![Availity logo]

Availity Essentials

Register your provider organization

Table of contents

Register an organization overview

If you are new to Availity and want to register your provider organization, you'll begin by creating your Availity user account. You 'll start by clicking **Register** on the Availity home page to create your user account. Refer to the next page in this guide to get started.

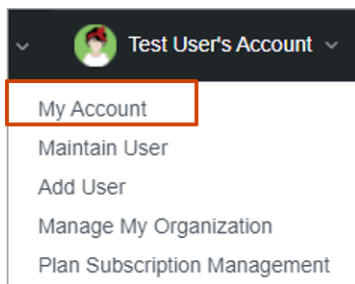We're excited that you're ready to begin the registration process with Availity!

Important: Creating a new user account only applies to users who are brand new to Availity and need to register either their provider or billing services organization.

Note: If you need to register a health plan or vendor organization, learn more on how to register your organization.
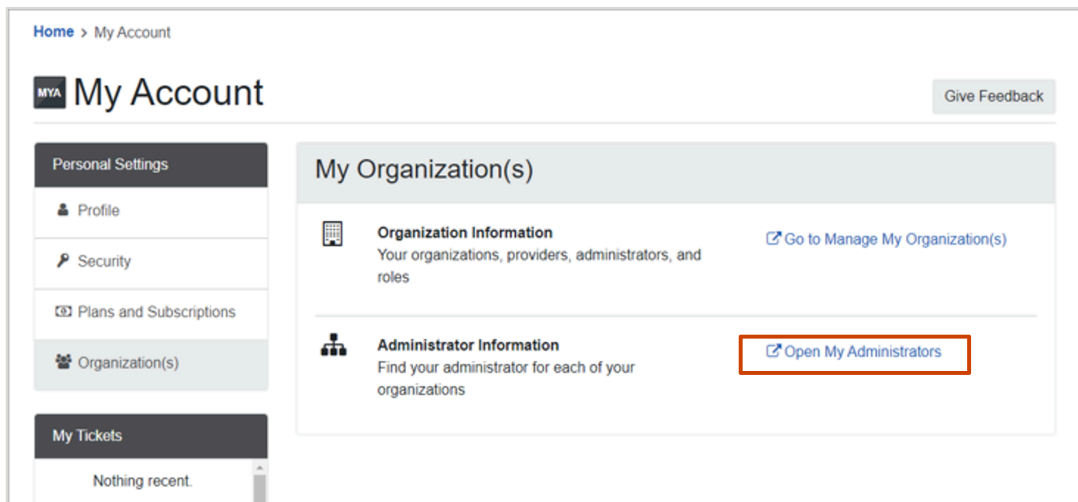
- If you are an existing user, an administrator or non-administrator, you already have an Availity user account and you can log in to Availity Essentials. There is no need to create a new user account.

- If you are an existing user, a non-administrator, and need to get added to another organization, contact your Availity administrator who manages the organization you wish to join. The administrator can add you to an organization by using the add user feature in Availity Essentials. Learn more about this feature later on in this guide.

  If you do not know who your Availity administrator is, you can easily find out. Follow these steps to identify the administrator and administrator delegates for your Availity organization(s):

  1. In the Availity Essentials menu bar, click **[Your Name's] Account** > **My Account**.

  2. On the My Account page, click the **Organization(s)** tab, and then click **Open My Administrators**.

- If you are an existing user and would like to be the administrator of an organization, you can register an organization from the Manage My Organization page in Availity Essentials.

Create a new user account

Important: Creating a new user account only applies to users who are brand new to Availity and need to register their provider organization.

When you set up your new user account, you'll be asked to do the following tasks in the wizard:

- Add information about yourself

- Set up security questions

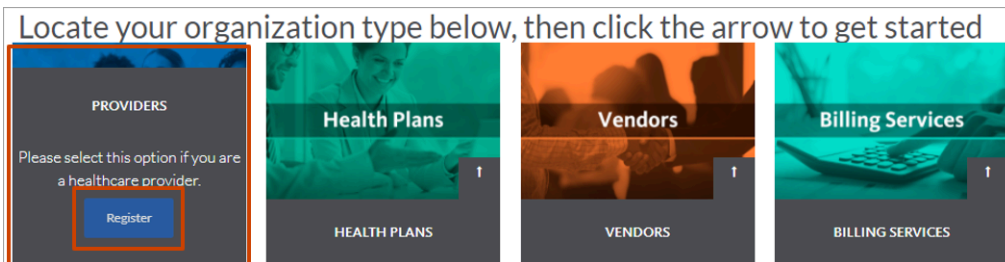- Verify your information

- Confirm your email address

Add information about yourself

To begin creating your user account, follow these steps:

1. Go to availity.com and in the upper-right corner of the page, click **Register**.
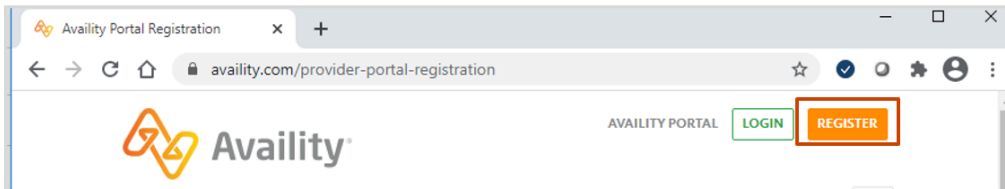
2. Scroll down the page, hover over the **Providers** tile, and then click **Register**.

3. On the Create Account page, enter information in the following fields:

- **First Name**

- **Last Name**

- **Email Address** – Enter a valid email address.

- **User ID** – Enter a valid user ID that contains 6 to 15 letters or numbers.

- **Password** – Enter a valid password. The password cannot contain your user ID or any spaces.

  Tip: Your new password must meet the following criteria:

  - 8 to 15 characters

  - At least one number

  - At least one uppercase letter

  - At least one lowercase letter

  - At least one special character, for example, -, @, #, $, %, *

- **Choose a region where you do business** – You can only select a region within the United States or a United States territory. If you do business in multiple regions, you can select more than one region when you register your organization on the Manage My Organization page after you complete this user registration.

