

LDAP_Servers

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

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:

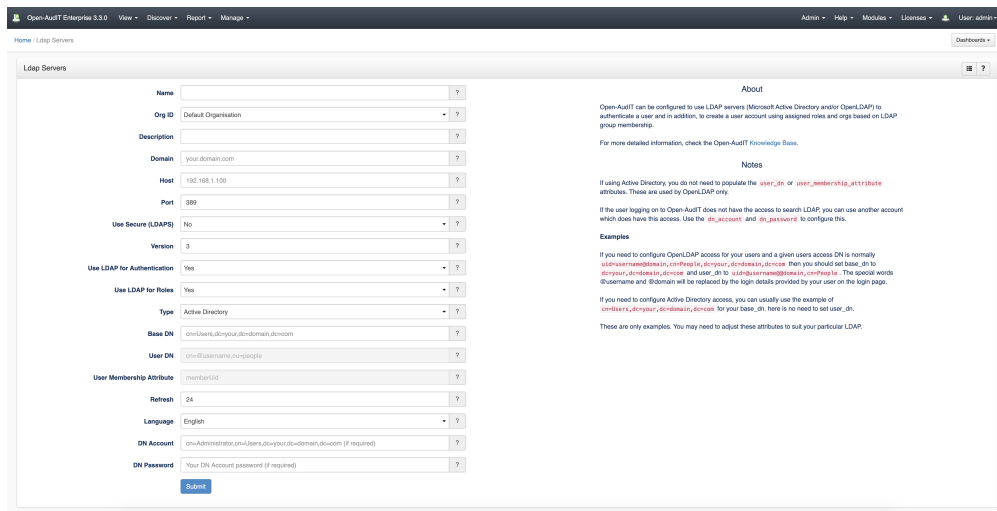
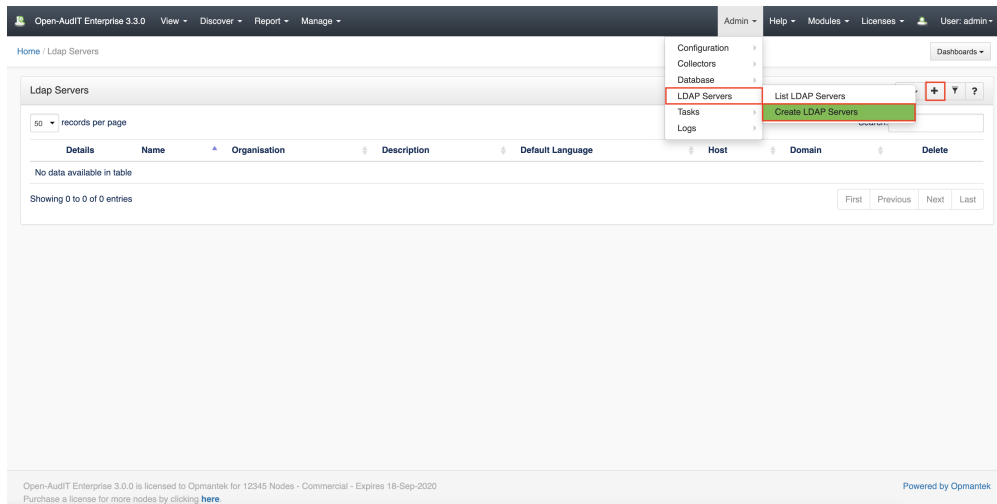
Linux – `/usr/local/omk/conf/opCommon.nmis`

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.

