AdminDroid

AdminDroid 365

Microsoft 365 & Active Directory Management Tool

Product FAQ

AdminDroid 365

Microsoft 365 & Active Directory Management Tool

PRODUCT FAQ

INSTALLATION & MAINTENANCE

MICROSOFT 365 PERMISSION

MICROSOFT 365 DATA COLLECTION

ADMINDROID ACTIVE DIRECTORY

SECURITY

INSTALLATION & MAINTENANCE

What are the system requirements?

System Requirements

- Operating System
    - Windows 8.1
    - Windows 10
    - Windows 11
    - Windows Server 2012
    - Windows Server 2012 R2
    - Windows Server 2016
    - Windows Server 2019
    - Windows Server 2022
    - Windows Server 2025
- Active internet connection is required.
- Minimum Hardware Requirements
    - RAM 8 GB or more
    - Disk space - 100 GB free
    - 8 vCPUs or more

Notes:

- Hardware requirements depend on the size of the tenant you are going to set up.
- For better performance please install the product in the Windows server machine.
- We recommend deploying the application in a machine that runs 24 x 7.
- The solution will auto adjust the workload execution based on the available RAM, so you don't need to worry about this factor.
- We highly recommend going with ‘SSD’ for storage in the AdminDroid installed machine. This would make the data processing much faster.
- AdminDroid will contact Microsoft 365 services at regular intervals to fetch report and audit data. Hence, the AdminDroid-installed machine needs to be turned on always.

How to update to newest version of the product?

You don't need to worry about updating the application with the latest available version. The product has an inbuilt auto-update module that will self-update the product to the latest version. It ensures that the latest features and security updates are available to you as soon as it is released.

Where does AdminDroid store the collected Microsoft 365 data?

AdminDroid is currently an on-premises application. The application is fully installed in your environment and stores all of your collected M365 tenant data in your installation machine.

What is the database used to store report data?

The product ships with a built-in PostgreSQL database which is used to store and query the report data.

The latest version of AdminDroid uses PostgreSQL version 15. The older versions will be using PostgreSQL version 13. However, you can reach out to us at 'support@admindroid.com' for upgrading your database to the latest version.

We take care of patching and updating the database instance using the auto-update module of the AdminDroid application.

How to change the default port number used by AdminDroid?

Please follow the below steps to access AdminDroid from a different port.

- Open **Internet Information Services (IIS) Manager**.
- From the left pane, expand **Sites**.
- Right-click on **AdmindroidOffice365ReportingSite** and select **Edit Bindings**.
- Click on **Add** button and enter your desired port leaving other settings intact.

Note: Please make sure that no other sites run on the port you choose. If a site already exists, you can follow the above steps and change it to a different port before applying.

What endpoints and ports do I need to whitelist on my firewall or proxy server?

Hosts need to be whitelisted:

- https://admindroid.com
- https://*.admindroid.com
- https://windows.net
- https://*.windows.net
- https://office.com
- https://*.office.com
- https://office365.com
- https://*.office365.com
- https://microsoft.com
- https://*.microsoft.com
- https://microsoftonline.us
- https://*.microsoftonline.us
- https://*.microsoftonline.com

Ports need to be whitelisted: Outbound 443.

Please check whether Microsoft 365 endpoints are allowed for access in your proxy and firewall.

Can I turn on HTTPS for the application?

To enable HTTPS for AdminDroid 365 portal, you can configure SSL certificates directly from the AdminDroid portal.

- Please navigate to the AdminDroid portal > Settings > Portal Settings > Connection page.
- Click 'Enable HTTPS', then select the Manage SSL Certificate option.
- Choose either Upload SSL or Create Self-signed option & click 'Apply'.
- Finally, change the Port and Host Name as per your requirement

Note:

Using a self-signed certificate is not recommended. You may also see a browser warning, but you can safely skip it to proceed.

Is AdminDroid a cloud-based application?

No, AdminDroid is only an on-premises application, and we don't offer a cloud solution at the moment. As the tool will automatically update the latest version, no maintenance is required.

If you wish, you can install the product in a cloud VM and access it as a cloud service. Alternatively, AdminDroid is also available on the Azure Marketplace, where you can purchase a cloud VM subscription along with a separate AdminDroid license.

When you host AdminDroid in cloud, we recommend implementing necessary IP/Region-based restrictions for accessing AdminDroid. It will help you to secure the instance from access threats.

Can we migrate AdminDroid from one machine to another?

Yes, it is possible to transfer AdminDroid from one machine to another without losing your current data.