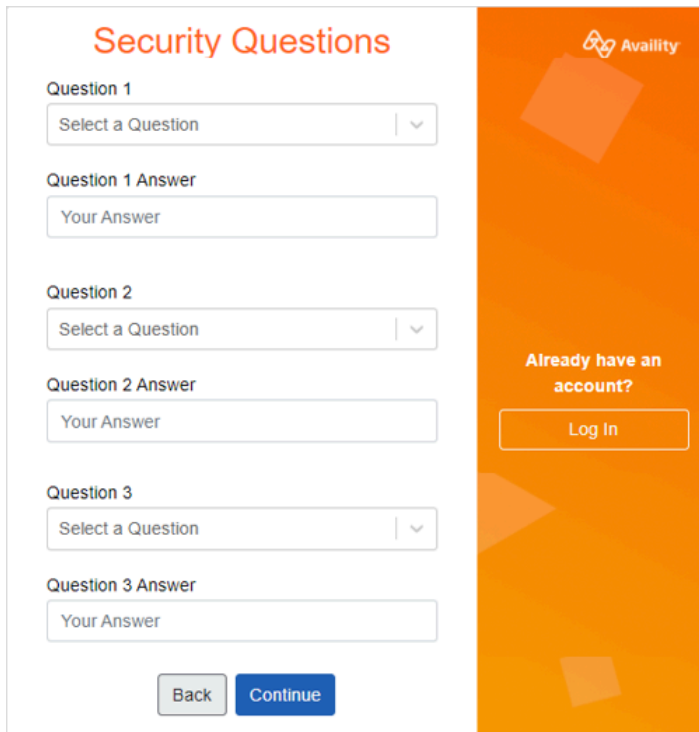 **Note:** You can always add additional regions later when you register your organization.

4. Click **Continue**.

5. Next, in the screen that follows, click the appropriate number of squares to identify the image in question.

Set up your security questions

On the Security Questions page, do the following:

Tip: When setting up your security questions, select questions and answers that will be easy for you to remember. You'll have to remember these security questions when you need to reset your password.
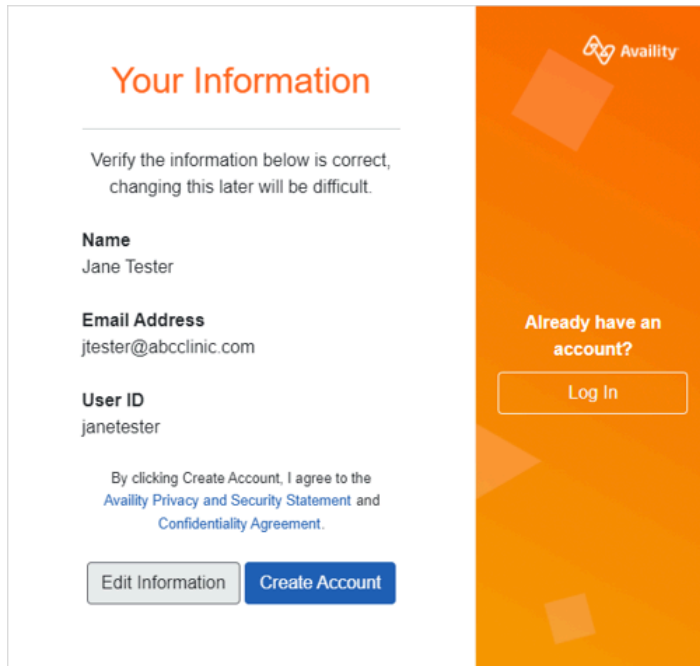
1. In each **Question** field, select a security question.

2. In each **Question Answer** field, enter your answer to the security question.

3. Click **Continue**.

Verify your information

On the Your Information page, do the following:
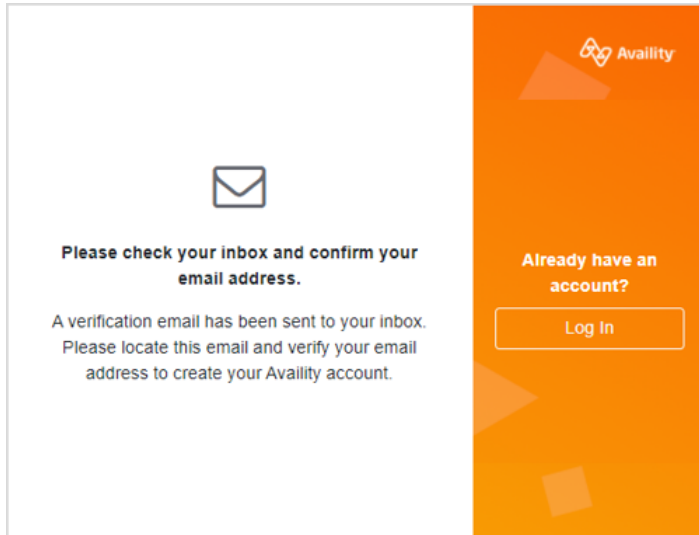

1. Review your information and make sure it is correct.

2. Click **Edit Information** to make any changes.

   Important: Making changes to your information might be difficult later on.
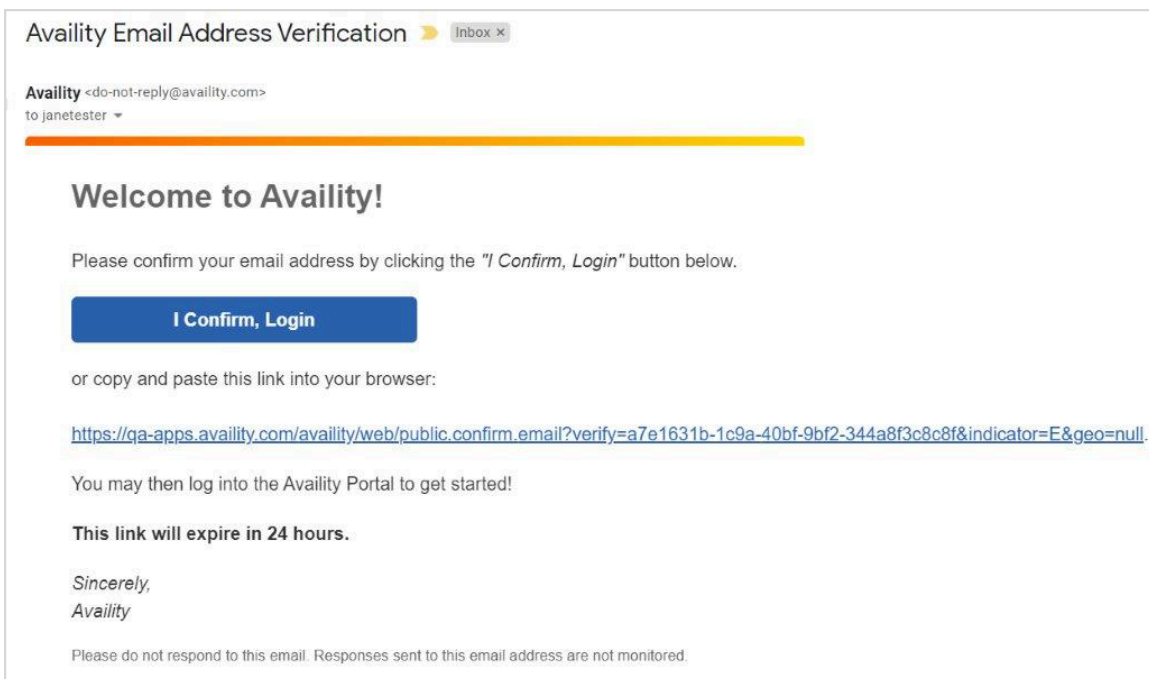
3. Click **Create Account**.

