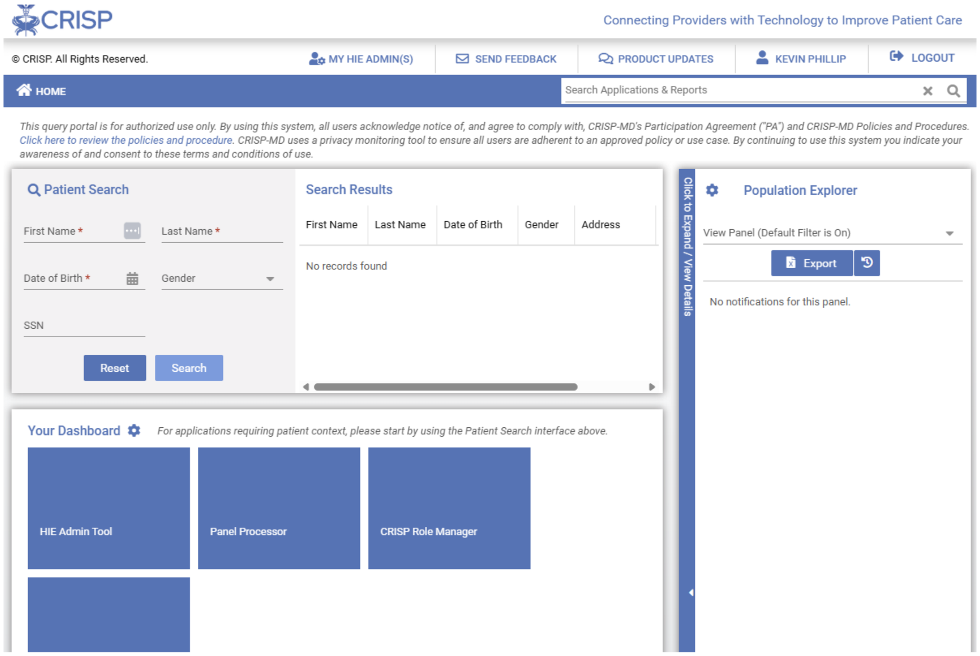
CRISP Portal Set Up User Guide

Background

This guide is The CRISP Portal provides secure access to patient information and care coordination tools. To protect patient privacy, users must complete a one-time account setup that includes creating login credentials and enabling additional security features like two factor authentication.

This guide walks users through the initial portal login and account setup process, including required security steps, how to access the portal in the future, and where to go if you need support.



This query portal is for authorized use only. By using this system, all users acknowledge notice of, and agree to comply with, CRISP-MD's Participation Agreement ("PA") and CRISP-MD Policies and Procedures. Click here to review the policies and procedure. CRISP-MD uses a privacy monitoring tool to ensure all users are adherent to an approved policy or use case. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use.

First Name	Last Name	Date of Birth	Gender	Address

No records found

No notifications for this panel.

For applications requiring patient context, please start by using the Patient Search interface above.

Access

Access to the CRISP Portal requires a valid participation agreement between your organization and CRISP. User access must be requested and approved by your organization's **HIE Admin** using the credentialing tool.

If you are unsure whether your organization has a participation agreement or do not know who your HIE Admin is, please contact **Technical User Support**.

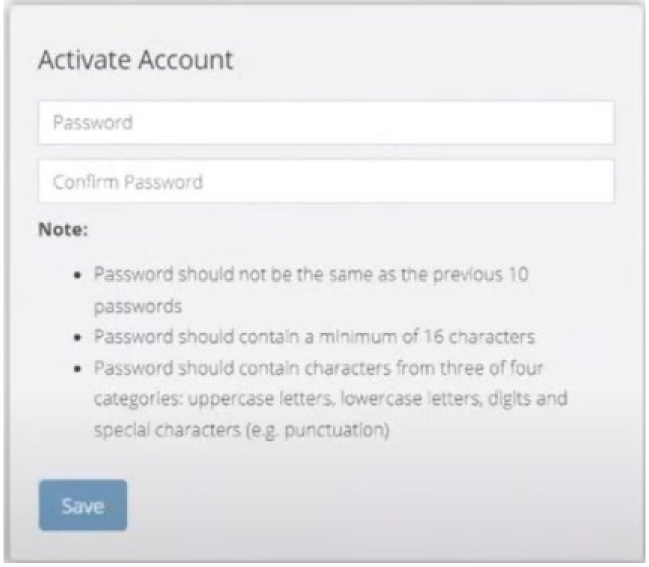
Portal Account Setup

Once your account is created, you will receive an email from **donotreply@hmetrix.com** with the subject line **"CRISP Portal Activation."** Click the activation link to begin setting up your account.

You will be prompted to create a password. Passwords must be at least **16 characters** and include:

- One capital letter
- One number
- One special character

After your password is set, you will complete the required security setup to finish activating your account.



