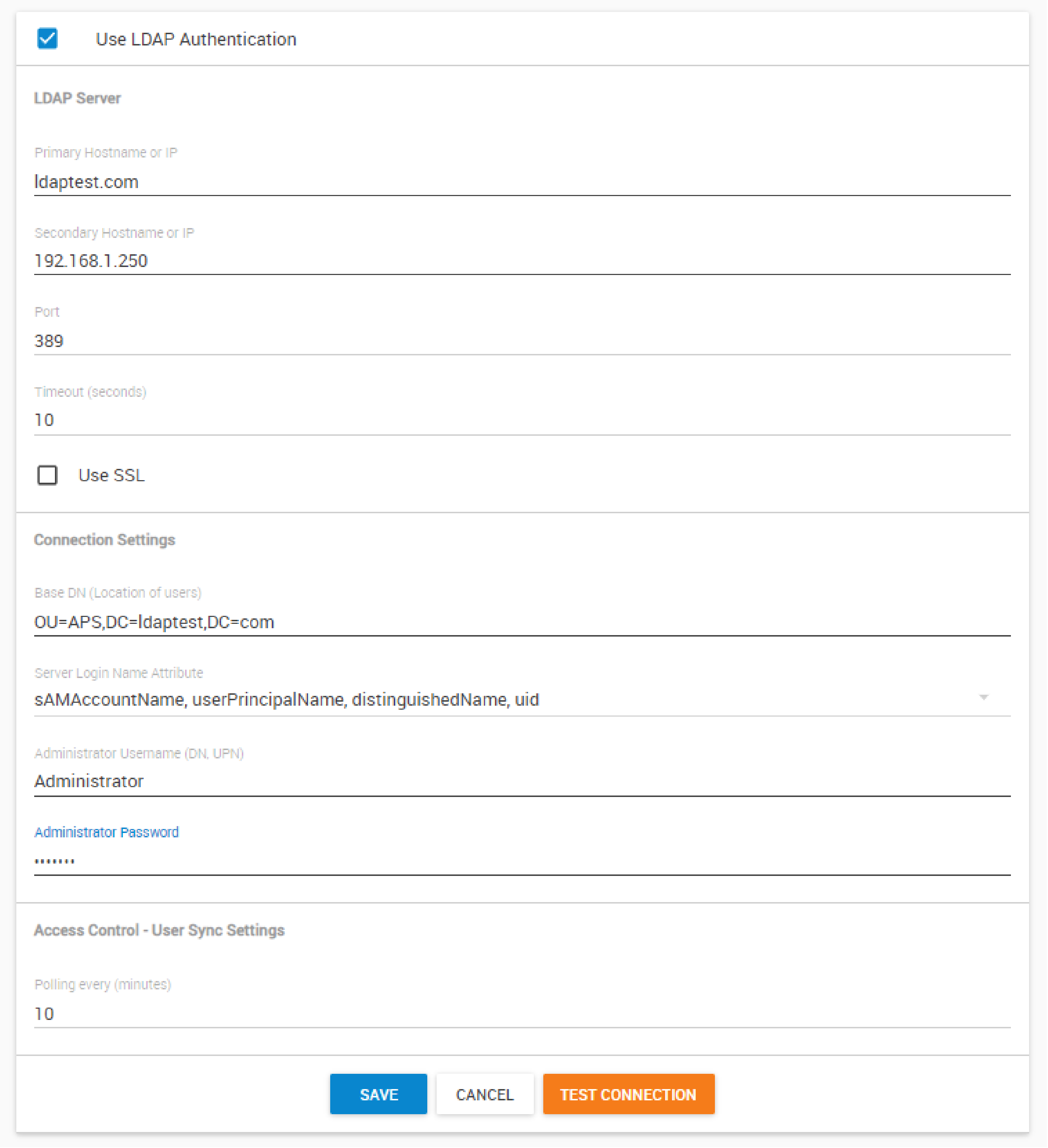
Administrator Username (DN, UPN)

Administrator Password

Access Control - User Sync Settings

Polling every (minutes)
10

You will need to fill out the connection parameters to the LDAP database; we will explain the settings below.



