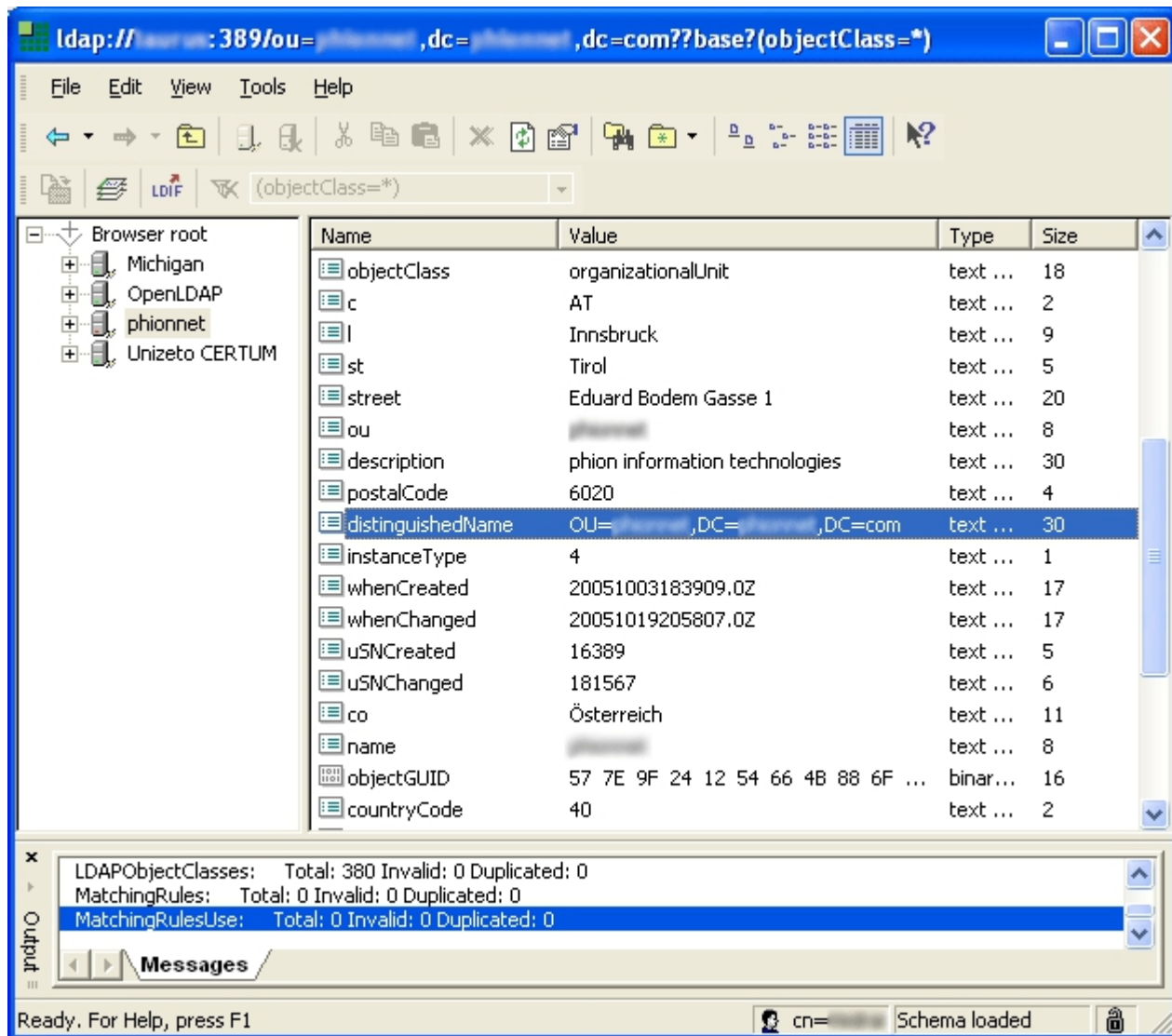

How to Configure LDAP Authentication

<https://campus.barracuda.com/doc/48202746/>

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 [FTP](#), [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 NextGen Firewall F-Series, 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 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 to **Yes**.
- **LDAP Admin DN / Password** – Name and password of the administrator who is authorized to perform LDAP queries.
- **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.
- **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 in group-based limitations.

9. Click **Send Changes** and **Activate**.

LDAP authentication through the remote management tunnel

To allow remote F-Series 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

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.