Confirm your email address

Availity sends a verification email to your inbox.

1. Check your email for the message, and locate the email that Availity has sent you.

2. In the email message, click the link to confirm your email address or click **I Confirm, Login**.

   Important: The link to verify your email address expires after 24 hours.

**3.** Once you verify your email, you'll receive the following confirmation. Log in to Availity Essentials.
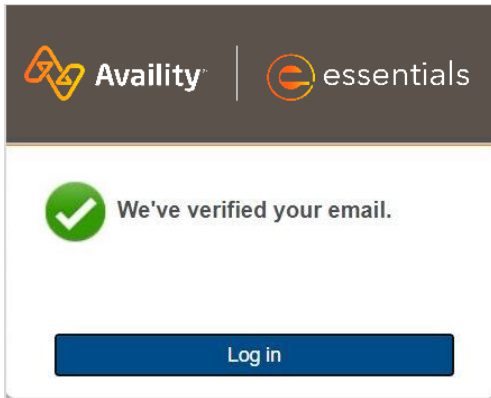
What's next?

After you log in to Availity Essentials, follow the steps to enroll and set up 2-step authentication.

Set up 2-step authentication

After you create your Availity user account and log in to Availity Essentials, you'll be prompted to enroll and set up 2-step authentication.

1. The Start page explains the purpose of the 2-step authentication process and why you are being asked to enroll. Click **Continue** to begin the enrollment.
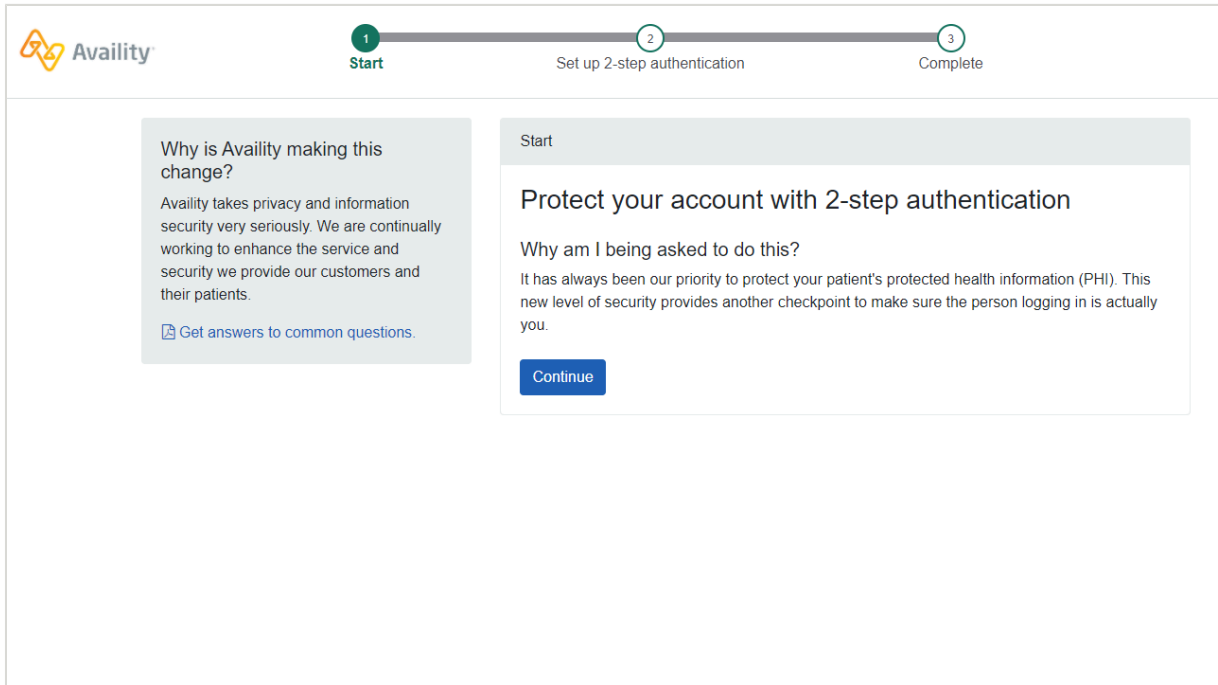
2. Select a method to receive the six-digit code:

   - **Use the Google Authenticator app to generate the code** – You can download this app to your Android (phone or tablet), iPhone, or iPad. Once the app is installed and set up on your device, you can start receiving codes.

     Note: You can only install the Google Authenticator app on a single device, for example, on an iPhone, and not on both an iPhone and iPad.

   - **Text me the code** – You will enter your phone number for your mobile phone device.

   - **Call me with the code** – You will enter your phone number. Currently, you cannot enter an extension number associated with your phone number.

     Note: At this time, only phone number within the United States are accepted.

     Note: You can register up to your devices on which to receive your six-digit, one-time code.

   If you do not have access to a direct-line office phone, cell phone, or tablet, you can use a hard token device as a method to receive the code. Click **My organization requires a different authentication method** to begin setting up the hard token. See the sections later on in this guide for further

explanations on the different methods to receive your code and high-level instructions on setting up the hard token method.

3. On the confirmation window, click **Confirm & Continue**.

4. In the **Code** field, enter the six-digit code you received on your device, and then click **Verify Code**. If the code has expired, then click **Resend Code** to have another code sent to your registered device.

Note: The codes are time-sensitive. Expiration times vary for the codes, depending on which method you selected to receive your code. You will have six minutes to enter the code from an incoming phone

call and three minutes from a text message. The Google Authenticator app generates a new code every 30 seconds, and each code expires after one minute and 30 seconds.

5. On the Complete page, to manage the backup codes, review the following options.

   • Click **Download** to save the text file that contains the backup codes to your computer, phone, or other device. Then search the **av-backup-codes-txt** file. You can rename the file to a name that is more familiar to you. Availity recommends that you move the file to a safe location on your device, which is accessible only to you. Never share your backup codes with your colleagues or anyone else.

   • Click **Add Another Device** to register another device (for example, office phone, mobile phone, or tablet). As a best practice, we recommend that you enroll at least one other device on which to receive the six-digit code in case you lose or do not have access to the original device that you registered.

   • Click **Continue** to access Availity Essentials.

   Important: Keep your backup codes in a safe place. You will need to refer to these backup codes to authenticate your account in case you cannot find the device that you originally registered to receive the six-digit codes.