☑ Use LDAP Authentication

LDAP Server

Primary Hostname or IP
ldaptest.com

Secondary Hostname or IP
192.168.1.250

Port
389

Timeout (seconds)
10

☐ Use SSL

Connection Settings

Base DN (Location of users)
OU=APS,DC=ldaptest,DC=com

Server Login Name Attribute
sAMAccountName, userPrincipalName, distinguishedName, uid

Administrator Username (DN, UPN)
Administrator

Administrator Password
•••••••

Access Control - User Sync Settings

Polling every (minutes)
10

LDAP Server

You can set a hostname for the LDAP server (APS v14 and up), or an IP address.
If there are multiple LDAP servers, you can configure a secondary hostname or IP for redundancy. Any available server will be able to authenticate users even if the others are unreachable (using DNS round-robin).

Note: DNS needs to be able to resolve this domain and hostname, otherwise it will not work! On a domain-joined PC this is not an issue. But with computers not added to the domain, check that you are using the LDAP server's IP in the DNS settings (must be the first DNS).

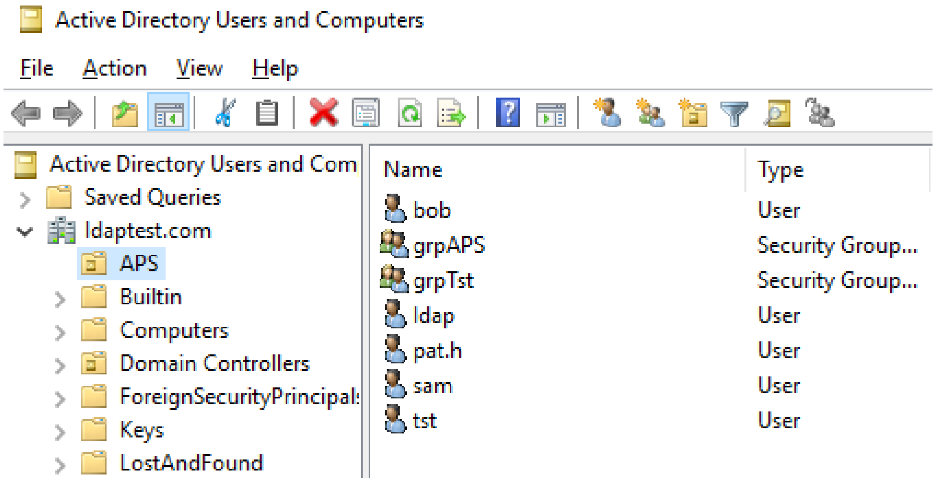
LDAP Port

The unencrypted LDAP port is **389** which should always work. It is recommended to use this for first time testing.
The secure port is **636**. You will need to click the option “use SSL” to enable the LDAPS protocol which supports encryption and establishes TLS/SSL upon connecting with the server.

User Location

This defines the LDAP location where APS should check for the user objects.
Since APS v14 the system supports finding users under the whole top-level domain, not just under a specified OU (Organizational Unit).

For example if you have a domain named *ldaptest.com* then configure the Base DN setting as:
`DC=ldaptest,DC=com`
Then APS will be able to find all users in the whole domain, regardless of which sub-OU they reside in.



