MANTRA REGISTERED DEVICE SERVICE

WINDOWS

MANTRA SOFTECH INDIA PVT LTD
# TABLE OF CONTENTS

1. Download link for Mantra RD Service Setup. ................................................................. 3
2. Mantra MFS100 Driver Setup Installation. ................................................................. 4
3. Mantra RD Service Installation. .................................................................................. 6
4. Public to L0 Conversion (MFS100 Registered Device) .............................................. 8
5. RD Service Test Application ...................................................................................... 9
6. Device Registration on Management Server ............................................................ 15
7. Technical Support ....................................................................................................... 15
1. Download link for Mantra RD Service Setup.
Registered device service of MFS100 is fully compatible with latest Aadhaar Authentication API 2.0 (rev 1).

Registered device service Setup for MFS100 is available on our download portal http://download.mantratecapp.com/Forms/DownloadFiles.

Install Mantra RD Service & MFS100 Driver Setup.
2. **Mantra MFS100 Driver Setup Installation.**
   
   1. **Start installation:**
      
      Right click on setup file and select “Run as administrator”.
      
      **Note:** To install MFS100 scanner drivers and necessary service, setup need to access system32 folder. In this case setup need administrator privileges.

2. **Welcome Wizard:**
3. Destination Location

![Destination Location Image]

4. Finish Driver Installation

![Finish Driver Installation Image]
3. **Mantra RD Service Installation.**

1. **Start installation:**
   - Right click on setup file and select “Run as administrator”.
   - **Note:** To install Mantra RD Service, setup need administrator privileges.

2. **Welcome Wizard:**

3. **Destination Location:**
4. Finish RD Service Installation:

After installation of RD Service, it can be found under Services form “Control Panel\All Control Panel Items\Administrative Tools”.

- Stop the service
- Restart the service
5. Public to L0 Conversion (MFS100 Registered Device)

- When RD Service will detect public device then it will convert it into registered device and user will be notified again with success response by RD Service.
- After that you need to unplug and plug your device.

- If your device is not listed at Mantra Management Server than user will be notified with below message so in this case you need to contact with our Servico Team at http://servico.mantratecapp.com Or +91-79-49068000.

- Once registered MFS100 device will be plugged to the system, RD service will detect it automatically and validate it on Mantra’s Management Server.
- Once validation competed then it will generate below popup for user information.
6. RD Service Test Application

1) HTTP: http://rdtest.aadhaardevice.com/
2) HTTPS: https://download.mantratecapp.com/rd/securedtest.html

- By running RD Service Test application, user can detect all RD Services installed in their system.

- User can get Device Information which is connected to its system.
By calling capture function of RD service, user can capture biometric data.

Management Server
- It is necessary that RD service installed in client machine must interact with Mantra’s Management Server.
- For that, client machine must access the domain https://aadhaardevice.com and it’s all sub-domains.

Proxy in Network (if proxy is required to connect internet)
- Please note, if you are using Proxy in your network then you need to change Mantra RD Service Logon.
- Open “Control Panel\All Control Panel Items\Administrative Tools\Services”
- Go to Mantra AVDM -> Properties -> Log On -> Change “Local System” to “This Account “ and enter system username & password as from you login to system.
Browser Configuration for Web RD Test

1) Chrome
   Open chrome browser and write below in url and click on Enable “Allow invalid certificates for resources loaded from localhost” and then click “RELAUNCH NOW”

   chrome://flags/#allow-insecure-localhost

   ![Chrome browser window showing the flag](image)

   Your changes will take effect the next time you relaunch Google Chrome.

   ![Relaunch button](image)
2) Firefox

Open Firefox browser and write below in url and click on “I Understand the Risks”, click “Add Exception”, it will open Add Security Exception popup and then click “Confirm Security Exception”.

https://127.0.0.1:8005
3) Internet Explorer

- Select a zone to view or change security settings.
- Internet, Local intranet, Trusted sites, Restricted sites.
- Click on "Custom Level" and "Enable" these options as per image and "Disable" smart screen filter as per this image.

- Security level for this zone.
- Custom settings.
- To change the settings, click Custom level.
- To use the recommended settings, click Default level.
- Enable Protected Mode (requires restarting Internet Explorer).

- Click "OK".

- Add URL shown in below images.
- 6. Add URL shown in below images.
- https://download.mantratecapp.com
- http://127.0.0.1
- http://download.mantratecapp.com
- http://localhost

- 7. If your site using only "http" instead of "https" then we can uncheck this box.
Uncheck this check box if it is checked.

Check all these check box if it is unchecked

Click "OK"

Restart "Internet Explorer" browser and then test again for capture finger

Date Time and Time Zone
7. Device Registration on Management Server
To list device pre-production or production, send serial number of device to servic@mantratec.com
+91-79-49068000.

8. Technical Support
Mantra Support Team
+91-79-49068000
support@mantratec.com & servicio@mantratec.com
This information can be shared with your clients or end user for any kind of technical support.