

স্মারক নম্বর: ১৩.০১.০০০০.০০০.১০০.৩১.০০২৩.২১.৪৩

তারিখ: ৬ ফাল্গুন ১৪৩২ বঙ্গাব্দ
১৯ ফেব্রুয়ারি ২০২৬ খ্রিস্টাব্দ

বিষয়: অফিসিয়াল ই-মেইল ব্যবহারের দিক-নির্দেশনা

সূত্র: ১। কম্পিউটার নেটওয়ার্ক ইউনিটের ২০/০৮/২০২৩ তারিখের ৪০১নং স্মারকের পত্র
২। বাংলাদেশ কম্পিউটার কাউন্সিল (বিসিসি)-এর ০৪/০২/২০২৬ তারিখের ই-মেইল।

উপর্যুক্ত বিষয় ও সূত্রস্থ (১)নং স্মারকের অনুবৃত্তিক্রমে জানানো যাচ্ছে যে, সাম্প্রতিককালে সরকারি অফিসিয়াল ই-মেইল ব্যবহার করে অ্যাকাউন্ট হ্যাকসহ বিভিন্ন প্রকার বেআইনি ও নৈতিক কর্মকান্ড পরিচালনা করার প্রবণতা লক্ষ্য করা হচ্ছে। একইসাথে সূত্রস্থ (২)নং স্মারকে বিসিসি কর্তৃক (ই-মেইলে) সতর্কতামূলক ব্যবস্থা হিসেবে নিয়মিত পাসওয়ার্ড পরিবর্তন এবং 2FA (Two Factor Authentication) ব্যবহার করার নির্দেশনা প্রদান করা হয়। এফগে, খাদ্য অধিদপ্তরের সকল কার্যালয়কে অফিসিয়াল ই-মেইল ব্যবহার-এ বিসিসি'র ইউজার-গাইডসহ (Self-Service Account Recovery&2FA) নিম্নরূপ দিক-নির্দেশনা প্রদান করা হলো:

১. অফিসিয়াল ই-মেইল অ্যাকাউন্ট শুধুমাত্র দাপ্তরিক কাজে ব্যবহার করতে হবে;
২. কোনো অবস্থাতেই অফিসিয়াল ই-মেইল এর পাসওয়ার্ড অন্য কারও সাথে শেয়ার করা যাবে না;
৩. **শক্তিশালী পাসওয়ার্ড** ব্যবহার ও নিয়মিত পাসওয়ার্ড পরিবর্তন করতে হবে। শক্তিশালী পাসওয়ার্ডের জন্য নিম্নের **Criteria** অনুসরণ করতে হবে:
 - Minimum of 8 characters
 - Includes both uppercase and lowercase letters (A-Z, a-z)
 - Contains at least one number (0-9)
 - Includes special characters (e.g., !, @, #, \$, %, ^, &, *)
৪. অচেনা বা বহিরাগত প্রেরকের কাছ থেকে প্রাপ্ত **লিংক বা সংযুক্তি (Attachment)** খোলার ক্ষেত্রে সর্বোচ্চ সতর্কতা অবলম্বন করতে হবে;
৫. কোনো **সন্দেহজনক বা ফিশিং ই-মেইল** ফরওয়ার্ড করা যাবে না; তাৎক্ষণিকভাবে ই-মেইল সাপোর্ট **টিম** অথবা datacenter@bcc.gov.bd ঠিকানায় রিপোর্ট করতে হবে;
৬. একান্ত প্রয়োজন ছাড়া বড় আকারের ফাইল সংযুক্ত করে ই-মেইল প্রেরণ এড়িয়ে চলতে হবে; প্রয়োজ্য ক্ষেত্রে অনুমোদিত ফাইল শেয়ারিং মাধ্যম ব্যবহার করতে হবে;
৭. অফিসিয়াল ই-মেইল আইডি ব্যবহার করে **ব্যক্তিগত নিবন্ধন, সাবস্ক্রিপশন বা সামাজিক যোগাযোগ মাধ্যমে** অ্যাকাউন্ট খোলা থেকে বিরত থাকতে হবে;
৮. শেয়ারড বা পাবলিক ডিভাইস ব্যবহার করে ই-মেইল অ্যাক্সেস করলে কাজ শেষে অবশ্যই **লগআউট** করতে হবে;
৯. ই-মেইল অ্যাকাউন্ট অধিকতর নিরাপদ করার লক্ষ্যে নিম্নোক্ত উপায়ে **Recovery Email** সেট করতে হবে;
Navigate to: **Login > Settings > Account Recovery > Add Recovery Email > Enter Verification Code from Recovery Email > Verified > Save**
১০. খাদ্য অধিদপ্তরের প্রত্যেক কার্যালয়ের সকল কর্মকর্তা/কর্মচারীর সমন্বয়ে **Cyber Security** বিষয়-এ কম্পিউটার নেটওয়ার্ক ইউনিটের সহায়তায় কমপক্ষে ২ (দুই) ঘণ্টার অনলাইন ট্রেনিং-এর আয়োজন করতে হবে।

