

How to Setup Up Authentication for your PowerShare Account

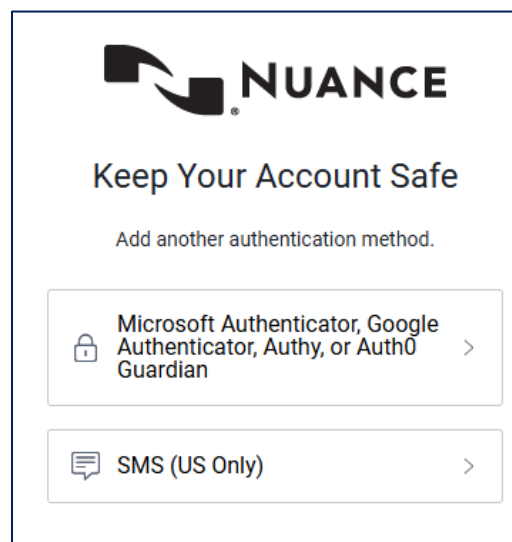
To help protect your PowerShare account, you will be asked to choose a security option when you create a new account. This extra step helps keep your personal information safe.

This guide explains the **two security options** available and how to set them up and manage them in your account.

You can choose one of the following options:

- **Text Message (SMS)** – A verification code is sent to your U.S. mobile phone
- **Authenticator App** – Use a supported smartphone app (Microsoft Authenticator, Google Authenticator, Authy, or Auth0 Guardian) to generate a secure one-time verification code.

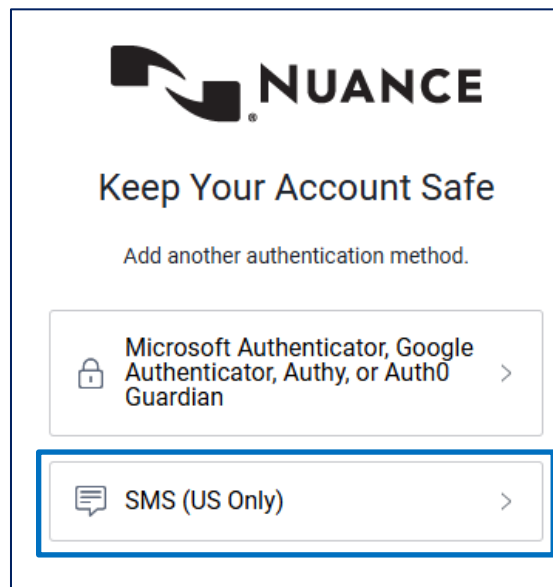
After you create your account and sign in for the first time, a pop-up message will ask you to add a security (authentication) method.



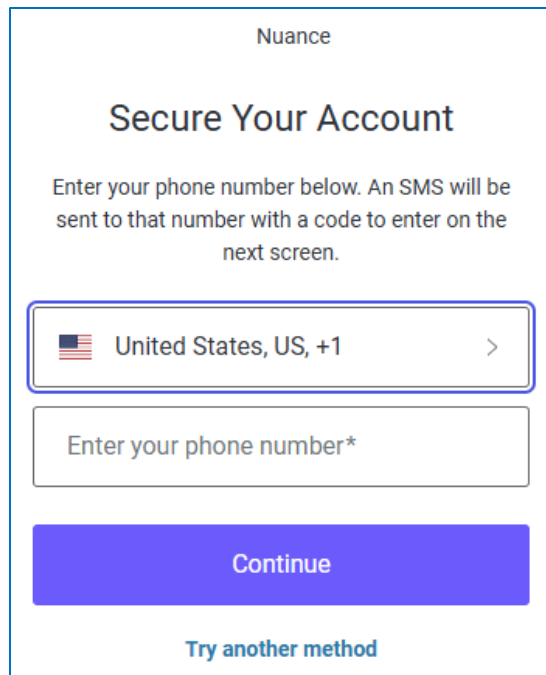
You can change your security method at any time in your patient account settings.