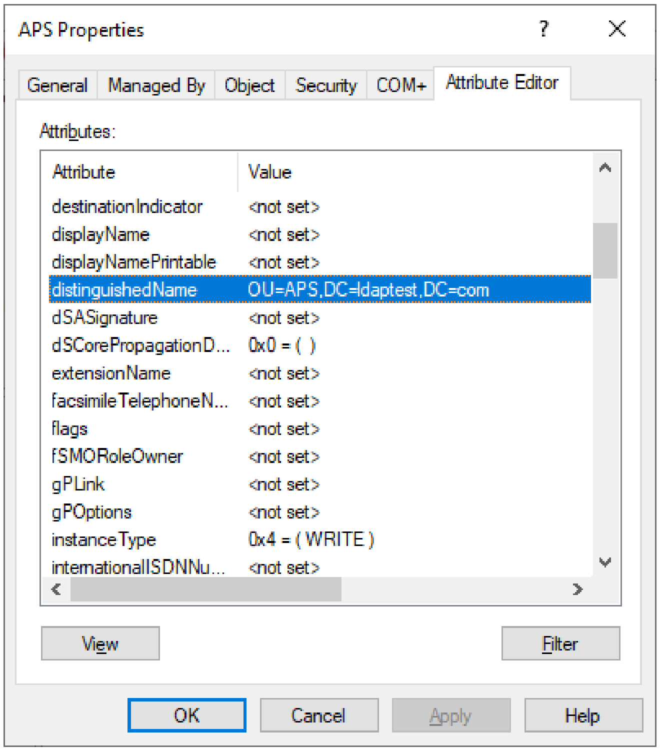
- Active Directory Users and Com
  - Saved Queries
  - ldaptest.com
    - APS
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipal:
    - Keys
    - LostAndFound

Name	Type
bob	User
grpAPS	Security Group...
grpTst	Security Group...
ldap	User
pat.h	User
sam	User
tst	User

However, if you need to restrict APS user login to a specified OU, define the OU location as well. Example to restrict logins only for users under the APS OU:

```
OU=APS,DC=ldaptest,DC=com
```

To find the correct format of the LDAP location, you can check it in **Active Directory Users and Computers console** by selecting the properties of an OU:



Attributes:

Attribute	Value
destinationIndicator	<not set>
displayName	<not set>
displayNamePrintable	<not set>
distinguishedName	OU=APS,DC=ldaptest,DC=com
dSASignature	<not set>
dSCorePropagationD...	0x0 = ( )
extensionName	<not set>
facsimileTelephoneN...	<not set>
flags	<not set>
fSMORoleOwner	<not set>
gPLink	<not set>
gPOptions	<not set>
instanceType	0x4 = (WRITE)
internationalISDNNu...	<not set>

It is the **distinguishedName** attribute's value. You may need to turn on the "Advanced features" in order to see the Attribute Editor tab.

Logon Attributes

With this setting you can define which attribute will be checked during logon with the LDAP database for a matching username.
By default all supported attributes are selected and enabled, but it can be set to a specific attribute for checking the login names.
The standard logon attribute is the SAMAccountName.

Available attributes (APS v14 and up):

- SAMAccountName
- userPrincipalName
- distinguishedName
- uid

APS v13 and below only checks the SAMAccountName attribute.

Note: During logon to APS, you can also use an LDAP login name which has a dot in the username ex.: bob.h

Administrator User

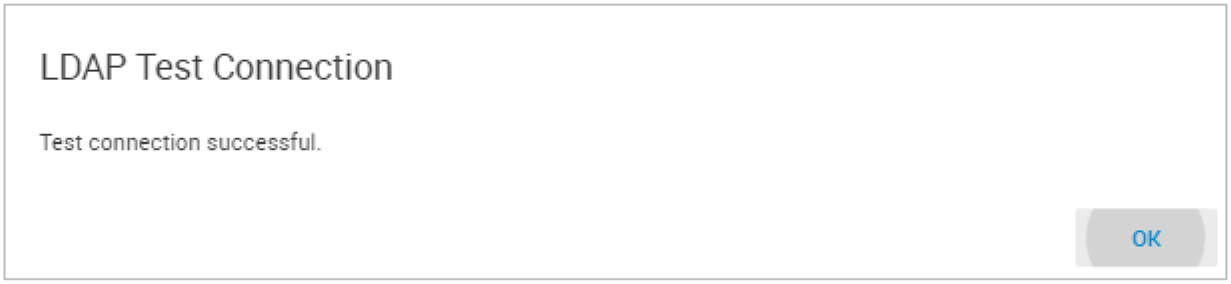
The administrator username should be a domain admin, who has access to read all parameters of the domain (no write access is needed for APS).

