



Controller General of Defence Accounts

System for Pension Administration (Raksha)

User Guide for Identification using Aadhaar Biometric

Identification via Aadhaar Biometric

Pensioner can perform identification from the portal via two modes:

- A. Manuel Life certificate (MLC).**
- B. Digital Life certificate (DLC).**

Digital Life Certificate can be given by Pensioner using following two ways:

- a) Identification via Jeevan Pramaan
- b) Identification via Aadhaar Biometric

In this document we have covered the steps on how the identification can be performed using Aadhaar Biometric.

Following is the broad categorization of the pre-requisites & steps involved on how to perform identification using Aadhaar Biometric.

1. **Download Mantra RD Service setup.**
2. **How to install Mantra -MFS100 driver setup installation**
3. **Mantra RD Service Installation.**
4. **MFS100 Registered Device detect.**
5. **RD Service Test Application.**
6. **Proxy Setting.**
7. **Browser Configuration for Web RD Test.**
8. **Device Registration on Management Server.**
9. **Technical Support.**
10. **Performing Digital Life certificate (DLC) by capturing Biometric.**

1. Download link for Mantra RD Service Setup.

Registered device service of MFS100 is fully compatible with latest Aadhaar Authentication API.

Registered device service Setup for MFS100 is available on our download portal

<http://download.mantratecapp.com/Forms/DownLoadFiles>

MANTRA PRODUCTS - DOWNLOAD

MFS100 & MIS100V2 RD Service (Aadhaar auth API 2.5 and E-Kyc API 2.5 compliance), MFS100 & MIS100V2 Driver and MFS100 Client service (Non-Aadhaar Application) setup including pre-requisites and test application.

WINDOWS Download MFS100 RD Service
[Aadhaar auth API 2.5 and E-Kyc API 2.5 compliance (also download and install driver setup)]
[Download User Manual](#)
[Download MFS100 RD Service](#)

WINDOWS Download MIS100V2 RD Service
[Aadhaar auth API 2.5 and E-Kyc API 2.5 compliance (also download and install driver setup)]
[Download User Manual](#)
[Download Mantra MIS100V2 RD Service](#)

WINDOWS Download MFS100 Client Service
[Aadhaar auth API 1.6 compliance]
[Download User Manual](#)
[Download MFS100 Client Service](#)

WINDOWS Download MFS100 Driver
[Download MFS100 Driver - Windows XP/7/8/10](#)

WINDOWS Download MIS100V2 Driver
[Download MIS100V2 Driver](#)

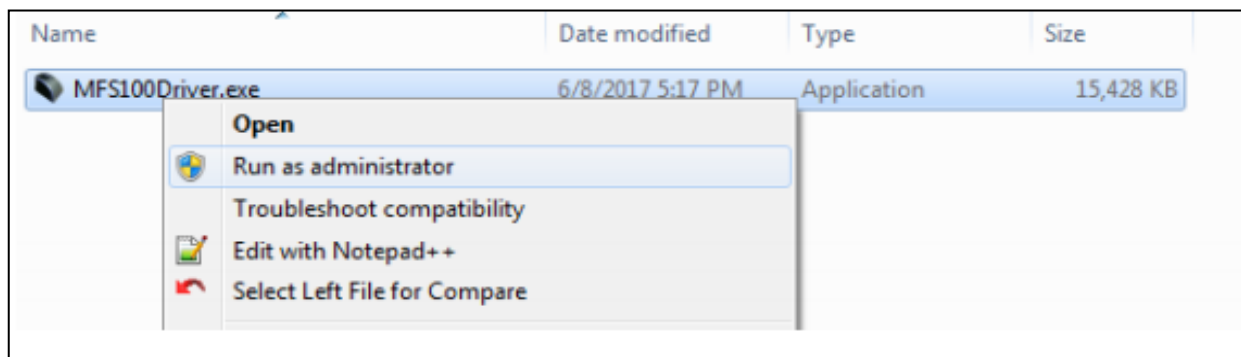
ANDROID Download MANTRA RD Service
[Aadhaar auth API 2.5 and E-Kyc API 2.5 compliance (also download and install driver setup)]
[Download User Manual](#)
[Download MFS100 RD Service](#)

