

AdminDroid Deployment

Fortifying Recommendations



Fortifying Recommendations

1. Set up a dedicated Server-Machine for Installation

We recommend installing the product on a dedicated client / Windows Server machine that will be running 24 x 7 and always connected to the internet for a seamless reporting experience. It will also allow you to enhance security by minimizing the attack surface.

2. Restrict Access to installation machine

Restrict Network Access to admit only required connections

Alongside the required [Firewall/Proxy settings](#), restricting network access using DNS and IP whitelisting is a valuable security measure that can significantly reduce the risk of unauthorized access and data breaches.

Enable HTTPS

Enabling HTTPS for AdminDroid is highly recommended. It is a critical security measure that can help to protect sensitive data over the network.

Refer our General FAQ for [steps to enable HTTPS for AdminDroid](#).

Disable Remote Access Ports

We recommend implementing necessary IP/Region based restrictions for accessing AdminDroid from remote machines. It will help you to secure the instance from access threats.

If you are planning to install AdminDroid in a cloud, then disabling remote access port is a must.

Allow Privileged Users Only

Restrict AdminDroid access to allow only users with legitimate administrative privileges. It ensures that only authorized personnel can manage the application and its sensitive data.

Allow only system account to access AdminDroid folders

AdminDroid runs using your LocalSystem (NT AUTHORITY\SYSTEM) account. As AdminDroid files do not require any interactive modifications by any user account, you shall go for this recommendation.

Note: We recommend testing this setting in different machine before implementing in AdminDroid installation machine.

Encrypt the Database Folder

Encrypting the database folder can safeguard sensitive information against unauthorized access and data breaches. By default, PostgreSQL doesn't provide any encryption at rest for entire DB.

You can implement the encryption method that is best suited for your environment. However, we recommend Using Windows' built-in EFS allows you to encrypt files and folders on NTFS file system volumes using a public-key system. Refer to the end of the document for steps.

3. Keep the installation server up to date

Maintaining up-to-date software versions on the AdminDroid server promptly addresses newly discovered vulnerabilities and security patches.

4. Schedule a regular backup for AdminDroid data

Scheduling regular backups ensures data recovery and restoration capabilities in case of accidental deletion or crashes.

Steps to encrypt DB using Windows EFS

➔ Create a recovery certificate in a different machine other than AdminDroid installation machine.

- Open Command Prompt with administrator privileges.
- Type: `cipher /r:C:\Recovery (cipher /r: <PathOfTheExport>)`
- Enter a password on prompt and save it securely.
- Now, move the **Recovery.cer** file to the AdminDroid installation machine.

➔ Enable EFS in the installation server, if not enabled already.

- Open the **Local Security Policy** tool.
- Navigate to **Security Settings » Public Key Policies**.
- Right-click on "EncryptingFileSystem" and select "Properties."
- In the General tab, choose 'Allow' for 'File encryption using EFS'.
- **Apply** the new settings and **save** the changes.

➔ Encrypt AdminDroid DB by running the below cmdlet in command prompt.

```
cipher /E /S:"PATH OF BASE FOLDER"
```

Usually DB path will be 'C:\Program Files\AdminDroid\Office 365Reporter\pgsql\data\base')

Note: As long as EFS certificate present in your system, AdminDroid uses this certificate for encrypting & decrypting the data.

➔ Restart AdminDroid in IIS

- Open Internet Information Services (IIS) Manager
- From the left pane, expand your computer name, and click on **Application Pools**.
- Now, right click on **AdmindroidOffice365ReportingAppPool** and click **Stop** .
- Please wait for 90 seconds and then click Start.

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/](https://www.linkedin.com/company/admindroid/)[reddit reddit.com/r/AdminDroid/](https://www.reddit.com/r/AdminDroid/)[X twitter.com/admiindroid](https://twitter.com/admiindroid)[f facebook.com/admindroid](https://www.facebook.com/admindroid)[yt youtube.com/admindroid](https://www.youtube.com/admindroid)[ad admindroid.com](https://admindroid.com)[g github.com/admindroid-community](https://github.com/admindroid-community)