Android Virtual Device

If you do not have an Android device to try out WSO2 IoT Server, follow this tutorial and enroll an Android Virtual Device (AVD) with WSO2 IoT Server.

![Checkmark icon]

**Before you begin**

1. Make sure to enable the virtualization technology on your basic input/output system (BIOS). This is required to create the Android virtual device.
2. Start the WSO2 IoT Server core profile.

```
------Navigate to the bin directory------
cd <IoT_HOME>/bin

------For Linux/MacOS/Solaris------
sh iot-server.sh

----------For Windows----------
iot-server.bat
```

Let's get started!

1. Sign in to the Device Management console.
Accessing the WSO2 IoT Server Consoles

Follow the instructions below to sign in to the WSO2 IoT Server device management console:

a. If you have not started the server previously, start the server.
b. Access the device management console.
   
   - For access via HTTP:
     http://<IOTS_HTTP_HOST>:9763/devicemgt/
     For example: http://localhost:9763/devicemgt/
   
   - For access via secured HTTP:
     https://<IOTS_HTTPS_HOST>:9443/devicemgt/
     For example: https://localhost:9443/devicemgt/

c. Enter the username and password, and sign in.

   The system administrator will be able to log in using admin for both the username and password. However, other users will have to first register with WSO2 IoT Server before being able to log into the IoTS device management console. For more information on creating a new account, see Registering with WSO2 IoT Server.

d. Click LOGIN. The respective device management console will change, based on the permissions assigned to the user.

For example, the device management console for an administrator is as follows:
2. Click Add under DEVICES.

3. Click **Try** to try out the virtual Android device.

4. Click Download the virtual Android device.

5. Unzip the downloaded android-tryIt.ZIP file.

6. Run the startEmulator script on your terminal.

   **Linux/Mac**
   ```
   cd <ANDROID_TRY_IT> ./startEmulator.sh
   ```

   **Windows**
   ```
   cd <ANDROID_TRY_IT> startEmulator.bat
   ```

7. Install the Android SDK on your computer by entering **n** when prompted.

   ```
   Do you have an Android SDK installed on your computer (y/n) ? :
   ```

   - **⚠️** If you have an Android SDK already installed on your computer, enter **y**, and provide its location when prompted.

8. Create the AVD by entering **y** when prompted.

   ```
   Do you want to create WSO2_AVD with default configs (y/n)?:
   ```

9. Next, the system prompts to create a custom hardware profile by requesting for device specific details. You can enter **no** as the response and skip this step.

   ```
   Do you wish to create a custom hardware profile [no]
   ```

10. If you have multiple AVDs, enter WSO2_AVD to continue with the tutorial.

    ```
    Enter AVD number to start (eg: 1) :
    ```

    - **⚠️** If you only have the **WSO2_AVD** on your computer, it starts automatically.

11. If you are running the script on a Mac or Windows OS, the system prompts to install the Hardware Accelerated Execution Manager (HAXM) to get the Android emulator running. Enter the **password** and proceed with the installation.

    ```
    Installing intel HAXM, Please wait ...
    Password:
    ```
Once the installation is complete, the system prompts you to restart your computer, and run the emulator.

Silent installation Pass!
Please restart your machine and run again.

If you are running the AVD for the first time, it takes a couple of minutes for the virtual device to start up and complete the agent installation process.

If you restart your computer as part of the HAXM installation process, make sure to start the WSO2 IoT Server core profile before running the emulator.

```
cd <IoT_HOME>/bin
sh iot-server.sh
```

12. After running the emulator, tap **SKIP AND GO TO ENROLLMENT**, which will direct you to install the device with WSO2 IoT Server in the default manner.

In WSO2 IoT Server, data containerization is implemented using the Managed Profile feature. For more information on how to **set up the Work-Profile**, see [Setting Up the Work Profile](#).

---

**WSO2 Device Management Agent**

Your device supports Android For Work. Set-up the work-profile first and let the Agent Control the Work Profile.

- [SETUP WORK-PROFILE](#)
- [SKIP AND GO TO ENROLLMENT](#)
13. Enter the server IP and the port as your server address in the text box provided and tap **START REGISTRATION**.

**Example:** Register the device via HTTP: **10.100.7.35:8280**

14. Type your details and tap **SIGN IN**. A confirmation message appears.

- **Organization**: This field is optional. You need to enter organization name only if you are running in a multi-tenant environment.

  - If you are not running in a multi-tenant environment, the default organization name is carbon.super. But you can choose to keep this field blank too.

- **Username**: Your WSO2 IoT Server username.
- **Password**: Your WSO2 IoT Server password.
Please sign in to register your device with WSO2 IoT Server.

Organization
carbon.super

Username
kim

Password
**********

SIGN IN
15. Read the policy agreement, and tap **AGREE** to accept the agreement.
16. Tap **ACTIVATE** to enable the WSO2 agent administrator on your device. A confirmation message appears after enabling the device admin.

![Activate device administrator?](image)

This will enable device administration

Activating this administrator will allow the app WSO2 Device Management Agent to perform the following operations:

- **Erase all data**
  Erase the phone's data without warning by performing a factory data reset.

- **Change the screen lock**
  Change the screen lock.

- **Set password rules**
  Control the length and the characters allowed in screen lock passwords and PINs.

