How to Configure User Authentication Using LDAP

https://campus.barracuda.com/doc/96022971/

If you make setting changes, allow a few minutes for the changes to take effect.

Sender authentication and recipient verification are a critical part of maintaining security of email flowing into and out of your organization. By identifying known trusted senders and recipients of email, you can block a large percentage of spam, viruses and malware from your network. Once you have entered information about your LDAP server, click **Test Settings** on the **Domain Settings** page to ensure that Email Gateway Defense can communicate with the server. LDAP server types supported include Active Directory, Novell eDirectory, and OpenLDAP.

LDAP Lookup

You can synchronize Email Gateway Defense with your existing LDAP server to automatically create accounts for all users in the domain. For more information about user accounts, see Managing User Accounts.

LDAP lookup configuration and LDAP authentication of user logins is done by domain on the **Domains > Domain Settings** page. On the **Domains** page, click **Edit** in the **Settings** column to the right of the domain name. Once you configure your LDAP settings on the **Domains > Domain Settings** page, click **Synchronize Now** to create user accounts for all users in your LDAP server.

Important

Email Gateway Defense connects with your network from various IP addresses, including performing LDAP lookups. To ensure that the service can connect with your network, allow traffic originating from the range of network addresses based on your Email Gateway Defense instance; see Email Gateway Defense IP Ranges for a list of ranges based on your Email Gateway Defense instance.

1. Log into https://login.barracudanetworks.com/ using your account credentials, and click **Email Gateway Defense** in the left pane.
2. Go to the **Domains** page, and click **Edit** in the **Settings** column to the right of the domain.
3. In the **Domains > Domain Settings** page, scroll to the **Directory Services** section, select **LDAP**, and click **Save Changes** at the top of the page.
4. In the **LDAP Configuration** section, configure the following variables:
    1. **LDAP Host** – The server utilized for LDAP lookups. If this setting is a hostname, and is contained in multiple A records, then fail-over capabilities are available if Email Gateway

Defense is unable to connect to one of the machines listed here.

2. **Port** – Port used to connect to the LDAP service on the specified LDAP Server. Typically port 389 is used for regular LDAP and LDAP using the STARTTLS mode for privacy. Port 636 is assigned to the LDAPS service (LDAP over SSL/TLS).
3. **Use SSL (LDAPS)** – By default, LDAP traffic is transmitted unsecured. You can make LDAP traffic confidential and secure by using Secure Sockets Layer (SSL)/Transport Layer Security (TLS) technology by selecting *Yes* for this option.
4. **Bind DN (Username)** – Username used to connect to the LDAP service on the specified LDAP Server. If in the form *accountname@domain.com*, the username is transformed into a proper LDAP bind DN, for example, *CN=accountname,CN=users,DC=domain,DC=com,* when accessing the LDAP server. Sometimes the default transformation does not generate a proper bind DN. In such cases, a fully formed and valid bind DN must be entered.
5. **Bind Password** – Password used to connect to the LDAP service on the specified LDAP Server.
6. **Base DN** – Base DN for your directory. This is the starting search point in the LDAP tree. The default value looks up the `defaultNamingContext` top-level attribute and use it as the search base. For example, if your domain is *test.com*, your Base DN might be *dc=test,dc=com*.
7. **Mail Attributes** – Attribute in your LDAP directory that contains the user's email addresses.

   The attributes listed in this field determine which user address is primary versus aliases for a user account. By default, the `mail` attribute is listed first. Take caution changing the order of the attribute as you may encounter unexpected results. For example, adding `proxyAddresses` as the first (primary) attribute in this field can create multiple accounts, one for each `proxyAddress`, and the `mail` attribute value is then listed as the alias.

5. Email Gateway Defense will sync to your LDAP server from certain IP addresses. Ensure that your network and LDAP server accept connections from the IP ranges listed in Email Gateway Defense IP Ranges.
   Use the **Test LDAP Configuration Settings** section, enter a valid email address in the **Testing Email Address** field to test your LDAP settings; if left blank, LDAP settings are only tested for connection.
6. Click **Test Settings**.
7. Optionally, expand the **Advanced LDAP Configuration** section, and set the following options:
   1. **User Filter** – Set to **Yes** to limit newly synchronized email users and linked email users strictly to this one domain.
   2. **Custom User Filter** – Filter used to limit the accounts that Email Gateway Defense creates when an LDAP query is made. For example, you could limit the LDAP synchronization to just users in certain sub-domains using the *mail*= parameter, or only synchronize user-objects in a certain organizational unit (OU) using the *ou*= parameter. Each type of LDAP server has specific query syntax, so consult the documentation for your LDAP server. For Microsoft Exchange syntax and examples, see the TechNet article https://learn.microsoft.com/en-us/windows/win32/adsi/search-filter-syntax.
      Example: Your list of valid users on your directory server includes 'User1', 'User2', 'User3', 'BJones', 'RWong', and 'JDoe', and you create the User Filter (name=*User*). In this case,

the service only creates accounts for 'User1', 'User2', and 'User3'.

8. In the **Directory Options** section, specify the following options:
    1. **Synchronize Automatically** – Set to **Yes** if you are using LDAP and want Email Gateway Defense to automatically synchronize your LDAP users to its database on a regular basis for recipient verification. With Microsoft Exchange server, the synchronization is incremental. Select **No** if you want to synchronize manually in case your LDAP server is not always available. To synchronize manually, click **Synchronize Now**.
    2. **Use LDAP for Authentication** – Set to **Yes** to enable LDAP for user login authentication. You can disable this setting if your LDAP server is unavailable for a period of time.
    3. **Authentication Filter** – Filter used to look up an email address and determine if it is valid for this domain. The filter consists of a series of attributes that might contain the email address. If the email address is found in any of those attributes, then the account is valid and is allowed by Email Gateway Defense.

The first time Email Gateway Defense receives a **Not Allowed** email for a valid user, the service does the following:

- Uses the email address of the recipient as the username of the account and auto-generates a password. If **Use LDAP for Authentication** is set to **No** on the **Domains > Domain Settings** page, the user receives an email with the login information so they can access their quarantine account, otherwise, the user can use single sign-on via LDAP lookup.
- Places the quarantined message in the account holder’s quarantine inbox.
- Sends a quarantine summary report to the account holder at the specified notification interval, as set on the **Users > Quarantine Notification** page. If **Allow users to specify interval** is set to **Yes** on this page, then the quarantine summary report is sent to the user on the schedule specifies on the **Settings > Quarantine Notification** page once they log into their account. The default is **Daily**.

© 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.