DeliverHealth
S O L U T I O N S

How to Log in Using Multi-Factor Authentication (MFA)

For InCommand and InScribe

Table of Contents

Using Multi-Factor Authentication (MFA)

eScription One applications now support a secondary level of security for logging in, called multifactor authentication. Multifactor authentication is another way to verify a user's identity, adding an extra level of security to the current login process.

To set up multifactor authentication, there will be a one-time procedure that requires you to download an authentication application called Auth0 Guardian onto your phone and create an account. Subsequently, when logging in, you will only need to accept a notification sent to your phone.

This one-time procedure does not need to be repeated for each transcription app. If you have set it up for InCommand, you do not need to set it up again for InScribe.

Enabling Multi-Factor Authentication for Transcriptionists

To enable MFA for transcriptionists, check the **Use Multi-Factor Authentication** check box on the Password and Security Options screen (InCommand> Maintenance> Transcriptionists> Edit 'transcriptionist').

Setting up Multi-Factor Authentication Using Auth0 Guardian

When logging in for the first time after the multi-factor authentication setting has been enabled, you will enter your login credentials as usual. Before the application opens, the 'Secure Your Account' screen appears. Here you begin the one-time multi-factor authentication setup.

Step 1: Download the Auth0 Guardian app

Auth0 Guardian is a free security app for performing multi-factor authentication. With the Guardian app, a notification is sent directly to your cell phone. There are no codes to manually enter; just press 'Allow' to accept the notification.

If you do not have the Auth0 Guardian app already installed on your phone, you must first download it from the Apple store (for iPhone) or Google Play (for Android). Choose the appropriate button to view the location of the app's download site. Search 'Auth0 Guardian' and download it to your phone.

Once you have the authentication app downloaded, open it. In your eScription One app, click **Continue** on the 'Secure Your Account' screen**.**
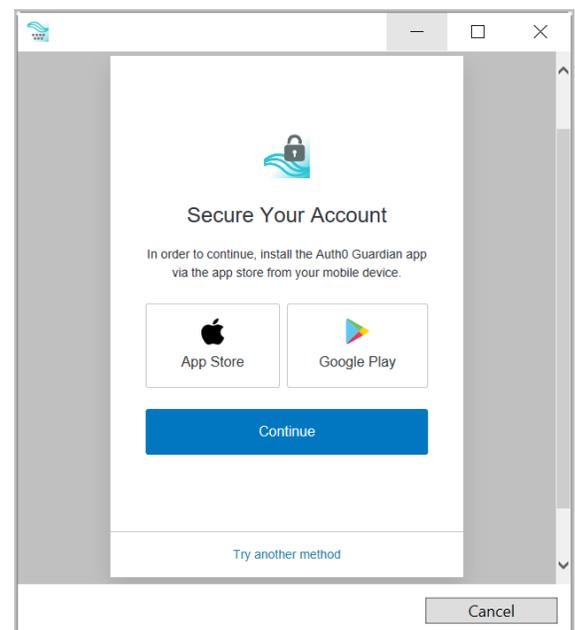
Note: Other authentication apps may work as well but are not officially supported.

