CRS Portal: Two Factor Authentication

User Guide

By CRISP, last updated 11/5/20

Contents

CRS Portal Two Factor Authentication

Background

As the CRISP Reporting Service (CRS) team continues expanding our services, it is imperative that we ensure patient data is kept private and secure. A second factor for authentication (2FA) will be added to the CRS Portal to improve security via the Authy App.

To log on:

1. Go to reports.crisphealth.org and enter your username + password
2. Enter your phone number to receive an activation text message (first time only)
3. Use the SMS text message link to download the Authy app
4. Receive a push notification from the Authy app to approve login

Once activated, a push notification will appear on the user's cell phone via the Authy app to approve all future account login attempts. This user guide describes in detail the 2FA activation and login process, as well as how a user can login within cellular service or update outdated phone numbers.

CRISP

User Guide

Two Factor Authentication Set Up

Step 1. Once the two-factor authentication feature is enabled for all new or existing CRS Portal users, you as a user will be prompted to set up 2FA on their next CRS Portal Login. You can access the CRS Portal by login to https://reports.crisphealth.org with your User ID and password.

Log in to CRISP Reporting Services (CRS) Portal

Email

Next

Reset your password?

Warning: CRISP policy prohibits username and password sharing.
Violation could result in account termination.

Questions or Concerns? Please contact the CRISP Customer Care Team at support@crisphealth.org or 877-952-7477.

© hMetrix   powered by hMetrix

Log in to CRISP Reporting Services (CRS) Portal

Password

Login

Reset your password?

Warning: CRISP policy prohibits username and password sharing.
Violation could result in account termination.

Questions or Concerns? Please contact the CRISP Customer Care Team at support@crisphealth.org or 877-952-7477.

© hMetrix   powered by hMetrix

Step 2. You will be presented with the prompt to Activate Two-Factor Authentication as shown in the Figure below. If you are not ready to activate 2FA, you may skip activation for the next 5 days. After 5 days the activation of 2FA is mandatory, and the skip button will disappear.

Step 3. You may enter your cellular phone number and activate 2FA by clicking the Activate button. When you click the Activate button, the CRS portal will validate that the phone number entered is a cellular phone number. If it is not a cellular phone number, a message is displayed, and you will be prompted to enter your cellular phone number once again.
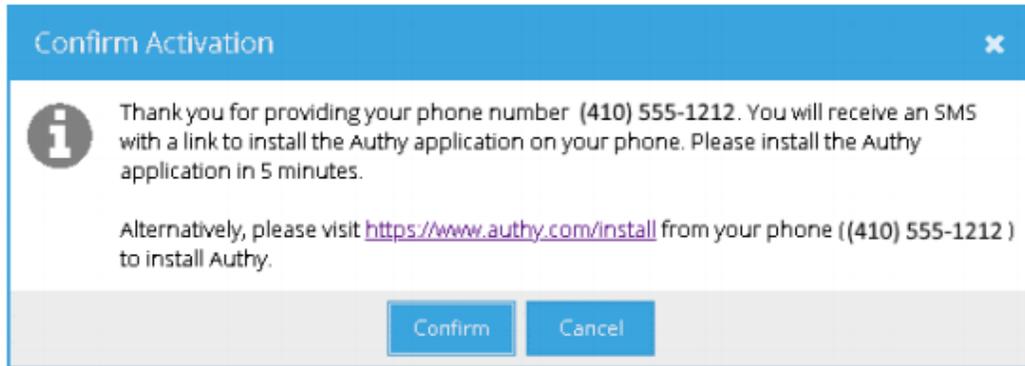
Step 4. After the phone number has been validated, a confirmation screen shown in the below figure will be displayed. On clicking Confirm, an Authy account will be created with the given phone number and store the account information with a database. If you click the 'Cancel' button a message will be displayed and will return you to the 2FA Activation screen.

