

# LDAP authorization function



The description is valid for software version [2.10.119.99](#) and newer.



. Activating the authorisation function via LDAP does not disable the inbuilt accounts, but supplements this mechanism. To use local accounts, select Authentication=Internal User in the [Storage](#) settings of the client application and continue to use the accounts created in the Storage module.

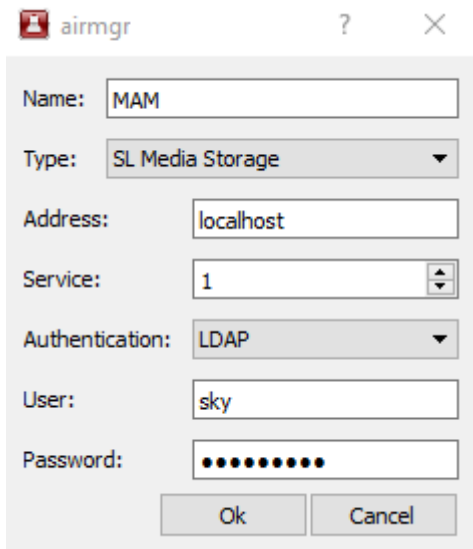
In the [2.10.37.99](#) version, the ability to authorise [media storage](#) users via the LDAP protocol has been added.

## General Information

- **LDAP (Lightweight Directory Access Protocol)** is an open standardised protocol used for various directory service implementations, including Active Directory. LDAP allows users to access resources based on the permissions configured by the directory service administrator.
- **Active Directory (AD)** is a proprietary implementation of Microsoft's directory service - a set of software services and databases for hierarchical representation of company resources (departments, computers, printers, network drives, etc.) and configuring access to them.

## How It Works

- In the [module Storage](#) (Administrator Control Panel→Status→Storage\_N→Manage Users...→Manage Groups→Add New Group) user groups are created that will correspond to the implemented technical process (for example: Skylark Editors, Skylark Operators, Skylark Users, etc.).
- In the Directory Service, user groups are created with the same names as defined in the Storage module. If you are using Active Directory, this can be done through the Active Directory Users and Computers snap-in `dsa.msc`.
- Users are only created in the Directory Service.
- Users created in the directory service are assigned the desired groups based on their role in the workflow.
- If the LDAP function is enabled in the Storage module and Authentication=LDAP authorisation type is selected in the client application, the specified username and password will be verified through the LDAP server.



- If authentication is successful, all groups assigned to the user will be retrieved from the memberOf attribute.
- The retrieved groups will be matched with the groups created in the Storage module, if a match is found, then [rights of such group](#) are assigned to the user. The built-in Everyone group is assigned to the user in any case.

In addition, user name, phone number and email address information can be downloaded from the directory service and synchronised on a regular basis.

When a user is authorised via LDAP, the login is cached for 30 seconds. This must be taken into account when working in a real system. For example, if a new group is assigned to a user in the directory service, its mapping may occur with the specified delay.

## Obtaining Data from Active Directory

You can obtain the data required to configure the function using the Get-ADUser command in the Power Shell. You must run Power Shell as an administrator to display all available data.

Command examples:

Display a summary of user information:

```
Get-ADUser -filter *
```

```
PS C:\Windows\system32> Get-ADUser -filter *
DistinguishedName : CN=sky0,OU=TestOU,DC=SRT,DC=local
Enabled           : True
GivenName        : sky1
Name             : sky0
ObjectClass      : user
ObjectGUID       : 
SamAccountName    : sky
SID              : S-1-
Surname          :
UserPrincipalName : sky@SRT.local
```

Output extended information about the selected user:

GetADuser -identify <USERNAME> -properties \*

```

PS C:\Windows\system32> Get-ADUser -identity sky -properties *

AccountExpirationDate      : 11.12.2023 0:00:00
accountExpires             : 133467156000000000
AccountLockoutTime        :
AccountNotDelegated       : False
AllowReversiblePasswordEncryption : False
AuthenticationPolicy      : {}
AuthenticationPolicySilo  : {}
BadLogonCount             : 0
badPasswordTime           : 0
badPwdCount               : 0
CannotChangePassword      : False
CanonicalName             : SRT.local/TestOU/sky0
Certificates               : {}
City                      :
CN                        : sky0
codePage                  : 0
Company                   :
CompoundIdentitySupported  : {False}
Country                   :
countryCode               : 0
Created                   : 10.11.2023 18:43:25
createTimeStamp           : 10.11.2023 18:43:25
Deleted                   :
Department                :
Description                :
DisplayName                : sky1
DistinguishedName         : CN=sky0,OU=TestOU,DC=SRT,DC=local
Division                  :
DoesNotRequirePreAuth     : False
dSCorePropagationData     : {15.11.2023 13:34:02, 01.01.1601 3:00:00}
EmailAddress              :
EmployeeID                :
EmployeeNumber            :
Enabled                   : True
Fax                       :
GivenName                 : sky1
HomeDirectory              :
HomedirRequired          : False
HomeDrive                 :
HomePage                  :
HomePhone                 :
Initials                  :
instanceType              : 4
isDeleted                 :
KerberosEncryptionType    : {None}
LastBadPasswordAttempt     :
LastKnownParent           :
lastLogoff                : 0
lastLogon                 : 0
LastLogonDate             : 15.11.2023 12:28:01
lastLogonTimestamp        : 133445140813525800
LockedOut                  : False
lockoutTime               : 0
logonCount                : 0
LogonWorkstations         :
Manager                   :
MemberOf                  : {CN=Skylark Operators,CN=Users,DC=SRT,DC=local}
MNSLogonAccount           : False
MobilePhone               :
Modified                  : 15.11.2023 13:34:02
modifyTimeStamp           : 15.11.2023 13:34:02

```

A short list of frequently used values:

- **DistinguishedName** - the entry's location in the directory,
- **MemberOf** - list of groups associated with the user,
- **SamAccountName** - user login (e.g. sky),
- **CN** - user's display container name (e.g. sky),
- **DisplayName** - user's visible name (e.g., "User Skylark"),
- **telephoneNumber** - phone number,

- **mail** - email,
- **ObjectClass** - specifies the object type (e.g. user - user).

# Configuration

## Server Part

LDAP server connection parameters are configured on the tab: Administrator Control Panel→Manage→Storages→Storage\_N→LDAP.

neovid

- [Status](#)
- [Manage](#)
- [Transfer](#)
- [API Keys](#)
- [License](#)
- [Users](#)
- [Files](#)
- [Logs](#)
- [Quit](#)

Configuration loaded    
CPU clusters:   Use NVENC for Preview

Video IO Boards Program Outputs Recorders Recording Managers Storages GPI Boards RSS Feeds Godot Engines Multiscreens

Storage 1

Service Enabled Name: Storage\_1 ( [Change](#) )

Storage parameters Volumes BXF Connector Archive parameters Web Proxy Metadata Connectors BroadView Connector

LDAP

Enabled

Server Address:

Encryption:

Enable User Name Mapping

Admin DN:

Admin Password:

Display Name Attribute:

User Search DN:

AD Object Class:

AD Object Identifier:

User Permissions Attribute:

Group Base DN:

Group Object Identifier:

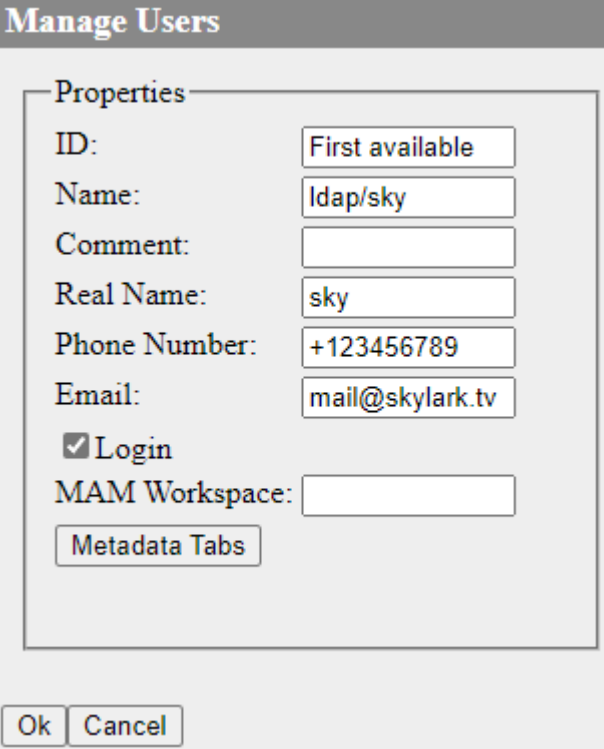
User Real Name Attribute:

User Phone Number Attribute:

User Email Attribute:

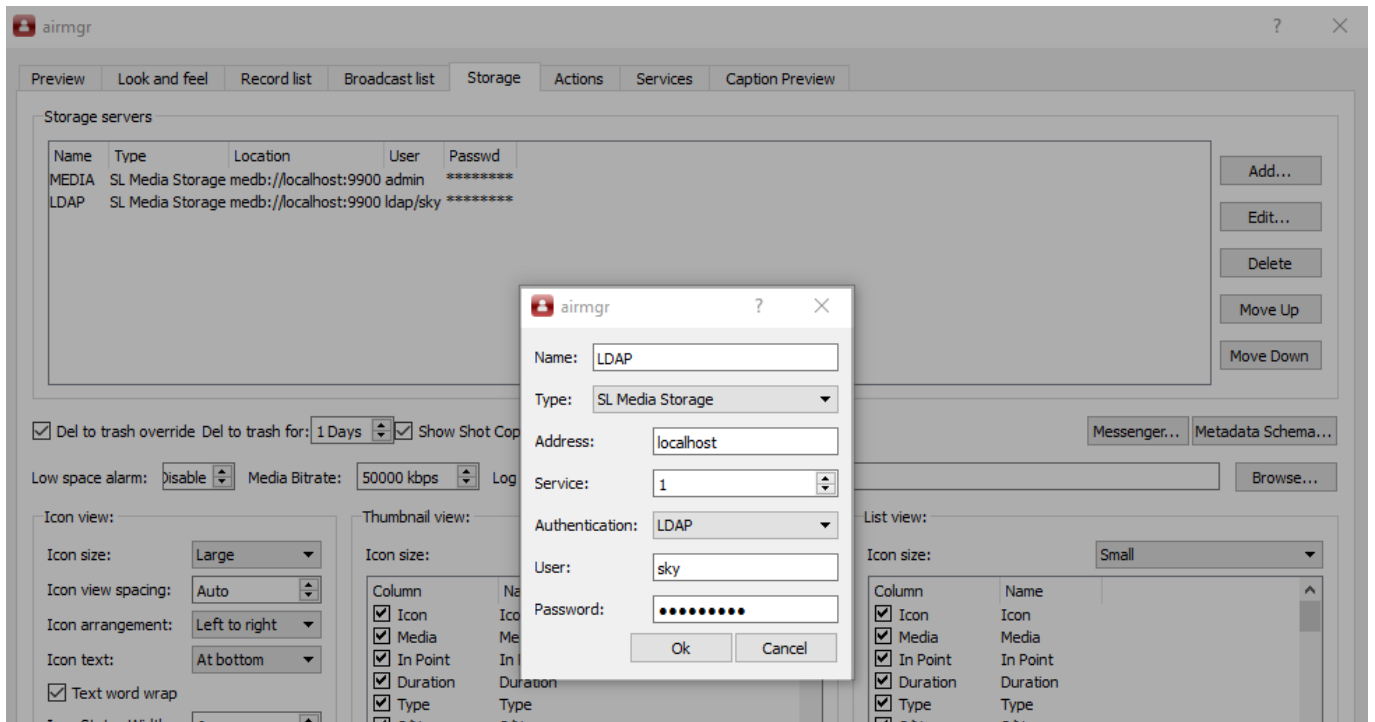
Parameter	Description
<b>Enabled</b>	Activates the LDAP connection function.
<b>Server Address</b>	The field specifies the address of the server with the directory service and the connection port in the format: ip_address : port. If no port is specified, the default TCP port is 389. Your directory service port may be different from the default.