Step 2: Scan the Activation (QR) code

Next, use the authentication app to scan the activation code that appears in your eSOne app by holding your phone up to the code. This will link the authentication app to your eScription One application.
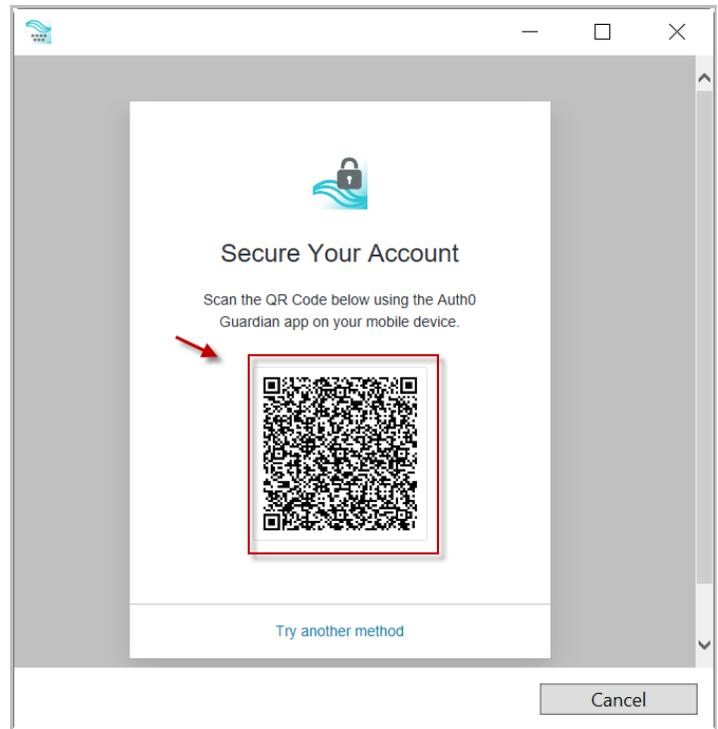
If the scanner does not automatically open, you may need to click the plus button at the top of the Guardian screen to add a new account.
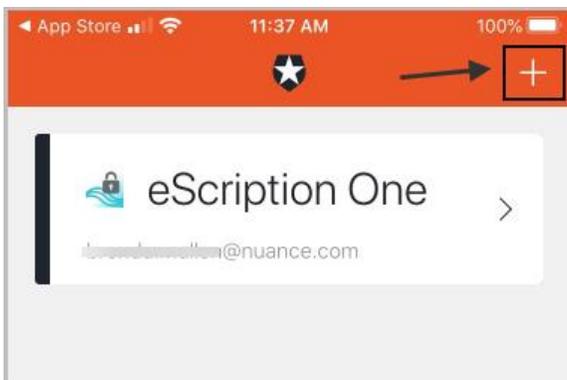
Step 3: Copy the Recovery Code

After scanning the QR code, you will receive a recovery code (on your eScription One app). If you need to log in and do not have your device, you can paste or enter this code to access your eSOne app. Copy the code and keep it somewhere safe.

Click the check box indicating that you have recorded the code, then click **Continue**.
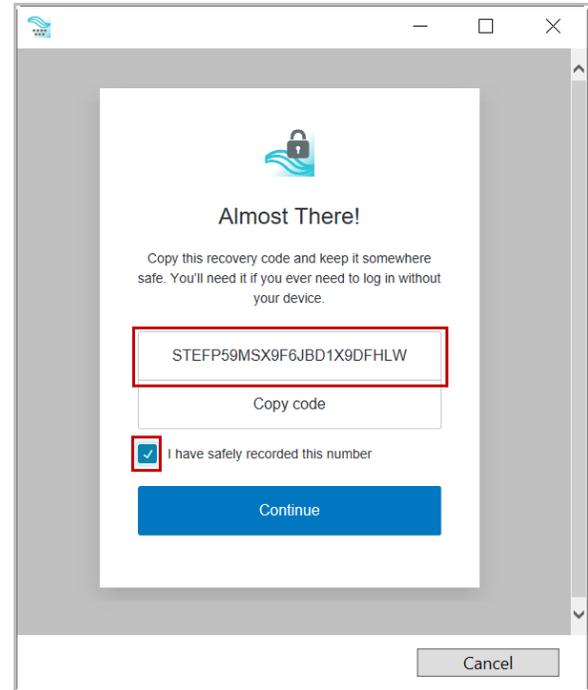
You now have an account to which a notification request will be sent each time you log in. The email on your account will be the email listed for you on the Transcription Information or User Information screen in InCommand.

