AdminDroid

# 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.**

- In the command prompt window, run the following command to create a recovery certificate:

  ```
  cipher /r:"PATH TO STORE CERTIFICATE AND KEY\NAME OF THE FILE"
  ```

  For example, `cipher /r:"D:\EFS\Recovery"`

- Then, enter a password on prompt and save it securely. There will be two files named **Recovery.CER** and **Recovery.PFX** will be created.
- Now, move the **Recovery.CER** file alone to the AdminDroid installation machine.
- Once moved, install the Recovery.CER certificate file by following the steps below.
  - Click on **Start** and open the **Edit Group Policy** tool.
  - Navigate to **Computer Configuration** » **Windows Settings** » **Security Settings** » **Public Key Policies.**
  - Now, right-click on "**Encrypting File System**" and select "**Add Recovery Agent**".
  - In the **Add Recovery Agent** tab, browse for the **Recovery.cer** and click next.
  - **Apply** the new settings and **save** the changes.

**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 "**Encrypting File System**" 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.

- Download the PSTools and extract the contents.
- Open the 'Command Prompt' as an administrator. Then, navigate to the directory where you extracted the files using the following command:

```
cd /d "PATH OF THE EXTRACTED FOLDER"
```

- Run PsExec using the following command to open a new command prompt window with system admin privileges:

```
PsExec.exe -s -i cmd.exe
```

```
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.