CRS Portal: Two Factor Authentication

User Guide

By CRISP, February 25, 2021

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 log in.

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in detail the 2FA activation and login process, as well as how a user can login within cellular service or update outdated phone numbers.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

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
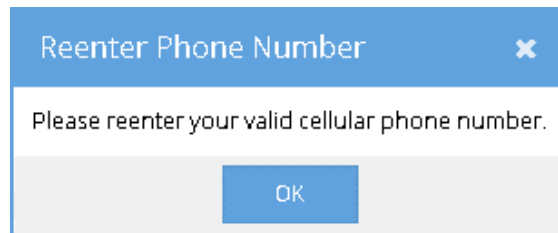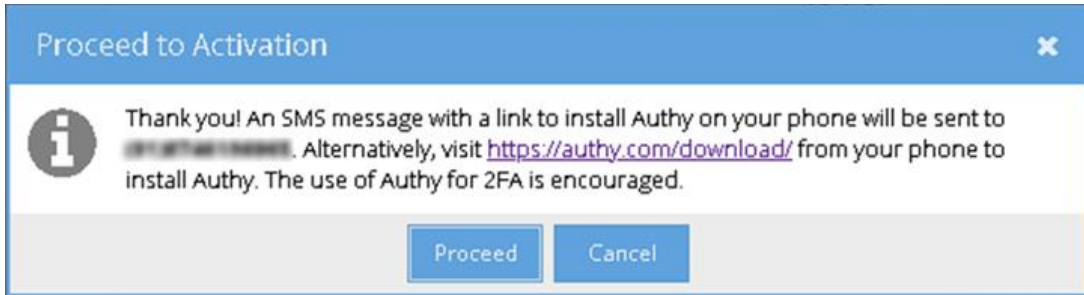
Authy and Other Authenticator Apps

Step 1. You will be presented with the prompt to Register 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.
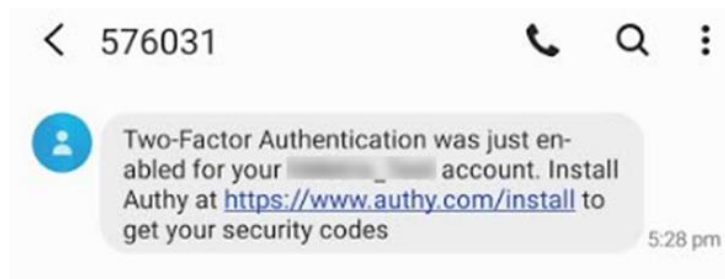

Step 2. You may enter your cellular phone number and register phone number with 2FA by clicking the Register button. When you click the Register button, the CRS portal will validate that the phone number entered is a cellular phone number. If it is not a cellular phone number, a message is displayed,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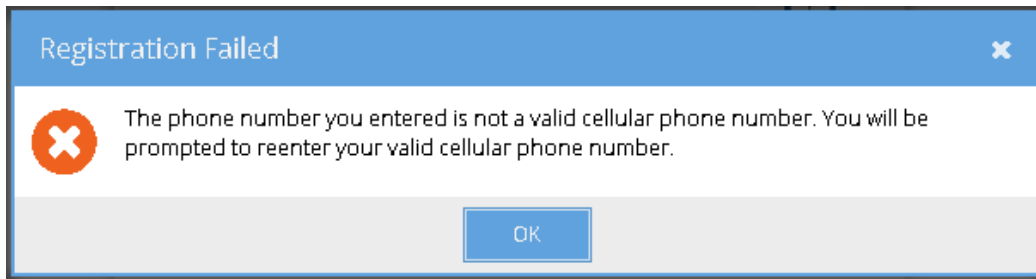
Step 3. After the phone number has been validated, a Proceed to Activation screen shown in the below figure will be displayed. On clicking Proceed, an Authy account will be created with the given phone number and you will take to Activate 2FA screen. If you click the 'Cancel' button a message will be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

Proceed to Activation ✕

Thank you! An SMS message with a link to install Authy on your phone will be sent to ▓▓▓▓▓▓▓▓▓▓. Alternatively, visit https://authy.com/download/ from your phone to install Authy. The use of Authy for 2FA is encouraged.

Proceed   Cancel

Reenter Phone Number ✕

Please reenter your valid cellular phone number.

OK

Step 4. 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.

< 576031

Two-Factor Authentication was just enabled for your ▓▓▓▓▓_▓▓▓ account. Install Authy at https://www.authy.com/install to get your security codes

5:28 pm

Twilio Authy 2-Factor Authentication

Authy   Tools   ★★★★☆ 31,131 👤

E Everyone

⚠ You don't have any devices.

⊞ Add to Wishlist   **Install**

Step 5. Use of Authy app is strongly preferred. You can also use an alternative authenticator app, such as Google Authenticator or Microsoft Authenticator. The alternative authenticator app can be used by scanning the QR code in below figure. Please follow the instructions from the alternative authenticator app to scan the QR code.

