

## How to Register a Device for MFA in the Zix Secure Email System

**Multi-Factor Authentication (MFA)** is another layer of security to protect your accounts from unauthorized users. This functionality requires a user to sign-in with a username and password, then confirm using a code sent to another device. These two layers of security make it more difficult for cybercriminals to access confidential data, because the criminal would need both your sign-in data AND the extra code from your device.

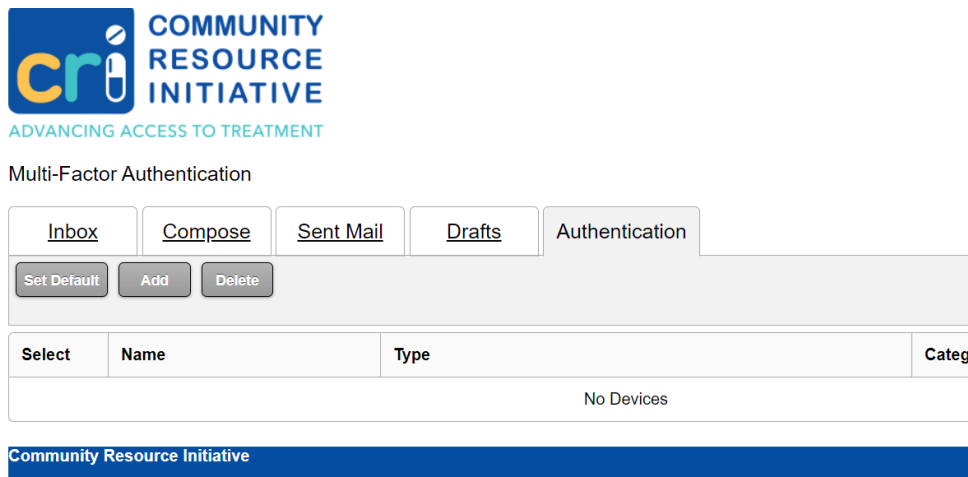
Although enabling MFA is optional, we strongly recommend that all users enable MFA for added email account security.

To set up and enable MFA on your email account, you will need a smart cellphone.

To use the Authentication App function, you will need to have an Authentication App like the “Microsoft Authenticator App”, or “Google Authenticator App” installed in advance. **The Zix Secure Email System does not have or provide its own proprietary authentication app.**

### Setting up MFA using your Phone’s Authentication App:

1. Click on this link to access CRI’s Zix secure email system.  
<https://web1.zixmail.net/s/welcome.jsp?b=crine> and proceed to sign in using your email and password.
2. Select the tab that states “**Authentication**”.



The screenshot shows the CRI Zix Secure Email System interface. At the top left is the CRI logo with the text "COMMUNITY RESOURCE INITIATIVE" and "ADVANCING ACCESS TO TREATMENT". Below the logo is the text "Multi-Factor Authentication". The interface features a navigation bar with tabs: "Inbox", "Compose", "Sent Mail", "Drafts", and "Authentication". The "Authentication" tab is selected. Below the navigation bar are buttons for "Set Default", "Add", and "Delete". A table with columns "Select", "Name", "Type", and "Categ" is shown, displaying "No Devices". The footer of the interface is a blue bar with the text "Community Resource Initiative".

3. Once you do, it will show you a **Register Multi-Factor Device** screen. A drop-down menu named “**Device Type**” will be there. “**Authentication App**” as a method to sign in. Select **Authentication App** and input a name for the device. Click **Next** to proceed.



#### Register Multi-Factor Device

This secure message portal requires multi-factor authentication. Register a multi-factor device. You can have multiple devices, but only one can be active at a time.

Device Type:

Authenticator Application

Name:

Cancel

Next

[Learn more](#) about receiving secure messages directly to your inbox.

For Customer Support, send an email message to [ITTeam@crihealth.org](mailto:ITTeam@crihealth.org).


We use cookies, find out why in our [cookie disclosure](#).

4. Scan the QR Code using your **Authentication App** or manually enter the generated key into your **Authentication App** and follow the directions provided by the app.



#### Register Device Cell Phone

Scan the QR Code or use the key with your authenticator application.



If setup using a QR Code is not supported, you may manually enter the following key:  
**KBIWVF3WHKGSCNDVKILVA7RSPPM7EESV**

Authentication Code:

Cancel

Next

5. Now whenever you sign in, you will get an authentication prompt using the **Authentication App**.