

www.rds.cms.hhs.gov

Select **Manage MFA Settings** in the upper right corner of the page.



2 Validate Information

Verify your RDS account by entering your **registered** account information. Click **Continue**.



Note: If you have not yet registered your account, please **register** before proceeding. Refer to <u>Registration</u>.

Optional: Register a Text-Enabled Device

Select **Continue** to register your mobile or text-enabled number. This is optional.

3

Select **Skip** to proceed to MFA activation without registering a device. Proceed to Step 4.

Add Optional Text-Enabled Device Select the Continue button to begin adding a Text-Enabled device to your account. Select the Skip button to skip this step. Continue

Why should I opt-in to receive SMS/texts from RDS?

- If you cannot log in to the RDS site due to MFA issues, you can request a **1-Time Token** as a single-use alternative to gain temporary access to your RDS account.
- Because the token code expires after 10 minutes of being sent, most users prefer to receive the 1-Time Token as a SMS/text rather than email. Refer to the Backup Option: 1-Time Tokens box below for more information.

If registering a text-enabled device, enter the phone number and click **Send Verification Code**. Enter the code sent to your device into the **Verification Code** field and click **Submit.** The code expires after 10 minutes.

Enter the Text-Enabled I	umber you want to register. CMS' RDS	Center will send an SMS with a six-digit Verifica
* Text-Enabled Device N	imber	
		Send Verification Code
Enter the six-digit Verific	ation Code that we sent you to confirm	n registration.
* Verification Code		Didn't receive a code?

4 Install App & Sync Time

On your mobile device, install and open the Google Authenticator app from the App Store.



Configure automatic time update/sync from within your device settings:

- Select Settings
- Select General
- Select Date & Time
- Toggle on Set Automatically

Ceneral	Date & Time	
24-Hour Tim	e	0
Set Automati	cally	
Time Trees		New York

5 Set Up Secure Key



Use the Google Authenticator app on your device to **scan the QR code** displayed on your desktop (found on the Activate Multi-Factor Settings page).

- Click the Plus icon and select Scan a barcode
 Aim your device's camera at the screen so the
- QR code fits inside the viewfinder
- Google Authenticator will scan it automatically

Trouble scanning? Try manual setup:

- 1. On your desktop, click the **gray box** to reveal your Key
- 2. In Google Authenticator, select Manual Entry
- 3. Enter **RDS_SWS (***your RDS username***)** in the Account field
- 4. Enter your Key into the Key field
- 5. Keep the Time Based toggle on
- 6. Click the Checkmark icon to add

Select th	is box if you	u are having trouble scar	nning the barcode.	•
If you ha manually Secret K	ve a probler y into Googl ey: <mark>52022</mark>	n scanning the barcode w e Authenticator of your ch SOQVLIVMSBD	ith your device, ente osen device.	r this key
		• —		
	<	Manual entry	× .	
	Accou	int		
	RDS_	SWS (JSmith)		
	Кеу			
	5ZOZ	2SOQVLIVMSBD	×	
	Time	based	-	

Use Secure Key

6

On your desktop, **enter the 6-digit code** shown in the Google Authenticator app. The code will change every 30 seconds.

Click **Activate** *before it changes.* If the code changes, simply re-enter the new code and click Activate.



You're all set!

You have successfully set up Multi-Factor Authentication for your RDS account!

Google Authenticator Activation Successful

Your Google Authenticator has been successfully activated.

Select **Continue** to log in.

Use the unique code displayed in Google Authenticator on your device **each time** you log in to the RDS Secure Website.

Continue

Backup Option: 1-Time Tokens

- RDS offers <u>1-Time Tokens</u> as a backup option in case you are unexpectedly having MFA issues and cannot login using your Google Authenticator code
- 1-Time Tokens are NOT intended to replace your personal MFA code

You can receive a 1-Time Token via SMS/text if you have registered a textenabled device with RDS

If your text-enabled device is lost or unavailable, RDS can send a 1-Time Token to your registered RDS email address

- Users cannot login using a 1-Time Token more than 3 consecutive times
- If you're having recurring MFA issues, please contact <u>CMS' RDS Center</u>



Visit RDS Website

On your desktop, go to the Retiree Drug Subsidy public website.

for Android devices

www.rds.cms.hhs.gov

Select Manage MFA Settings in the upper right corner of the page.



2 Validate Information

Verify your RDS account by entering vour registered account information. Click Continue.



Note: If you have not yet registered your account, please **register** before proceeding. Refer to Registration.

3 **Optional: Register a Text-Enabled Device**

Select Continue to register vour mobile or text-enabled number. This is optional.

Select Skip to proceed to MFA activation without registering a device. Proceed to Step 4.

Add Optional Text-Enabled Device Select the Continue button to begin adding a Text-Enabled device to your account. Select the **Skip** button to skip this step. Skip Continue

Why should I opt-in to receive SMS/texts from RDS?

If you cannot log in to the RDS site due to MFA issues, you can request a **1-Time** Token as a single-use alternative to gain temporary access to your RDS account.

Text-Enabled Number

Because the token code expires after 10 minutes of being sent, most users prefer to receive the 1-Time Token as a SMS/text rather than email. Refer to the **Backup** Option: 1-Time Tokens box below for more information.

4 Install App & Sync
On your mobile device,

install and open the **Google Authenticator** app from the Play Store.



Time

Open the app and click on the menu at the upper-right corner.

Google Authenticator	:
 Select Settings Select Time correction for coc Select Sync now 	les
← Time correction for codes	
Sync now About this feature	

Set Up Secure Key



Use the Google Authenticator app on your device to scan the QR code displayed on your desktop (found on the Activate Multi-Factor Settings page).

- Click the Plus icon and select Scan a QR code Aim your device's camera at the screen so the
- QR code fits inside the viewfinder Google Authenticator will scan it automatically

Trouble scanning? Try manual setup:

- 1. On your desktop, click the gray box to reveal your Key
- 2. In Google Authenticator, select Enter a setup key
- 3. Enter RDS_SWS (your RDS username) in the Account field
- 4. Enter your Key into the Key field
- 5. Select **Time Based** from the drop down
- 6. Click Add



Use Secure Key

6

On your desktop, enter the 6-digit code shown in the Google Authenticator app. The code will change every 30 seconds.

Click Activate before it changes. If the code changes, simply re-enter the new code and click Activate.



You're all set!

If registering a text-enabled device, enter the

Code. Enter the code sent to your device into

the Verification Code field and click Submit.

Enter the Text-Enabled Number you want to register. CMS' RDS Center will send an SMS with a six-digit Verification

Send Verification Cod

The code expires after 10 minutes.

phone number and click Send Verification

You have successfully set up Multi-Factor Authentication for vour RDS account!

Google Authenticator Activation Successful ×

Your Google Authenticator has been successfully \checkmark activated

Select **Continue** to log in.

Use the unique code displayed in Google Authenticator on your device each time you log in to the RDS Secure Website.

Backup Option: 1-Time Tokens

- RDS offers 1-Time Tokens as a backup option in case you are unexpectedly having MFA issues and cannot login using your Google Authenticator code
- 1-Time Tokens are NOT intended to replace your personal MFA code

You can receive a 1-Time Token via SMS/text if you have registered a textenabled device with RDS

If your text-enabled device is lost or unavailable, RDS can send a 1-Time Token to your registered RDS email address

- Users cannot login using a 1-Time Token more than 3 consecutive times
- If you're having recurring MFA issues, please contact CMS' RDS Center