1. Install the latest version of AdminDroid Microsoft 365 Reporter from our website in the target machine.
2. Ensure that both installations are running the **same version** of AdminDroid. You can verify that by navigating to **Support** page in the product's left navigation menu.
3. Turn off the 'AdminDroid' Application Pool in both old and new Installations.
   - Open **IIS Manager**.
   - Now in the Connection pane (you can find this in LHS of IIS Manager), select the **'Application Pools'** and select to **'AdmindroidOffice365ReportingAppPool'** from the list.
   - Right-click 'AdmindroidOffice365ReportingAppPool' and click **'Stop'**.
4. Delete the installation folder (Microsoft 365 Reporter) in the new installation. The product will be usually installed in 'C:\Program Files\AdminDroid\Microsoft 365 Reporter'.
5. Now go to the AdminDroid installation folder in the old installation and copy the installation folder ('C:\Program Files\AdminDroid\Microsoft 365 Reporter) and paste it in the new installation machine.
6. Once all the files are copied, **turn on** the 'AdmindroidOffice365ReportingAppPool' in the target machine.

Now, you can access the AdminDroid application using the shortcut provided in the desktop of the target machine.

Please have the initially installed files in the same location for up to a week. This will serve as a back-up until its confirmed that everything is working fine in the new location.

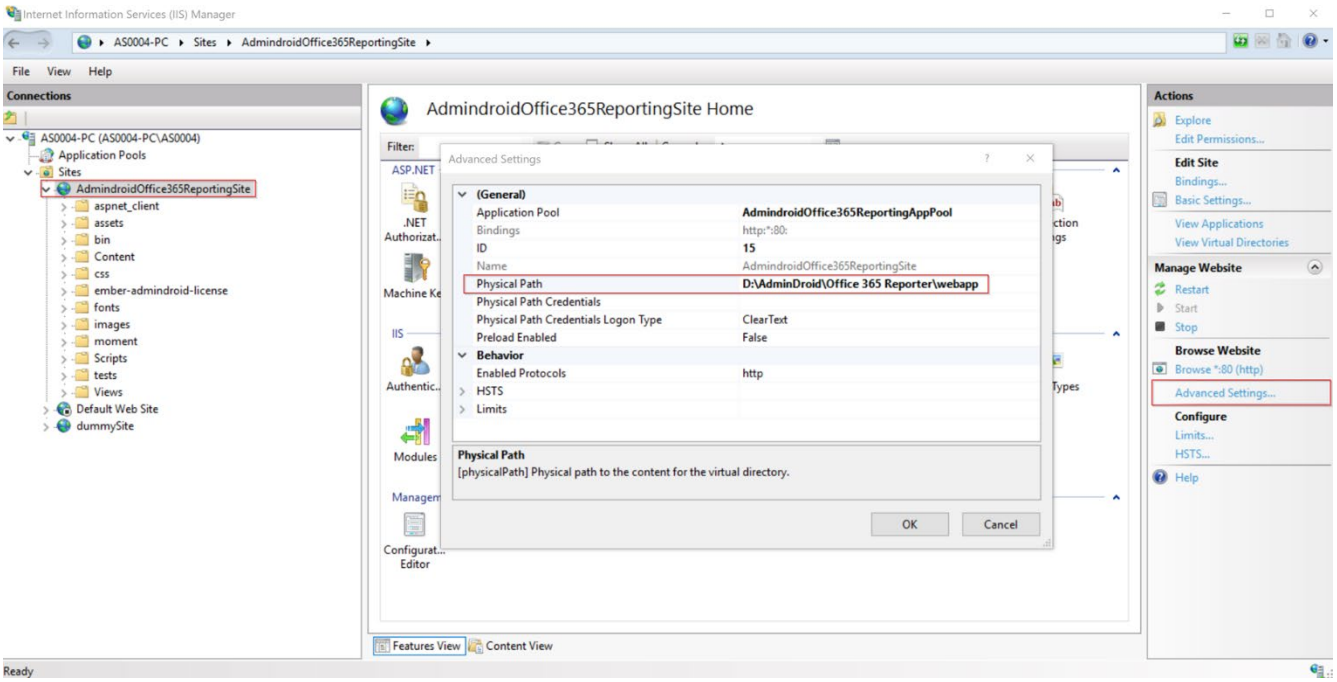
Can we migrate AdminDroid from one disk drive to another?

Yes, it is possible to move AdminDroid from one disk drive to another without losing your current data.

- Stop AdminDroid from Internet Information Services Manager.
  - Open **IIS Manager** from the AdminDroid installed server.
  - Navigate to **Application Pools** from the left menu.
  - Right click on **AdmindroidOffice365ReportingAppPool** and click Stop.
  - Again, on the left pane, expand **Sites**.
  - Right click on **AdmindroidOffice365ReportingSite** and click **Manage Website > Stop**.