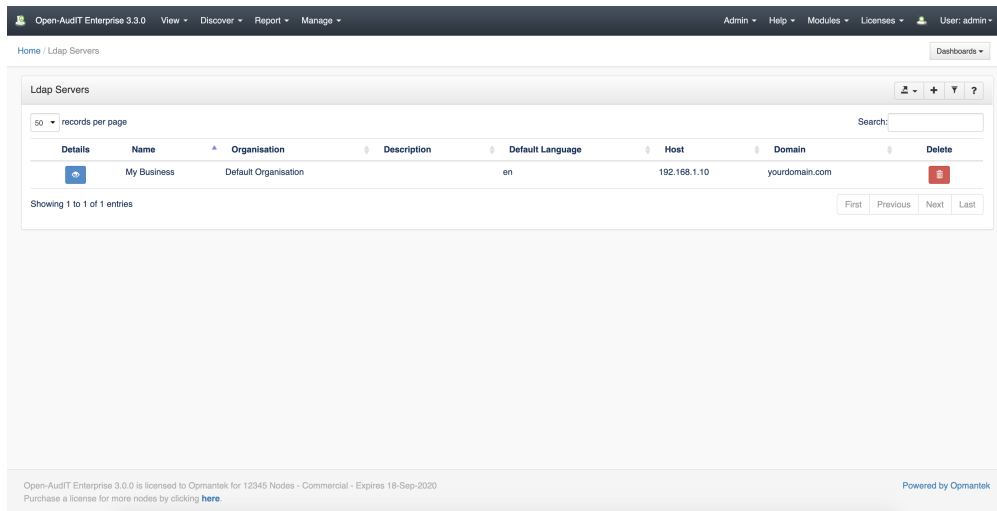


View a LDAP Server Details

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 schema for the database is below. It can also be found in the application if the user has database::read permission by going to menu: Admin -> Database -> List Tables, then clicking on the "ldap_servers" table.

```
CREATE TABLE `ldap_servers` (
  `id` int(10) unsigned NOT NULL AUTO_INCREMENT,
  `name` varchar(200) NOT NULL DEFAULT '',
  `org_id` int(10) unsigned NOT NULL DEFAULT '1',
  `description` text NOT NULL,
  `lang` varchar(200) NOT NULL DEFAULT 'en',
  `host` varchar(200) NOT NULL DEFAULT '',
  `port` varchar(200) NOT NULL DEFAULT '385',
  `secure` enum('y','n') NOT NULL DEFAULT 'n',
  `domain` varchar(200) NOT NULL DEFAULT '',
  `type` enum('active directory','openldap') NOT NULL DEFAULT 'active directory',
  `version` int(1) unsigned NOT NULL DEFAULT '3',
  `base_dn` varchar(200) NOT NULL DEFAULT '',
  `user_dn` varchar(200) NOT NULL DEFAULT '',
  `user_membership_attribute` varchar(200) NOT NULL DEFAULT 'memberUid',
  `use_roles` enum('y','n') NOT NULL DEFAULT 'n',
  `dn_account` varchar(200) NOT NULL DEFAULT '',
  `dn_password` varchar(250) NOT NULL DEFAULT '',
  `refresh` int(10) unsigned NOT NULL DEFAULT '24',
  `refreshed` datetime NOT NULL DEFAULT '2000-01-01 00:00:00',
  `edited_by` varchar(200) NOT NULL DEFAULT '',
  `edited_date` datetime NOT NULL DEFAULT '2000-01-01 00:00:00',
  PRIMARY KEY (`id`)
) ENGINE=InnoDB AUTO_INCREMENT=9 DEFAULT CHARSET=utf8;
```

A typical entry looks as below.

```

        id: 8
        name: My Business
        org_id: 1
    description: LDAP
        lang: en
        host: 192.168.1.200
        port: 389
        secure: y
        domain: ldap.mybusiness.com
        type: active directory
        version: 3
        base_dn:
        user_dn:
    user_membership_attribute: memberUid
        use_roles: n
        dn_account: nmis
        dn_password: znfN8ixkwOqEmtEaDJocqZ/5hyIQi3Ih2NuJLBt
/SAniG5p4uqN4qJbJcSFT1BNiVgWSRR3XBhFqXjfljCxghg==
        refresh: 24
        refreshed: 2000-01-01 00:00:00
        edited_by: Open-AudIT Enterprise
        edited_date: 2017-05-22 03:30:39

```

API / Web Access

You can access the /ldap_servers collection using the normal Open-AudIT JSON based API. Just like any other collection. Please see the API documentation for further details.

Access is provided as part of a roles permissions. Ldap Servers is a standard resource and can have create, read, update and delete permissions.

The API routes below are usable from both a JSON Restful API and the web interface. The Web application routes are specifically designed to be called from the web interface (a browser).

API Routes

Request Method	ID	Action	Resulting Function	Permission Required	URL Example	Notes	Example Response
POST	n		create	ldap_servers::create	/ldap_servers	Insert a new ldap server entry.	
GET	y		read	ldap_servers::read	/ldap_servers/{id}	Returns a ldap server details.	
PATCH	y		update	ldap_servers::update	/ldap_servers/{id}	Update an attribute of a ldap server entry.	
DELETE	y		delete	ldap_servers::delete	/ldap_servers/{id}	Delete a ldap server entry.	
GET	n		collection	ldap_servers::read	/ldap_servers	Returns a list of ldap servers.	
POST	n	import	import	ldap_servers::create	/ldap_servers/import	Import multiple ldap servers using a CSV.	

Web Application Routes

Request Method	ID	Action	Resulting Function	Permission Required	URL Example	Notes
GET	n	create	create_form	ldap_servers::create	/ldap_servers/create	Displays a standard web form for submission to POST /ldap_servers.
GET	y	update	update_form	ldap_servers::update	/ldap_servers/{id}/update	Show the ldap server details with the option to update attributes using PATCH to /ldap_servers/{id}
GET	n	import	import_form	ldap_servers::create	/ldap_servers/import	Displays a standard web form for submission to POST /ldap_servers/import.