Activate Account

Note:

- Password should not be the same as the previous 10 passwords
- Password should contain a minimum of 16 characters
- Password should contain characters from three of four categories: uppercase letters, lowercase letters, digits and special characters (e.g. punctuation)

Two Factor Authentication

To protect patient data, all CRISP Portal users must enable two-factor authentication (2FA) as part of account setup.

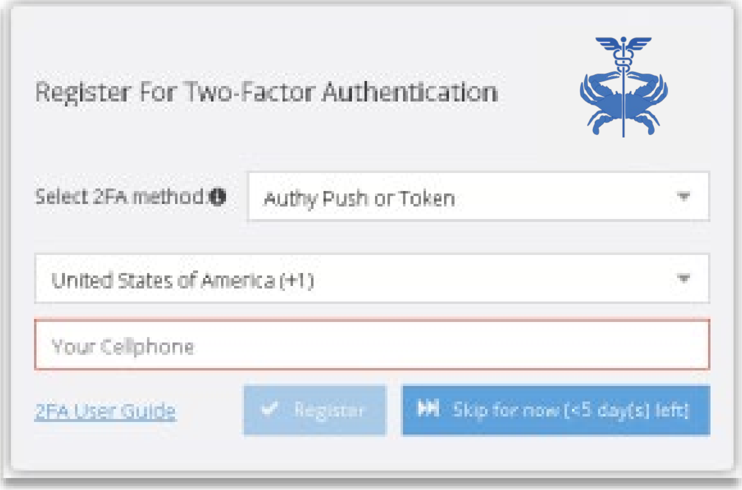
Users may choose one of the following options:

1. Twilio Authy app (preferred)
2. Other authenticator apps (e.g., Google Authenticator, Microsoft Authenticator, Duo)
3. Security key (e.g., YubiKey)

Set by Set 2FA Setup

Step 1: Choose a 2FA Method
From the dropdown menu, select **Authy Push or Token** (preferred).

- Note: The **Security Key (FIDO2)** option requires a hardware key and is covered later in this guide.



Register For Two-Factor Authentication

Select 2FA method: Authy Push or Token

United States of America (+1)

Step 2: Register Your Phone Number

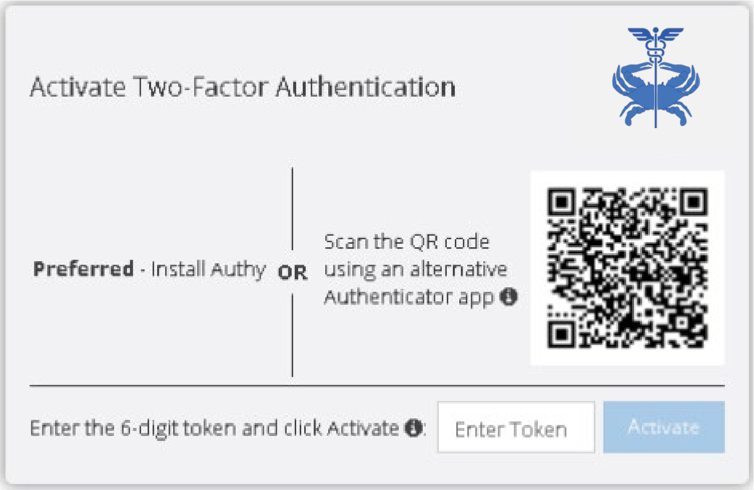
Enter your **cellular phone number** and select **Register**.

- The system will verify that the number is a mobile number.
- If the number cannot receive SMS messages, you will be prompted to enter a different number.

Step 3: Activate Authy

Once your phone number is validated, select **Proceed to Activation**.

- This creates your Authy account and opens the **Activate 2FA** screen.
- Selecting **Cancel** will return you to the previous screen.



Activate Two-Factor Authentication

Preferred - Install Authy **OR** Scan the QR code using an alternative Authenticator app

Enter the 6-digit token and click Activate: Enter Token Activate

Step 4: Download an Authenticator App

You will receive a text message from Authy with a download link.

- Follow the link to install the **Authy app** on your device (preferred).
- You may also use another authenticator app (e.g., Google Authenticator or Microsoft Authenticator) by scanning the on-screen QR code.

Step 5: Complete Activation

Open your authenticator app and locate the **6-digit code** for CRISP.

- Enter the code on the **Activate 2FA** screen and select **Activate**.
- If the code is valid, you will be granted access to the CRISP Portal.