Step 5. Authy will send an SMS text message like the one shown below. Authy will autodetect the device type and redirect you to the appropriate download link. Clicking the link will prompt you to download the Authy application onto your registered device.
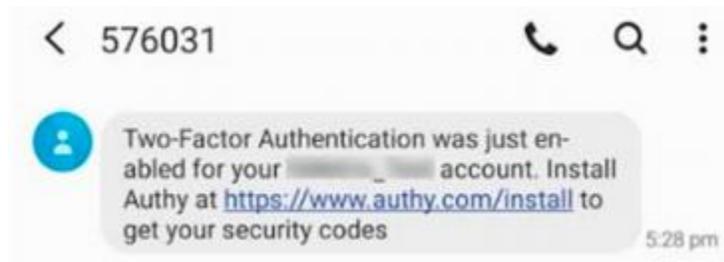
Step 6. While waiting for you to install Authy, a message will appear in the screen as below; Waiting for Authy Installation. The CRS Portal will automatically check the installation status. When you install the Authy app, the CRS Portal will automatically send the Authy Push notification and move to the approval screen. If the app is not installed within the configured time, a message as shown in will be displayed and you will be redirected the activation screen to retry the activation process.
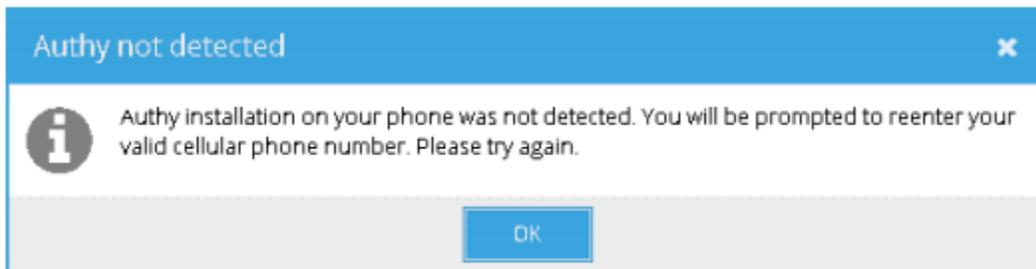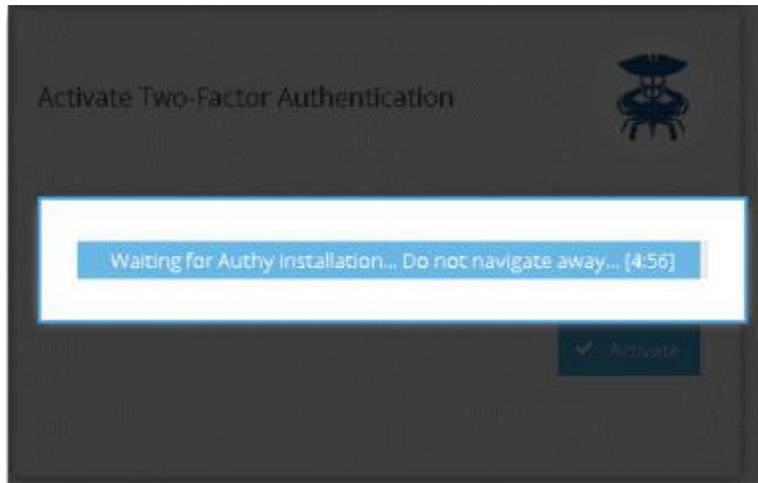
Two Factor Authentication Login

Once 2FA has been activated and Authy has been downloaded, a push notification will appear on your cell phone via the Authy app to approve all future account login attempts. The steps below describe the process of user login with the 2FA feature enabled.

Step 1. You can access the CRS Portal by login to https://reports.crisphealth.org with your User ID and password. After logging in, the CRS Portal will use the Authy ID and send a Push notification message to the Authy app on your phone for you to verify your identity.