Install Mantra RD Service & MFS100 Driver Setup

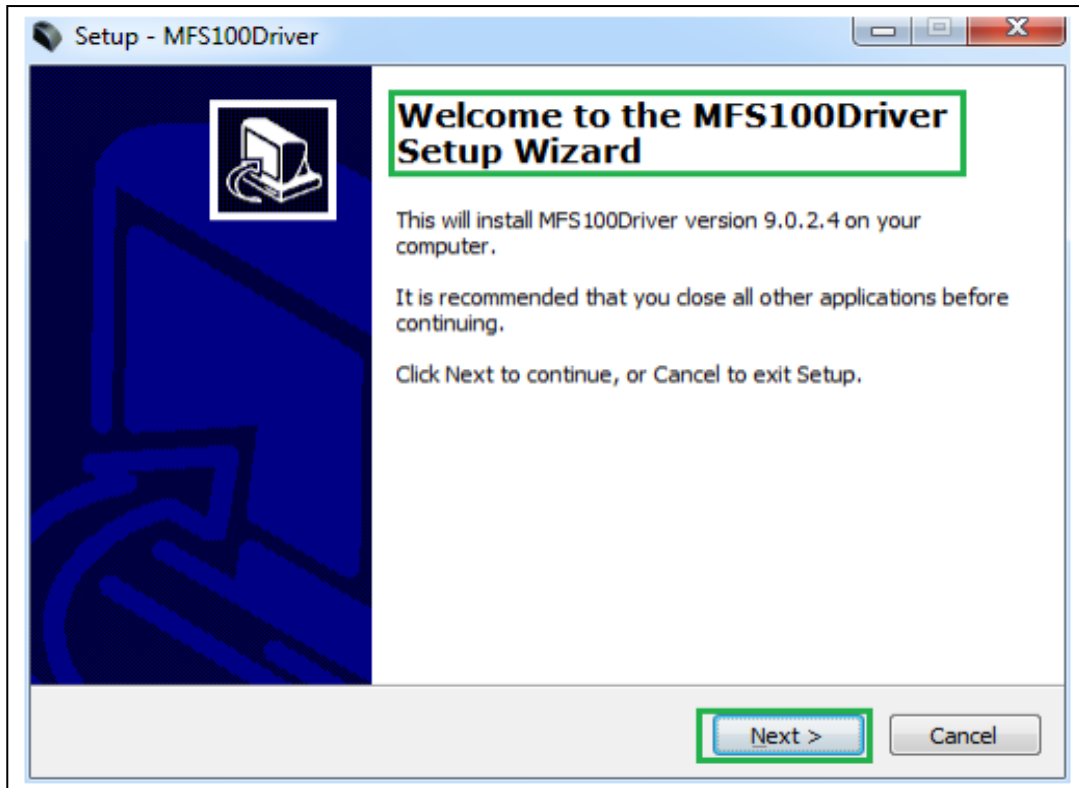
2. Mantra MFS100 Driver Setup Installation.

- Right click on setup file and select **"Run as administrator"**.

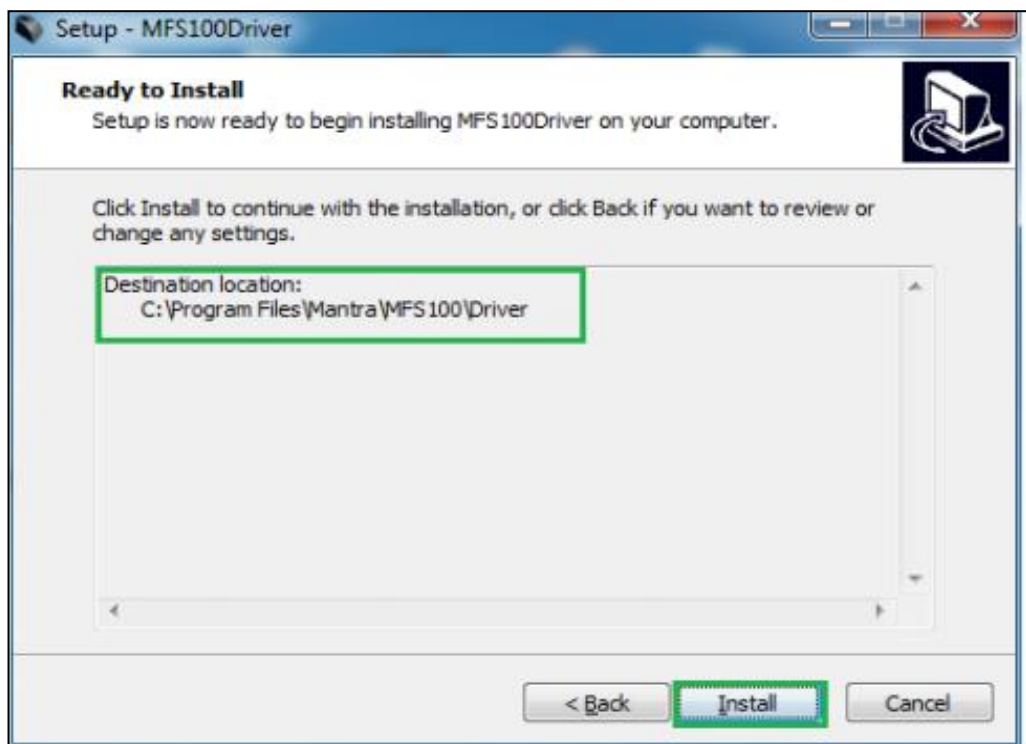
Note: To install MFS100 scanner drivers and necessary service, setup need to access system32 folder. In this case setup need administrator privileges.



