# Getting Started

https://campus.barracuda.com/doc/96021119/

Be sure to read about License Definitions for the Barracuda Email Protection portfolio.

Barracuda Data Inspector automatically scans your OneDrive for Business and SharePoint data for both sensitive information and malicious files. New issues are automatically identified without the need to configure scanners or schedules, and customizable email alerts keep you fully informed so you can respond quickly.

## Activate Data Inspector

Barracuda Networks recommends using a Microsoft 365 Global Admin account to set up Data Inspector. If you do not use a Microsoft 365 Global Admin account, Data Inspector will only scan files for the OneDrive account used during sign up.

To sign up for a free scan from the Barracuda Networks website:

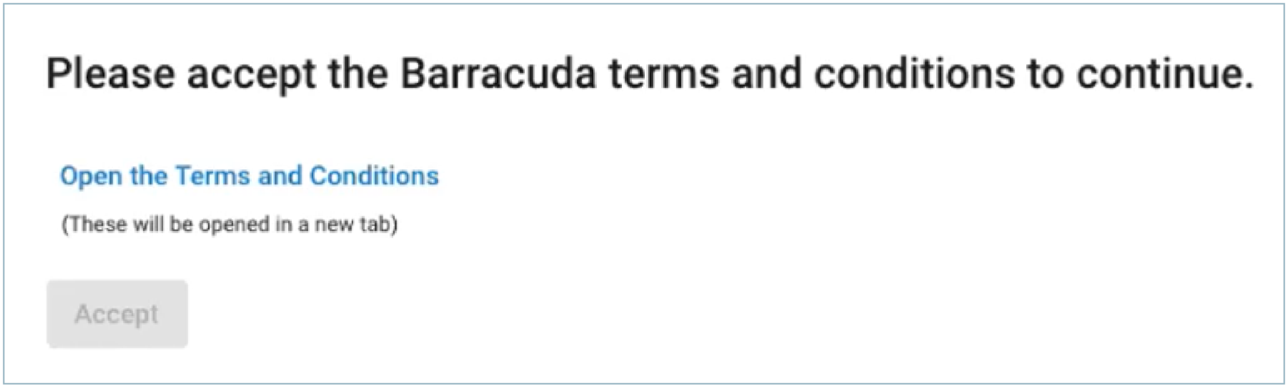
1. Navigate to https://www.barracuda.com/products/data-inspector.
2. Click **Free Scan**, complete the form with your information, and click **Submit Request**.
3. An email will be sent to the email address you provided. Click on the link in that message to be redirected to the Data Inspector login page.
4. Click **Sign Up with Your Office 365 Account For Your Free Scan** (or to **Sign In** if you already have a Barracuda Data Inspector account).
5. If you are not already signed into your Microsoft 365 account, enter your administrator account login information, and click **Sign in**. If you are already signed in, this step does not appear.
6. You will then be brought to the Data Inspector Setup Wizard.

## Setup Wizard

To log into Barracuda Data Inspector you must have a Barracuda Cloud Control account. If you do not already have an account, go to https://login.barracudanetworks.com/ and click **Create a User**. Enter your name, email address, and company name, and specify whether this is a partner account.
Click **Create User**. (For partners, be sure to read How to Add a Managed Customer Account and Partner Accounts.) Follow the instructions emailed to the entered email account to create your Barracuda Cloud Control account. See Password Complexity Policies before setting up your

password.

1. Go to https://login.barracudanetworks.com and log in with your Barracuda Cloud Control credentials.
2. Click on **Data Inspector** using the product menu.
3. If this is the first time you have signed into Data Inspector, you are redirected to the setup wizard.
4. Click **Open the Terms and Conditions** to open a new tab. After reviewing the information, close the tab and click **Accept** in the wizard. Note: the **Accept** button will not become active until you review the Terms and Conditions.

