

## Understanding Directory Integration

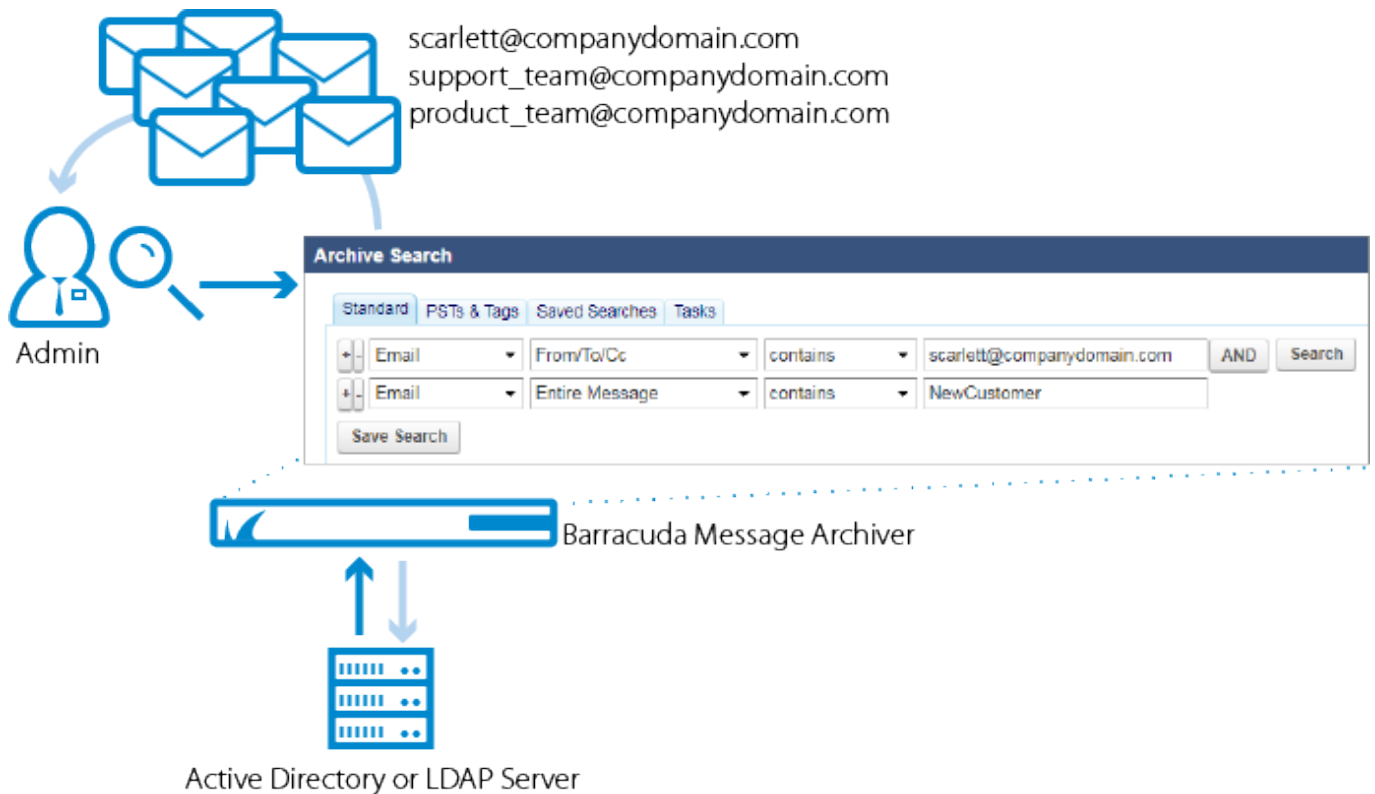
<https://campus.barracuda.com/doc/73695824/>

Configure the Barracuda Message Archiver to use your LDAP server to authenticate individual users and verify user group membership on the **USERS > Directory Services** page. Once you enter the server details, click **Test LDAP** to test the entered settings. If you are unsure of any of the settings, enter the server name and IP address, and use the **LDAP Discovery** option to display recommended settings. Once configured, users can log in to the Barracuda Message Archiver using their LDAP/Active Directory (AD) credentials and search their archived messages. By default, users are granted access once directory services are configured.

Through the authentication service defined on the **Directory Services** page, the Barracuda Message Archiver can determine which users have access to messages that have been sent to a list. This allows administrators and auditors to search on a user and have the search results return all messages to which a user has access.

For example, the administrator wants to return all messages for Scarlett related to the customer NewCustomer. Because Scarlett is a member of the support\_team and product\_team groups, the results return all messages for **scarlett@companydomain.com**, **support\_team@companydomain.com**, and **product\_team@companydomain.com**, as illustrated in figure 1.