Step 2. You may retrieve pending Push transactions by opening the Authy app. You should verify the information presented on the Authy Authenticator screen before clicking Approve. Should you not recognize the Push request, you should click Deny. If you click Approve, the CRS Portal will grant access to the Landing Page. If the you click Deny in the Authenticator app, then the CRS Portal will denied the log in and you will be redirected to the Login page.
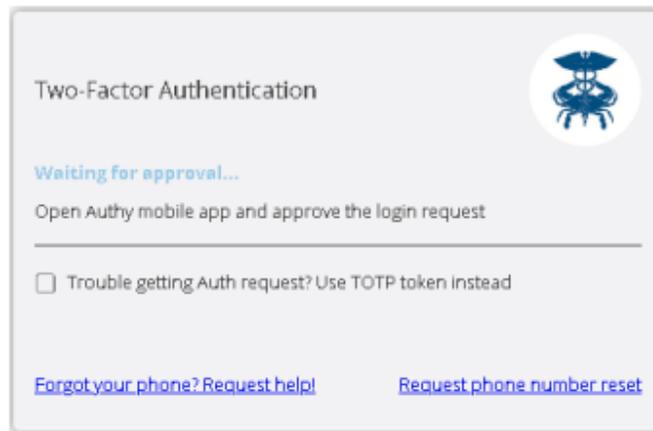
Login with TOTP 2FA

Authy's Push notification system requires cellular connectivity. Time based One-Time Password (TOTP) allows you to authenticate into the CRS Portal without cellular connectivity on your phone. You can generate a TOTP in the Authy application and enter the TOTP token into the CRS Portal instead of the Push approval. The steps below describe the process of user login with TOTP 2FA number.

Step 1. You can access the CRS Portal by login to https://reports.crisphealth.org with your User ID and password. After logging in, the CRS Portal will use the Authy ID and prompt you for a TOTP token and send a Push notification message to the Authy app on the phone for you to verify their identity.

Step 2. You can click to check the option box next to 'Trouble receiving an Auth request? Use TOTP Token Instead".

Step 3. Then you can generate the TOTP token by opening the Authy application on your phone and select the CRS Portal tab. The screen will display a token that changes every 30 seconds as shown below.


Step 4. Enter the TOTP token and click Verify to enter the CRS Portal.

Change Phone Number

If you need to change your phone number, you may click on the Request phone number reset link in the CRS Portal 2FA screen. An email will be sent to support@crisphealth.org, requesting a Support team member to approve or deny the request. A support team member will verify your identity to approve the request is legitimate. If approved, you must repeat the activation process described in Two Factor Authentication Set Up section above.
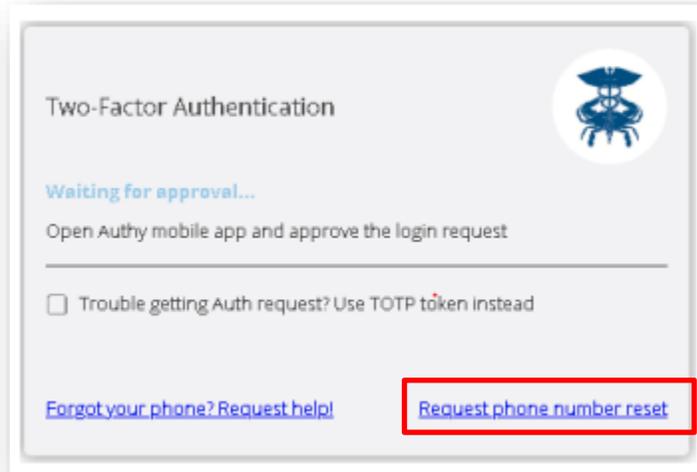
Suspend 2FA

If you have forgot or misplace your phone temporality but require important reporting information from the CRS Portal, you may click on the 'Forgot your phone? Request help!' link in the CRS Portal 2FA screen. An email will be sent to support@crisphealth.org, requesting a support team member to approve or deny the request. A support team member will verify your identity to approve the request is legitimate. If approved, the user will be allowed to login to the CRS Portal without 2FA for a temporary period. CRISP will monitor these requests closely and has strict protocols in place prevent malicious behavior. Please note this feature is only available during normal office hours.