Text Message (SMS)

- This option sends a verification code to your mobile phone.
- To use this option, select **Text Message (U.S. phone number only)**.

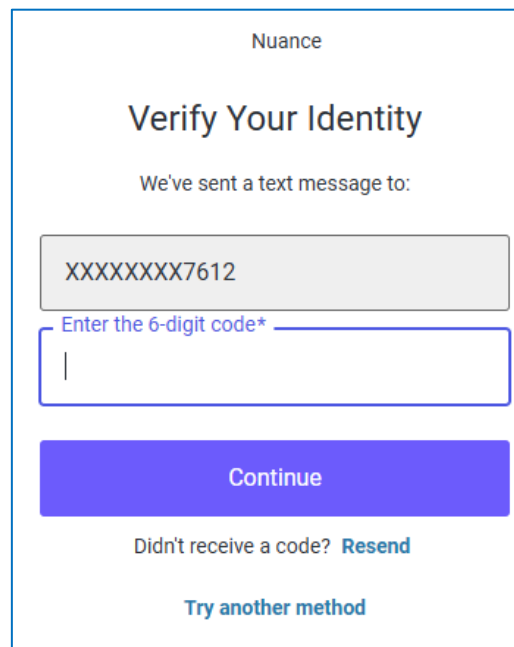


- Enter the mobile phone number you want to use and select **Continue**. This number will be saved and used for future logins.



The image shows a mobile app screen titled "Secure Your Account" by Nuance. It instructs the user to enter their phone number, stating that an SMS with a code will be sent to that number. There is a dropdown menu for the country, currently set to "United States, US, +1". Below this is a text input field labeled "Enter your phone number*". At the bottom, there is a large blue "Continue" button and a link that says "Try another method".

- You will receive a 6-digit code on your mobile phone.
- Enter this code in the **Enter the 6-digit code** field, then select **Continue**.



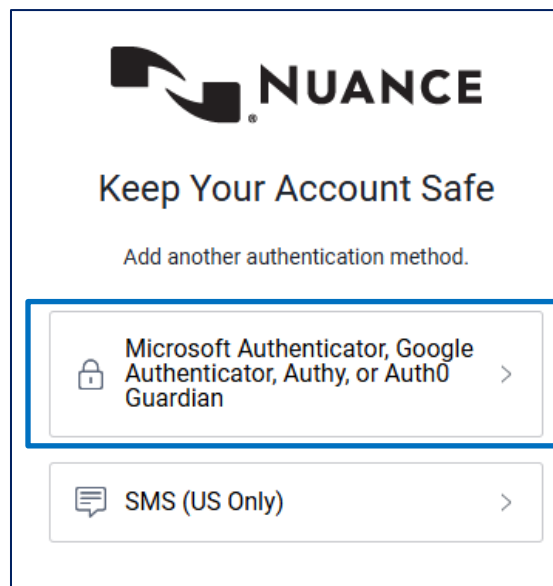
The image shows a mobile app screen titled "Verify Your Identity" by Nuance. It states "We've sent a text message to:" followed by a grey box containing the text "XXXXXXXX7612". Below this is a text input field with the label "Enter the 6-digit code*" and a single vertical line indicating where to enter the code. At the bottom, there is a large blue "Continue" button, a link that says "Didn't receive a code? Resend", and a link that says "Try another method".

- Your account is now set up to receive text message codes.
- **For future sign-ins** (after you enter your password) a 6-digit code will be automatically sent to your phone.
- Enter this code on the **Verify Your Identity** screen to finish signing in.