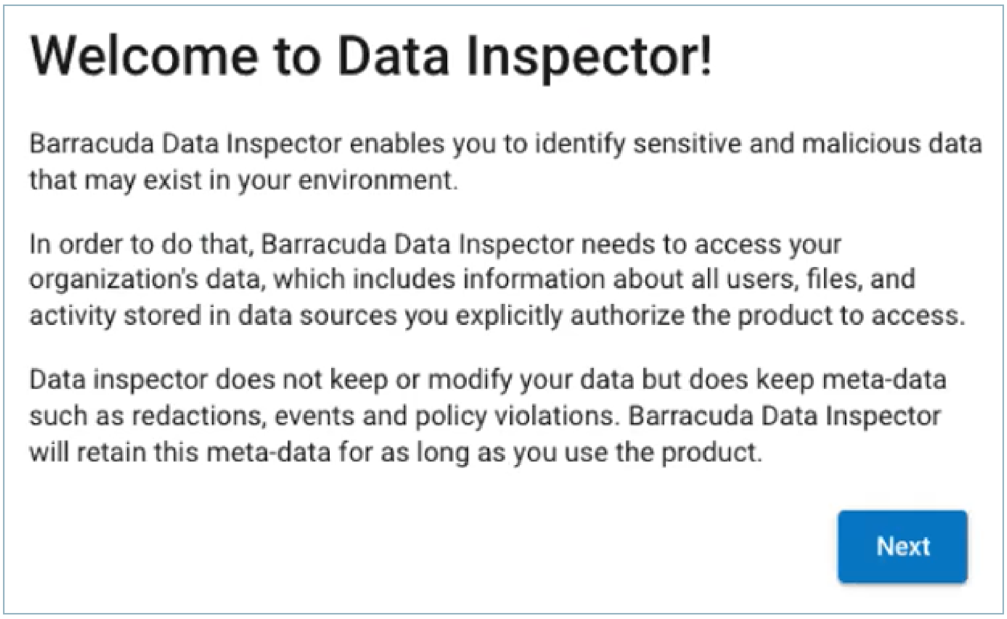


Please accept the Barracuda terms and conditions to continue.

Open the Terms and Conditions

(These will be opened in a new tab)

5. Review the welcome information and click **Next**.



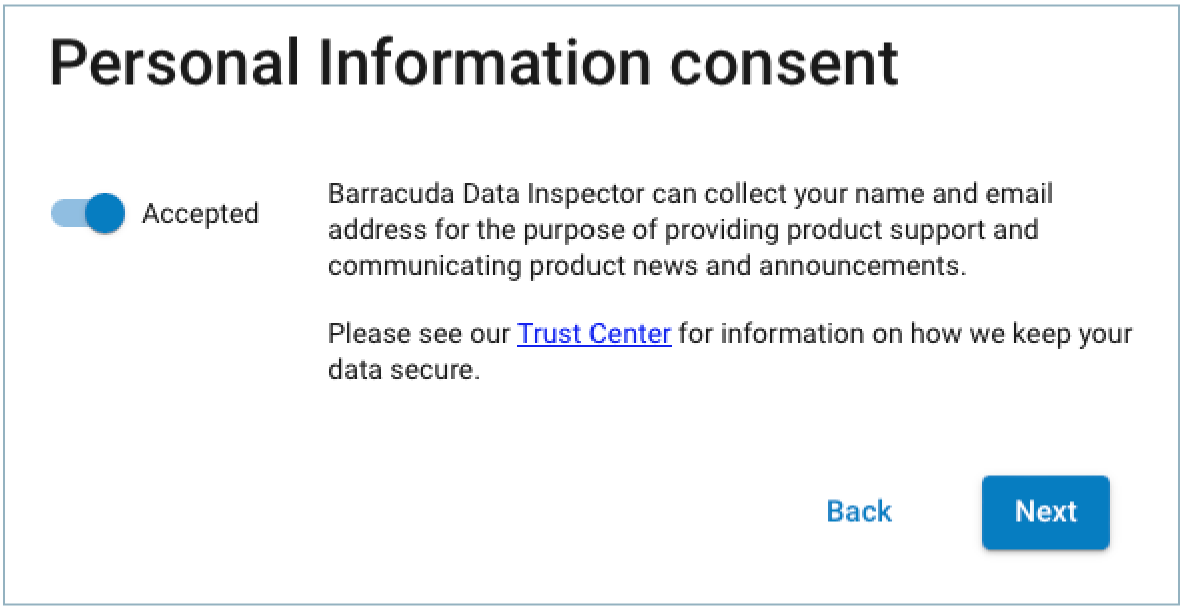
Welcome to Data Inspector!

Barracuda Data Inspector enables you to identify sensitive and malicious data that may exist in your environment.

In order to do that, Barracuda Data Inspector needs to access your organization's data, which includes information about all users, files, and activity stored in data sources you explicitly authorize the product to access.

Data inspector does not keep or modify your data but does keep meta-data such as redactions, events and policy violations. Barracuda Data Inspector will retain this meta-data for as long as you use the product.

6. Enable Barracuda Data Inspector to collect your name and email address to better provide product support and keep you aware of product news and announcements. This is optional. You can click on the **Trust Center** link to learn about how we protect your information.
   You can update your consent later from **Settings > Data**.
   Click **Next**.



