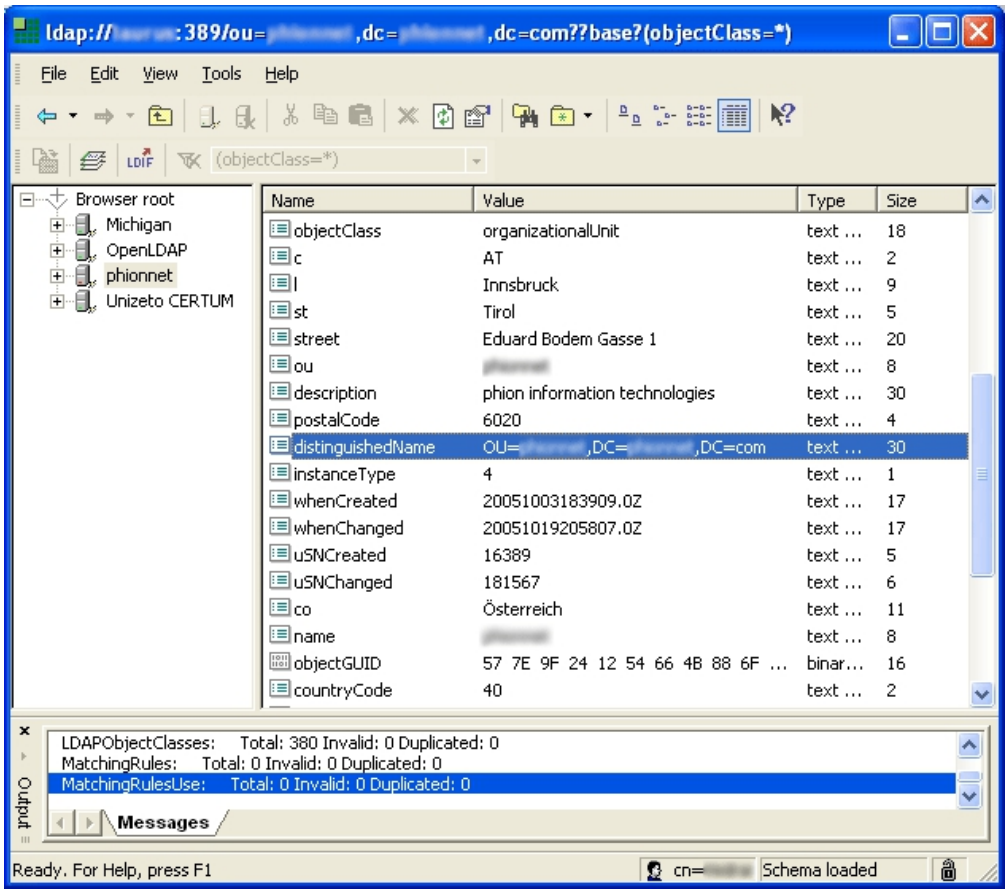
How to Configure LDAP Authentication

https://campus.barracuda.com/doc/72516163/

Lightweight Directory Access Protocol (LDAP) is used for storing and managing distributed information services in a network. LDAP is mainly used to provide single sign-on solutions. It follows the same X.500 directory structure as Microsoft Active Directory.

