

How to Configure LDAP Authentication

<https://campus.barracuda.com/doc/43224177/>

To authenticate users on a Lightweight Directory Access Protocol (LDAP) server, configure the Barracuda NextGen Firewall X-Series to use LDAP as an external authentication scheme. You can add LDAP configurations for one or more LDAP servers. Connect the X-Series Firewall with your LDAP servers and specify the search settings for the LDAP directory. To reduce load querying for large environments, you can filter unwanted group membership information by creating group filter patterns.

Configure LDAP Authentication

Configure the X-Series Firewall to look up users on your LDAP server.

1. Go to the **USERS > External Authentication** page.
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. Select whether to use **LDAP Encryption (SSL)** for data exchanged with the LDAP directory.
14. Enter LDAP fields containing email addresses in the **Additional Mail Fields**. Separate multiple entries with a comma.

Add LDAP

Base DN:	<input type="text" value="OU=example,OU=external,"/>
Use SSL:	<input checked="" type="checkbox"/>
Server Name:	<input type="text" value="example.com"/>
Server Port:	<input type="text" value="389"/>
User Field:	<input type="text" value="cn"/>
Password Field:	<input type="text" value="userPassword"/>
Anonymous:	<input type="text" value="Yes"/>
Admin DN:	<input type="text" value="CN=Administrator,OU=exai"/>
Admin Password:	<input type="password" value="....."/>
Group Attribute:	<input type="text"/>
LDAP Encryption:	<input type="radio"/> Yes <input checked="" type="radio"/> No

Mail Lookup




Additional Mail Fields:

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.

15. 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 X-Series Firewall.

Existing Authentication Services

Type	Name	Server	Actions	
 LDAP				
	OU=example,OU=extern...	example.com	 	

Figures

1. ldap01_67.png
2. ldap02_67.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.