Your eScription One application will now open.
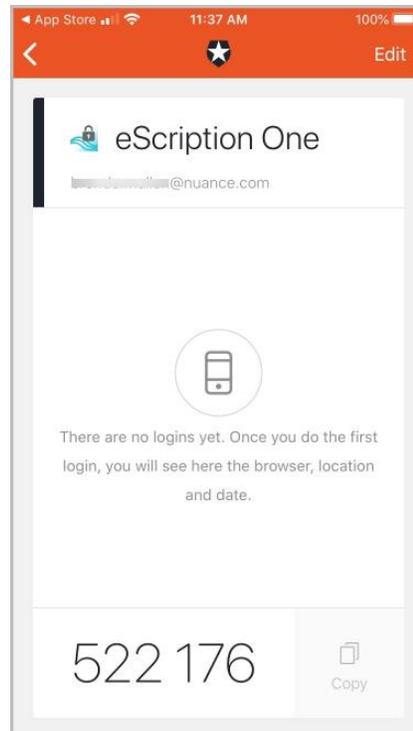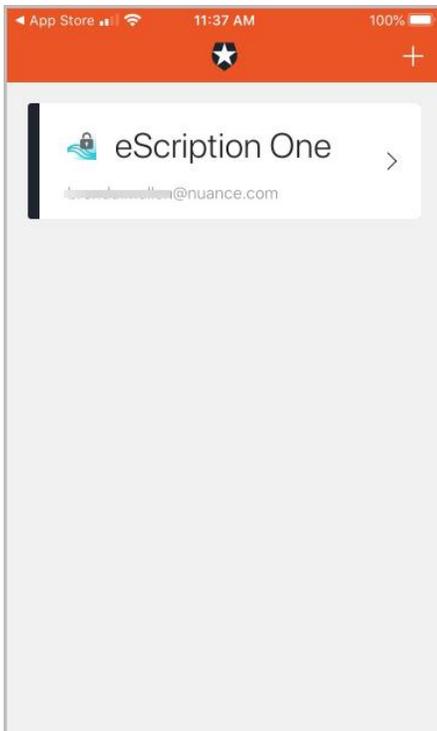
You have successfully set up multifactor authentication. Remember to have your phone nearby when you log in from now on. See the next section for details.

Logging in with Multi-Factor Authentication

Once you have completed the initial MFA setup process above, you will subsequently log in to eScription One apps as shown in the steps below.

1. Open the Guardian app.

2. In your eScription One app, enter your login credentials.

   The Verify Your Identity screen opens, indicating that a notification has been sent to your phone and is awaiting confirmation.

3. In the Guardian app, click **Allow**.
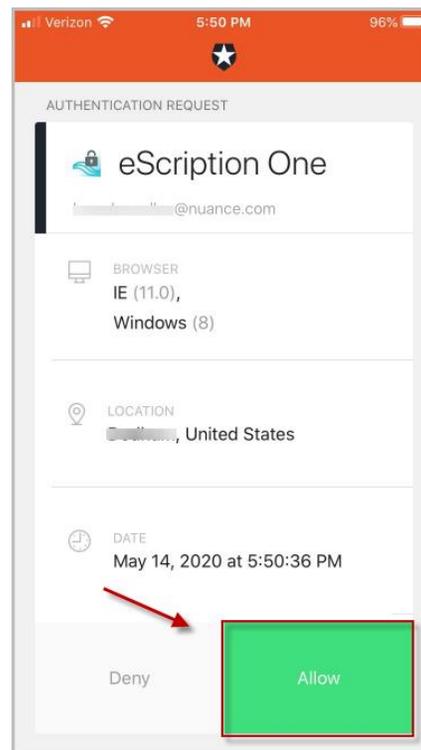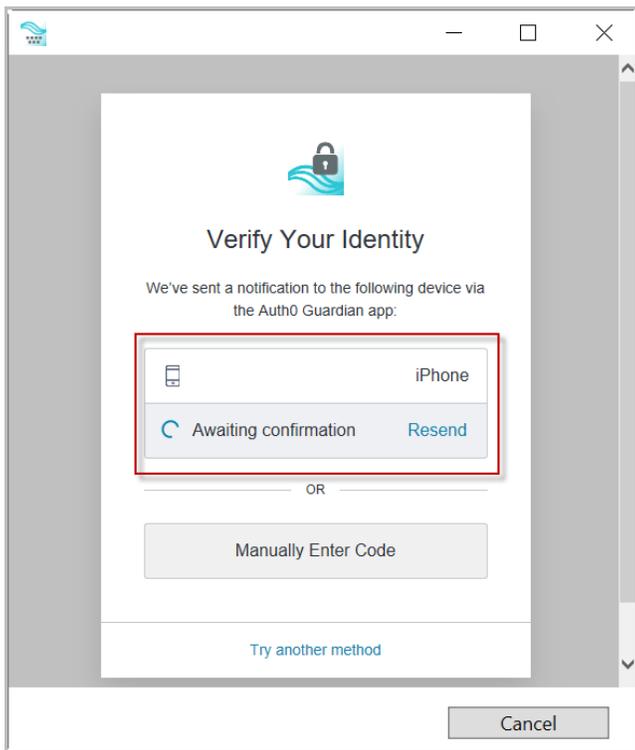
After successful authentication, you will automatically be logged into your eScription One app.

