RDS MFA Activation

Quick Start Guide

for Apple devices

1 Visit RDS Website

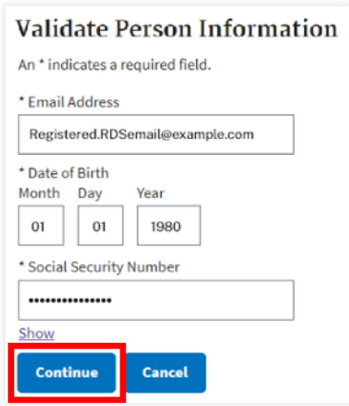
On your desktop, go to the Retiree Drug Subsidy public website.

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**.

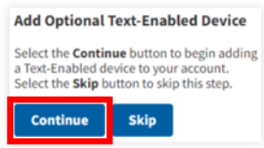


Note: If you have not yet registered your account, please **register** before proceeding. Refer to Registration.

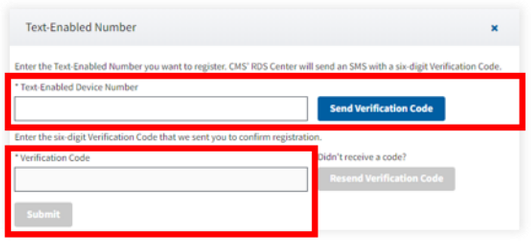
3 Optional: Register a Text-Enabled Device

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

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



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.



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

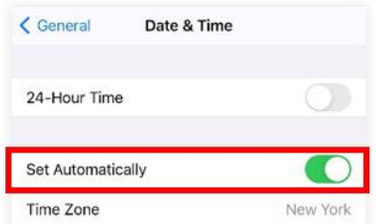
- If you cannot log in to the RDS site due to MFA issues, you can request a **1-Time Token** as a single-use alternative to gain temporary access to your RDS account.
- Because the token code expires after 10 minutes of being sent, most users prefer to receive the 1-Time Token as a SMS/text rather than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

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**



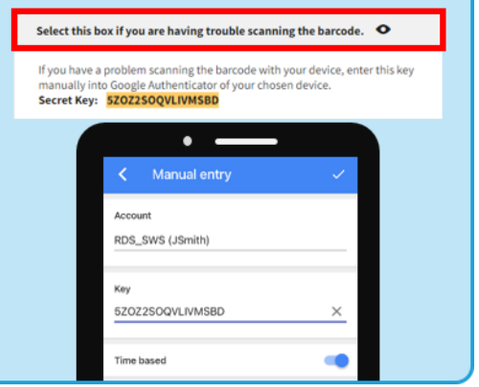
5 Set Up Secure Key

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:

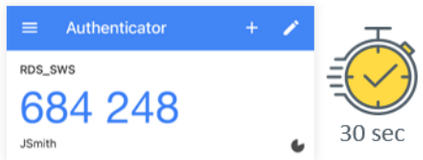
1. On your desktop, click the **gray box** to reveal your Key
2. In Google Authenticator, select **Manual Entry**
3. Enter **RDS_SWS (*your RDS username*)** in the Account field
4. Enter **your Key** into the Key field
5. Keep the **Time Based** toggle on
6. Click the **Checkmark icon** to add

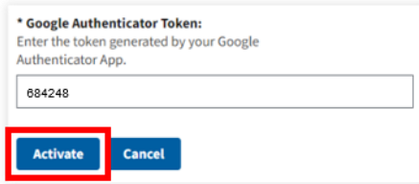


6 Use Secure Key

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

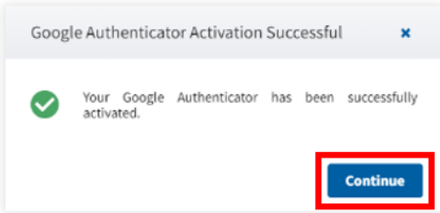
Click **Activate** *before it changes.* If the code changes, simply re-enter the new code and click Activate.