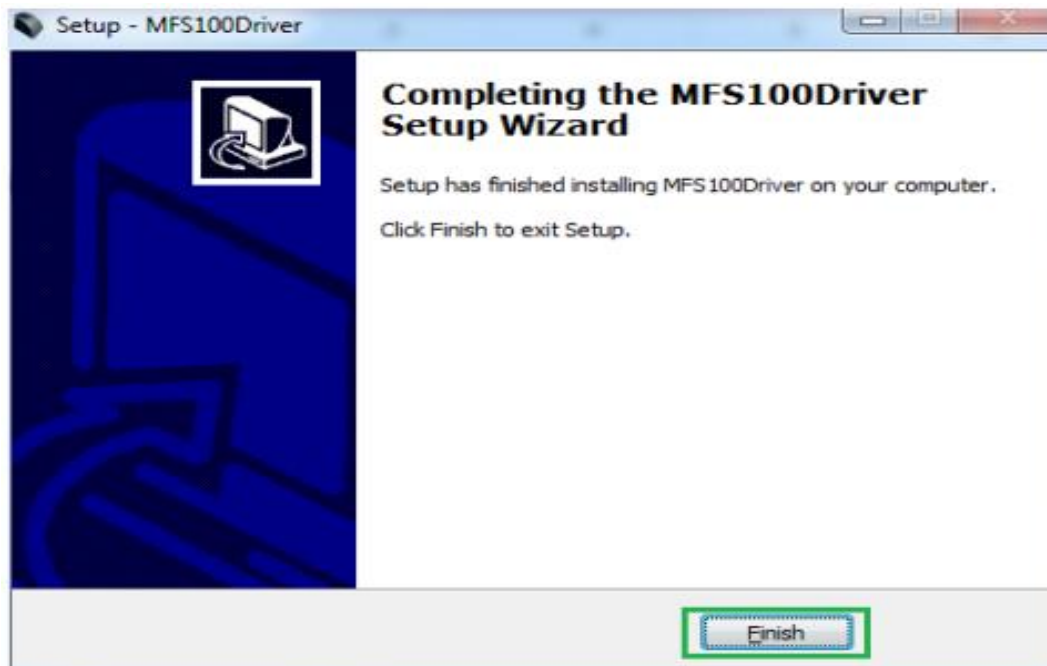
ii. Click on “**Next**” button.



iii. Click on “**Install**” to install the Driver.



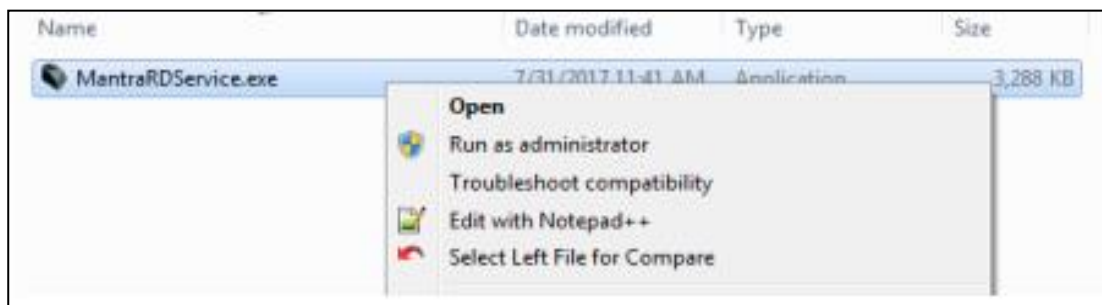
- iv. Click on **“Finish”** to finish the installation process.



3. Mantra RD Service Installation.

- i. Right click on setup file and select **“Run as administrator”**.

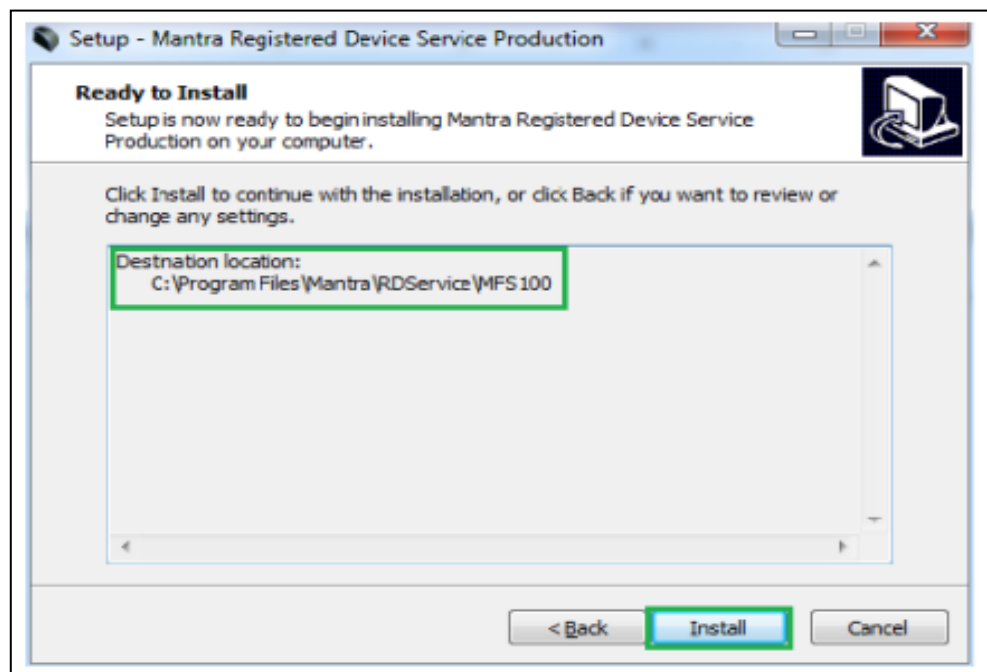
Note: To install Mantra RD Service, setup need administrator privileges.



