

Data Privacy for the Barracuda Email Threat Scanner

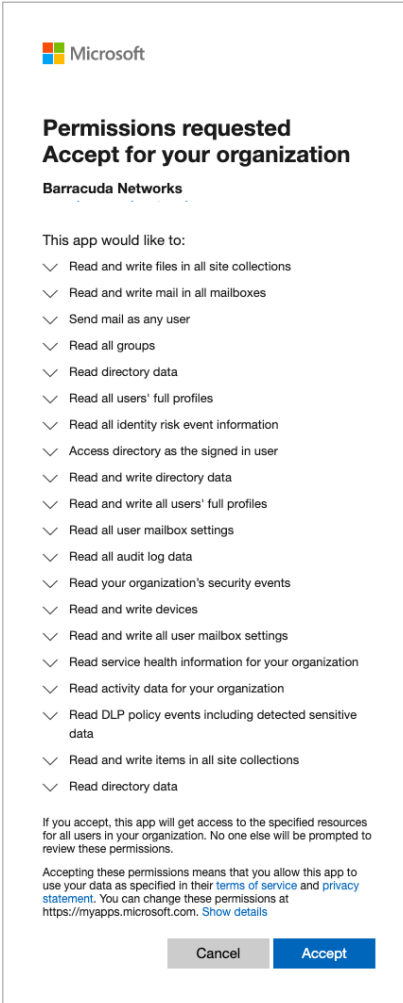
The Barracuda Email Threat Scanner (ETS) is a web-based service that scans Office 365 accounts for advanced threats and spear phishing attacks that hide inside users' mailboxes. ETS uses Office 365's official public APIs to inspect emails and attachments in your account.


When you sign up for a scan, you will be asked to connect Office 365 to ETS. During this process, a Microsoft web page will ask you to grant permission to allow ETS to access your account.

Once you grant permission, the cloud-based scan will run in the background and will not interfere with your account in any way.

What Information Does the Email Threat Scanner Have Access To?

- ETS never gains access to your Office 365 credentials.
- ETS uses standard OAuth protocol to authenticate with Office 365.
- ETS access is limited to the information it needs to find cybersecurity threats.
- Emails and attachments are not stored permanently and are immediately removed from our systems once the analysis is complete – typically within a fraction of a second.
- ETS will pull metadata about users, mail folders and emails, and will only store data related to any threats found for the sole purpose of showing the information in your threat report.



 Microsoft

Permissions requested
Accept for your organization

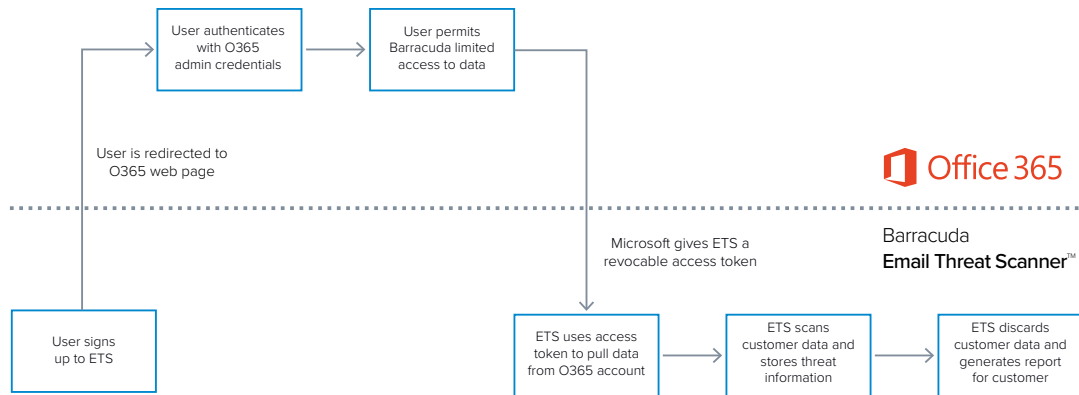
Barracuda Networks

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](#)



How We Protect Your Data Privacy

- ETS uses access token to pull data from Office 365 account
- ETS will only access emails and attachments for the sole purpose of identifying threats in your account. Threat information will only be used to generate your personalized threat report and will not be shared with any external parties.
- The threat analysis is conducted on secure servers that are hosted on Amazon Web Services and in Barracuda's data centers. All storage systems are encrypted, and all servers are tightly controlled and audited for stringent security standards.
- In cases where debugging or maintenance work is required, a minimal number of Barracuda engineers will be permitted to access the data necessary for this purpose.
- Our [Privacy Policy](#) page has more information about our practices and procedures.

FAQ

Can I revoke ETS's access to my Office 365 account?

Yes. You can revoke permissions at any point in time through your Azure AD application dashboard:

- Visit your Azure portal <https://portal.azure.com>
- Access 'Enterprise Applications'
- Search for 'Barracuda'
- Locate and click on 'Email Threat Scanner' application
- Go to 'Properties' and select 'Delete'

Why does ETS ask for write access to my mailboxes?

We ask for write access because we allow customers to upgrade their account to Barracuda Sentinel, which offers real-time remediation of the threats it detects.

- ETS doesn't make any changes to your account without you explicitly doing it in the ETS UI. Operations that change Office 365 are clearly marked and require user confirmation.

Why does ETS ask for site collections permissions?

We ask for site collections permissions because we are building threat scanning capabilities for SharePoint, which will be offered soon through ETS.