To activate 2FA, you need to enter a 6-digit token in Activate 2FA screen. This 6-digit token is available on the newly added CRISP LogOnce tab in the Authy app or the alternative authenticator app. You need to enter the 6-digit token in the textbox and clicking the Activate button. If the token is valid LogOnce will grant access to CRS portal. Otherwise, you need to reenter a valid token. If you refresh or close the browser tab before activation is complete, you need to start over again from the Registration screen.

FIDO2 Token

This method of two-factor authentication is the most secure. It requires a hardware or software token than conforms to the FIFO2 standard. Examples are an Yubikey 5 series key, a Google Titan Security key or a Feitian ePass FIDO2 key. The instructions below assume that you have configured a pin on such a key.

Step 1. You will be presented with the prompt to Register 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.
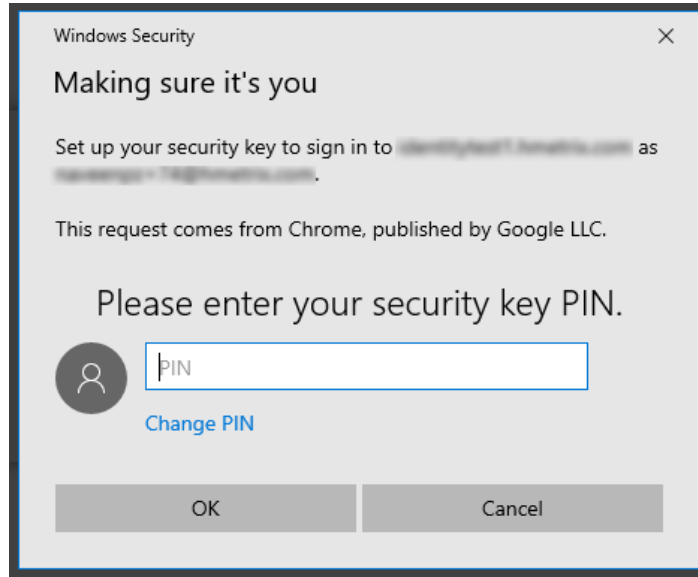
Step 2. Insert the FIDO2 token into the USB port and click the register button to register the token with the CRS portal.

Step 3. Enter the pin on the next screen, as shown below, and click OK.

Step 3. You will be prompted to touch the FIFO2 token's button or biometric scanner. Once you do so, the token will be registered against your LogOnce account and you will be redirected to CRS portal.

If you refresh or close the browser tab before registration is complete, you need to start over again.
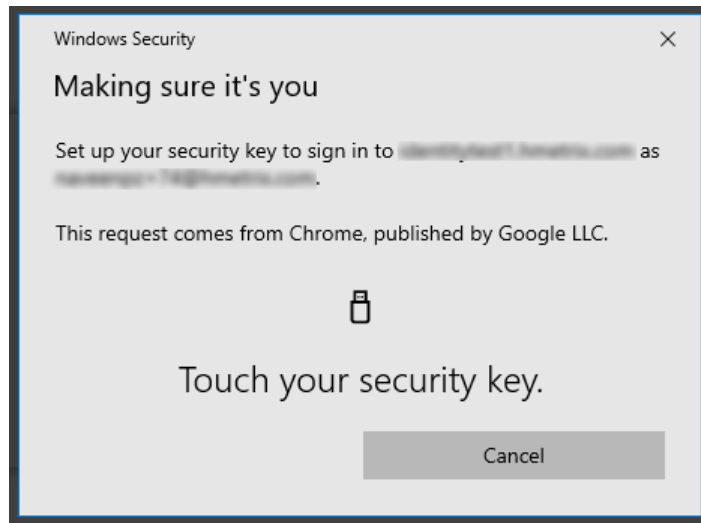
Two Factor Authentication Login

Once 2FA has been activated, when you access the CRS Portal by login to https://reports.crisphealth.org with your User ID and password, a push notification will appear on your cell phone via the Authy app or you need to enter the 6-digit token from Authenticator app or use a FIDO2 token to verify your identity. For all future account login attempts you need to follow the steps described below.