Note: The entire list of backup codes displays when you first enroll in 2-step authentication and also Availity generates another set of 10 backup codes after using your last code. When you log

back in to Availity Essentials after you have enrolled in 2-step authentication, the list of backup codes does not display. Click **View My Backup Codes** to display the entire list of codes.
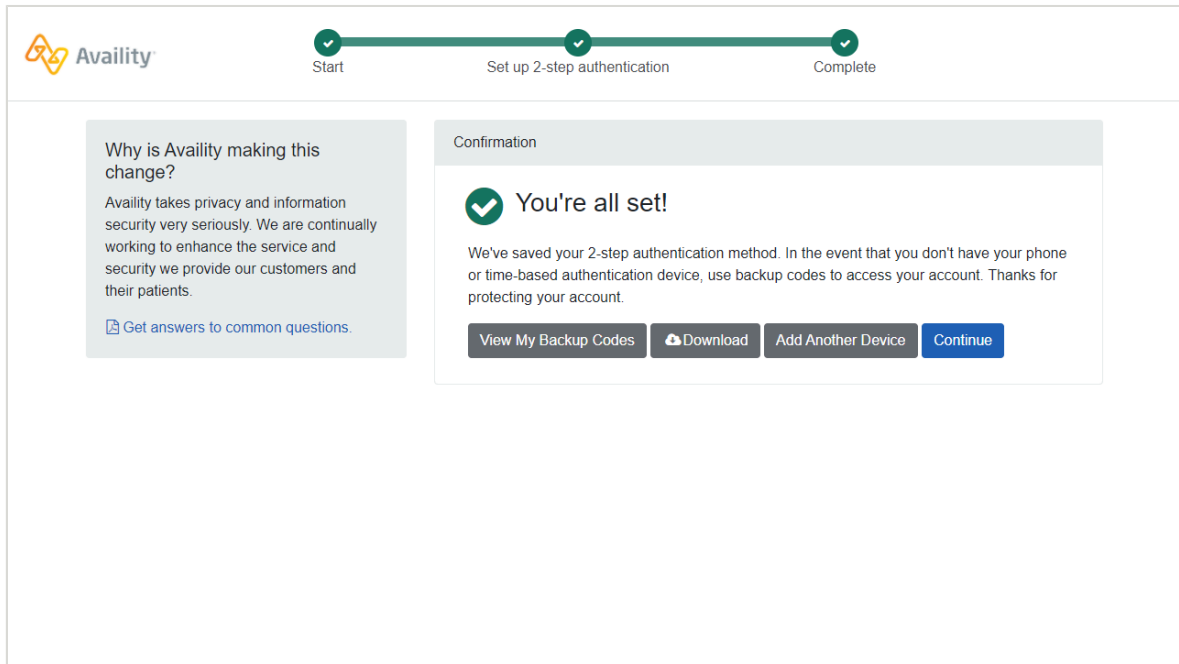
What's next?

After you have set up 2-step authentication, you are brought to the Availity Essentials home page. In the **Notification Center** section, you have messages waiting for you:
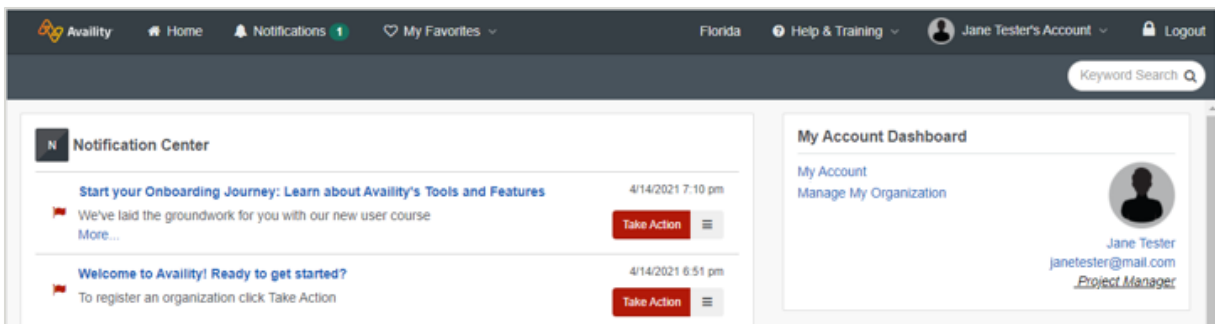
- Click **Start your Onboarding Journey: Learn about Availity's Tools and Features** to take a great introductory class and learn about the functions and applications in Availity Essentials. Or,

- Click **Welcome to Availity! Ready to get started?** to jump right in to registering your organization with Availity.

  Important: If you are new to Availity and are attempting to become the primary administrator by registering an organization, you'll get prompted to verify your identity in the beginning of your registration journey. See Verify your identity later in this guide.

Methods to receive your code

- Google Authenticator

- Text

- Phone call

- Hard token

Google Authenticator

Google Authenticator is an app that you can install on your Android (phone or tablet), iPhone, or iPad. Once Google Authenticator is installed on your device, you'll use this app to receive your code. When you select the **Google Authenticator** option and then click the **Generate a Google Authenticator Key**, additional setup instructions display on the following page.

Tip: Availity accepts the usage of any authenticator application that supports the open-standard authorization protocol or framework (OAuth). Popular options include Google Authenticator or Microsoft Authenticator.
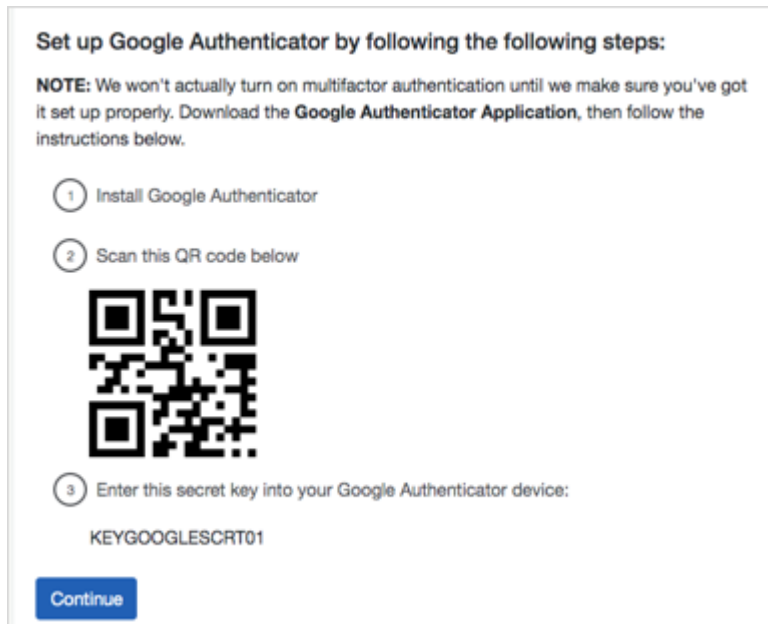
Learn more about how to install the Google Authenticator app on your device.

Note: You can only install the Google Authenticator app on a single device, for example, on your iPhone, and not on both your iPhone and iPad.

Text

When you select text as the method to receive your code, you will enter your phone number, and then we'll send a text to your mobile phone that contains your six-digit code.