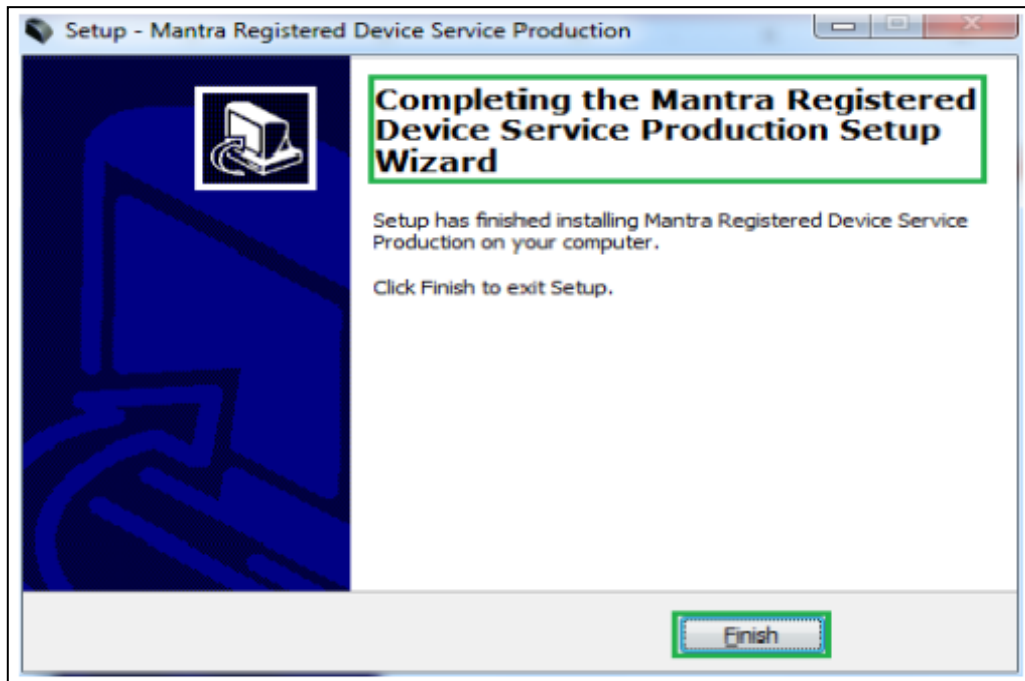
ii. Click on “Next” button.



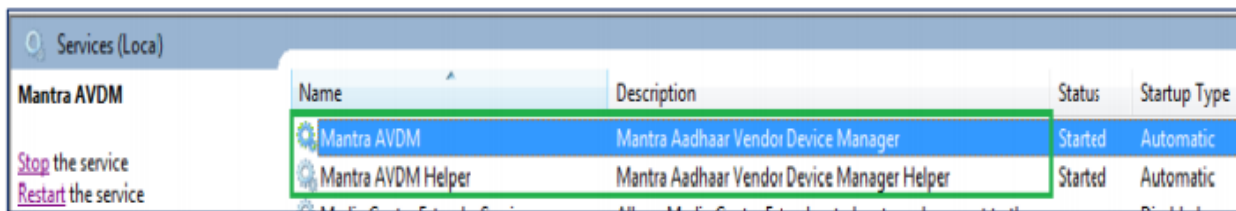
iii. Click on “Install” to install the Driver.



iv. Click on **“Finish”** to finish the installation process.



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



4. MFS100 Registered Device detect.

- i. When RD Service will detect public device, it will convert it into registered device and user will be notified again with success response by RD Service.
- ii. After that user need to unplug and plug his/her device.

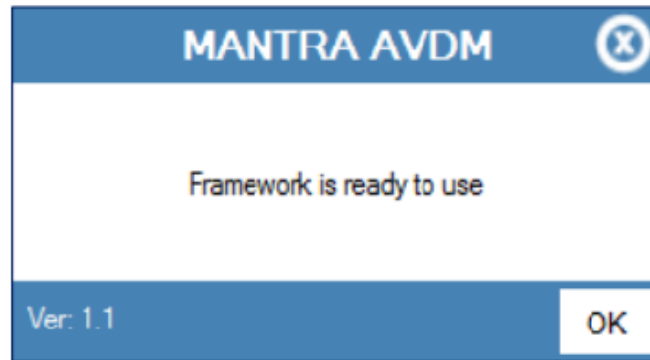


- iii. If the device is not listed at Mantra Management Server than user will be notified with below message. In such cases user needs to contact with our Service Team at <http://servico.mantratecapp.com>.



- iv. Once registered MFS100 device will be plugged to the system, RD service will detect it automatically and validate it on Mantra's Management Server.

v. Once validation completed then it will generate below popup for user information.



5. RD Service Test Application

a) HTTP : <https://rdtest.aadhaardevice.com/>

b) HTTPS : <https://rdtest.aadhaardevice.com/> (Test https URL if your website is in https).