Authenticator App

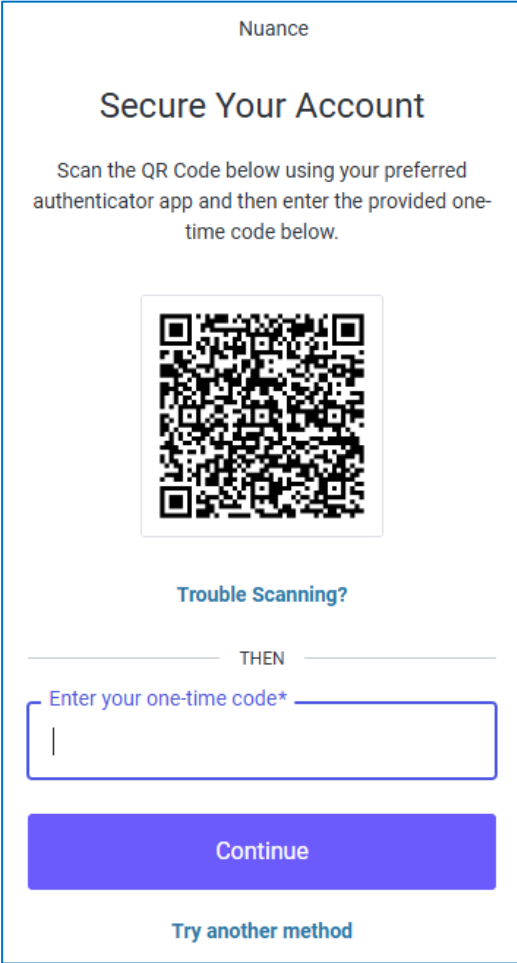
This option requires the downloading of an authenticator app on your smartphone (Microsoft Authenticator, Google Authenticator, Authy, or Auth0 Guardian).

- Please be sure you have downloaded an authenticator app before moving forward with this option.
- This option creates a one-time verification code that appears in your authenticator app.
- To use this option, select **Microsoft Authenticator or similar**.



- On your mobile phone or device, open your authenticator app and scan the QR code shown on the **Secure Your Account** screen.
- **Please do not scan the QR code in this guide - only the QR code from your mobile device will work.**
- Keep the authenticator app open after scanning the QR code.
- A 6-digit code will appear. Enter the code on the next screen and select **Continue**.
- Your account is now set up to receive codes through the authenticator app.

For future sign-ins (after you enter your password) you **do not** need to scan the QR code again. Simply open the authenticator app and enter the 6-digit code shown on the screen.



Nuance

Secure Your Account

Scan the QR Code below using your preferred authenticator app and then enter the provided one-time code below.



[Trouble Scanning?](#)

THEN

Enter your one-time code*

Continue

[Try another method](#)

MEDICAL DEVICE DISCLAIMER. Microsoft products and services (1) are not designed, intended or made available as medical devices, and (2) are not designed or intended to be a substitute for professional medical advice, diagnosis, treatment, or judgment and should not be used to replace or as a substitute for professional medical advice, diagnosis, treatment, or judgment

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

© 2026 Microsoft Corporation. All rights reserved.

Frequently Asked Questions

Q: Are group email distribution lists supported by MFA?

A: No. For security and auditing purposes, each user must have their own individual login and email account.

Q: Will I need to complete Multi-Factor Authentication (MFA) every time I sign in?

A: Yes

Q: Will PowerShare have access to my password?

A: No. Your password is managed by the Identity Provider and is not stored or managed by PowerShare. This separation helps enhance security by keeping authentication and authorization processes independent.

Q: Is there a time limit to reset my password after I begin MFA enrollment?

A: Yes. The password reset link sent by email expires after 3 hours. If the link expires, you can restart the enrollment process to receive a new link.

Q: What happens if I lose the phone I use for Multi-Factor Authentication (MFA)?

A: If you lose access to your phone, select **Try Another Method** during sign-in to receive a one-time verification code by email. Email can be used as a backup verification method but cannot be configured as your default MFA method.

Q: Is there a timeout period for inactivity in PowerShare?

A: Yes. Users will be logged out of PowerShare after 15 minutes of inactivity.

Q: For any questions or issues with MFA, whom should I contact?

A: PowerShare Support: support@nuancepowershare.com