

LDAP_Servers

- [Introduction](#)
- [How Does it Work?](#)
- [Creating a LDAP Server Entry](#)
- [View a LDAP Server Details](#)
- [Database Schema](#)
- [API / Web Access](#)

Introduction

Open-Audit can be configured to use LDAP servers (Microsoft Active Directory and/or OpenLDAP) to authenticate and authorize a user and in addition, to create a user account in Open-Audit using assigned roles and orgs based on LDAP group membership.

How Does it Work?

If using Active Directory, you do not need to populate the `user_dn` or `user_membership_attribute` attributes. These are used by OpenLDAP only.

If the user logging on to Open-Audit does not have the access to search LDAP, you can use another account which does have this access. Use the `dn_account` and `dn_password` to configure this.

Examples:

If you need to configure OpenLDAP access for your users and a given users access DN is normally `uid=username@domain,cn=People,dc=your,dc=domain,dc=com` then you should set `base_dn` to `dc=your,dc=domain,dc=com` and `user_dn` to `uid=@username@domain,cn=People`. The special words `@username` and `@domain` will be replaced by the login details provided by your user on the login page.

If you need to configure Active Directory access, you can usually use the example of `cn=Users,dc=your,dc=domain,dc=com` for your `base_dn`. here is no need to set `user_dn`.

These are only examples. You may need to adjust these attributes to suit your particular LDAP.

If you are using Open-Audit Professional or Enterprise and you enable LDAP and you wish for user accounts to be automatically created at logon, you must edit the (text) file:

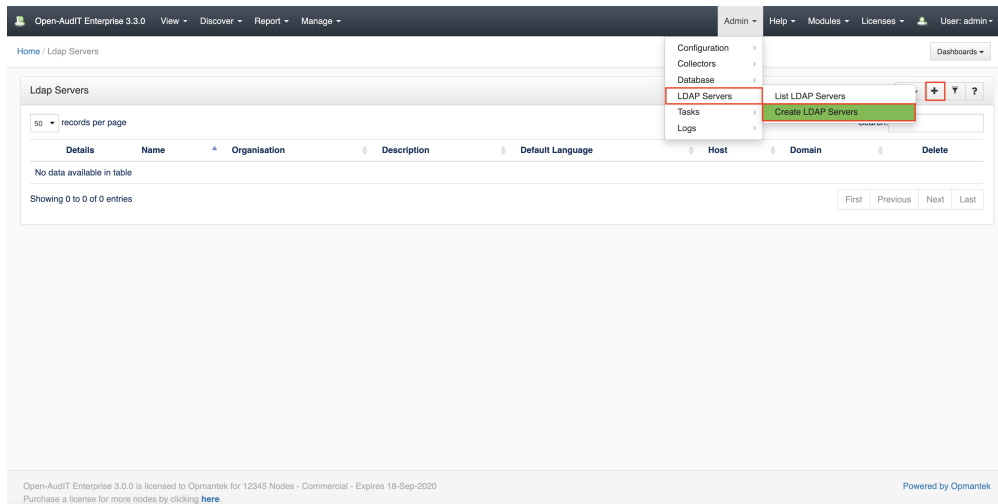
Linux – `/usr/local/omk/conf/opCommon.nmis`

Windows – `c:\omk\conf\opCommon.nmis`

And ensure that `auth_method_1` is set to `openaudit`.

Creating a LDAP Server Entry

A LDAP Server can be created using the web interface if a user has a role that contains the `ldap_servers::create` permission. Go to menu: Admin -> Ldap Servers-> Create Ldap Server. There is also a create button on the collection page.



The screenshot shows the 'Ldap Servers' configuration form in the Open-Audit Enterprise 3.3.0 interface. The form is divided into two main sections: 'Ldap Servers' on the left and 'About' on the right. The 'Ldap Servers' section contains various input fields and dropdown menus for configuring an LDAP server. The 'About' section provides information about LDAP servers and configuration examples.