Access Control Sync

This setting currently has no effect, since all LDAP users who log in at least once will be automatically imported and created under APS Access Control. After this process, the card ID and door access permissions can be customized for them.

Note: The LDAP users will NOT be removed from APS access control list when you disable or remove the LDAP user from the LDAP side, but they will no longer be able to log in or access the doors with APS.

After seting the LDAP parameters, save them first and press the **'Test Connection**' to check if APS can connect to the server.



LDAP Test Connection

Test connection successful.

If the information is correct, the test connection should be successful.

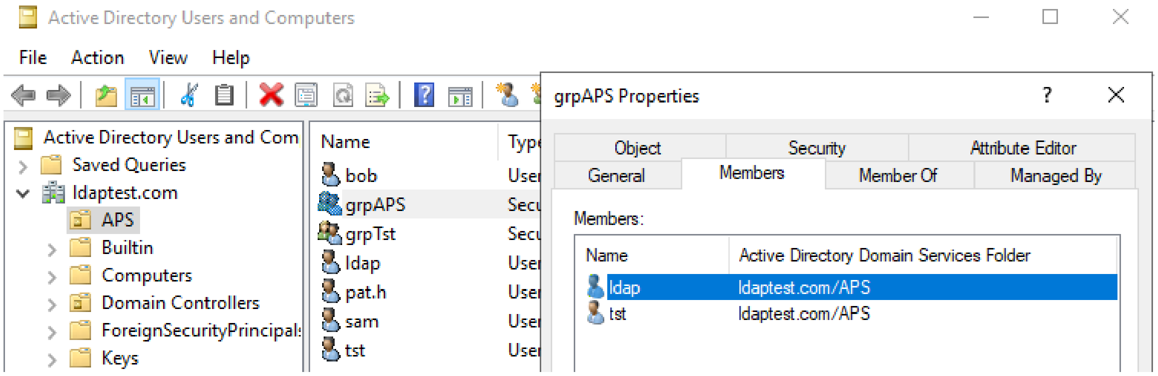
Note that you will need to reenter the Administrator password when you make changes to the LDAP settings.

Managing Permissions

1. Managing permissions with groups

Since APS v14 and up, the default LDAP user permissions are controlled by the **LDAP User Group** permissions within the APS Account Settings.
By default, this group has no permissions defined, therefore all LDAP users will have just “guest” rights, and won’t be able to see or manage almost anything in APS. With this default access level, you won’t be able to see any hosts or settings or logs.

The recommended way to manage LDAP user rights is to create groups in the local APS database with matching group names as with the LDAP security group’s name, and customize the group’s access levels.
We will show this below with an example.



Name	Active Directory Domain Services Folder
ldap	ldaptest.com/APS
tst	ldaptest.com/APS