You can enroll up to three devices on which to receive your six-digit code.

Phone call

When you select a phone call to receive your code, you will enter your phone number, and then we'll call you back. A recording gives you your six-digit code.

You can enroll up to three devices on which to receive your six-digit code.

Note: At this time, you cannot enter phone extensions that associate with your phone number.

Hard token

A hard token, also known as a security token or authentication token, randomly generates and displays a one-time code. This code authenticates your Availity user account and permits log in to Availity Essentials.

Hard tokens

The following questions and answer are designed to help you better understand hard tokens—what they are, when they are used as a method for 2-step authentication, and who can help you with the installation and setup.

What is a hard token?

A hard token, also known as a security token or authentication token, randomly generates and displays a one-time code. This code authenticates your Availity user account and permits log in to Availity Essentials.

Depending on the type of hardware device that you purchase, the code can either display on the computer or on the panel of the token device.

Who would use a hard token for 2-step authentication?

If you do not have access to a direct-line office phone, cell phone, or tablet at your organization, you can use a hard token as a method to enroll in 2-step authentication. Your organization might require that each employee authenticate using hard token devices instead of using a cell phone or tablet device.

Who will set up and install the hard token?

If you need assistance in installing the hard token, ask your IT administrator, someone at your company's help desk department, or a representative from your third-party IT vendor. Once the hard token is installed on your computer, then refer to the How to Set Up Hard Tokens page. To finish setting up the hard token device, refer to the manufacturer's instructions on how to scan the QR code or enter the secret key.

Important:

The hard token you use for Availity 2-step authentication must be based on the open authorization protocol also referred to as the OAuth framework. Please note that Availity Client Services cannot assist you with the installation, setup, or troubleshooting of hard token devices. Availity also does not cover the cost of purchasing a hard token device.

Can I have both google authenticator and a hard token device as 2-step authenticationmethods?

No, you cannot install both Google Authenticator and a hard token device. You can have only one of these methods set up with Availity—either the Google Authenticator app or a hard token device—but not both.

What happens if I already have google authenticator or a hard token device already set up?

If you have Google Authenticator or a hard token device set up and you try to add another open authorization device, a warning message displays that detects you already have one of these time-based devices:

> **ⓘ Warning!** Looks like you've already set up a time-based security device (i.e. Google Authenticator or Hard Token) for your Availity account.

Availity™

Register an organization

In Availity Essentials, register your organization from the Manage My Organization page. At this time, new users who have recently created an account can only register an organization for a healthcare provider and a billing service from the Manage My Organization page. Existing administrator users who have an Availity user account can register an organization directly from the Manage My Organization page.

Note: If you are the person who registers your organization, you are automatically the primary administrator of the organization.

Important: Before you begin the registration process, here are few things that you need to gather about yourself and your organization:

Healthcare Provider or Health Service Provider

Healthcare providers need to provide:

- Tax ID (EIN or SSN)

- NPI (if you have one)

- Primary specialty/taxonomy

- Check or EFT information from a health plan that you submit to (recommended)

1. As a new user, you are not yet associated with an Availity organization. Existing users, go to step 2.

As a new user, follow these informational prompts:

    a. On the Welcome to Availity prompt, click **Next**.
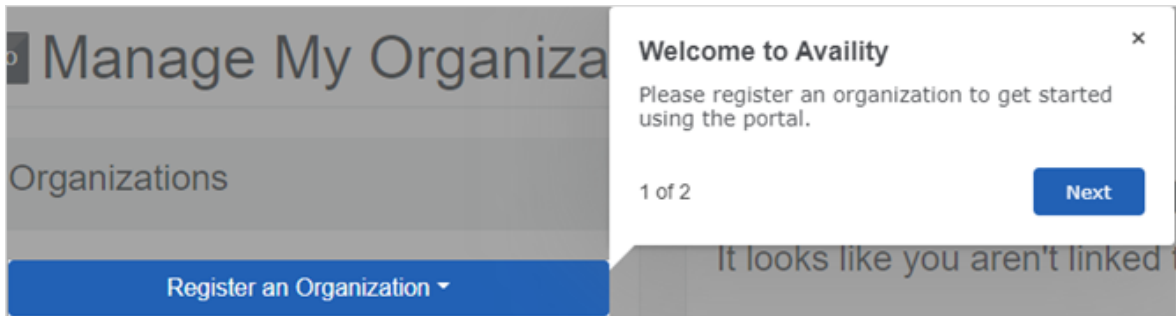
    b. On the Register an Organization prompt, click **End Tour**.
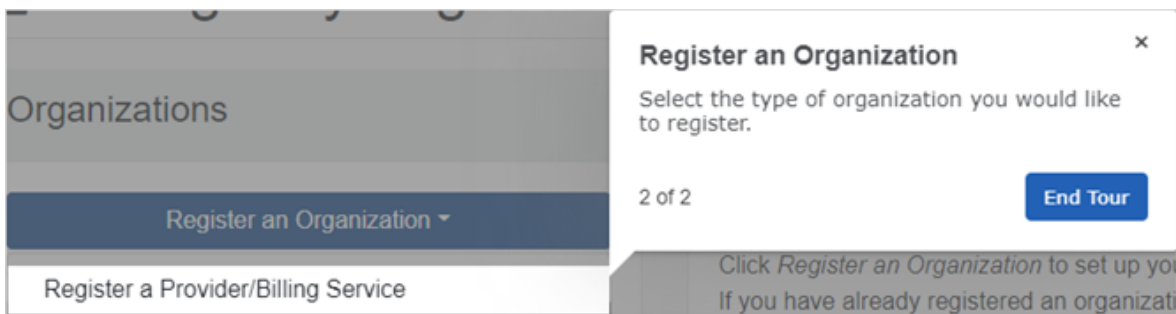
    c. On the Manage My Organization page, click the **Register an Organization** menu, and then select **Register a Provider/Billing Service**.
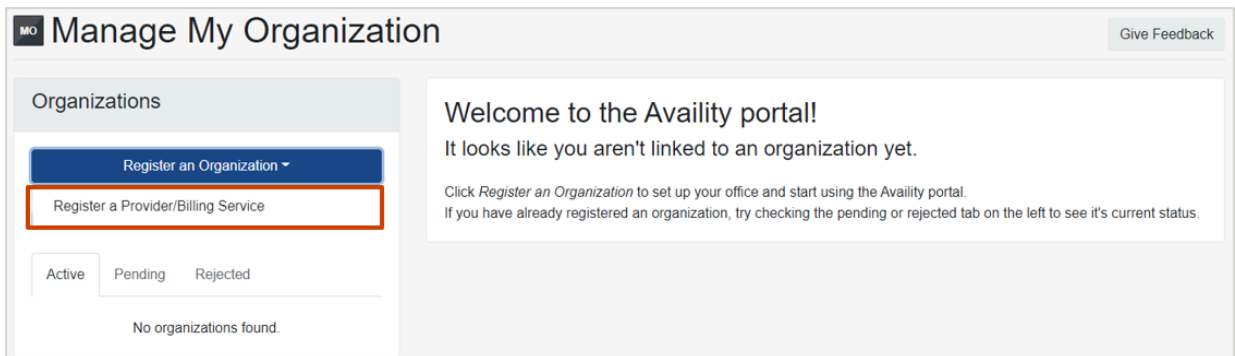
    d. Go to step 3 where you'll need to verify your identity.