7 You're all set!

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



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 text-enabled 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

RDS MFA Activation

Quick Start Guide

for Android devices

1 Visit RDS Website

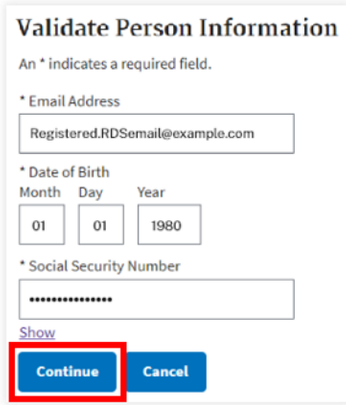
On your desktop, go to the Retiree Drug Subsidy public website.

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**.

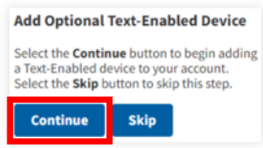


Note: If you have not yet registered your account, please **register** before proceeding. Refer to Registration.

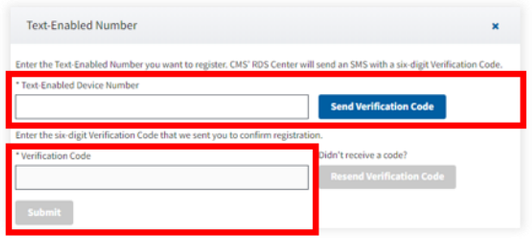
3 Optional: Register a Text-Enabled Device

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

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



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.



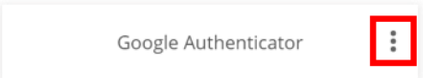
Why should I opt-in to receive SMS/texts from RDS?

- 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.

4 Install App & Sync Time

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

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



- Select **Settings**
- Select **Time correction for codes**
- Select **Sync now**

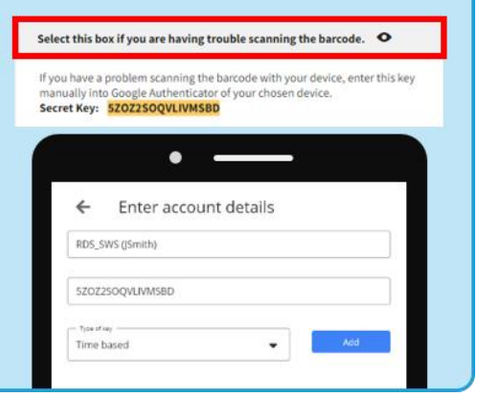
5 Set Up Secure Key

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 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:

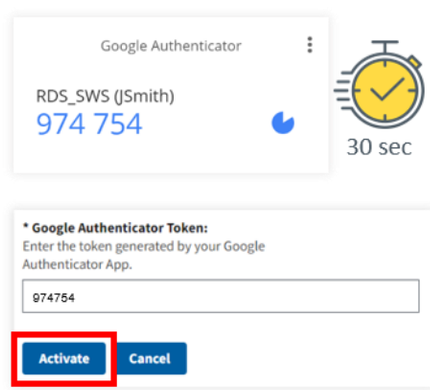
1. On your desktop, click the **gray box** to reveal your Key
2. In Google Authenticator, select **Enter a setup key**
3. Enter **RDS_SWS (*your RDS username*)** in the Account field
4. Enter **your Key** into the Key field
5. Select **Time Based** from the drop down
6. Click **Add**



6 Use Secure Key

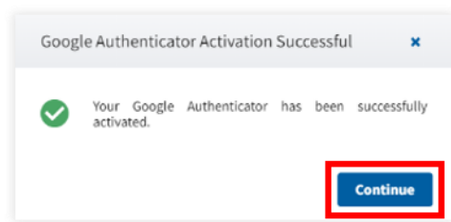
On your desktop, **enter the 6-digit code** shown in the Google Authenticator app. The code will change every 30 seconds.

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



7 You're all set!

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



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 text-enabled 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