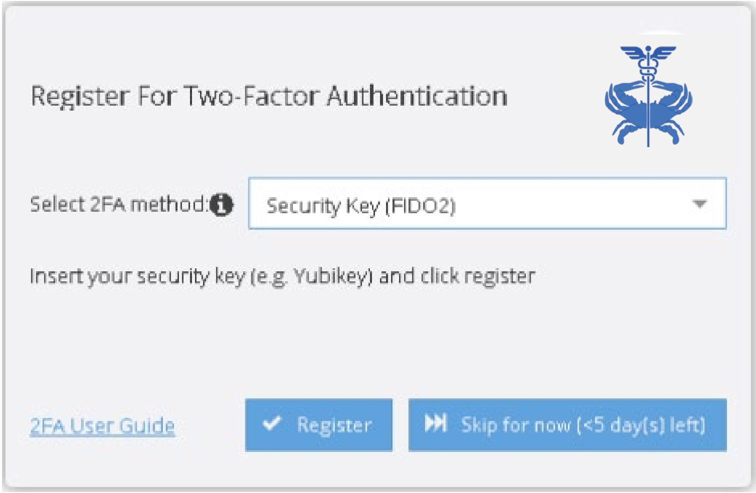
Important: Do not refresh or close your browser until activation is complete. If you do, you will need to restart the 2FA setup process.

Security Key (FIDO2) Setup (optional)

Using a security key (FIDO2) is the most secure two-factor authentication option. This method requires a compatible hardware or software security key, such as YubiKey, Google Titan, or Feitian ePass.

Before you begin:

- You must have a FIDO2-compatible security key.
- A PIN must already be set on the key.
- Security keys cannot be copied, backed up, or replaced. Each key is unique.



Register For Two-Factor Authentication

Select 2FA method: Security Key (FIDO2)

Insert your security key (e.g. Yubikey) and click register

Step 1: Select Security Key

- From the 2FA method dropdown, select Security Key (FIDO2).

Step 2: Register the Key

- Insert the security key into your device's USB port and select Register.

Step 3: Verify the Key

- When prompted, enter the security key PIN and select OK.
- The prompt may look different depending on your operating system.

Step 4: Complete Registration

Touch the security key's button or biometric sensor when prompted. Once complete, the key will be registered to your CRISP Portal account and you will be logged in.

Important: Do not refresh or close your browser during setup. If the process is interrupted, you will need to restart security key registration.

Logging In After Account Setup

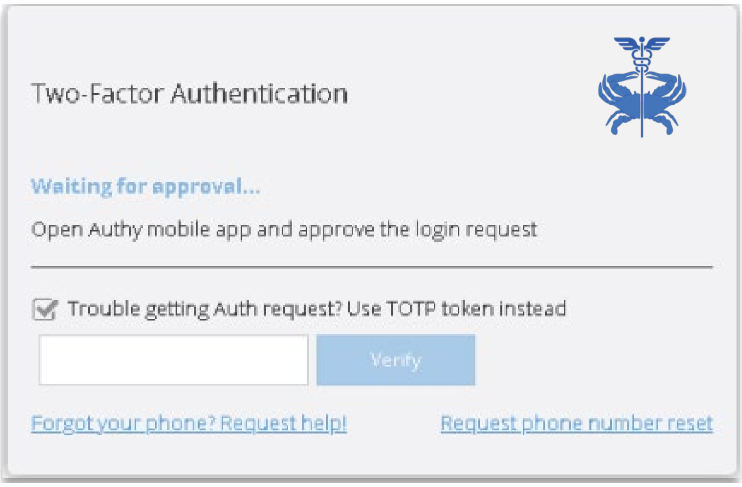
Once two-factor authentication (2FA) is enabled, log in to the CRISP Portal at **https://portal.crisp.org** using your username and password. You will then verify your identity using one of the methods you previously set up.

Login Via Authy

Push Notification (Preferred)

1. After entering your username and password, open the **Authy app** on your phone.
2. Review the login request and select **Approve** to continue or **Deny** if you do not recognize the request.
3. If approved, you will be logged into the CRISP Portal.

Push notifications require cellular or internet connectivity.

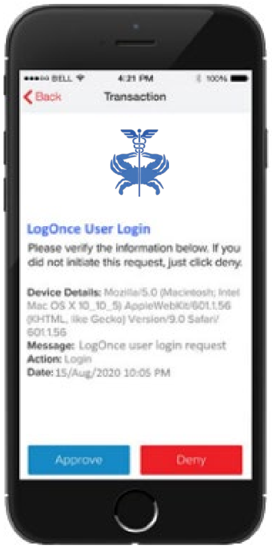


Two-Factor Authentication

Waiting for approval...

