

How to Configure User Authentication with Azure AD

<https://campus.barracuda.com/doc/96022972/>

Important: If you are moving from LDAP to Azure AD, you must delete all Email Gateway Defense users you created with LDAP before synchronizing to Azure AD.

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

See also: [How to Restore LDAP or Azure AD Directory Services](#)

Azure Active Directory

Configure recipient verification with Azure Active Directory (AD) to allow end users to sign into Email Gateway Defense using their Azure AD credentials. Once logged in, users can view their quarantine messages.

Note: If when setting up your Microsoft 365 Enterprise applications you set **Users can consent to apps accessing company data on their behalf** to **No**, users might not be able to log into Email Gateway Defense without administrator consent. To resolve this issue, reauthorize Azure AD from the **Domain Settings** page in the web interface. See the *Azure Active Directory Authentication* section of [How to Restore LDAP or Azure AD Directory Services](#) for step-by-step instructions on Azure AD reauthorization.

Single Sign-On

You can configure Single Sign-On (SSO) for a domain so that authenticated users can access all or a subset of the restricted resources by authenticating just once using their Azure AD credentials. SSO is a mechanism where a single set of user credentials is used for authentication and authorization to access multiple applications across different web servers and platforms, without having to re-authenticate.

The SSO environment protects defined resources (websites and applications) by requiring the following steps before granting access:

- Authentication: Authentication verifies the identity of a user using login credentials.

- **Authorization:** Authorization applies permissions to determine if this user may access the requested resource.

Set Up Azure AD Authorization

Complete the steps in this section for each domain you want to synchronize with your Azure AD directory.

1. Log into <https://login.barracudanetworks.com/> using your account credentials, and click **Email Gateway Defense** in the left pane.
2. Click **Domains**, and click **Edit** in the **Settings** column for the desired domain.
3. In the **Domains > Domain Settings** page, scroll to the **Directory Services** section, and select **Azure AD**, and click **Save Changes** at the top of the page.
4. Scroll down to the **Status** section, and click **Authorize**.
5. The **Authorize Azure AD** dialog box displays. Click **Continue**.
6. When prompted, log into your Microsoft 365 account as a global administrator.
7. In the **Authorization** page, click **Accept** to authorize Email Gateway Defense to connect to your Azure AD directory.
8. In the **Domain Settings** page, the **Status** field displays as **Active**; the **Authorized Account** and **Authorization Date** display below the status:

Directory Services

You can use either Azure AD or LDAP directory services to enable single sign on and synchronization of users lists.

Type	<input type="radio"/> LDAP <input checked="" type="radio"/> Azure AD <input type="radio"/> None
Status	Active (Revoke Authorization)
	Authorized Account: organizationname.info
	Authorization Date: 3/28/2018, 11:44:24 AM

9. In the **Synchronization Options** section, select **Synchronize Automatically**. When selected, Email Gateway Defense automatically synchronizes with your Azure AD directory daily and adds/updates your users. Note that the sync can take up to 24 hours or longer. If you encounter sync issues, such as new users not being properly synced between your Azure AD directory and Email Gateway Defense user list, click **Sync Now** to manually synchronize Email Gateway Defense with your Azure AD directory. If you select **Manual**, you must click **Sync Now** to synchronize Email Gateway Defense with your Azure AD directory and add/update users.

Note that selecting **Sync Now** may take longer than anticipated due to possible timeout errors.
10. To use SSO, click **Yes** for **Enable Single Sign On**. Once enabled, users are prompted to log into their Microsoft 365 account when accessing their messages in Email Gateway Defense.
11. To use the **Test Azure AD Configuration Settings** section, enter a valid email address in the **Testing Email Address** field to test your Azure AD settings.
12. Click **Test Settings**.

Directory Services

You can use either Azure AD or LDAP directory services to enable single sign on and synchronization of users lists.

Type ☐ LDAP ☒ Azure AD ☐ None

Status Active [\(Revoke Authorization\)](#)
Authorized Account: [REDACTED]
Authorization Date: 3/13/2020, 3:51:37 PM

Directory Options

Synchronization Options ☐ Synchronize Automatically ☒ Manual Sync Now Sync finished at 3/13/2020,

Enable Single Sign On ☒ Yes ☐ No

Test Azure AD Configuration Settings

Testing Email Address:
For testing Azure AD settings only. Enter a valid primary email address.

Test Settings

13. Click **Save** at the top of the page to save your settings and return to the **Domains** page.

If you previously set up LDAP authentication with Email Gateway Defense, your settings are not lost when you select **Azure AD** for a selected domain. Note, however, turning off Azure AD disables SSO and new users are not synchronized but recipient verification continues to function. For more information, see [How to Restore LDAP or Azure AD Directory Services](#).

Figures

1. authorization.png
2. testAzureAD.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.