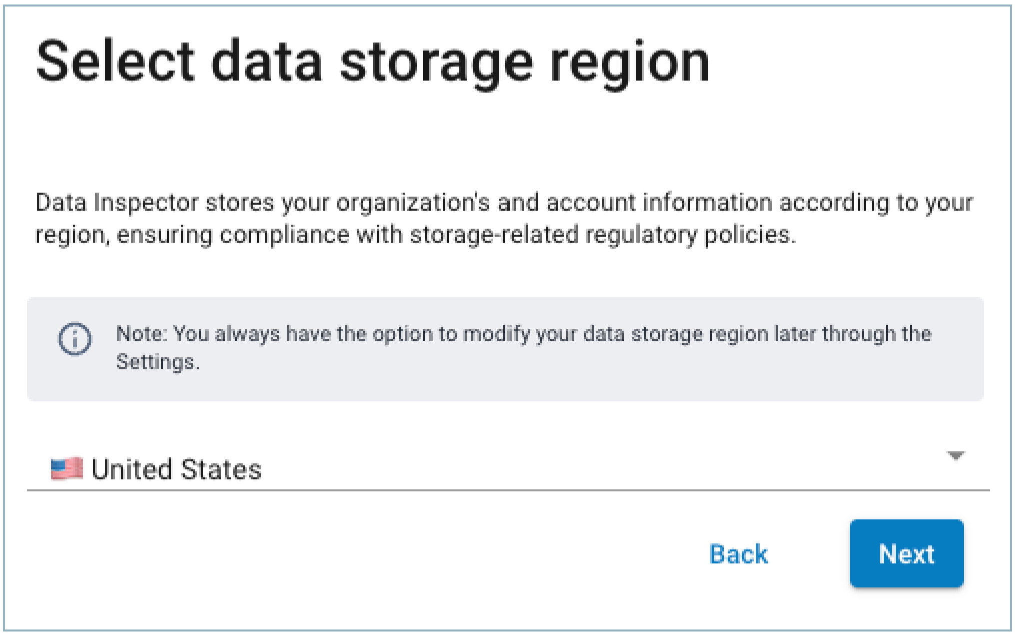
Personal Information consent

Accepted

Barracuda Data Inspector can collect your name and email address for the purpose of providing product support and communicating product news and announcements.

Please see our Trust Center for information on how we keep your data secure.

7. If asked to select a data storage region, choose from the dropdown list of available geographic locations.
   Click **Next**.



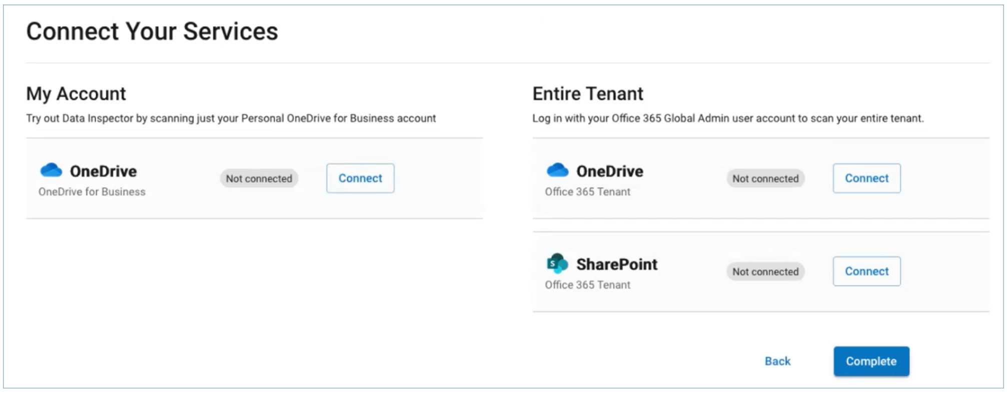
Select data storage region

Data Inspector stores your organization's and account information according to your region, ensuring compliance with storage-related regulatory policies.

Note: You always have the option to modify your data storage region later through the Settings.

United States

8. Select the OneDrive or SharePoint data source you want to connect to Data Inspector. You can scan an entire Microsoft 365 tenant or an individual OneDrive account. Note that selecting an entire tenant will require Microsoft 365 global administrator privileges.