Open Authy mobile app and approve the login request

☑ Trouble getting Auth request? Use TOTP token instead



LogOnce User Login

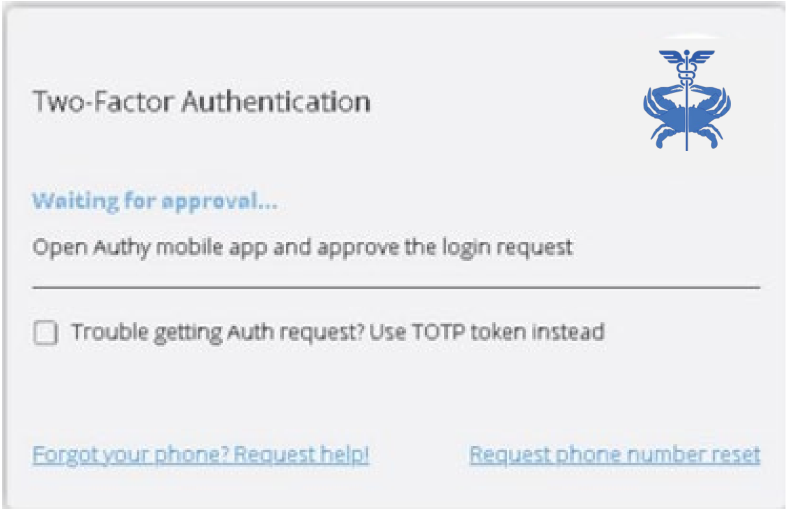
Please verify the information below. If you did not initiate this request, just click deny.

Device Details: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/601.1.56 (KHTML, like Gecko) Version/9.0 Safari/601.1.56
Message: LogOnce user login request
Action: Login
Date: 15/Aug/2020 10:05 PM

One-Time Passcode (TOTP)

If you do not receive a push notification, you can use a one-time passcode instead.

1. On the 2FA screen, select **"Trouble receiving an Auth request? Use TOTP Token instead."**

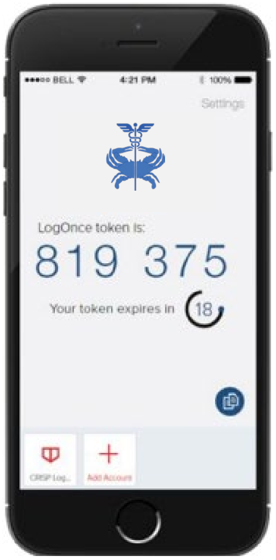


Two-Factor Authentication

Waiting for approval...

Open Authy mobile app and approve the login request

☐ Trouble getting Auth request? Use TOTP token instead



LogOnce token is:

819 375

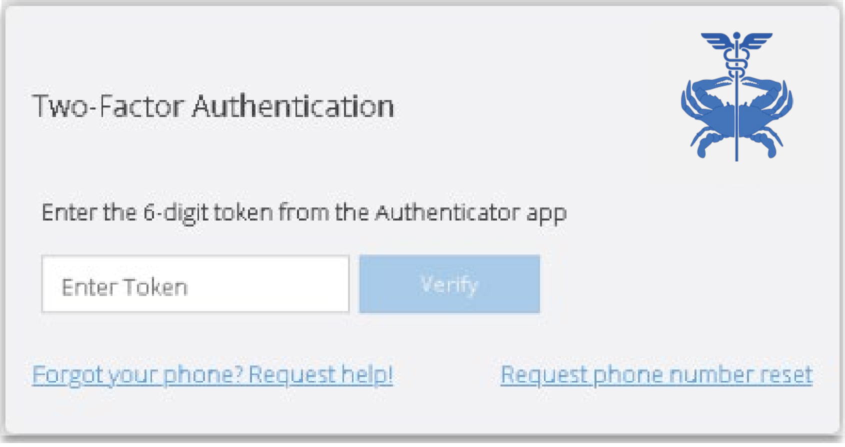
Your token expires in 18

2. Open the Authy app and select the **CRISP Portal** entry to view the 6-digit code.
3. Enter the code and select **Verify** to log in.

Login Using Other Authenticator Apps

If you set up 2FA using Google Authenticator, Microsoft Authenticator, or another app:

1. After entering your username and password, open your authenticator app.
2. Generate the **6-digit one-time passcode**.
3. Enter the code on the verification screen and select **Verify**.



Two-Factor Authentication

Enter the 6-digit token from the Authenticator app

Login Using a Security Key (FIDO2)

If you registered a security key, you must use the same key each time you log in.

1. After entering your username and password, insert your security key into your device.
2. Enter the key PIN when prompted and select OK.
3. Touch the key's button or biometric sensor to complete login.

If you forget or lose your security key, select Cancel on the security key screen to request assistance with suspending or resetting 2FA.

Support/Assistance

For most access and account-related questions, users should first contact their organization's **HIE Admin**, who can assist with account requests, permissions, and access issues.

If you do not know who your HIE Admin is, or if you need additional assistance, CRISP Support is available. CRISP Support can help with portal access issues, login problems, and general technical questions.

- 📧 **Email:** support@crisphealth.org
- 📞 **Help Desk:** 877-952-7477
- 📚 **Training Materials & FAQs:** https://www.crisphealth.org