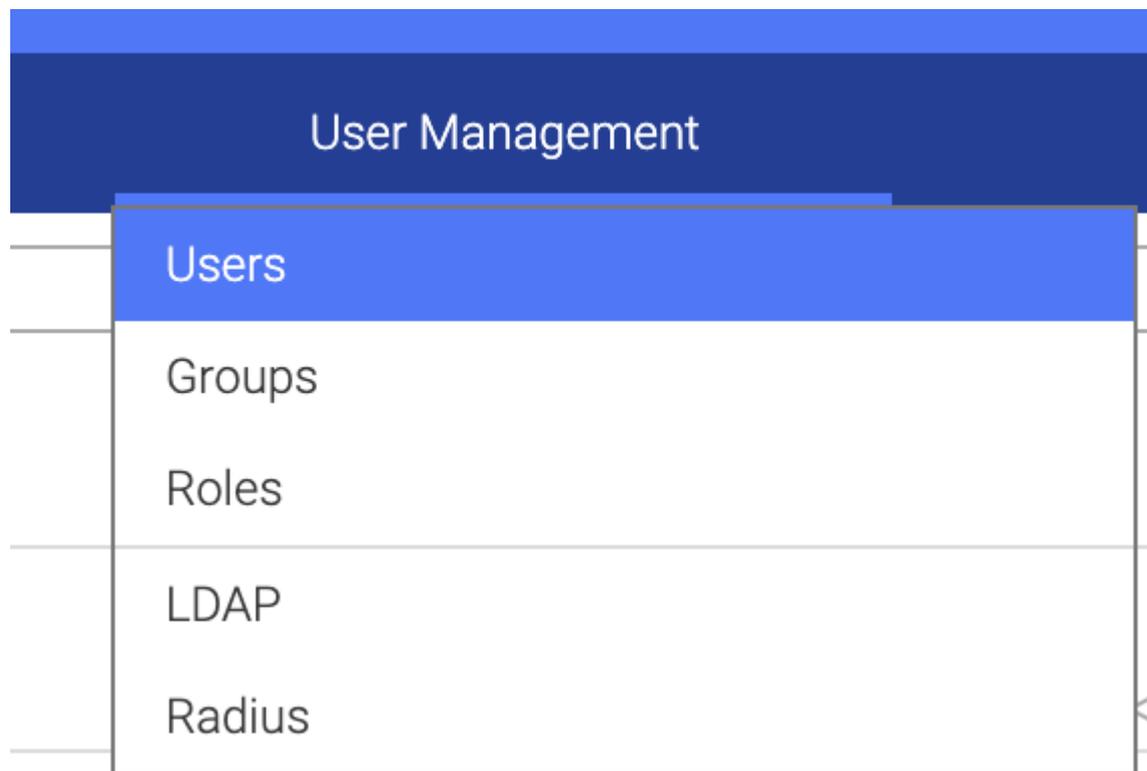


# User Management

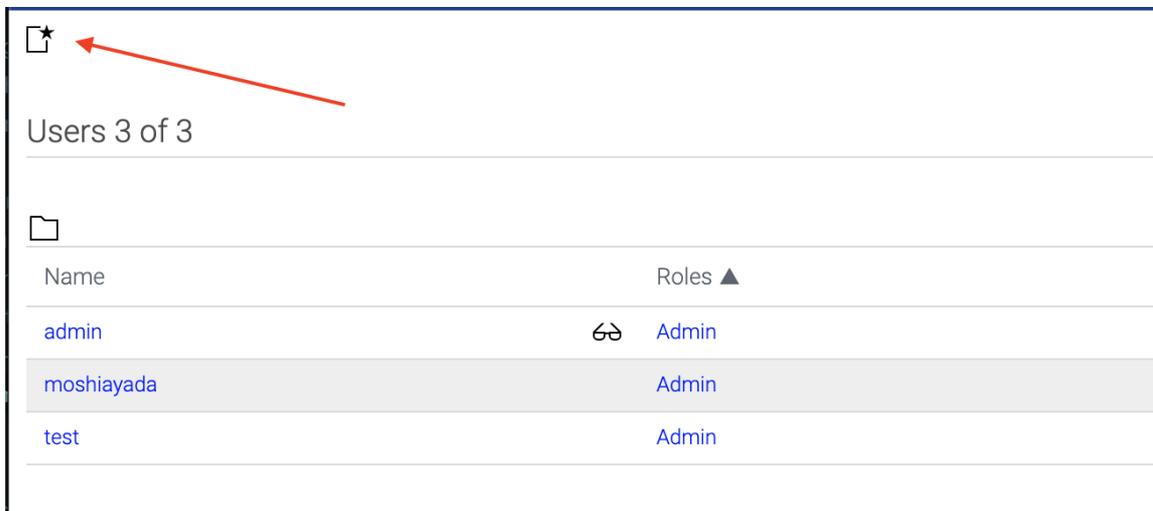
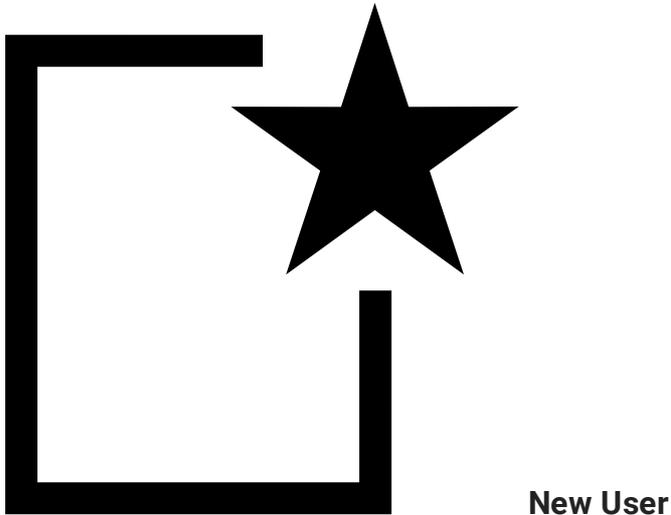
---

## How to Create Users

To create an user in the top navigation bar, click **User Management > Users**



The Users page will show up and you can click on the icon



The **New User** window appears. From there, you can create an user:



New User

Login Name

Comment

Authentication  Password   LDAP Authentication Only

Roles  ▼

Groups  ▼

Host Access  Allow all and deny  Deny all and allow

Interface Access  Allow all and deny  Deny all and allow

Cancel

Save

## Understanding the Terms

### New Scan Window

1. **Login Name:** Username that the person will use to login into Mageni Vulnerability Platform.
2. **Comment:** If you want to insert a comment. For example: "Auditor"
3. **Authentication:** How you will authenticate the users. You can use **LDAP Integration**, so the users will authenticate with the Microsoft Active Directory Credentials or with a local password which is encrypted in the database.
4. **Roles:** The order in which you want to scan a network. It could be random, sequential and reverse.
5. **Groups:** The maximum number of plugins executed per hosts.
6. **Host Access:** The IT assets that can be scanned by the user.
  - a. Allow all and deny: Allow the user to scan all hosts and define which assets the user **is not authorized** to scan.
  - b. Deny all and allow: Deny the user to scan all hosts and define which assets the user **is authorized** to scan.
7. **Interface Access:** If the virtual appliance uses several interfaces, you can define which one the user may use to launch an scan.
  - a. Allow all and deny: Allow the user to use all interfaces and define which interfaces the user **is not authorized** to use to launch a scan.
  - b. Deny all and allow: Deny the user to use all interfaces and define which interfaces the user **is authorized** to use to launch a scan.

### Advice

It is a good practice to define which hosts the user can scan, in that way you will have a solid control over the network.