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

Initialized Framework Discover AVDM Device Info	Select Option to Capture			
	AVDM	(NOTREADY)Secure Mantra Authentication Vendor Device Man		
	Timeout	10000	PidVer	2.0
	Wadh			
	DataType	X		
		Env	PP	
				Finger Count 1 Finger Type FMR
				Iris Count 0 Iris Type SELECT
				Face Count 0 Face Type SELECT

ii. User can get Device Information which is connected to its system.

Initialized Framework

Discover AVDM

Device Info

Select Option to Capture
AVDM
Timeout
Wadh
Data Type

(NOTREADY)Secure Mantra Authentication Vendor Device Man
10000
PidVer
2.0
Env
PP
Finger Count
1
Finger Type
FMR
Iris Count
0
Iris Type
SELECT
Face Count
0
Face Type
SELECT

PERSONAL IDENTITY(PI)

Name	Match Value	Select
Match Strategy	* Exact Partial	
Local Name	Local Match Value	Select
DOB	Gender	Select
Phone	Email	
DOB Type		

PERSONAL ADDRESS(PA)

Care Of	Building
Landmark	Street
Locality	PO Name
City	Sub Dist
District	State
Pin Code	Match Strategy
	* Exact

PERSONAL FULL ADDRESS(PFA)

Match Strategy	* Exact Partial Fuzzy	Match Value	Select	Local Match Value	Select
Address Value				Local Address	

Capture

Reset

avdm/device info

<?xml version="1.0"?>
<DeviceInfo>
 <additional_info>
 <Param name="srno" value="" />
 <Param name="sysid" value="" />
 <Param name="ts" value="2020-03-17T17:50:07+05:30" />
 </additional_info>
</DeviceInfo>

iii. By calling capture function of RD service, user can capture biometric data.

Capture

Reset

avdm/device info

<?xml version="1.0"?>
<DeviceInfo>
 <additional_info>
 <Param name="srno" value="" />
 <Param name="sysid" value="" />
 <Param name="ts" value="2020-03-17T17:50:07+05:30" />
 </additional_info>
</DeviceInfo>

pid options

<?xml version="1.0"?> <PidOptions ver="1.0"> <Opts fCount="1" fType="0" iCount="0" pCount="0" format="0" pidVer="2.0" timeout="10000" posh="UNKNOW" env="PP" /> </PidOptions>

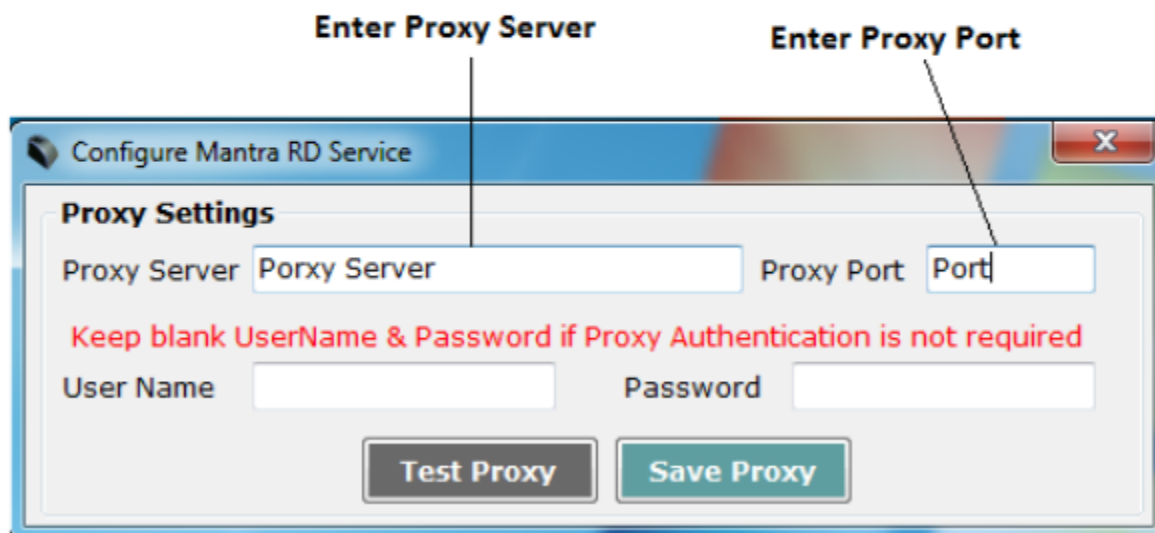
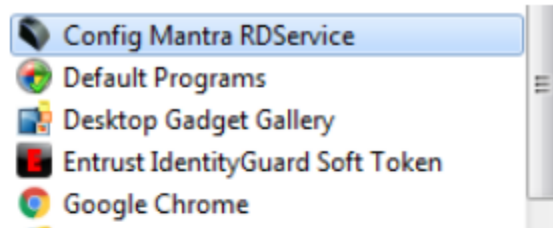
pid data