- **Copy** AdminDroid folder from C:\Program Files\AdminDroid to your desired location. Let's say D:\AdminDroid.
- Update the new location in IIS Manager.
    - Now, open IIS Manager again. Navigate to **Sites > AdmindroidOffice365ReportingSite**.
    - On the right pane, click on **Advanced Settings**.
    - In the appeared Dialog Box, modify the **Physical Path** property to **D:\AdminDroid\Office 365 Reporter\webapp** and click OK.
- Start AdminDroid from IIS Manager.
    - Right-click **AdmindroidOffice365ReportingSite** on the left pane and select **Manage Website > Start**.
    - Select **Application Pools**, Right click on **AdmindroidOffice365ReportingAppPool** and click Start.

Now, AdminDroid must be running from the new location. **Please have the initially installed files in the same location for up to a week**. This will serve as a back-up until its confirmed that everything is working fine in the new location.



Can we have a live hands-on experience of AdminDroid functionalities without installing the product?

Yes, you can check out our live demo instance from our website to view, and have a hands-on experience on the available functionalities.

You shall download and install AdminDroid from our website. Right from the product setup, every product functionality is very simple to implement, understand and use. We have laid out all the user interface elements properly and made sure that it shouldn't arise any confusion to the end user.

What kind of support does AdminDroid provide?

We offer both email and voice support to assist with your queries.

Email Support: Available 24×6, we respond promptly to all your queries including sales, licensing, product, technical, and feature-related queries, providing the guidance and information you need.

If you need any assistance, please reach out to us at support@admindroid.com. We'll get back to you as soon as possible.

Voice Support: Available 24×6, you can contact us at support@admindroid.com to schedule a remote session. Whether you need a product walkthrough, or live troubleshooting, we're here to help.

MICROSOFT 365 PERMISSION

How does AdminDroid collect Microsoft 365 data?

AdminDroid creates an enterprise application called 'AdminDroid Agent' in Entra ID, which uses Microsoft Graph APIs, CSOM, and PowerShell cmdlets to securely collect Microsoft 365 data. You don't need to install any PowerShell modules as AdminDroid will take care of using the latest supported modules.

Why does AdminDroid require a Global Admin authorization?

AdminDroid requires Global Admin authorization to create the necessary enterprise applications and assign with relevant permissions for the proper functioning of AdminDroid. Alternatively, you can authorize using an account that has both “Privileged and Application” Administrator roles.

Note: The application won’t store the password of the authorized account. Once you authorize initially, AdminDroid will be assigned with the ‘directory access as user’ permission on behalf of the authorized account.

Can we remove global admin role after the initial authorization?

Yes. After initial authorization, you can downgrade the authorized user's role from Global Admin to Global Reader, and AdminDroid data collection will continue normally.

However, when a feature that requires new permissions is released, you must re-authorize using Global Admin privileges at that time to access those features.

What applications does AdminDroid create in my tenant?

AdminDroid creates separate enterprise applications for different functions. Each application has a specific purpose and only has the permissions required for that function.

AdminDroid 365 - Created during the initial authorization, this service principal collects initial Entra data alongside creating a delegated service application - “AdminDroid App”.

AdminDroid App - This delegated application acts on behalf of the authorized user to create and assign required API permissions for “AdminDroid Agent”, when you enable ‘Advanced Features’ in AdminDroid.

AdminDroid Agent - This application executes all data collection and management tasks in AdminDroid using the assigned API permissions.

You can find here the list of enterprise applications created by AdminDroid.

What changes will be made in my tenant using the Service Application?

By default, the Service Application is used only to collect Microsoft 365 data and does not create, modify, or delete anything in your tenant.

AdminDroid also offers management capabilities that let you create, modify, or delete Microsoft 365 objects directly from the AdminDroid console. It does not make changes to your tenant unless you explicitly perform or automate management action in AdminDroid.

What are the graph API permissions that AdminDroid uses to collect the Microsoft 365 data?

AdminDroid uses various Microsoft Graph APIs to collect data from your tenant. The following permissions are required to ensure seamless data collection and management across Microsoft 365..