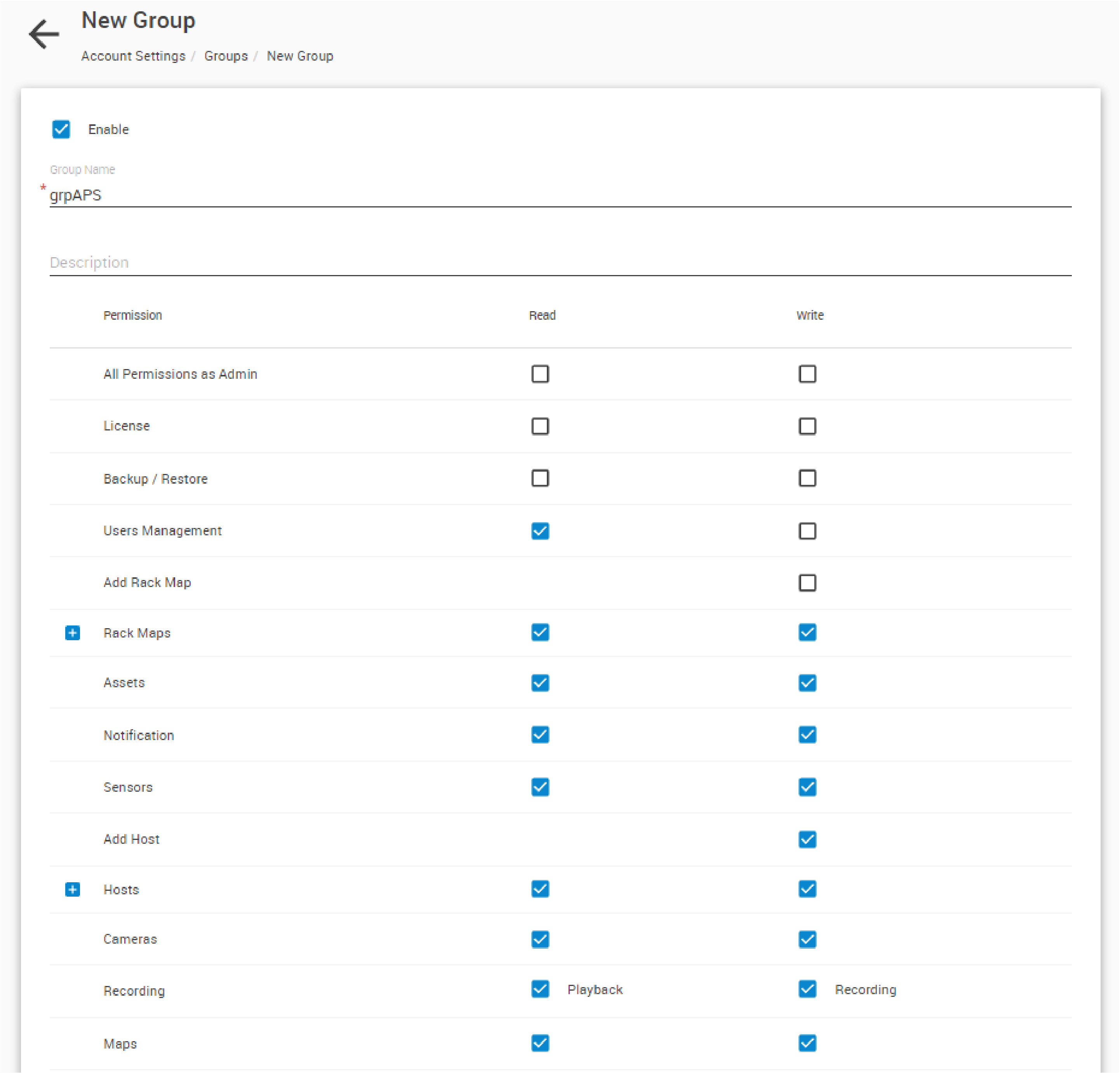
Assume that you have a group in LDAP with the name “grpAPS”. There are users added to this group already.
Now create the same group name in APS **Account Settings** as it is in LDAP: “grpAPS”.

This way you can set custom rights for specific user groups. You can set “grpAPS” to have read-write access to some parts of APS, and allow only specific hosts to be visible for example.

Important: No need to recreate every user’s logins in APS, only the group name. All users who are a member in that group of the LDAP database will be able to log in with the customized rights for that group.

Note that LDAP user group membership changes are recognized immediately (at logon) and restrictions apply accordingly.

See an example picture below with customized APS read/write access settings for this group.



