NANPA
North American Numbering Plan Administrator

Two-Factor Authentication User Guide

Version: 1.0

Version History

Revision History		
Date	Version	Description
October 28, 2024	1.0	Outlines the steps to download and use Google Authenticator for two-factor authentication in the NANP Administration System.

1   Introduction

1.1   Purpose

The NANP Administration System (NAS) requires two-factor authentication therefore, NAS users will need to set up a secondary authenticator such as Google Authenticator, which is the recommended authenticator. The Google Authenticator application may be downloaded to a computer (PC or MAC) or smartphone. Although not the recommended method, users may add the Google Authenticator extension to a web browser (i.e., FireFox, Chrome).

This document outlines the steps to locate and download the Google Authenticator application onto a computer or smartphone or add the Google Authenticator extension to a web browser (i.e., FireFox, Chrome).

1.2   Content Summary

This document will guide NAS users through the following tasks related to Google Authenticator:
- Section **2 Download Google Authenticator Application** to a computer or smartphone
- Section **3 Add an Extension to Web Browser**
- Section 4 Add NANP Administration System (NAS) to Google Authenticator

NOTE: The user is required to download the application to a computer or smartphone <u>or</u> add the extension to a web browser.
NOTE: For ease of implementation, NANPA recommends adding the application to a computer or smartphone.

1.3   Related Documents

The procedures provided in this document are as of the publication date of the document. Since Google Authenticator is a third-party application and is being downloaded from other third-party services there may be slight differences in the actual process.

1.4   Conventions

This document presents the text that appears on screens (e.g., toolbar items, field labels and button text) as well as internal and external document references. Toolbar items, field names and internal document references are shown in **bold black**, internal document references are hyperlinked, and external document references are *black italicized*.

1.5   Preparations

1.5.1   Company Authorization

Users may need company authorization to download the application on company computers or smartphones. Checking internal procedures and acquiring authorization is the responsibility of the user.

1.5.2   NANP Administration System (NAS) Registration

An approved NAS registration is required to add two-factor authorization for NAS to Google Authenticator. NANPA encourages users to acquire authorization and download the application or add the web browser extension prior to submitting a NAS registration, however, an approved registration and the application or web browser extension is required to add two-factor authentication for NAS and to complete the log in process.

1.6   Troubleshooting

Any questions or issues may be emailed to <u>support@nanpa.com</u> or call 866-623-2282.

2   Download Google Authenticator Application

Users may need company authorization to download the application onto company computers or smartphones. Acquiring authorization is the responsibility of the user.

2.1   Download Application to Computer or Smartphone

Users will go to the application store on their computer or smartphone:

- Google Play for PC and Android devices.
  NOTE: A Gmail account is required.
- App Store for MAC and iPhone.
  NOTE: An Apple ID is required.

Enter "Google Authenticator" into the **Search** box and hit enter.

A list of applications will appear. Select the **Get** button next to **G2FA for Google Authenticator**.

Once the application has downloaded, the user has completed their NAS registration and received their temporary password, proceed to Section **4 Add NANP Administration System (NAS) to Google Authenticator.**

3   Add an Extension to Web Browser

The Google Authenticator application extension may be added to a web browser when a user is unable to add the application to their computer or smartphone.

- For Chrome proceed to Section **3.1 Adding Authenticator to Chrome**.
- For FireFox proceed to Section 3.2 **Adding Authenticator to FireFox**.

3.1   Adding Authenticator to Chrome

Adding a Google Authenticator extension to Google Chrome is an option when the application cannot be downloaded.

Open Google Chrome and select the Extensions icon. From the drop-down menu select Manage Extensions. The Extensions page will open, next select Chrome Web Store from the right-side menu and the Chrome Web Store will open.

Enter "Authenticator" into the **Search** box, then select the **Authenticator** extension. The authenticator description will open, then select **Add to Chrome**.

Once the addition is complete, an information window will appear and the Extension will appear under the Extensions icon.

NOTE: The Authenticator extension will likely show under **Manage Extensions** until opened for the first time.

Once the extension has been added, the user has completed their NAS registration and received their temporary password, proceed to Section **4 Add NANP Administration System (NAS) to Google Authenticator**.