If you do not receive the notification, you can choose to have the notification resent, or you can manually enter the code at the bottom of the Guardian app (see below).

If you do not receive a notification, you can choose **Manually Enter Code**.
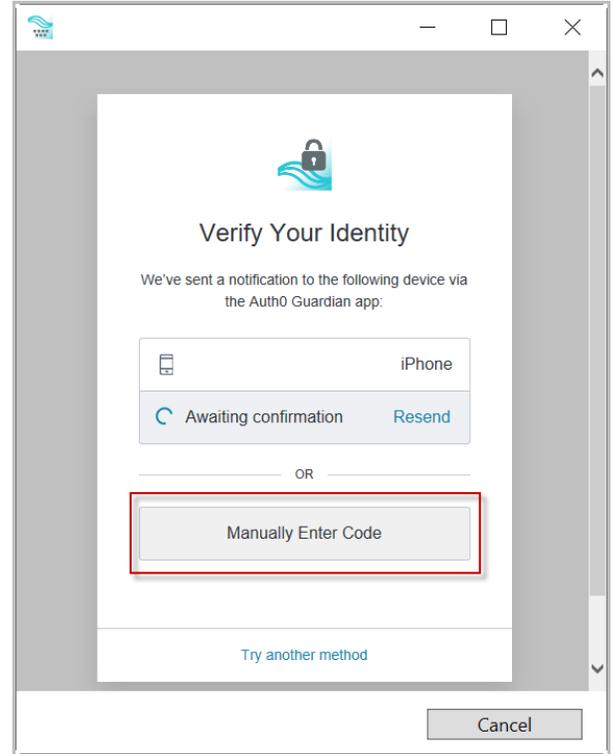
Enter the code appearing at the bottom of the Guardian app.
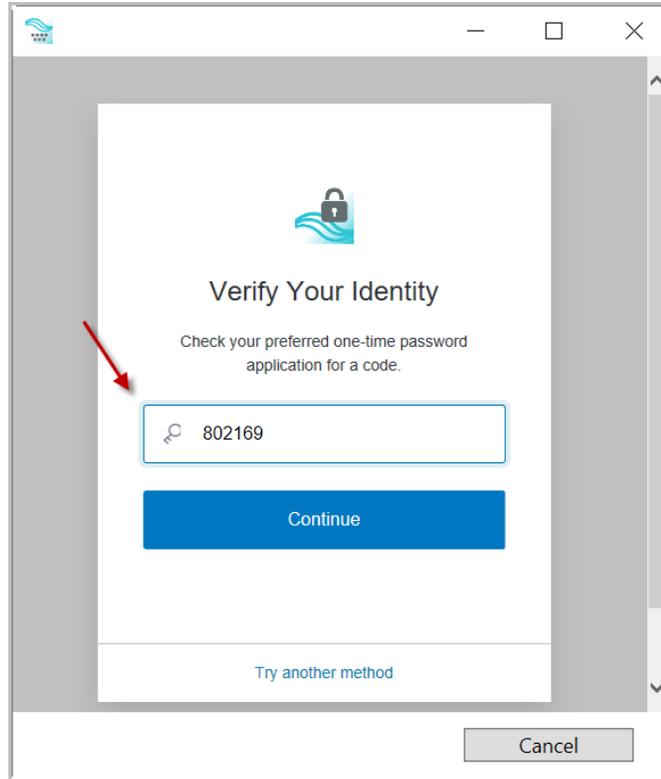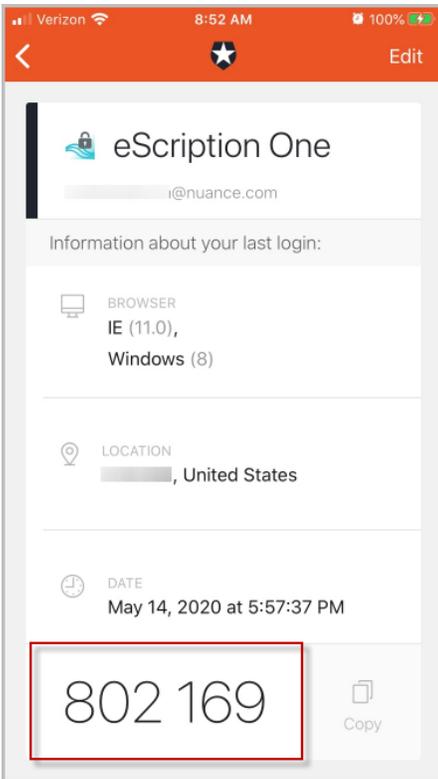
Click **Continue**. After successful authentication, you will automatically be logged into your eScription One app.