### Figure 1. Group Membership.



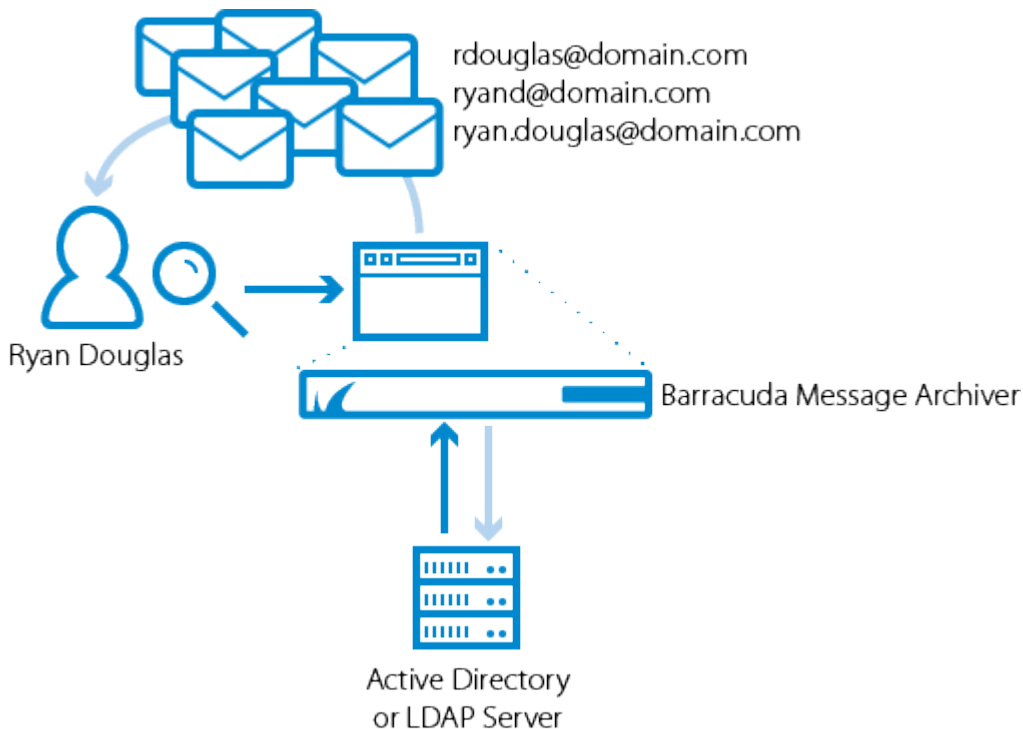
## LDAP Accounts

Associated an LDAP user or LDAP group to a Barracuda Message Archiver role and list of email addresses on the **USERS > LDAP User Add/Update** page.

## Email Aliases

LDAP users often have one primary email address that is their user account name along with several aliases for convenience. For example, **rdouglas@domain.com** also receives messages as **ryand@domain .com** and **ryan.douglas@domain .com**. For organizations that use LDAP, messages sent to any alias are accessible from the primary user account.

**Figure 2. User aliases.**



You can enter an LDAP group name in the **LDAP User/Group** field on the **USERS > LDAP User Add/Update** page and select a role for that group. When a member of that group logs in to the Barracuda Message Archiver, they log in with the assigned role.

## Include/Exclude Rules

You can define exclude/include rules on the **USERS > LDAP User Add/Update** page to set permissions on whose mail the LDAP user or group members can view. The addresses must belong to a user, group, or public folder on a configured LDAP server. When a configured user runs a search, the following rules are in place:

1. Mail for addresses added to the **Exclude these Addresses** list are not displayed unless the mail includes the user performing the search to assure that a user can always see their own mail.
2. The **Exclude these Addresses** list always takes precedence; addresses added to the **Include these Addresses** list are searchable *unless* the **Exclude these Addresses** list blocks the mail.
3. Because a user with the Admin or Auditor role can by default view all mail, users set to these roles can only edit their **Exclude these Addresses** list.
4. If a user is *not configured* and is a member of a group, then the include/exclude rules assigned to that group apply to that user. Additionally, if the unconfigured user is a member of multiple groups, then the privileges for all of those groups are merged and that user is assigned the *least privileged role* of those groups. This allows the Admin to apply include/exclude rules to

all users of a distribution group.

- Example 1: If Zoe is not individually configured but is a member of the distribution group HR, then the Admin can set the include/exclude rules for the group HR, and Zoe uses these settings when searching mail rather than seeing only her own mail.
- Example 2: If Josh is not individually configured but is a member of the distribution group HR which has an Auditor role, and Josh is also a member of the group Employees which has a User role, Josh has only the User role privileges when running a search.

5. A user cannot run a **Search As User** Search on the **BASIC > Search** page on a user that is on their **Exclude these Addresses Exclusion Rules** block list.

## Figures

1. authentication\_BMA.png
2. EmailAliasing.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.