## LDAP Integration

---

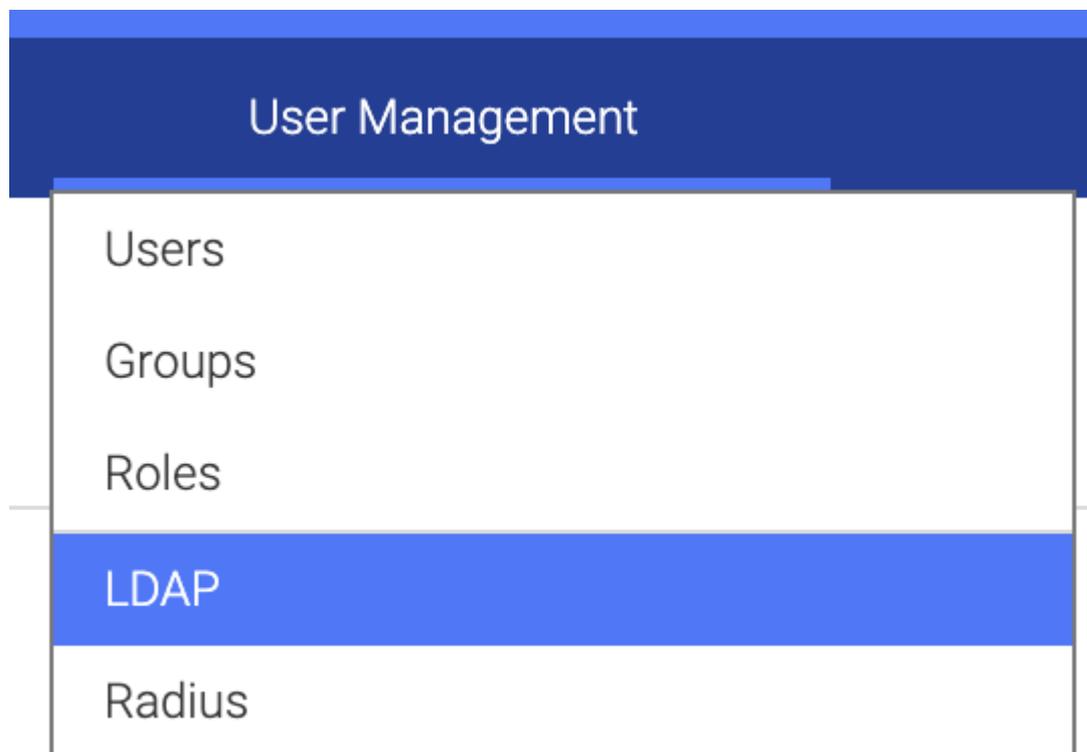
## LDAP Authentication

### Info

Before you proceed, please note that in order to integrate Mageni Vulnerability Platform with LDAP **it is required, to secure the communication, LDAPS**. If you don't know how to configure LDAPS, you can visit:

1. <https://social.technet.microsoft.com/wiki/contents/articles/2980.ldap-over-ssl-ldaps-certificate.aspx>
2. <https://www.openldap.org/doc/admin24/tls.html>
3. <https://pdhewaju.com.np/2017/03/02/configuring-secure-ldap-connection-server-2016/>

In the top navigation bar, click **User Management > LDAP**



The LDAP page will show up and you can click on the icon **Edit Authentication**



## LDAP per-User Authentication

---

The LDAP Integration window appears. From there, you set up the integration. You will need:

1. The Hostname of the LDAP Server or Domain Controller
2. The DistinguishedName (DN). %s replaces the username.
3. The certificate in .cer format.

The screenshot shows a dialog box titled "Edit Authentication" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Enable:** A checkbox that is checked.
- LDAP Host:** A text input field containing "WIN-E043V40AIV6.magenidc.local".
- Auth. DN:** A text input field containing "%s@magenidc.local".
- CA Certificate:** A text input field containing "magenidc.cer" with a "Choose File" button to its left.

At the bottom of the dialog, there are two buttons: "Cancel" on the left and "OK" on the right.

Once that you have those items, click Ok. You will see all the details.



## LDAP per-User Authentication

Enabled	Yes
LDAP Host	WIN-E043V40AIV6.magenidc.local
Auth. DN	%s@magenidc.local
Activation	2019-06-08T14:58:27-04:00
Expiration	2020-06-07T14:58:27-04:00
MD5 Fingerprint	10:01:4d:0e:ec:a7:b6:9e:07:44:ab:8e:29:4f:2c:1a
Issued by	DC=local,DC=magenidc,CN=magenidc-WIN-E043V40AIV6-CA

From there, you can go to the menu: **User Management > Users** and you will see that the option for LDAP Authentication now is working. You can enable it for the users and click "Save".

The screenshot shows a 'New User' dialog box with the following fields and options:

- Login Name: Unnamed
- Comment: (empty)
- Authentication:  Password,  LDAP Authentication Only (indicated by a red arrow)
- Roles: (dropdown menu)
- Groups: (dropdown menu)
- Host Access:  Allow all and deny,  Deny all and allow
- Interface Access:  Allow all and deny,  Deny all and allow

Buttons: Cancel (bottom left), Save (bottom right)