Parameter	Description
<b>Encryption</b>	Select the encryption mode: <ul style="list-style-type: none"> <li>• <b>None</b> - no encryption,</li> <li>• <b>SSL</b> - use SSL encryption,</li> <li>• <b>TSL</b> - use TSL encryption.</li> </ul> Please note that for LDAPS (LDAP over SSL) secured connections, TCP port 636 is normally used. For non-encrypted connections, the default TCP port is 389. Your directory service port may be different from the default.
<b>Enable User Name Mapping</b>	Option enables the ability to read additional attributes of directory accounts, which allows you to read the user login (SamAccountName field) in Active Directory.
<b>Admin DN</b>	The field specifies the DistinguishedName value for the account that will be used to retrieve data from the directory. The account must have the appropriate permissions to access the attributes of the directory.
<b>Admin Password</b>	The field specifies the password for the account that will be used to retrieve data from the catalogue. The password is encrypted when saved.
<b>Display Name Attribute</b>	The name of the attribute that will be matched with the login of the user being authorised in the media storage. In fact, enabling this feature activates the index construction for the Display Name Attribute→AD Object Identifier transformation. For Active Directory this field will have the value - SamAccountName. If no match is found, the attempt to authorise the user will fail with an error: LDAP Auth error received on bind attempt.
<b>User Search DN</b>	The directory path to the location of the user accounts where the user to be authorised will be searched. For example, it can be found using the DistinguishedName value. Example value: OU=TestOU,DC=DomainName,DC=local.
<b>AD Object Class</b>	Sets the searched ObjectClass value for objects of type user, which allows you to filter other object types if they are in the same location specified by the 'User Search DN'. Most often this field will have the value user.
<b>AD Object Identifier</b>	The object identifier used for directory-side authentication. The value of this attribute will be directly matched to the user name being authorised unless the 'Enable User Name Mapping' option is used. If no match is found, the attempt to authorise the user will fail with an error: 'LDAP Auth error received on bind attempt'. Example value: CN.
<b>User Permissions Attribute</b>	The name of the attribute that will be used to search for assigned groups. Example value for Active Directory: MemberOf.
<b>Group Base DN</b>	The path in the directory to the location of the user group records where the assigned groups will be searched. Example value: OU=TestOU,DC=DomainName,DC=local.
<b>Group Object Identifier</b>	The name of the identifier/attribute whose value will be matched against the group names found in the user account. Example value: CN.

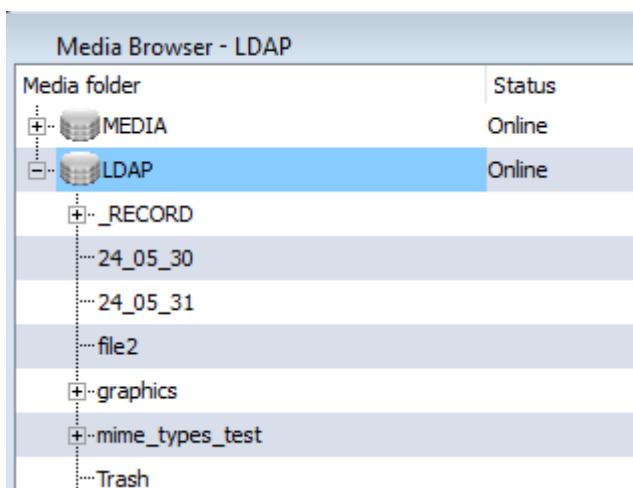
Parameter	Description
<p><b>User Real Name Attribute</b></p>	<p>The name of the attribute containing the real name of the user. The information will be broadcast to the corresponding fields of the account in media storage:</p>  <p>Added in version 2.10.65.99.</p>
<p><b>User Phone Number Attribute</b></p>	<p>Name of the attribute containing the phone number. Added in version 2.10.65.99.</p>
<p><b>User Email Attribute</b></p>	<p>The name of the attribute containing the user's email address. Added in version 2.10.65.99.</p>

### Client Side

To start using LDAP accounts, on the [Storage| tab](#) of client applications, select Authentication=LDAP and specify your directory service account details.



If the connection is successful, the media storage will switch to the online status and you will see the folders and files:



## Application

The function can be used as part of [MAM servers](#) in large companies with centralised user account management based on directory services.

From: <https://wiki.skylark.tv/> - [wiki.skylark.tv](https://wiki.skylark.tv/)

Permanent link: <https://wiki.skylark.tv/modules/storage/ldap>

Last update: **2025/01/16 09:22**