Login via Authy

Push Authentication

Step 1. If you have registered with the Authy app, 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 you click Deny in the Authenticator app, then the CRS Portal will deny the log in and you will be redirected to the Login page.
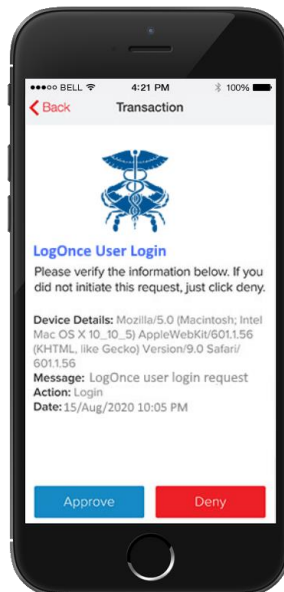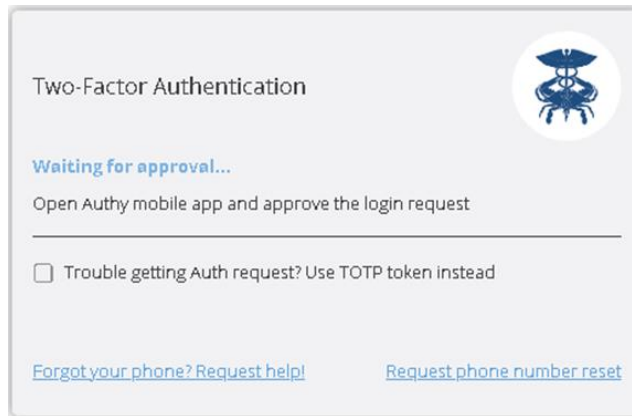
TOTP Authentication

Authy's Push notification system requires cellular connectivity. Time based One-Time Password (TOTP) allows you to authenticate in 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. After login to CRS portal, on the 2FA screen if you have not received the push notification from Authy due to some reason, you can use the TOTP token Authy app to verify your 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.

Login via other Authenticator apps

If you activated 2FA using an alternative authenticator app such as Google or Microsoft Authenticator, you need to follow the steps described below. A Time based One-Time Password (TOTP) allows you to authenticate in CRS Portal without cellular connectivity on your phone.

Step 1. After login to CRS portal, you will be redirected to a screen like the one below.

Step 2. Generate the 6-digit TOTP token using the registered Authenticator application on your phone.

Step 3. Enter the token and click Verify complete 2FA.

Login via FIDO2 Token

If you activated 2FA using FIDO2 token, you need to follow the steps described below. You need to use the same token that you have registered with the CRS portal.
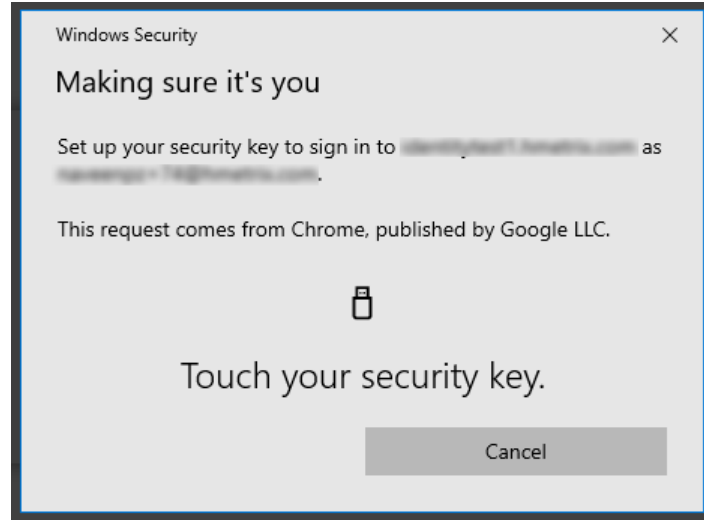
Step 1. After login to CRS portal, you will be redirected to OS security screen like the one below. You need to enter the pin and click OK button to continue.
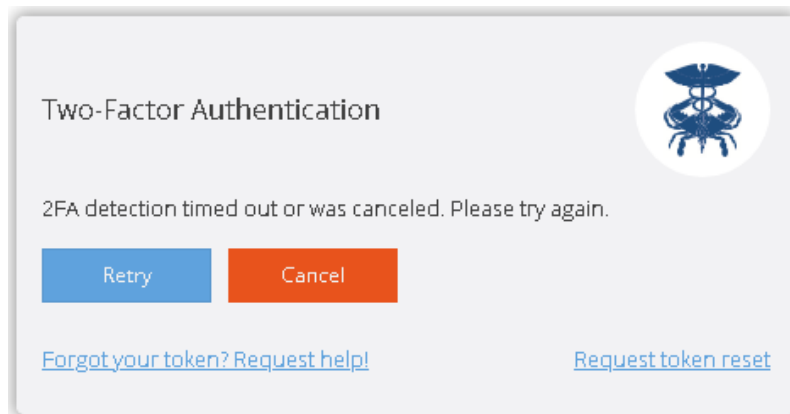
Step 2. You will be prompted with a screen below, where you need to touch the security key. If the token is valid then you will be redirected to CRS portal.

Step 3. If you like to send a suspend 2FA request or reset token request, click on the cancel button.

Step 4. You will be redirected to below screen where you have got the links for both options. Other than that, on clicking the Retry button you will be redirected to Step 1 and on clicking the Cancel button you will be redirected to the login screen.

Reset Phone Number or FIDO2 Token

If you need to reset your phone number or FIDO2 token, you may click on the 'Request phone number reset' or 'Request token 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 or FIDO2 token temporarily but require important reporting information from the CRS Portal, you may click on the 'Forgot your phone? Request help!' or 'Forgot your token? 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 ascertain that the request is legitimate. Once the request is 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.