2. As an existing user, you are already associated with an Availity organization.

Follow these steps to register another organization:

    a. Click the **Register an Organization** menu, and then select **Register a Provider/Billing Service**.
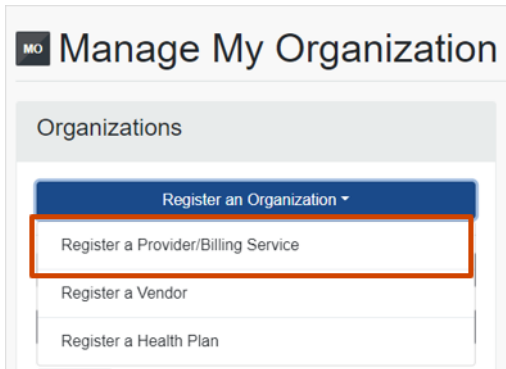
    Note: When you select **Register a Vendor** or **Register a Health Plan**, you leave Availity Essentials and are directed to either the vendor registration website or the health plan registration website to finish registering your organization.

    b. Read the Warning message that displays. The message lists a few common functions where you do not need to create another organization. Click **Continue Adding New Organization**.
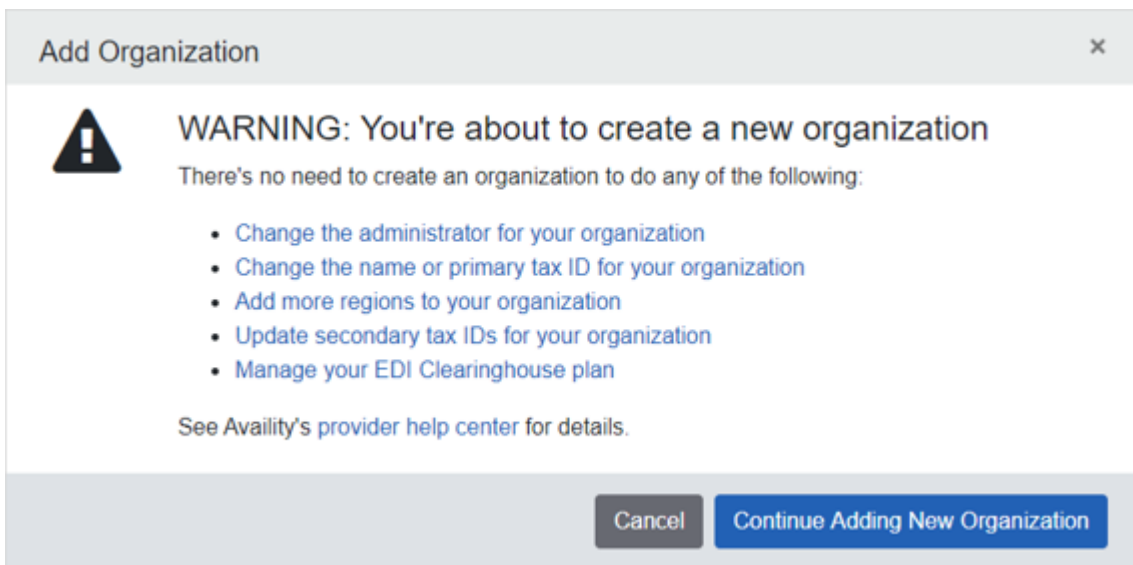
3. Click **Take me to Identity Verification**.

    Note: When you register an organization, you automatically become the Availity administrator for that organization. You will be prompted to verify your identity if you are a first-time administrator. Refer to the procedures to Verify your identity online or Verify your identity manuallyin this guide. With manual

ID verification, you'll need to print out a form, complete the information, and then mail the form back to the designated address.

Note: For users whose identity has already been verified, you'll proceed to the next step and won't need to go through identity verification.

4. Verify or change any personal information and then click **Next**.

Tip: Select the check box to use a nickname for your organization account instead of your legal name. In the **Preferred Name field**, enter your nickname.

Note: If you have previously verified your identity with Availity or if you have recently created your Availity account, your legal first and last names automatically display in the fields.

5. Select the organization type you are registering.

Healthcare Provider or Health Service Provider

  a. Enter the name of your organization.

  b. For the tax ID, enter an employer identification number (EIN) or social security number (SSN), and select the appropriate type.

  c. Enter your organization's NPI or select the check box if your organization does not require an NPI. Optionally, enter an atypical NPI.

  d. Select the organization agreement check box, and then click **Next**.

6. Enter your organization's primary service location.

Healthcare Provider or Health Service Provider

    a. Clear the check box if the billing and physical address are not the same, and then enter the organization's billing address.

    b. Select the taxonomy codes. You can select more than one code.

    c. Select your payers' regions. You can select more than one region.

    d. Select the check box if you need a secure FTP mailbox to share EDI files with your health plans, and then click **Next**.

7. To verify your organization and obtain faster approval, provide information from a valid check you have received from an available health plan in the last six months, and then click **Next**.

   Note: Select **None of these** if you do not have a check or EFT from any of the available payers.

8. Review your information. Click the **Edit** link to update your personal or organization information, and then click **Submit**.

9. Review the next steps for your submitted registration.

- Click the **Organization Agreement** link to review and then print the agreement.

- If you selected to exchange EDI transactions through SFTP, go to the Availity home page for instructions on setting up your SFTP mailbox. A notification displays when the organization is approved.

- Click the **Manage My Organization** link to view the status of your registration.

Home > Organization Registration

Organization Registration

Give Feedback

MY REGISTRATION IS

100%

COMPLETE

What's Next? Manage Organization

Next Steps

Thanks for registering to create an organization account.

Your application ID is **3177330**.

WHAT'S NEXT?

🖨 Print this page and the Organization Agreement for reference.

✉ Once approved, view your notifications on the Availity home page for instructions on setting up your SFTP mailbox

👥 We are processing your application. Please visit Manage My Organization to view the status of your registration.

Print   Home   Manage My Organization

What's next?

Go to the Manage My Organization page to check the status of your organization's registration. On the Manage My Organization page, you'll see if your registration is either *Active*, *Pending*, or *Rejected*.

If your registration is automatically approved, the *Active* status and the color green are associated with the organization.

If your organization is not automatically approved, the status is either *Pending* or *Rejected*. Organizations in a *Pending* status are associated with the color yellow and have updates in the **Notes** section that let you know your application is currently under review.

