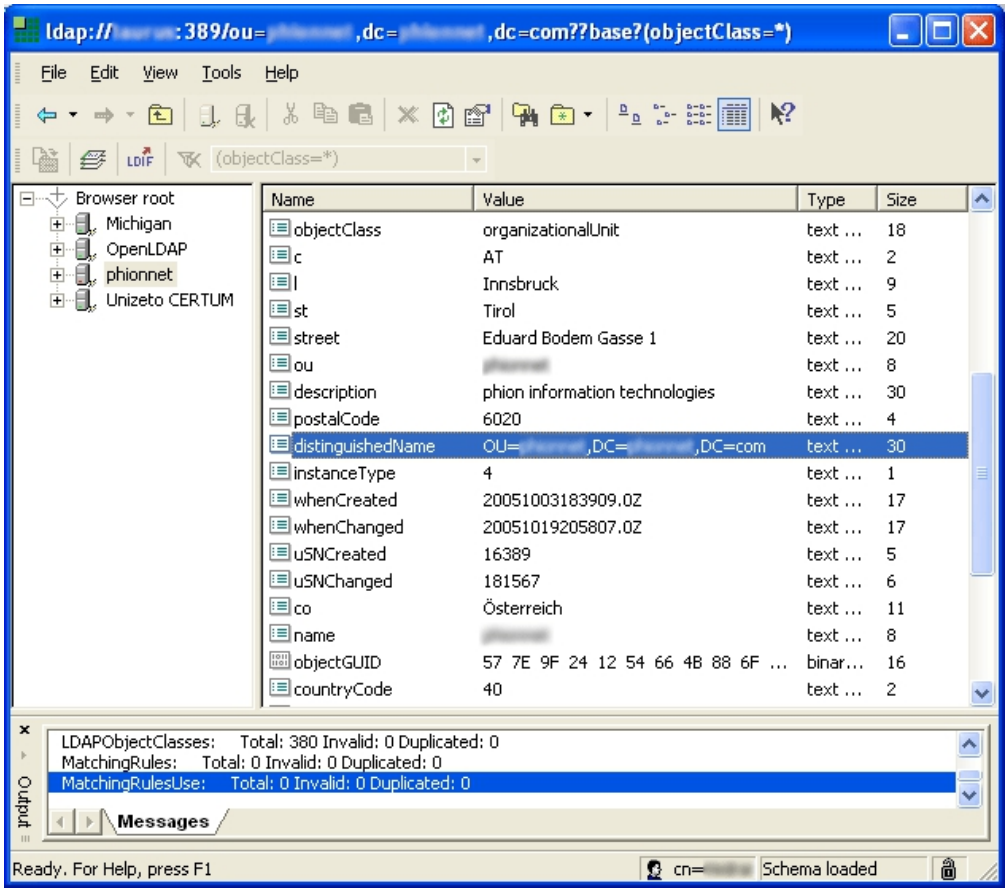
How to Configure LDAP Authentication

https://campus.barracuda.com/doc/96026630/

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 URL Filter, VPN, or Firewall Authentication and Guest Access, 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 **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Authentication Service**.
2. In the left navigation pane, select **LDAP Authentication**.
3. Click **Lock**.
4. Enable LDAP as an external directory service.
5. In the **Basic** table, add a new entry for each Base DN. You can configure the following settings:
   - **LDAP Base DN** – Distinguished name for the user organizational unit.
   - **LDAP Server / Port** – IP address and port of the LDAP server (default: port 389).
   - **LDAP User / Password Field** – Name of the user identification and password attribute in the LDAP directory.
   - **Anonymous** – If authentication is not required, set it to **Yes**.
   - **LDAP Admin DN / Password** – Name and password of the administrator who is authorized to perform LDAP queries.
     The password can consist of small and capital characters, numbers, and non-alpha-numeric symbols, except the hash sign (#).
   - **Group Attribute** – Name of the attribute field on the LDAP server that contains group information. The attribute fields on the LDAP server are customizable. If you are unsure about the required field name, ask the LDAP server administrator to provide the correct information.
     Services that process group information (for example, URL Filter) require group attribute specification. If not set, they will not be able to match group conditions.
   - **Cache LDAP Groups** – Enabling caching for selected LDAP group objects to reduce network traffic and server load on the LDAP server.
     The local LDAP group cache contains the following objects: **memberof** attributes in **person** objects**, memberUid** in **posixGroup** objects (NIS or RFC2307 schema), and **member** attributes in **groupOfNames** objects.
   - **Offline sync (every min./hour)** – Select how often the local LDAP group cache is refreshed.
   - **Additional Mail Fields** – Allows definition of comma-separated additional fields to 'mail'.
   - **Use SSL** – If the authenticator must use SSL for connections to the authentication server, select this checkbox.
     For certificate verification to work, the LDAP's server name must be DNS resolvable. When using hostnames (recommended as used in certificates for SSL communication), you must create a host firewall rule to match the traffic because the dynamic network object is no longer pre-filled with the authentication server address. For more information, see Host Firewall.
   - **Logon to Authenticate** – Select this checkbox if the authenticator must log directly into the LDAP server to verify user authentication data. When selected, the LDAP server does not expose user passwords. Instead, the server hides user passwords, even from

administrators.

6. Click **OK**.
7. If group information is queried from a different authentication scheme, select the scheme from the **User Info Helper Scheme** list.
8. In the **Group Filter Patterns** table, you can add patterns to filter group information from the directory service.
   Example:
   - **Group Filter Pattern**: *SSL*
   - **User01**: `CN=foo, OU=bar, DC=foo-bar, DC=foo`
   - **User02**: `CN=SSL VPN, DC=foo-bar, DC=foo`

   In this example, User01 does not have the *SSL* pattern in its group membership string and will not match group-based limitations.
9. If you experience issues that authentication fails, ensure that:
   1. The LDAP server is also serving the attribute **memberOf** attribute. Some servers require you to enable plug-ins for handling certain attributes.
   2. You add an appropriate value for the parameter **memberOf** in your query.
10. Click **Send Changes** and **Activate**.

LDAP Authentication Through the Remote Management Tunnel

To allow remote CloudGen Firewalls to connect to the authentication server through the remote management tunnel, you must activate the outbound **BOX-AUTH-MGMT-NAT** Host Firewall rule. By default, this rule is disabled.

Figures

1. ldap_inf.png