MANTRA MFS110 REGISTERED DEVICE SERVICE

# WINDOWS

MANTRA SOFTECH INDIA PVT LTD



#### TABLE OF CONTENTS

1. Mantra MFS110 Driver Setup Installation.	3
2. Mantra MFS110 RD Service Installation.	4
5. L1 Registered Device (MFS110 Registered Device)	7
6. RD Service Test Application	8
7. Proxy Setting	10
8. Browser Configuration for Web RD Test	11
9. Device Registration on Management Server	13
10. Technical Support	13
11. Dev Support	13



## 1. Mantra MFS110 Driver Setup Installation.

#### 1. Start installation:

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

Note: To install MFS110 scanner drivers and necessary service, setup need to access system32 folder. In this case setup need administrator privileges.



2. Welcome Wizard and Destination Location:





## 3. Finish Driver Installation





## 2. Mantra MFS110 RD Service Installation.

#### 1. Start installation:

- > Right click on setup file and select "Run as administrator".
- > Note: To install Mantra MFS110 RD Service, setup needs administrator privileges.

MantraMFS110RDServ <sup>®</sup>	Open	754 KB
	Run as administrator	
	Troubleshoot compatibility	
	Pin to Start	

## 2. Welcome Wizard:

elect Start Menu Folder		F
Where should Setup place the program's shortcuts?		(10)
Setup will create the program's shortcuts in the following St	art Menu	folder.
o To continue, dick Next, If you would like to select a different folder.	click Prow	
(Default)	Brow	vse
Don't create a Start Menu folder		

**3.** Destination Location:



ady to Install			)
on your computer.	) Mantra MFS110 Registered	Device Service	6
Click Install to continue with the insta change any settings.	allation, or click Back if you w	ant <mark>to</mark> review or	
Destination location: C:\Program Files\Mantra\RDSer	vice\MFS110		^
Start Menu folder: (Default)			
<i>c</i>			2

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".

Services (Local)					
Mantra MFS110 AVDM	Name	Description	Status	Startup Type	Log On As
CONTRACTOR A	Antra AVDM	Mantra Aad	Running	Automatic	Local Syste
Stop the service	🖏 Mantra MFS110 AVDM	Mantra MFS	Running	Automatic	Local Syste
Mestary the service	Mantra MIS100V2 AVDM	Mantra MIS	Running	Automatic	Local Syste

# 5. L1 Registered Device (MFS110 Registered Device)

- When RD Service will detect device then it will convert it into registered device and user will be notified 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 <u>http://servico.mantratecapp.com</u> Or +91-79-49068000.





- Once registered MFS110 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.

MANTRA MFS110 AVDM	8
Framework is ready to use	

## 6. RD Service Test Application

- 1) HTTP : <u>http://rdtest.aadhaardevice.com/</u>
- 2) HTTPS : <u>https://rdtest.aadhaardevice.com/</u> (Test in https URL if your website is in https)
- By running RD Service Test application, user can detect Mantra RD Services installed in the system.

Initialized Framework	Discover AVDM	Device I	nfo	Capture	Rese	t				
Select Option to Capture										
				Wadb	Finder Cour	nt	Face Cou	nt	Iris Type	_

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



nitialized Frame	ework	Disc	over AVDM	Device Info	Capture	9	Reset						
Select Option to	Capture												
VDM					DataType	Wadh		Finger Count		Face Count		Iris Type	
(READY-11100)Mantra MFS110 Authentication Vendor Device Manager					X 🗸			1	~	0	~	SELECT	•
īmeout		PidVer		Env	Client Key			Iris Count		Finger Type		Face Type	
10000	~	2.0	~	PP 🗸	Enter text			0	~	FMR	~	SELECT	`
Timeout		PGCount			OTP								
20000	~	2	~		Enter text								
AVDM / Devic	e Info							Pid Option	s				
xml version="<br <deviceinfo dplo<br="">mc="MIIDzTCC/ 1TSVBMIEwxIFI</deviceinfo>	1.0"?> J="MANTRA.I ArWgAwIBAgi 3PQzExCzAJI	IISIPL" rdsid="RENE IMjAwMEE4NjAwDC BgNVBAsTAklUMSL	ESAS.MANTRA.0 IYJKoZihvcNAQE JwlwYDVQQKEx	101" rdsVer="1.0.0" mi="MFS110" ELBQAwgZsxHzAdBgkqhkiG9w0BC xNYW50cmEgU29mdGVjaCBJbmRj	QEWEHJkQG1hbnRy bYSBQdnQgTHRkMRI	YXRIYy5jb20xFj IwEAYDVQQHE	AUBgNVBAMTDU wIBaG1IZGFiYWQ						