- **Monitor screen-unlock attempts**
  Monitor the number of incorrect passwords typed when unlocking the screen, and lock the phone or erase all the phone's data if too many incorrect passwords are typed.

**CANCEL**  **ACTIVATE**

17. Tap **ALLOW** to allow the WSO2 Android agent to make and manage phone calls, to access photos, media, files, and the device location.

![Allow WSO2 Device Management... to make and manage phone calls?](image)

1 of 3  **DENY**  **ALLOW**

18. Set a PIN code of your choice with a minimum of 4 digits and tap **SET PIN CODE**. The PIN code is used to secure your personal data. Thereby, the WSO2 IoT Server is not able to carry out critical operations on your personal data without using this PIN.

Example: If the device management admin needs to wipe your device or remove data from the device, he/she cannot directly wipe it without the PIN code. You have to provide the PIN code to get your device wiped or you can log into the device management console and wipe your device by entering the PIN code. A confirmation message appears.
19. You have now successfully registered your Android device. Tap Device Information to get device specific information, and tap Unregister if you wish to unregister your device from WSO2 IoT Server.
20. Navigate to the device management console and click **View** under devices to confirm that your device is registered.

21. Click the device and navigate to the DEVICE DETAILS page.
Check out the following features available on the DEVICE DETAILS page:

- **Device Details**: The top-left section of the DEVICE DETAILS page displays the following device information that are automatically retrieved when you register the device with WSO2 IoT Server.

<table>
<thead>
<tr>
<th>Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device owner and device name</td>
<td>Indicates the name of the device owner and the name given by the device owner to the device (e.g. Admin's Android Virtual Device). You can edit the device name via the DEVICES page.</td>
</tr>
<tr>
<td>Model</td>
<td>The type of the device.</td>
</tr>
<tr>
<td>Ownership</td>
<td>Indicates the device ownership as either BYOD or COPE.</td>
</tr>
<tr>
<td>Status</td>
<td>Indicates whether the device is active, inactive or removed from WSO2 IoT Server.</td>
</tr>
<tr>
<td>Battery level</td>
<td>Indicates the battery level of the device.</td>
</tr>
<tr>
<td>RAM usage</td>
<td>Indicates the RAM usage of the device as a percentage.</td>
</tr>
<tr>
<td>Local storage</td>
<td>Indicates the device memory consumption.</td>
</tr>
<tr>
<td>External storage</td>
<td>Indicates the external memory consumption.</td>
</tr>
</tbody>
</table>

- **Device Operations**: The following operations are supported for Android in WSO2 IoT Server:

<table>
<thead>
<tr>
<th>Operation</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ring</td>
<td>Ring the device via WSO2 IoT Server. (e.g., If you click the Ring operation, the virtual device starts ringing and a notification gets displayed. To stop the ringing tap OK on the notification.) This is useful to locate a misplaced device.</td>
</tr>
<tr>
<td>Device Lock</td>
<td>Lock the device via WSO2 IoT Server. This is useful when a device gets lost or stolen.</td>
</tr>
<tr>
<td>Location</td>
<td>Retrieve the device location.</td>
</tr>
<tr>
<td>Clear Password</td>
<td>Remove a device lock.</td>
</tr>
<tr>
<td>Operation</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Reboot</td>
<td>Reboot or restart the device. By default, this operation is inactive for AVD.</td>
</tr>
<tr>
<td>Upgrade Firmware</td>
<td>Upgrade device firmware to a newer version over-the-air (OTA). By default, this operation is inactive for AVD.</td>
</tr>
<tr>
<td>Mute</td>
<td>Enable the silent profile of the device.</td>
</tr>
<tr>
<td>Message</td>
<td>Send a message to the device via WSO2 IoT Server. Device admins can use this device operation to send private and group messages to device owners.</td>
</tr>
<tr>
<td>Change Lock-code</td>
<td>Change the passcode or lock code of the device.</td>
</tr>
<tr>
<td>Enterprise Wipe</td>
<td>Unregister the device from WSO2 IoT Server.</td>
</tr>
<tr>
<td>Wipe Data</td>
<td>Carry out a factory reset on the device. To perform this operation, the user must provide the PIN specified during the device registration.</td>
</tr>
</tbody>
</table>

- **Operations Log**: This section lists the operations that have been performed on the device and their statuses:
  - **IN-PROGRESS**: The operation processing at the WSO2 IoT Server side is in-progress and has not yet been delivered to the device.
  - **PENDING**: WSO2 IoT Server has delivered an operation to the device and is waiting for a response from the device.
  - **COMPLETED**: WSO2 IoT Server has received a response from the device, for an operation.
  - **ERROR**: An error has occurred while carrying out the operation.

The operations log gets updated at regular intervals through a polling mechanism. Click on the **Refresh Log** button to view the latest operations log. For more information on changing the polling interval, see Android Configurations.

- **Applications**: This section lists all the applications installed on the device.
- **Location**: This section indicates the geographical location of the device.
- **Policy Compliance**: This section indicates whether the device complies with the policies enforced on the device. For more information on adding a policy and enforcing it on a device, see Policy Management.
What's next?

- Create a policy and see how it is applied on the device. For more information, see Policy Management.
- Add your enrolled device or devices to a group. Grouping allows you to monitor and view device data of many devices in one go. For more information, see Grouping Devices.
- Rename your enrolled device so it will be easy for you to find your device. For more information, see Renaming a Device.