<?xml version="1.0"?>
<PidData>
 <Resp errCode="0" errInfo="Success" fCount="1" fType="0" nmPoints="37" qScore="66" />
 <DeviceInfo dPid="MANTRA.MSIPL" rdsId="MANTRA.WIN.001" rdsVer="1.0.1" mi="MFS100"
mc="MIIIEFzCCAv+gAwIBAgIEAas/ADANBgkqhkiG9w0BAQsFAADCBTEqMCgGA1UEAxMhRFRMgThFudHJhIFNvZnR1Y2ggSW5kaWwEgUHZ0Ex0ZCA1MU0wSwYDVQQzE0RCIDImMyBTA6FwYXRoIEhlleGg3Bw3NpdGUgR3VqYXJhdCBIaWdoIEhndXJ0IFMgRyBI
alldod2F5IEFobWVjYjZDESMBAGA1UECRJQWntZWRhYmFkMRAwDgYDVQQLEwdHdmlphcmF0MRlWcAYDVQQLEW1uZmNoYm1jYmVxJTAgbG9uB0THE1hbnRyYSB0b2Z0ZWNoIE1uZG1hIFB2dCBMdGQxHjAcBgNVBAsTFUJpb211dHJpYyBNYV51ZmFjdHMyZTE0MAwGA1UECHMFTVNjUEwxZjAqBgNVBACTFUJITVEUeUJBRDEQAA4A1UECBMHR1VVKQV3B0VDELMAkGA1UE
MDMyOTASMHYwOFowgBAXjTAjBgNVBAMTHE1hbnRyYSB0b2Z0ZWNoIE1uZG1hIFB2dCBMdGQxHjAcBgNVBAsTFUJpb211dHJpYyBNYV51ZmFjdHMyZTE0MAwGA1UECHMFTVNjUEwxZjAqBgNVBACTFUJITVEUeUJBRDEQAA4A1UECBMHR1VVKQV3B0VDELMAkGA1UE
BnhKCSU4x3DAI8gkqhkiG9w0BQCEwF0M1chBvcnRabWVudHJhdGVjLmVubTCCAS1wDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJTS/gcEZAIE/EPhCq4rVvK7JDL3tFEKgCC4reNhT7gSAM2Jgr6oRgG8y7BqS8C3ctBdFKYD9jrfuakr0159uKIdMPkPaPy
Jhws7Q2pZv+y9yhUk406mtCXC+IhXhVNPMyAwHsw1f80ixweiYr7Tc7QPav1QZ710+KzrmHyDsNhxkHx86IXhvoro+hwUNLdC7MkMf+upDpuTz6NTf0EY77uq7Laq7c03HMFKEw4RYNzu0MxcqpF0z8d7vJpTzCaCIpQ23diAxg/p9T7Kdon61Qw5LEvOCF
XFgzSp5PzUseV14T001RtEn80IQx+a1SICYZr+EpFjUwk101cAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAcQHS29vMt8zzv1x8+fJTZTXvYU0bywOkdeYzi0WTc18dbb4ASzn14wzHtoPGFDzQISs56UR1Z2ku0VHvubnrFQI7Xglz21ZEthFDQ1XRSIh0n6

6. Proxy Setting

Proxy in Network (if proxy is required to connect internet)

- i. After installation of RD Service (updated on 04-Dec-2017) below Application – Config Mantra RD Service shortcut will be available on 'desktop' as well as in 'All Programs'.



- ii. Enter Username and Password if Proxy Authentication is required otherwise keep as Blank.



- iii. On "OK" Message of Test Proxy, click on **Save Proxy**.
- iv. You need to "**Unplug and Plug**" device so RD Service will take that proxy setting to communicate "Mantra Management Server".

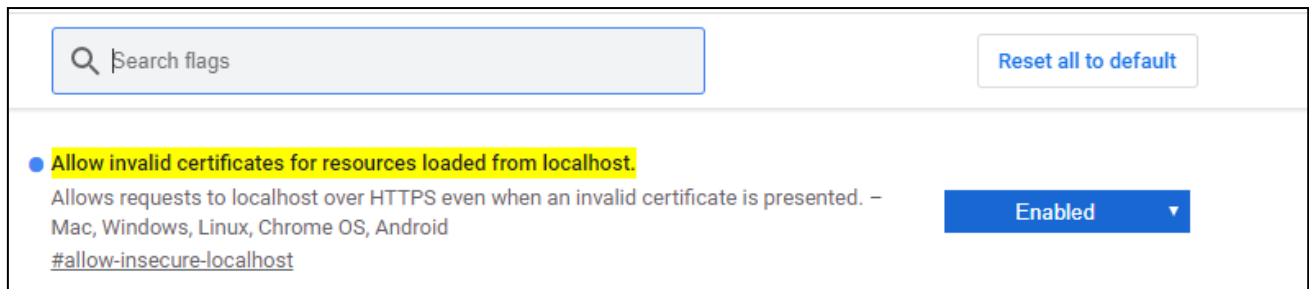


7. Browser Configuration for Web RD Test

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”