Organizations in a *Rejected* status are associated with the color red and have updates in the **Notes** section that let you know your application has been rejected. Rejected organizations might be missing certain forms and supporting documentation.

Verify your identity

If you are the primary administrator for your organization, you need to verify your identity before you can register an organization.

You can verify your identity by entering information about yourself online. Or, you can verify your identity through a manual process. The manual process involves downloading and completing Availity's Identity Verification form, getting the form notarized, and then mailing it to the address indicated on the form.

The following page displays to begin the identity verification process. Click **Continue** to begin.

Verify your identity online

You'll need to verify your identity when you register an organization with Availity.

1. To verify your information online, click **Verify Identity Online**.

2. On the Identity Verification page, complete the required information, select the agreement of terms at the bottom of the page, and then click **Continue**.

Note: If your identity is a potential match with the trusted third-party that we use, another form might display asking you for more information, such as your SSN, to confirm your identity.

Enter the additional information requested, and then click **Verify identity** online. If you choose not to enter the information, click **I want to verify manually**.

3. Review and confirm your information and then click **Next**.

   Important: Make sure you review your information. Click **Back** to make changes. Later on, you might not get a chance to correct your personal information.

4. Click **Continue** to answer a series of questions about yourself.

Here's an example question on the quiz:

5. Once you have answered the questions correctly, click **Continue** on the Confirmation page. You are directed back to the Organization Registration page to complete the registration of your organization.

   Note: If you do not answer the questions correctly, then you are prompted to manually verify your identity.

Verify your identity manually

You can verify your identity manually instead of online when you register an organization with Availity. You'll need to complete the following tasks for manual identity verification:

- Complete an initial online form

- Download the Identity Verification form

- Complete the form

- Get the form notarized

- Mail the form back to the address indicated on the form
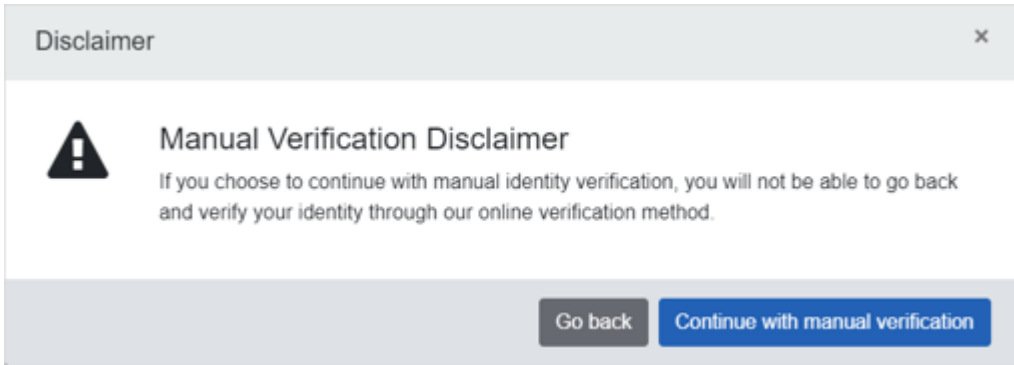
Important: Manually verifying your identity takes longer than verifying your identity online.

1. To manually verify your identity, click **Verify Identity Manually**.
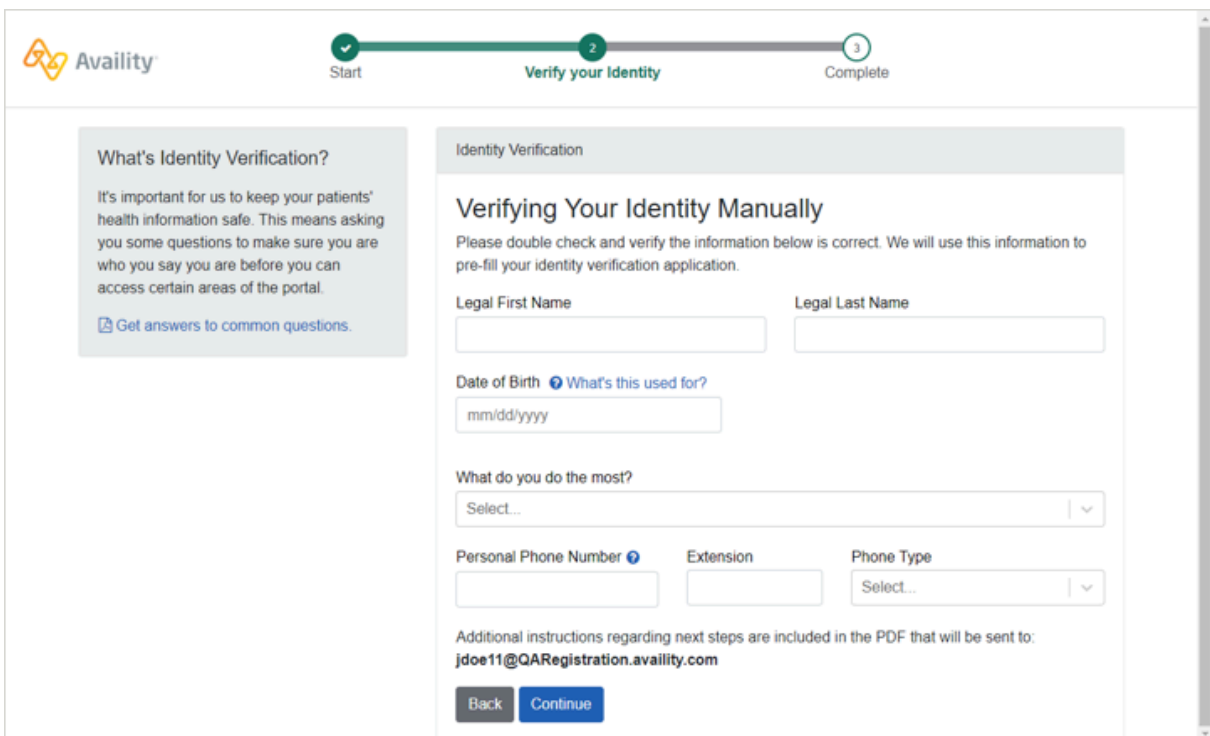
2. Click **Continue with manual verification** to begin the manual verification method for your identity. Click **Go back** to continue with the online verification process.

    Tip: When you select the manual verification method, you'll be able to go back later and change to the online verification method.

3. On the Verifying Your Identity Manually page, complete the required information, and then click **Continue**.

4. On the confirmation page, click **Continue** to get directed back to the Organization Registration page to complete the registration of your organization.

