ad
AdminDroid

DATA SECURITY
AND
PERMISSIONS

MODERN AUTHENTICATION

YOUR DATA IS IN YOUR CONTROL

NO NEED FOR SERVICE ACCOUNT

WE DON'T STORE ADMIN PASSWORD

OFFICE 365 SINGLE SIGN-ON

AdminDroid Data Security

Overview

Data security is our primary focus while building AdminDroid Office 365 Reporting tool. AdminDroid's security experts know that every Office 365 admin is concerned about the security and confidentiality of their reporting data. Hence, unlike other reporting applications, AdminDroid will not ask for your administrator password or keep your Office 365 data in the cloud. Rather, it will be stored on your desired local computer protected by your organization's security.

Office 365 modern authentication

AdminDroid is the first in the industry to offer complete modern authentication support to connect to Exchange Online and other Office 365 services. It will help you to follow high security standards such as Security Defaults, MFA (multi-factor authentication), Conditional Access Policy, Disabling Office 365 Basic Authentication and so on.

Your Data is in your control

AdminDroid can be installed in any of your existing on-premises client/server machine. In this approach, all of your Office 365 reporting and auditing data are stored in a computer in your control; thus, offering control over your data.

No need for Service Account

AdminDroid does not require you to set up a Service Account or enter any existing account credentials as it makes use of the Graph API with a token-based authorization model. Just login to Office 365 and start using AdminDroid!

We don't store your admin password

As the product is built using [Azure AD consent framework](#) , we will never ask your administrator account password to collect the reporting data. With few mouse clicks, you can grant the requested access to the AdminDroid application and start seeing your Office 365 reporting data in seconds!

Office 365 single sign-on

We threw away the classic login page and secured the application with the Office 365 single sign-on. You can just log in with your configured Office 365 account to access this application. The first click takes you to your Reporting data, right away.

AdminDroid Permission Requisites

Permissions required for basic reporting

To get the basic reports (Azure AD Reports which includes Users, Groups, Licenses, etc.) to work, you need to sign-in/authorize the AdminDroid application using the Global Administrator account.

When you authorize the AdminDroid application, Microsoft will verify the authorization and it will create an entry in your Azure AD application list and provide an authorization token which will be used to fetch the report information.

In the above communication, your credentials are not provided to the AdminDroid application. Only the authorization token will be used to fetch the report information periodically from Office 365 services.

Permissions required for advanced reporting

To get the reporting on Audit Reports, Exchange Online, SharePoint Online etc., a service application is generated in your Azure AD with your consent.

The Service Application will be used to fetch the reporting data from Office 365 services. To see the applications created for AdminDroid by Microsoft, please access the Azure AD Applications in the Azure portal.

AdminDroid

Our mission is to solve everyday challenges of IT admins and save their time. We strive to provide admin-friendly software with a user-friendly interface, at a budget-friendly pricing. Try AdminDroid, and you'll love how it simplifies your Microsoft 365 management!

For a live demonstration of our flagship tool, AdminDroid Microsoft 365 Reporter, visit below.

Live Demo **Download**

Connect with us

in linkedin.com/company/admindroid/   reddit.com/r/AdminDroid/   X twitter.com/admiindroid

f facebook.com/admindroid   youtube.com/admindroid   ad admindroid.com

github.com/admindroid-community