Logging into InCommand

When logging in to InCommand for the first time after the multi-factor authentication setting has been enabled, you will see some minor changes. You will be redirected to our new authentication service with a look and feel similar to the old login experience.

Enter your login credentials as usual:
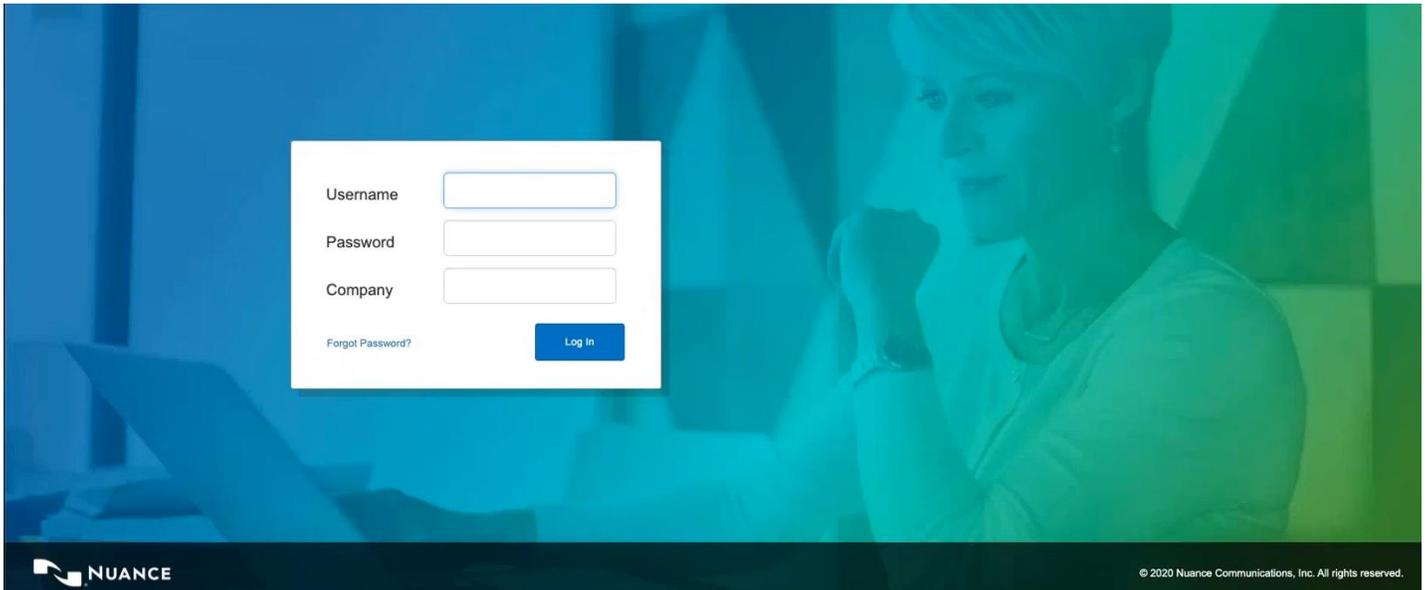
Resetting Multi-Factor Authentication

An option called **reset multi-factor authentication** has been added to the **Password and Security Options** screen (Maintenance> Transcriptionists> Edit 'transcriptionist'). This option allows transcription managers to reset MFA for users who cannot log in with MFA after having done so previously.