Common Permissions

(The following permissions are required for both capability selections)

- **AuditLog.Read.All** - Read all audit log data
- **Policy.Read.All** - Read your organization's policies
- **IdentityRiskEvent.Read.All** - Read all identity risk event information
- **Reports.Read.All** - Read all usage reports
- **ReportSettings.ReadWrite.All** - Read and write all admin report settings
- **SecurityEvents.Read.All** - Read your organization’s security events
- **DeviceManagementConfiguration.Read.All** - Read Microsoft Intune device configuration and policies
- **DeviceManagementManagedDevices.Read.All** - Read Microsoft Intune devices
- **AuditLogsQuery.Read.All** - Read audit logs data from all services
- **Sites.FullControl.All** - Have full control of all site collections
- **Exchange.ManageAsApp** - Manage Exchange As Application
- **Application.ReadWrite.All** - Read and write all applications

Insights Capability

(Permissions required for reporting and insights)

- **ChannelMember.Read.All** - Read the members of all channels
- **UserAuthenticationMethod.Read.All** - Read all users' authentication methods
- **ChannelSettings.Read.All** - Read the names, descriptions, and settings of all channels

- **Directory.Read.All** - Read directory data
- **TeamMember.Read.All** - Read the members of all teams

Management Capability

(Permissions required for management and administrative actions)

- **Directory.ReadWrite.All** - Read and write directory data
- **User.ReadWrite.All** - Read and write all users' full profiles
- **RoleManagement.ReadWrite.Directory** - Read and write all directory RBAC settings
- **UserAuthenticationMethod.ReadWrite.All** - Read and write all users' authentication methods
- **ChannelSettings.ReadWrite.All** - Read and write the names, descriptions, and settings of all channels
- **ChannelMember.ReadWrite.All** - Add and remove members from all channels
- **Policy.ReadWrite.AuthenticationMethod** - Read and write all authentication method policies
- **User.EnableDisableAccount.All** - Enable and disable user accounts
- **User-PasswordProfile.ReadWrite.All** - Read and write all password profiles and reset user passwords
- **User.DeleteRestore.All** - Delete and restore all users
- **User-Phone.ReadWrite.All** - Read and write all user mobile phone and business phones
- **User-Mail.ReadWrite.All** - Read and write all secondary mail addresses for users
- **TeamMember.ReadWrite.All** - Add and remove members from all teams
- **Group.ReadWrite.All** - Read and write all groups
- **User-LifeCycleInfo.ReadWrite.All** - Read and write all users' lifecycle information

Teams Deep Insights (DI)

- **Callrecord.read.all** - Read all call records
- **Chat.read.all** - Read all chat messages
- **ChannelMessage.Read.All** - Read all channel messages
- **Presence.Read.All** - Read presence information for all users

Exchange Deep Insights (DI)

- **Mail.Read** - Read mail in all mailboxes

Note: Though we have the write permission to the directory, AdminDroid will not write (Create/Update/Modify...) anything without your approval.

Where is the Service Application information stored?

The Service Application information is encrypted and stored in your AdminDroid's installation location, inside a password-protected database.

Note: This database protection is not only for Service Application information; It applies for all your data collected from Microsoft 365.

Will the Service Application incur any Microsoft 365 license cost?

No, the created Service Application doesn't require any license.

MICROSOFT 365 DATA COLLECTION

Does AdminDroid support modern authentication?

Yes, completely. AdminDroid uses modern authentication for everything from login to collecting data from your Microsoft 365 tenant.

How does AdminDroid refresh the report data?

AdminDroid provides near-real-time reports that auto-refreshes at specific intervals. AdminDroid always ensures that you see the latest data inside any report or dashboard.

You can manually refresh the data anytime using the '**Sync Now**' option provided in the application.

Microsoft 365 Application	Refresh Frequency
Entra	10 minutes
Audit Log, Email Log, Sign-in Log	10 minutes
Exchange, Microsoft Teams	24 hours
SharePoint	24 hours
Microsoft 365 Usage Reporting Data*	6 hours

*Microsoft API usually returns the Microsoft 365 usage data with a **48 hours delay**, and hence, you will face the same in the AdminDroid usage reports.

For up-to-date usage data, you shall refer to our Analytics reports. For instance, if you wish to get near real-time email statistics, refer to the section under 'Reports > Email > Analytics'.

What is the retention period for collected Microsoft 365 data?

This tool doesn’t enforce any restriction on how long you can keep your auditing and reporting data. You can retain your data as per your company policy using AdminDroid’s Retention settings.

Can we manage multiple tenants using AdminDroid?

Yes, AdminDroid can manage multiple tenants in a single portal efficiently. You can add tenants in the '**Settings > Tenant**' page from the left pane of your AdminDroid portal. It also offers effort-free delegation options. You can delegate any Microsoft 365 users to access one or more tenants.

ADMINDROID ACTIVE DIRECTORY

(Setup, Permissions & Data Collection)

How can I connect AdminDroid to my Active Directory domain? Are there any prerequisites?