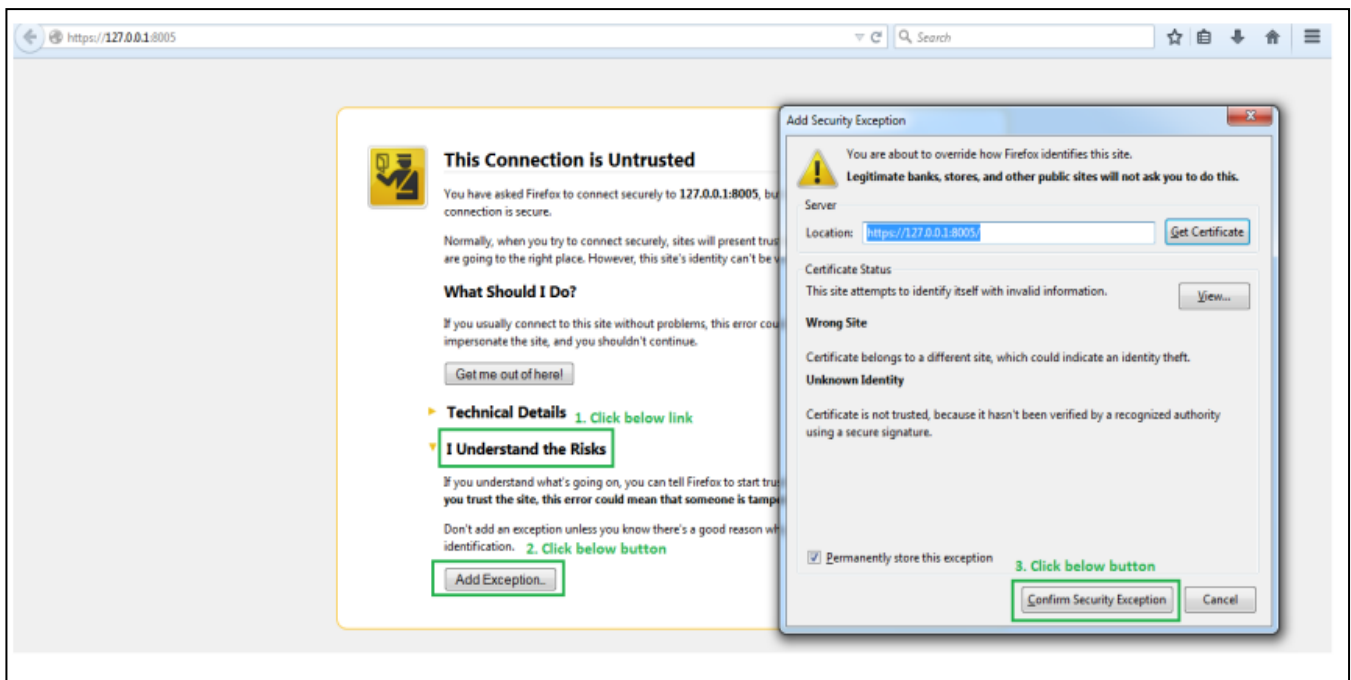
chrome://flags/#allow-insecure-localhost



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



8. Device Registration on Management Server

To list device pre-production or production, send serial number of device to servico@mantratec.com

9. Technical Support

Mantra Support Team:

support@mantratec.com & servico@mantratec.com

This information can be shared with your clients or end user for any kind of technical support.

10. Digital Life certificate (DLC). using Capture Biometric.

- i. After Pensioner logs into the Portal, he/she needs to click on to the “**Identification**” link available in the left menu bar.
- ii. There is an option available as “**Aadhaar**”. Pensioner needs to select that option for performing Identification using Aadhar Biometric. For Digital Life Certificate (DLC) pensioner Aadhar number and area Pin Code should be in system. If these details are not available in SPARSH for the pensioner, he/she cannot perform Digital Life certificate (DLC).
 - a) Identification->Perform Identification-> Aadhar mode -> Select from available services → Capture Biometric.
 - b) You can choose from multiple devices listed under “Select from Available Services” by clicking on drop down button.

The screenshot displays the 'Principal Controller of Defence Accounts (Pension)' portal. The header includes the organization's name in Hindi and English, along with government and ministry logos. The user 'SANJIVE SINGH' is logged in, with a last login time of 12-Jan-2022 11:44:40. The main section is titled 'Resurfacing Identification' and offers two options: 'Manual Life Certificate' and 'Aadhar' (selected). Below this, there is a dropdown menu for 'Select from available services *' showing '(READY)Secure Mantra Authentication Vendor Device Manag'. The 'Aadhar No *' field contains 'XXXX XXXX 9058' and the 'Pin Code(As per Aadhar Address) *' field contains '380006'. A declaration checkbox is present, stating the user's consent to the biometric authentication process. At the bottom, there is a 'Capture Biometric' button.

- c) Pensioner needs to click on the check box available above “**Capture Biometric**” button, if he agrees with the declaration/acknowledgment provided.

- d) After clicking on “**Capture Biometric**” button to capture the thumb impressions. Once captured successfully, Pensioner will see a message on the screen as “**Aadhar Biometric validated successfully**”.

11. Identification from Service Center using Aadhar Biometric:

- From left menu select Service request and Grievance → Select Pensioner Detail for authentication.
- In “**Authentication Type**”, select “Aadhaar Biometric” option.
- Click on “**Proceed**”.