3.2   Adding Authenticator to FireFox

Adding the Authenticator extension to FireFox is an option when the application cannot be downloaded.

Open FireFox and select the Extensions icon. From the drop-down menu select Manage Extensions. The Extensions page will open.

Enter "Authenticator" into the **Search** box, then select the **Authenticator** extension. The authenticator page will open, then select **Add to FireFox**. A pop-up window will appear, select **Add**. Another pop-up will appear, select the checkbox **Allow this extension to run in Private Windows** and the **Okay**.

Once the addition is complete, the Extension will appear under the Extensions icon.

Once the extension has been added, the user has completed their NAS registration and received their temporary password, proceed to Section **4 Add NANP Administration System (NAS) to Google Authenticator**.

4   Add NANP Administration System (NAS) to Google Authenticator

To add two-factor authentication for the NANP Administration System (NAS) the following must be completed:
- the Google Authenticator application has been downloaded or the web browser extension added.
- a NAS user registration has been submitted and approved and the user has their temporary password email.

4.1   Add NAS Two-Factor to Google Authenticator

From the NANPA home page (https://www.nanpa.com), select **LOGIN** located in the upper right corner, then the **Log In to NAS** screen will be displayed (Figure 4-1).

Enter the **Username** created for the NAS account and the temporary **Password** provided in the registration approved email. Select **Login**, NAS will provide the **Multi-Factor Verification Setup** screen (Figure 4-2).

Figure 4-1

Figure 4-2

The user will either open the Google Authenticator application on their computer or smartphone or the web browser Authenticator extension.

Once the application is open, there are two ways to add the NAS two-factor authentication to Google Authenticator.

1. Take a screen shot of the QR code, open Google Authenticator (Figure 4-3) and drag and drop the image of the QR code in Google Authenticator.
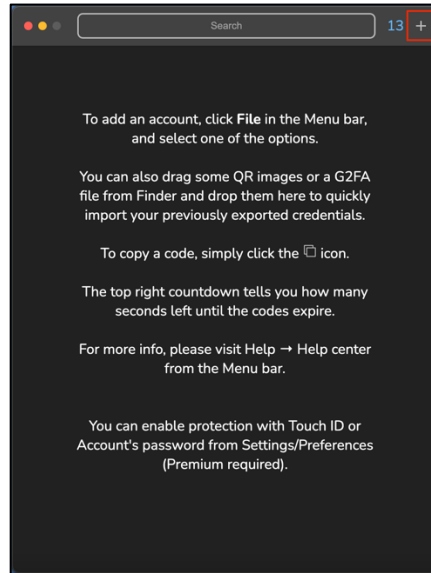
NOTE: This is the easiest option.

Figure 4-3

2. Open Google Authenticator, select the plus symbol (+) or pencil symbol in the upper right corner, then select **From a Setup key** (see red box in Figure 4-4). Authenticator will provide a pop-up, enter the **Name** you want to represent the account (e.g., NAS) and the **Key** provided on the **Multi-Factor Verification Setup** screen.
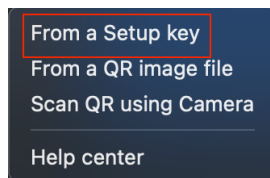

Figure 4-4

When the NAS two-factor has been successfully added, the account and two-factor code will be displayed in Google Authenticator (Figure 4-5).
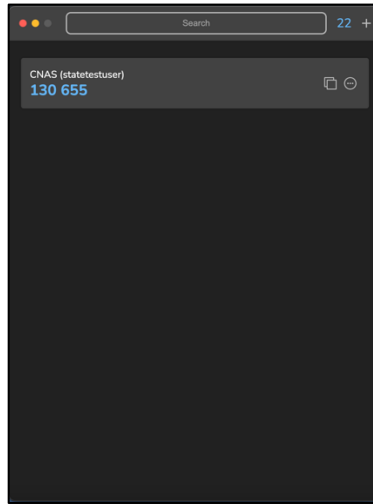
Figure 4-5

Enter the code displayed in Google Authenticator for the NAS account in the **Verification Code** field on the **Multi-Factor Verification Setup** screen to complete the set up (Figure 4-6).

Figure 4-6

Enter the **Username** and the temporary **Password** once more, then **Login** to access the system (Figure 4-7).

Figure 4-7