To connect AdminDroid to your Active Directory domain, you need to authorize it using an account with **Built-in Administrator, Domain Admin, or Enterprise Admin** privileges. Additionally, the host machine (where AdminDroid is installed) must be on the same network as the on-premises AD domain, or accessible via a secure connection, to perform data collection.

How is my Active Directory domain automatically added to AdminDroid?

By default, if the machine where AdminDroid is installed is already domain joined to your Active Directory domain, AdminDroid will automatically detect and activate Active Directory reporting using the Windows identity that the AdminDroid service/process itself runs as — not your login, and not a saved admin credential.

If that service account lacks AD read rights, AdminDroid will not be able to perform data collection using LDAP queries.

Do any agents need to be installed in our Active Directory environment?

No. AdminDroid is a completely agentless solution. Data collection is performed using LDAP queries and Windows API calls after the required permissions are granted during the initial authorization process.

How does AdminDroid collect data from the on-premises Active Directory environment?

AdminDroid uses LDAP queries to collect statistical data from Active Directory. For event-based (audit) data, AdminDroid uses internal Windows API calls to retrieve information from the Event Viewer logs of the required machines.

What Group Policy Object (GPO) firewall rules are required for AdminDroid Active Directory data collection, and why?

AdminDroid requires specific Windows Firewall rules to securely communicate with Domain Controllers. These are automatically configured via a Group Policy Object (GPO) when machines are added under the Audit Settings page.

Rule Group Name: AdminDroidAuditor

The following inbound firewall rules are enabled within this rule group:

- NPC-In (Remote Administration)
- RPC (Remote Procedure Call)
- RPC-EPMAP (Remote Endpoint Mapper)

Without these firewall configurations, Active Directory data collection may fail or remain incomplete.

What authentication method does AdminDroid use for Active Directory communication?

AdminDroid uses LDAP Bind over Port 389 for Active Directory communication.

During authentication:

- The connection first attempts to use Kerberos authentication.
- If Kerberos is unavailable or unsupported, it automatically falls back to NTLM authentication.

This behavior follows the standard Windows authentication negotiation process.

How frequently is Active Directory data synchronized?

Category	Refresh Frequency
Report Objects (Users, Computers, Contacts, Groups, Organizational Units, Printers)	10 minutes
Audit Data	30 minutes
Non-Replicated Attributes (e.g., Last Logon Time)	30 minutes

SECURITY

What is the login method used for this application?

AdminDroid has built-in support for Microsoft 365 single sign-on (SSO). Hence, the authorization is handled by Microsoft 365 login page.

Can I use 2FA or MFA for this application?

Yes, as the product supports SSO with Microsoft 365, if you enabled 2FA or MFA to your Microsoft 365 account then the same authentication is enforced to access this application i.e., the same security standards that you follow for your Microsoft 365 account can be incorporated for AdminDroid.

How does the data security work?

Protecting customer data is our highest priority. AdminDroid is designed to make sure that customers retain full control over their collected data, including where it's stored, how it's accessed, and what security measures are applied.

To further strengthen your deployment, we recommend following the best security practices outlined in our Fortifying Deployment Recommendations guide. It provides comprehensive guidance on securing your AdminDroid environment and implementing recommended security configurations.

Does AdminDroid send any data out of the installation machine?

No, AdminDroid does not process your Microsoft 365 data outside the installation machine.

We only store the admin email address used during the product installation. This email address is used to communicate important product updates, including security advisories and new feature announcements.

We do collect anonymous statistics about your usage of the product functionalities to better prioritize our upcoming features and enhancements. This information is never shared with third parties.

For more information about how we collect and use data, please refer to our Privacy Policy.

Does AdminDroid application comply with the General Data Protection Regulation (GDPR)?

AdminDroid is designed with privacy and security in mind. As an on-premises solution, all Microsoft 365 data collected by AdminDroid remains within your environment, allowing you to retain full control over your data, storage, access, and retention. We store all the information in the database with an encrypted password, and you can access the data only through your configured Microsoft 365 credentials.

Who can access the report's data?

Access to AdminDroid is restricted to authorized users in your Microsoft 365 tenant. AdminDroid uses its own role-based access control under 'Settings > Admins' page, allowing you to grant access to users regardless of their Microsoft 365 administrative role.

Also, AdminDroid's 'granular role-based access delegation' functionality will allow you to control which reports, dashboards, and data each user can access.

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

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

facebook.com/admindroid youtube.com/admindroid admindroid.com

github.com/admindroid-community

© 2026 AdminDroid. All Rights Reserved.