Getting Started

https://campus.barracuda.com/doc/71238152/

- If you have completed a Barracuda Email Threat Scan, you can start a free Barracuda Impersonation Protection trial by clicking the **Start a Free Trial** link, located in the upper and lower right corners of your free scan report.
- If you are a Managed Service Provider (MSP), go to MSP Topic - Getting Started.

Barracuda, Microsoft 365, and Azure AD

Impersonation Protection monitors *licensed Microsoft 365* mailboxes.

Note that in hybrid email deployments, Impersonation Protection only monitors Microsoft 365 mailboxes; Impersonation Protection does not monitor mailboxes that are part of on-premises solutions.

For Account Takeover suspicious sign-in data, Barracuda Networks requires full Azure AD (Active Directory) tenants. It does not always receive sign-in data from hybrid environments that include both on-premise active directory and Azure AD.

Logging in for the First Time and Connecting Your Microsoft 365 Account

This process requires Microsoft 365 global tenant administrator credentials.

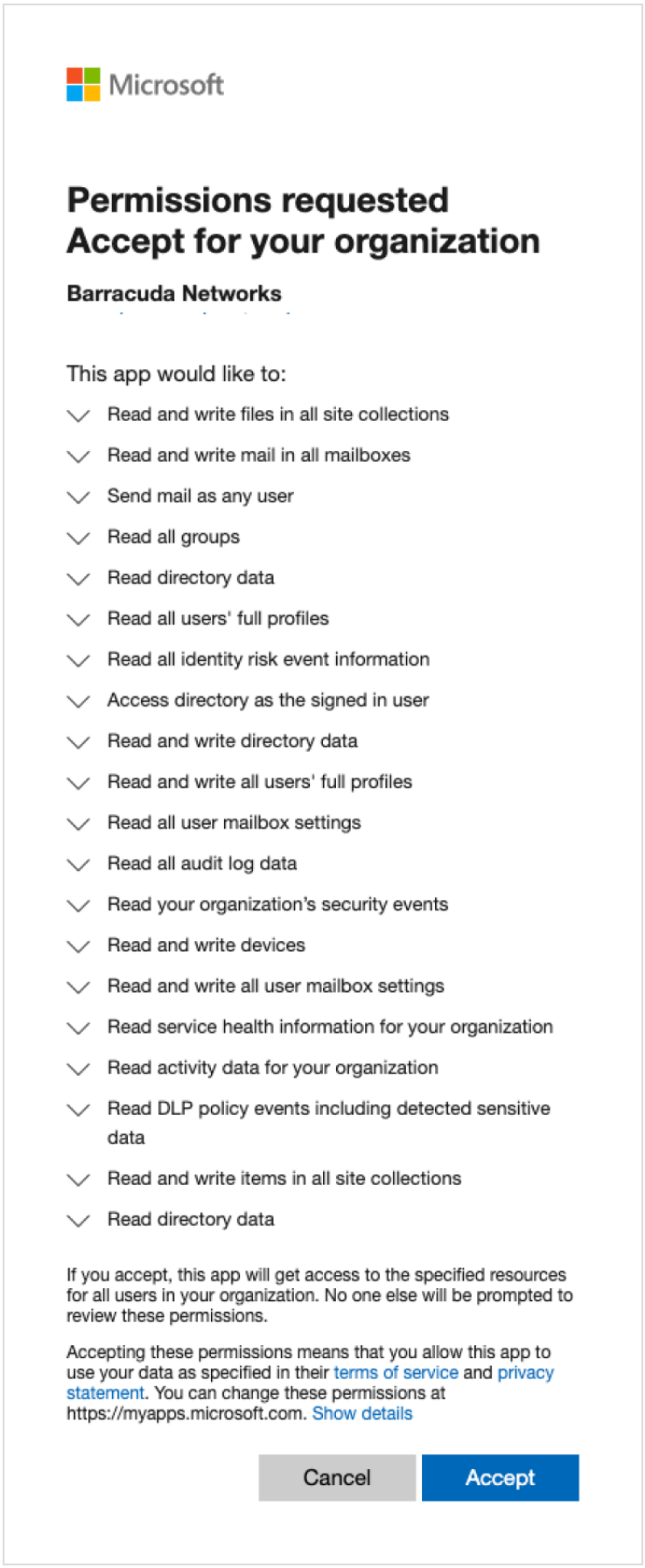
If you have a hybrid environment that includes Microsoft Exchange, it can take up to 30 days for Impersonation Protection to protect an account after it is migrated to Microsoft 365. It is best to wait until migration to Microsoft 365 is fully complete before activating Barracuda.

Complete the following steps to enable Impersonation Protection to protect your Microsoft 365 account:

1. Navigate to https://sentinel.barracudanetworks.com.
   - **If you do not already have a Barracuda account** – Enter your email, create a password, and click **Get Started**. Provide information for your account and click **Get Started**.
   - **If you have a Barracuda account** – Enter your email and password and click **Sign In**.

   Note that for your first login, Barracuda Networks requires a linking code, but does not require a serial number.

2. Click **Connect to Microsoft 365**. Optionally read about the permissions needed.


Microsoft
Permissions requested
Accept for your organization
Barracuda Networks
This app would like to:
Read and write files in all site collections
Read and write mail in all mailboxes
Send mail as any user
Read all groups
Read directory data
Read all users' full profiles
Read all identity risk event information
Access directory as the signed in user
Read and write directory data
Read and write all users' full profiles
Read all user mailbox settings
Read all audit log data
Read your organization's security events
Read and write devices
Read and write all user mailbox settings
Read service health information for your organization
Read activity data for your organization
Read DLP policy events including detected sensitive data
Read and write items in all site collections
Read directory data
If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.
Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com. Show details
Cancel
Accept

3. When Microsoft 365 opens, log in as a global tenant administrator.
4. Review the permissions required by Barracuda and click **Accept**.
   After you sign up, Barracuda will take anywhere from several hours to several days (depending on the size of your account) to fully learn your environment. After the initial learning phase is completed, you will receive an email notifying you that Impersonation Protection is now available.

Note that if you add mailboxes to your Microsoft 365 account at a later date, Barracuda Networks requires up to 72 hours to learn about these new mailboxes and begin monitoring and protecting them.

If you use a Signature Service with Microsoft 365, you may need to take an extra step to ensure Impersonation Protection does not flag/remediate your internal email.

Managing Users

Manage users who have administrative access to your Barracuda account within Barracuda Cloud Control.

To add or remove users:

1. Go to http://login.barracudanetworks.com and sign in.
2. Navigate to **Home > Admin > Users**.
3. Perform the desired action:
   - To add a user, click **Add Users**.
     Specify the information for the user, following the instructions in How to Add Users and Configure Product Entitlements and Permissions. Be sure to specify entitlements for Impersonation Protection for all users that need access to Impersonation Protection.
   - To remove a user, select an existing user and click **Remove User**.

Seamless Connection to Automatic Remediation and Incident Response

You can access your licensed or trial version of Automatic Remediation (and Incident Response, if purchased) directly from here. Click the menu button in the top left corner of the page and select **Automatic Remediation** or **Incident Response**.

- If you already have a licensed or trial version of Automatic Remediation (and optionally Incident Response), it will open in a new browser tab.

- If you do not yet have a license or trial for Automatic Remediation (and optionally Incident Response), a sign-up page displays. You can sign up for a license or free trial on that page.

If you purchased Incident Response: When viewing the details of an attack, you can click **Search for Similar Messages** to open Incident Response to locate incidents similar to the one you are currently viewing.

Figures