Before You Begin

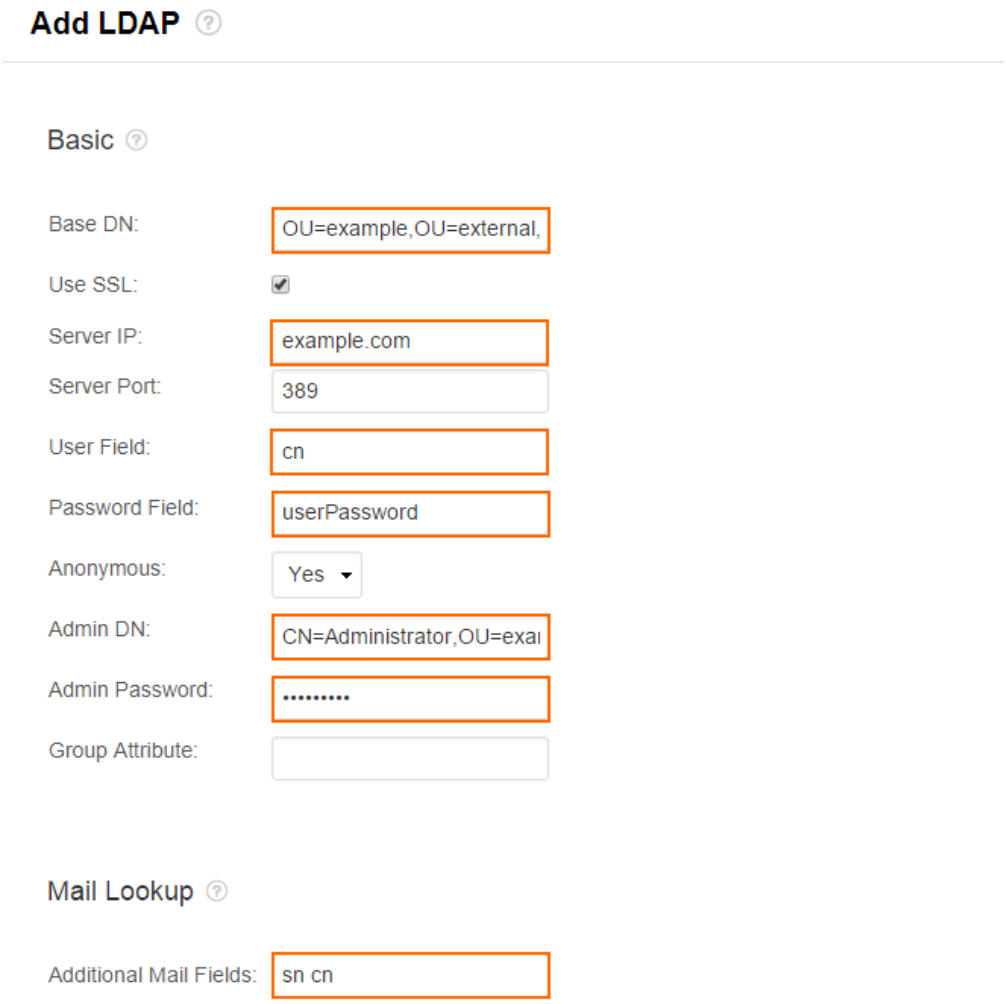
To use services such as VPN, you may need to gather group information. The distinguished name (DN) containing the group information is needed for external authentication using LDAP. With an arbitrary LDAP browser, you can gather DNs for the LDAP authentication scheme. Open the LDAP browser and connect to your domain controller to retrieve the distinguished name.



Configure LDAP Authentication

To configure LDAP for external authentication with the Barracuda CloudGen Firewall, complete the following steps:

1. Go to **USERS > External Authentication**.
2. Click the **LDAP** tab.
3. In the **Basic** section, click **Add**.
4. In the **Base DN** field, enter the Distinguished Name (DN) where the search in the LDAP directory should be started at. Separate multiple entries with a comma. E.g., `OU=yourcompany,OU=external,O=sales,O=world,C=AT`
5. (Optional) Select **Use SSL** if your LDAP server supports SSL connections.
6. Enter the IP address or hostname of the LDAP server in the **Server Name** field.
7. In the **User Field**, enter the name attribute of the LDAP searching user field used in your LDAP directory. E.g, `cn`
8. Enter the LDAP **Password Field** used in your LDAP directory.
9. Select **Anonymous** if authentication is not required.
10. In the **Admin DN** field, enter the Distinguished Name of the administrator who is authorized to perform requests.
11. Enter the **Admin Password** for the administrative user.
12. In the **Group Attribute** field, specify the name of the attribute field on the LDAP server containing group information.
13. Enter LDAP fields containing email addresses in the **Additional Mail Fields**. Separate multiple entries with a comma.



When selecting **Logon to Authenticate**, the authenticator will log on to the LDAP server to verify user authentication data. Use this option when the LDAP server does not expose user passwords, not even to the administrator.

14. Click **Save**.

The configuration is now added to the **Existing Authentication Services** table, and your LDAP domain users can use the LDAP authentication service to be authenticated on the firewall.

Figures

1. ldap_inf.png
2. ldap01_67.png