New Group

Account Settings / Groups / New Group

☑ Enable

Group Name

* grpAPS

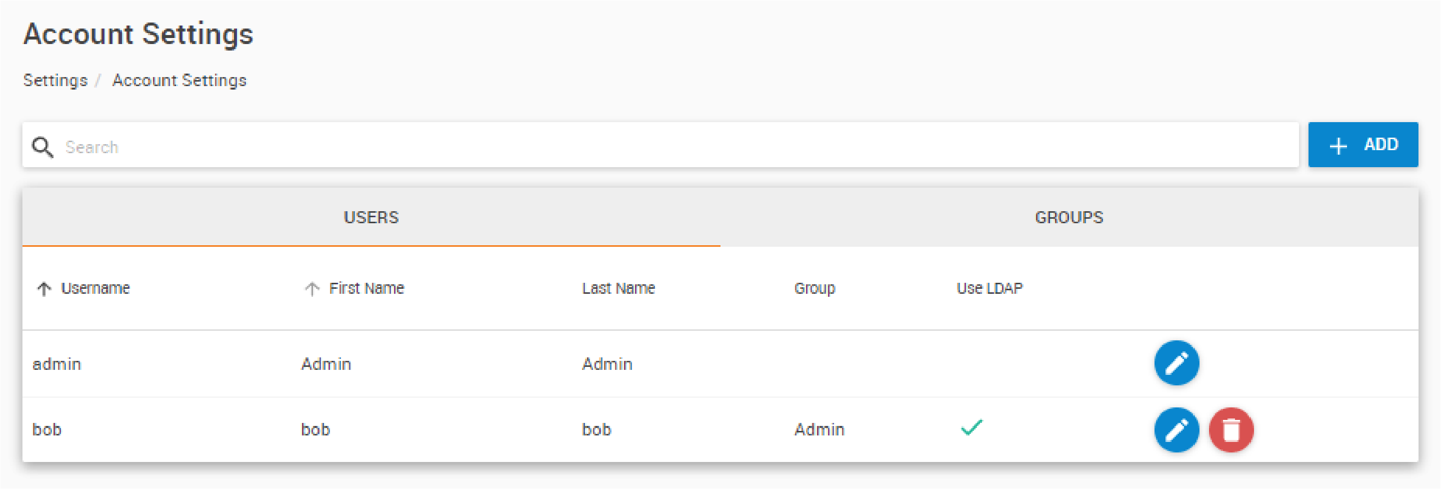
Description

	Permission	Read	Write
	All Permissions as Admin	☐	☐
	License	☐	☐
	Backup / Restore	☐	☐
	Users Management	☑	☐
	Add Rack Map		☐
⊞	Rack Maps	☑	☑
	Assets	☑	☑
	Notification	☑	☑
	Sensors	☑	☑
	Add Host		☑
⊞	Hosts	☑	☑
	Cameras	☑	☑
	Recording	☑ Playback	☑ Recording
	Maps	☑	☑

2. Managing permissions with users

If the LDAP option is configured for APS, you will see an additional LDAP Authentication column and an “Enable LDAP” option in the User & Group management.

Note: Enabling LDAP authentication for the built-in admin user is not allowed.



Account Settings

Settings / Account Settings

↑ Username	↑ First Name	Last Name	Group	Use LDAP
admin	Admin	Admin		
bob	bob	bob	Admin	✓