For this option to appear for the transcriptionist, the following conditions must be met:

- MFA is turned on for the company.

- MFA is turned on for the transcriptionist.

- The user has logged in at least once with MFA enabled.

    Note: At this time, you must use the "reset multi-factor authentication" button **before** removing the entry from the Guardian app or uninstalling the Guardian app. Otherwise, you will need to contact support for assistance.

To do a reset:

1. Click the **reset multi-factor authentication** button.
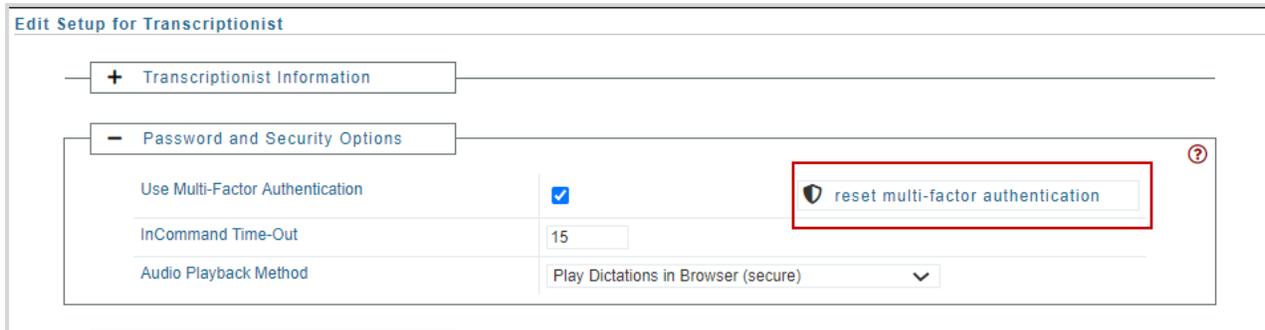
A pop-up confirmation window appears.
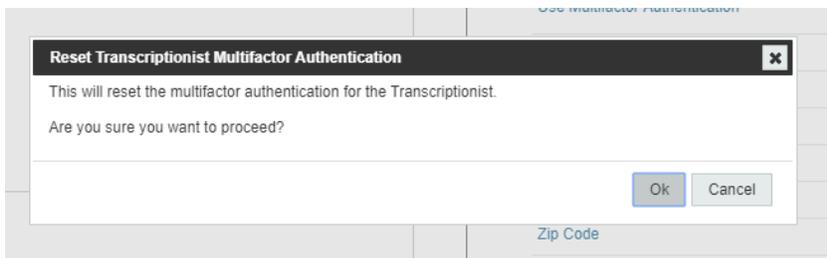
2. Click **Ok**

The reset proceeds and a new pop up appears stating that authentication has been reset.
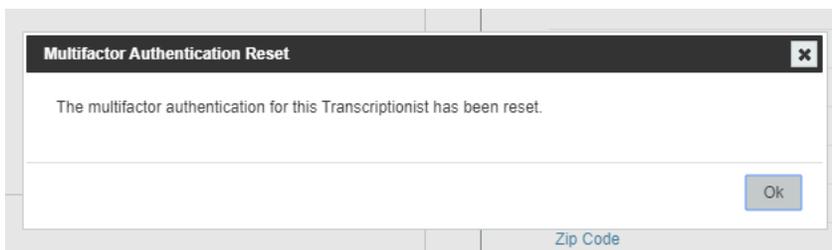
3. Click **Ok**.

The user can now begin MFA registration again.

Note: The 'reset multi-factor authentication' button remains on the Password and Security Options screen after a profile is reset.

Additional Support

Get additional assistance for eScription One applications here:

– **Phone Support**: 1-800-858-0080

– **Support Email**: esone.support@DeliverHealth.com