Connect Your Services

My Account

Try out Data Inspector by scanning just your Personal OneDrive for Business account

OneDrive
OneDrive for Business — Not connected — Connect

Entire Tenant

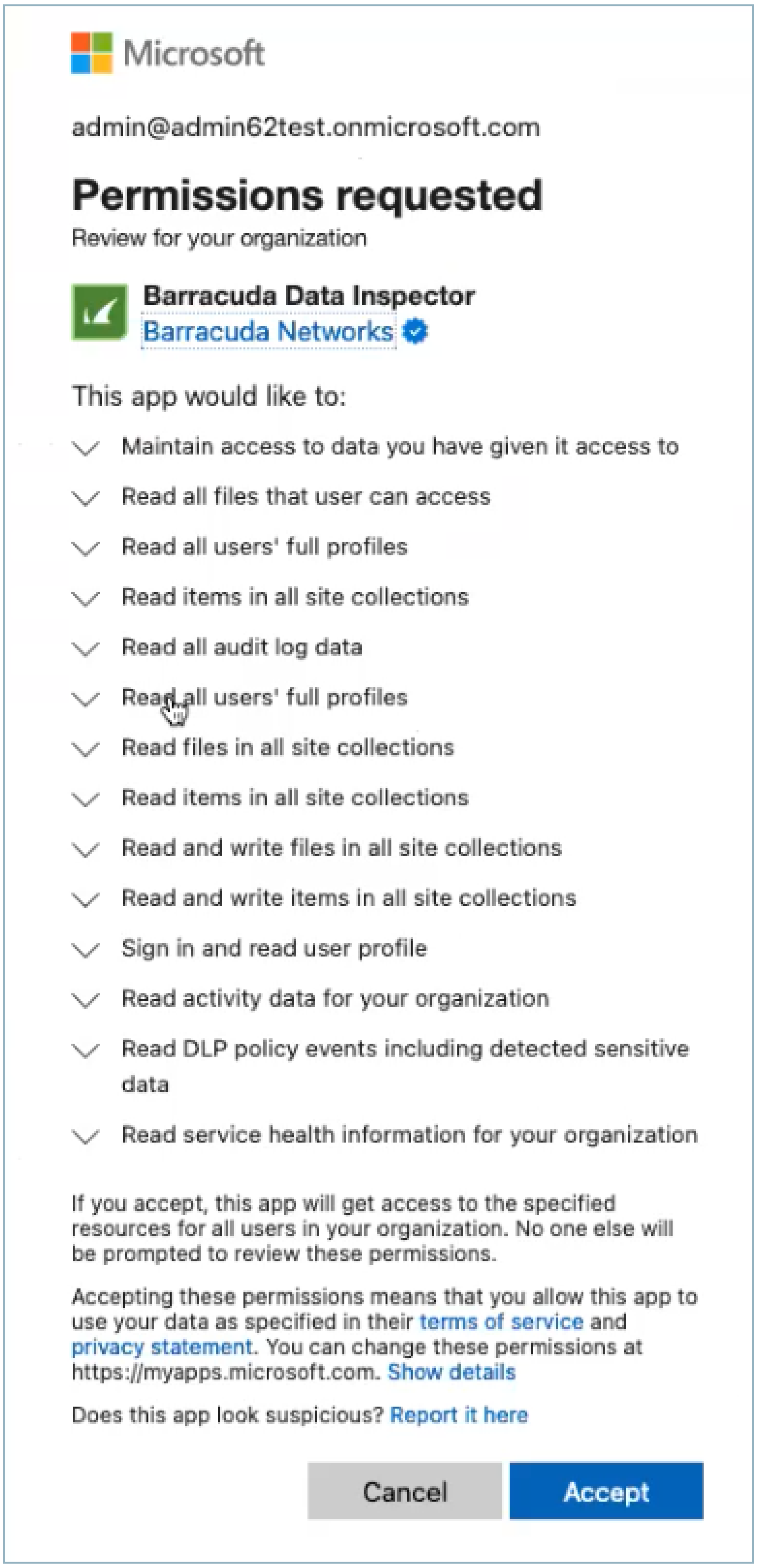
Log in with your Office 365 Global Admin user account to scan your entire tenant.

OneDrive
Office 365 Tenant — Not connected — Connect

SharePoint
Office 365 Tenant — Not connected — Connect

Back — Complete

9. A new pop-up window prompts you to enter your Microsoft 365 administrator account login information.
10. Review the permissions requested by Microsoft. Then click **Accept** to authorize Data Inspector to access your details.



Microsoft

admin@admin62test.onmicrosoft.com

Permissions requested

Review for your organization

Barracuda Data Inspector
Barracuda Networks

This app would like to:

- Maintain access to data you have given it access to
- Read all files that user can access
- Read all users' full profiles
- Read items in all site collections
- Read all audit log data
- Read all users' full profiles
- Read files in all site collections
- Read items in all site collections
- Read and write files in all site collections
- Read and write items in all site collections
- Sign in and read user profile
- Read activity data for your organization
- Read DLP policy events including detected sensitive data
- Read service health information for your organization

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

Does this app look suspicious? Report it here

11. You are redirected back to the wizard. Click **Complete** to start the scan.

As Data Inspector scans your files, the **Detections** page will begin to populate with information about the sensitive data or malicious files.

## Figures