रक्षा लेखा प्रधान नियंत्रक (पेंशन)
Principal Controller of Defence Accounts (Pension)



GOVERNMENT OF INDIA | MINISTRY OF DEFENCE | A A A*

[Home](#) [About SPARSH](#) [Pension Orders & Information](#) [Contact & Support](#) [Service Center Locator](#) [FAQs](#)

 **Service Center**
Last Login : 07-Jan-2022 15:01:41





**Service Request And Grievance**



Channel Type

Pensioner Details

Select	Sr. No.	Pensioner Name	Account Status
☒	1	SAROJ SINGH	Active
☐	2	SANJIVE SINGH	Inactive

Authentication Type *

☐ Send OTP ☒ Aadhar Biometric

Proceed

- iv. Now proceed to Aadhaar Biometric Authentication Screen → Select From Available services → Click on the checkbox, displaying the self-declaration → Click on Capture Biometric.

The screenshot shows the 'Aadhaar Biometric Authentication' page. At the top, there is a header with the Government of India logo, the text 'रक्षा लेखा प्रधान नियंत्रक (पेंशन)' and 'Principal Controller of Defence Accounts (Pension)', and navigation links like 'Home', 'About SPARSH', 'Pension Orders & Information', 'Contact & Support', 'Service Center Locator', and 'FAQs'. A 'Service Center' section shows the last login as '07-Jan-2022 15:01:41'. The main content area is titled 'Aadhaar Biometric Authentication' and includes a radio button for 'Aadhar No', a dropdown for 'Select from available services *' (currently showing '(READY)Secure Mantra Authentication Vendor Device Mana'), and input fields for 'Aadhar No *' (masked as 'XXXX XXXX 4683') and 'Pin Code(As per Aadhar Address) *' (masked as '382421'). Below these fields is a checkbox for a self-declaration statement. At the bottom, there is a 'Capture Biometric' button.

रक्षा लेखा प्रधान नियंत्रक (पेंशन)
Principal Controller of Defence Accounts (Pension)

Home About SPARSH Pension Orders & Information Contact & Support Service Center Locator FAQs

Service Center
Last Login : 07-Jan-2022 15:01:41

Aadhaar Biometric Authentication

☒ Aadhar No

Select from available services *

(READY)Secure Mantra Authentication Vendor Device Mana

Aadhar No *

XXXX XXXX 4683

Pin Code(As per Aadhar Address) *

382421

☐ I hereby state that I have no objection in authenticating myself with Aadhaar based authentication system and consent to providing my Aadhaar number, Biometric data for Aadhaar based authentication for Authenticating my identity from APOnline Limited.I understand that the Biometrics I provide for authentication shall be used only for authenticating my identity through the Aadhaar Authentication system for that specific transaction and for no other purposes. I understand that APOnline shall ensure security and confidentiality of my personal identity data provided for the purpose of Aadhaar based authentication.

Capture Biometric

- v. After clicking on “**Capture Biometric**”, user will see a message as “**Aadhaar Biometric validated successfully**”.

Note*: Further steps to perform identification via Aadhaar Biometric is same as mentioned in **Process No 10** explaining the steps for identification.

12. Track Status from Service Center using Aadhar Biometric:

Now claimant/pensioner can get authenticated using Aadhaar biometric. Following are the steps mentioned below:

- i. From Menu select Track status → Enter Token no, Personal Number or Mobile Number → Click on Authentication type as **"Aadhar Biometric"** and click on **Proceed**.
- ii. Now proceed to **Aadhar Biometric Authentication** → Select from Available services → Click on check box of self-declaration → Click on **Capture Biometric**.

रक्षा लेखा प्रधान नियंत्रक (पेंशन)
Principal Controller of Defence Accounts (Pension)

Home About SPARSH Pension Orders & Information Contact & Support Service Center Locator FAQs

Service Center
Last Login : 07-Jan-2022 15:01:41

Track Status

Token No	Name	Personal/PRAN/GPF/Cadet/Regimental Number
		88887852P

Mobile Number

Authentication Type *

☐ Send OTP ☒ Aadhar Biometric

Proceed

Aadhar Biometric Authentication

☒ Aadhar No

Select from available services *

रक्षा लेखा प्रधान नियंत्रक (पेंशन)
Principal Controller of Defence Accounts (Pension)

Home About SPARSH Pension Orders & Information Contact & Support Service Center Locator FAQs

Service Center
Last Login : 07-Jan-2022 15:01:41

Aadhar Biometric Authentication

☒ Aadhar No

Select from available services *

(READY)Secure Mantra Authentication Vendor Device Mana

Aadhar No *

XXXX XXXX 4683

Pin Code (As per Aadhar Address) *

382421

☐ I hereby state that I have no objection in authenticating myself with Aadhaar based authentication system and consent to providing my Aadhaar number, Biometric data for Aadhaar based authentication for Authenticating my identity from APOnline Limited. I understand that the Biometrics I provide for authentication shall be used only for authenticating my identity through the Aadhaar Authentication system for that specific transaction and for no other purposes. I understand that APOnline shall ensure security and confidentiality of my personal identity data provided for the purpose of Aadhaar based authentication.

Capture Biometric

iii. After clicking on Capture Biometric, user will see a message as **"Aadhar Biometric validated successfully"**.

iv. The details with respect to Token Number will be displayed post verification/validation.