5. In the meantime, check your email from Availity. In the email message, click the link to download and print the manual Identity Verification application form.
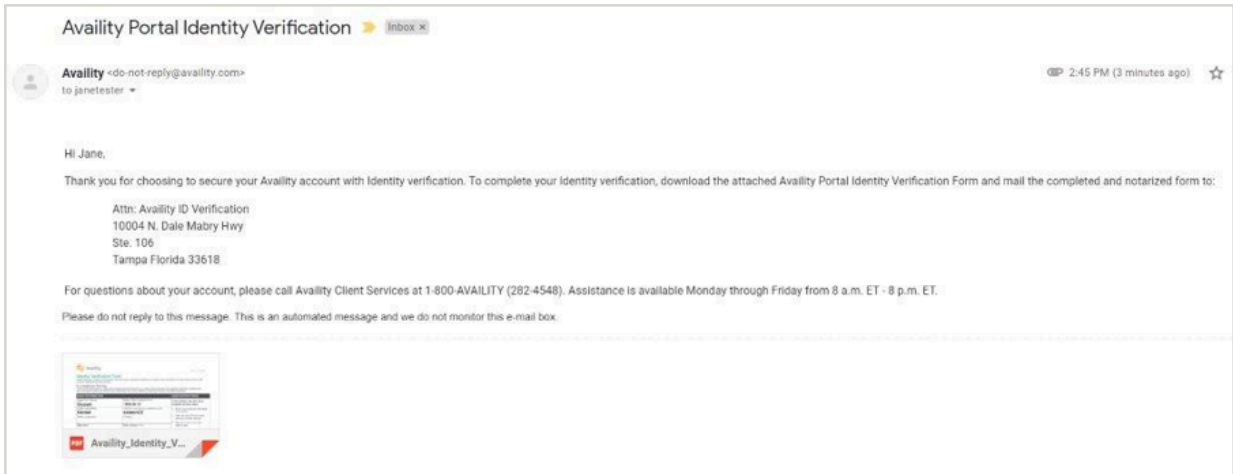
Tip: Remember, you'll need to get the form notarized, and then return the form by mail to the address that is on the form.

Add users overview

As the administrator for your Availity Essentials organization, you are responsible for setting up new users. Due to regulations, each user must have his or her own user account with a unique user ID and password. *Users cannot share user IDs and passwords.*

You can quickly add users in any of the following ways:

- Add new users one at a time.

- Add existing users to additional organizations.

- Use a spreadsheet to upload multiple users at once.

- Copy a user from one organization to another.

Before adding users, familiarize yourself with the concept of Availity Essentials roles and permissions. Be sure to assign roles carefully based on each user's job function. Some roles have legal implications related to HIPAA laws.

Add an existing user to additional businesses

The add user feature allows you to add an existing Availity Essentials user to your organization(s). This could be useful, for example, if a new employee in your business has an existing Availity Essentials user ID from a previous employer. Or, if you are the administrator for multiple Availity Essentials organizations, and you want to move some of your users between those organizations.

1. On the Add User page, select the **This is an existing user ID** check box.

   Tip: If you are administrator for another business to which the user belongs, you can use the maintain user feature to determine the user's existing Availity Essentials user ID.

2. In the **User ID** field, type the user's existing user ID.

3. If you are the administrator for multiple organizations, select the check box next to each organization to which you want to add the user. To add the user to all of your organizations, select the check box at the top of the check box column.

4. Click **Next**.

5. If the system locates the correct user, select **Yes** to the question **Do you want to associate this user with your organization?**

   Note: If an error message displays indicating the user ID you entered is not in our records, check the user ID and try the search again, or enter the individual as a new user.

6. Assign roles to the new user based on the user's job function.

7. Perform final steps in the add user process.

Roles and permissions overview

As the administrator for your Availity Essentials organization, you are responsible for assigning roles to users in your organization based on each user's job function. Assigning roles is part of the process when you add a new Availity Essentials user with the add user feature. In addition, you can assign or remove roles for existing users at any time using the maintain user feature.

- A **role** is a group of job functions, or permissions. Each role consists of one or more permissions.

- A **permission** is a job function or, more specifically, access to a feature in Availity Essentials that allows the user to perform a job function. You cannot assign individual permissions. You must assign the role to which the permission belongs. However, some roles include only one permission.

Note:

- The roles and permissions available to you and your users depend on your organization type and the region (state or geographic location) to which your organization belongs in Availity Essentials. For example, an organization registered as a hospital in Florida will have access to different roles and permissions than an organization registered as a physician practice in Oklahoma. The person who registered your organization with Availity specified your organization type and region(s) at the time of registration.

- Not all payers or vendors support all permissions. In fact, there are a number of permissions that only a single payer supports.

- Some roles have legal implications related to laws. Be sure to assign roles to each user carefully based on the user's job function.

Assign roles

Assigning roles is part of the add user process for administrators. Roles determine which Availity Essentials features users can access. Before assigning roles to users, familiarize yourself with Availity Essentialsroles and permissions. This will help you decide which roles are appropriate for each user. Some roles have legal implications related to HIPAA laws. Be sure to assign roles carefully based on each user's job function.

Note: When a business first registers with Availity, Availity creates a user account for the administrator of that business, and assigns to it all roles that are available to the business at the time of registration approval. As administrator, you can change the roles assigned to your user account at any time using the maintain user feature. However, you cannot remove the administrator role from your account. To change the administrator for your business, contact Availity Client Services at 800-282-4548 (800-AVAILITY).

1. After you complete the Add User page and click **Next**, the Role for [User Name] page displays. Choose an option for assigning roles to the user:

   • If the user needs a unique set of roles, make sure **This user needs a new set of roles** is selected (this is the default). In the roles table, select the check box next to each role you want to assign to the user. To assign all available roles, select the check box at the top of the roles table.

   • Select **This user needs the same set of roles as an existing user**, if appropriate. In the **Assign the same role(s) currently assigned to** field, select the existing user who has the roles you want to assign to the new user.

   Note: Click **More Info** in the roles table to view the permissions that are associated to a specific role, along with the payers and vendors that support those permissions.

2. If you are adding the user to multiple businesses, and you want the user to have the same set of roles in each of those businesses, select the check box labeled **Assign [User Name] the same roles in all organizations** at the bottom of the roles table. This will save you steps in the add user process.

   Note: Leave this check box blank if you want the user to have different roles for each business. For example, for one business you may want the user to submit claims, run eligibility and benefits inquiries, and submit authorizations and referrals; for another business, you may want the same user only to submit claims. As administrator, you determine which roles the user can access for each of your businesses.

3. Click **Next**.

4. On the Review and Submit page, review the roles you selected for the user before you submit them. If you need to edit your selections, click **Edit Info**.

   Note: You cannot edit user information such as name, email address, and phone number at this point in the process. Users can edit this information themselves later using the my account feature.

5. When you are satisfied with the roles you have selected for the user, click **Submit**.

6. On the User Information Saved page, click **E-mail** or **Print** to provide the user with his or her user ID and temporary password.

Important: You will not have access to the user's temporary password after you leave the User Information Saved page. The user must log in to Availity Essentials with his or her temporary password within 60 days.