Ldap Servers Configuration Fields:

- Name: [Text Field]
- Org ID: [Dropdown Menu]
- Description: [Text Field]
- Domain: [Text Field]
- Host: [Text Field]
- Port: [Text Field]
- Use Secure (LDAPs): [Dropdown Menu]
- Version: [Text Field]
- Use LDAP for Authentication: [Dropdown Menu]
- Use LDAP for Roles: [Dropdown Menu]
- Type: [Dropdown Menu]
- Base DN: [Text Field]
- User DN: [Text Field]
- User Membership Attribute: [Text Field]
- Refresh: [Text Field]
- Language: [Dropdown Menu]
- DN Account: [Text Field]
- DN Password: [Text Field]

About Section:

Open-Audit can be configured to use LDAP servers (Microsoft Active Directory and/or OpenLDAP) to authenticate a user and in addition, to create a user account using assigned roles and groups based on LDAP group membership.

For more detailed information, check the Open-Audit Knowledge Base.

Notes

If using Active Directory, you do not need to populate the `user_dn` or `user_membership_attribute` attributes. These are used by OpenLDAP only.

If the user logging on to Open-Audit does not have the access to search LDAP, you can use another account which does have this access. Use the `dn_account` and `dn_password` to configure this.

Examples

If you need to configure OpenLDAP access for your users and a given users access DN is normally `uid=username@ldap.example.com`, then you should set `base_dn` to `dc=your_domain,dc=com` and `user_dn` to `uid=username@ldap.example.com`. The special words `%username` and `%domain` will be replaced by the login details provided by your user on the login page.

If you need to configure Active Directory access, you can usually use the example of `cn=Administrator,cn=Users,dc=your_domain,dc=com`. For your base_dn, there is no need to set `base_dn`.

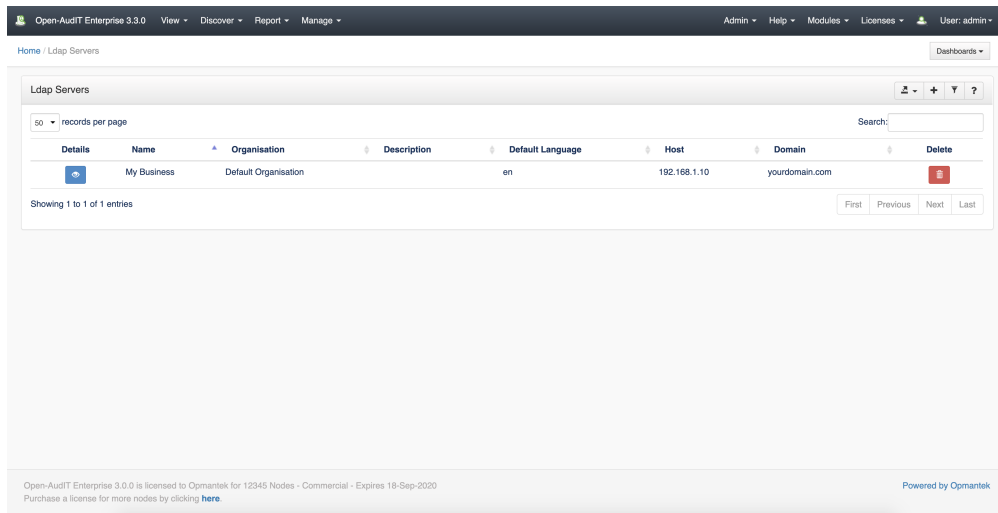
These are only examples. You may need to adjust these attributes to suit your particular LDAP.

View a LDAP Server Details

Go to menu: Admin -> Ldap Servers-> List Ldap Servers.

You will see a list of Ldap Servers. You can view the details of a Ldap Server by clicking on the blue view icon.

You can also edit or delete the entry.



Database Schema

The database schema can be found in the application if the user has database::read permission by going to menu: Admin -> Database -> List Tables, then clicking on the details button for the table.

API / Web Access

You can access the collection using the normal Open-Audit JSON based API. Just like any other collection. Please see [The Open-Audit API documentation](#) for further details.