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

	Discover AVDM	Device Info	Captur	e Reset						
elect Option to Capture										
/DM			DataType	Wadh	Finger Count		Face Count		Iris Type	
(READY-11100)Mantra MFS110 Au	thentication Vendor Device Manag	jer 🗸 🗸	X 🗸		1	~	0	~	SELECT	~
meout I	Pid\/er	Env	Client Key		Iris Count		Finger Type		Face Type	
10000 🗸	2.0 🗸	PP 🗸	Enter text		0	~	FMR	~	SELECT	~
Fimeout I	PGCount		OTP							
20000 🗸	2 🗸		Enter text							
	PI " rdsid="RENESAS MANTRA (	101" rds\/er="1.0.0" mi="MFS110"			fType="0" i	Count="0" )" timeout=	pCount="0" pgCour "10000" pTimeout=	nt="2" form:	at="0"	- 12
<deviceinfo dpid="MANTRA.MSI&lt;br&gt;mc=" miidztccarwgawibagiimj;<br="">1TSVBMIEwxIFBPQzExCzAJBg1 xCzAJBgNVBAgTAkdKMQswCQ</deviceinfo>	AwMEE4NjAwDQYJKoZIhvcNAQ WBAsTAKIUMSUwIwYDVQQKEx YDVQQGEwJJTjAeFw0yMTA0MT	ELBQAwgZsxHzAdBgkqhkiG9w0BC xNYW50cmEgU29mdGVjaCBJbmRj 'UwNDQwMDRaFw0yMTA1MTQxM'	QEWEHJkQG1hbnRy oYSBQdnQgTHRkMR TEyNTBaMIGwMSQw	YY XRIYYSID2UXFJAUBGNYDAMI DU RIWEAYDVQQHEwlBaG1IZGFiYWQ vIgYJKoZIhveNAQkBFhVzdXBwb3J ▼	env="PP" / <td><ul> <li><custop< li=""> <li> </li></custop<></li></ul></td> <td>tions&gt;</td> <td>mantrakey</td> <td>sn="UNKNUUWN" "value=""/&gt;</td> <td>-</td>	<ul> <li><custop< li=""> <li> </li></custop<></li></ul>	tions>	mantrakey	sn="UNKNUUWN" "value=""/>	-

## MANTRA REGISTERED DEVICE SERVICE API 1.09



## Mantra 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 <u>https://aadhaardevice.com</u> and it's all subdomains.

## 7. Proxy Setting

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

After installation of RD Service below Application – Config Mantra MFS110 RDService shortcut will be available on 'desktop' as well as in 'All Programs'.





in the second seco		
oxy Server :	Pro	oxy Port :
eep blank UserName 8	& Password if Proxy Authentic	ation is not required.
er Name	Password	
lest Pro	xy Save Proxy	Reset
lect Certificate Formal	t : Select Certificate Format	~

- Enter Username and Password if Proxy Authentication is required otherwise keep as Blank.
- > On "OK" Message of Test Proxy, click on **Save Proxy**.
- You need to "Unplug and Plug" device so RD Service will take that proxy setting to communicate "Mantra Management Server".

## 8. Browser Configuration for Web RD Test

Note: Only incase you are using the <a href="https://rdtest.aadhaardevice.com/">https://rdtest.aadhaardevice.com/</a> link otherwise skip this step.

1) Chrome

<u>Optional</u>: To request on HTTP  $\rightarrow$  Change flag  $\rightarrow$  '<u>Block insecure private network requests</u>' on web browser from '<u>chrome://flags/#block-insecure-private-network-requests</u>' URL address.  $\rightarrow$  Change flag to <u>DISABLED</u> status.

#### https://127.0.0.1:11100 (Port will be from 11100 to 11120)



Block insecure private network requests.			
Prevents non-secure contexts from making subresource requests to more-private IP	Default	×	
Mac, Windows, Linux, ChromeOS, Android, Fuchsia, Lacros #block-insecure-private-network-requests	Default Enabled Disabled		
Send Private Network Access preflights			
Enables sending Private Network Access preflights ahead of requests to more-private IP addresses. Failed preflights display warnings in DevTools without failing entire request. See also: https://developer.chrome.com/blog/private-network-access-preflight/ – Mac, Windows, Linux, ChromeOS, Android, Fuchsia, Lacros <u>#private-network-access-send-preflights</u>	Default	~	
Respect the result of Private Network Access preflights			
Enables sending Private Network Access preflights ahead of requests to more-private IP			
addresses. These preflight requests must succeed in order for the request to proceed. See	Default	~	

#### 2) Firefox

Optional: To request on HTTP  $\rightarrow$  Change flag - '<u>Block insecure private network requests</u>' on web browser from '<u>about:config</u>'  $\rightarrow$  '<u>network.websocket.allowInsecureFromHTTPS'</u> URL address.  $\rightarrow$  Change flag to <u>TRUE</u> status.

https://127.0.0.1:11100 (Port will be from 11100 to 11120)



$\leftarrow$	С û	Sirefox about:config		170% 🏠	\ ⊕	⊛ <del>0</del>	
٩	network.webs	socket.allowInsecureFromHTTPS	5	Show only modifie	modified prefer		
	network.web allowinsecure	osocket. eFromHTTPS	true		≑	5	

## 9. Device Registration on Management Server

To list device pre-production or production, send serial number of device to <u>servico@mantratec.com</u> 079-49068000(Ex-1)

## **10. Technical Support**

Mantra Support Team 079-49068000(Ex-1) <u>servico@mantratec.com</u> This information can be shared with your clients or end user for any kind of technical support.

## 11. Dev Support

Mantra Support Team <u>devsupport@mantratec.com</u> This information can be shared with your clients or end user for any kind of technical support.