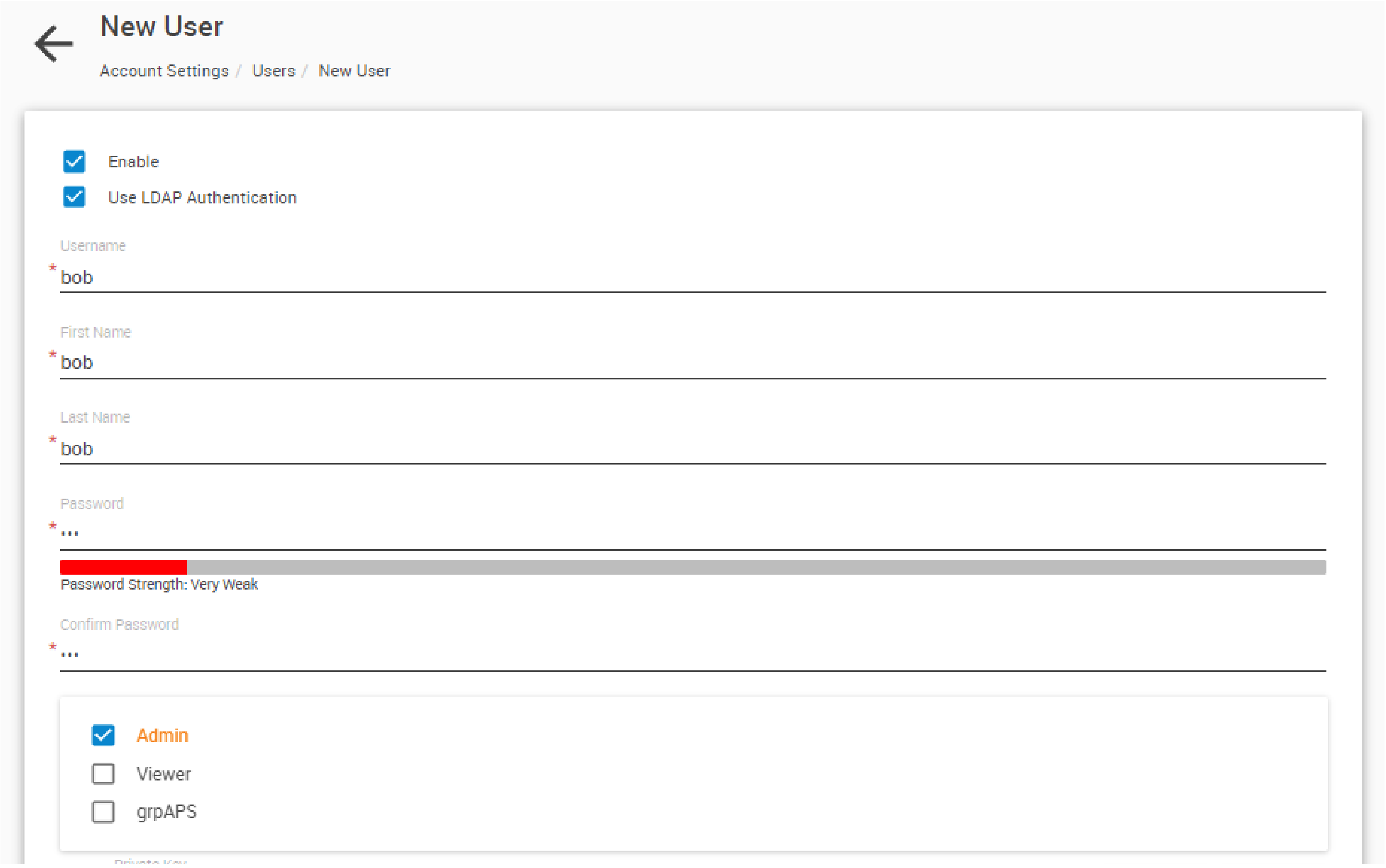
By creating the user in the APS local database, you will be able to customize the desktop layout and force using a different security group for that user (if the LDAP group membership would set a different group permission).

If you have an existing local user with the same login name as on LDAP, and then enable LDAP authentication for it, the custom desktop settings will be preserved (migrated).

The LDAP password only works when LDAP is enabled for the account, otherwise it will use the APS password.

If you disable a user account in LDAP which has been added to Access Control, the user will not be able to log in but will not be removed from APS Access Control list.

See an example picture below with a new user that has LDAP authentication turned on, but a different security group is chosen.



New User

Account Settings / Users / New User

☑ Enable

☑ Use LDAP Authentication

Username
* bob

First Name
* bob

Last Name
* bob

Password
* •••

Password Strength: Very Weak

Confirm Password
* •••

☑ Admin

□ Viewer

□ grpAPS

Configured this way, this user will be able to get Admin permissions within APS, even if the LDAP user group is just a standard user.

Please contact support@akcp.com if you have any further technical questions or problems.

Thanks for Choosing AKCP!