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 they 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 cellphone for both methods.

To use the Text Message (SMS) function to set up MFA, please follow the step-by-step instruction in the section about Text Message (SMS) on pages 1-2.

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.** To use your authentication application please follow the instructions in the section on pages 3-4.

**Setting up MFA using Phone Text Message (SMS)**

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



1. Once you do, it will show you a **Register Multi-Factor Device** screen. A drop-down menu named “**Device Type**” will be there. You can choose to use “Text Message (SMS)” or an Authentication App as a method to sign in. Select **Text Message (SMS)** and input a name and number for the device. Click **Next** to proceed.



1. Once you have clicked **Next**, you will be brought to an **Account Verification** screen. A **Verification Code** will have been sent via **Text Message (SMS)**, and you will need to input the code where it says **Verification Code**. Then select **Verify**.



1. Now whenever you sign in, you will get a **Verification Code** sent to your cell phone’s text, and you will need to put that **Verification Code** into the website to get in.

 **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**” and click the “Add” button.



1. Once you do, it will show you a **Register Multi-Factor Device** screen. A drop-down menu named “**Device Type**” will be there. You can choose to use “**Text Message (SMS**)” or “**Authentication App**” as a method to sign in. Select **Authentication App** and input a name for the device. Click **Next** to proceed.



1. 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. Remember, you must already have the Authenticator App installed on your phone (see page 1).



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