এ অবস্থায়, খাদ্য অধিদপ্তরাধীন সকল কার্যালয় প্রধানকে দাপ্তরিক যোগাযোগের ক্ষেত্রে উপরের নির্দেশাবলি অনুসরণপূর্বক দাপ্তরিক (Official) ই-মেইল একাউন্ট ব্যবহার করার জন্য নির্দেশক্রমে অনুরোধ করা হলো।

এতে যথাযথ কর্তৃপক্ষের অনুমোদন রয়েছে।

সংযুক্তি: বিসিসি'র-মেইল, Self-Service Account Recovery & 2FA

সংযুক্তিসমূহঃ

- (১) Self-Service Account Recovery
- (২) Two-Factor Authentication (2FA)
- (৩) বিসিসি-এর ০৪-০২-২০২৬ তারিখের ই- মেইল



১৯-০২-২০২৬

মোঃ আনিসুর রহমান
প্রোগ্রামার

ফোন : +৮৮-০২-৪১০৫২৯৯৭

ইমেইল : sys@dgfood.gov.bd

বিভরণ (জ্যেষ্ঠতার ক্রমানুসারে নয়):

- ১। মহাপরিচালক (অতিরিক্ত দায়িত্ব), মহাপরিচালকের দপ্তর, খাদ্য অধিদপ্তর।
- ২। অতিরিক্ত মহাপরিচালক (চলতি দায়িত্ব), অতিরিক্ত মহাপরিচালকের দপ্তর, খাদ্য অধিদপ্তর।
- ৩। পরিচালক, প্রশাসন/সববি/চসসা/হিসাব ও অর্থ/সংগ্রহ/পটকা/প্রশিক্ষণ বিভাগ, খাদ্য অধিদপ্তর, ঢাকা।।
- ৪। আঞ্চলিক খাদ্য নিয়ন্ত্রক, ঢাকা/চট্টগ্রাম/খুলনা/রংপুর/রাজশাহী/বরিশাল/সিলেট/ময়মনসিংহ।
- ৫। সাইলো অধীক্ষক (সকল)।
- ৬। অতিরিক্ত পরিচালক, অভ্যন্তরীণ নিরীক্ষা বিভাগ, খাদ্য অধিদপ্তর।
- ৭। অতিরিক্ত পরিচালক (চলতি দায়িত্ব), এমআইএসএন্ডএম বিভাগ, খাদ্য অধিদপ্তর।
- ৮। জেখানি।
- ৯। চলাচল ও সংরক্ষণ নিয়ন্ত্রক (সকল)।
- ১০। উখানি (সকল).....।
- ১১। ব্যবস্থাপক (সকল)..... এবং
- ১২। ভারপ্রাপ্ত কর্মকর্তা (সকল).....।

স্মারক নম্বর: ১৩.০১.০০০০.০০০.১০০.৩১.০০২৩.২১.৪৩/১ (১)

তারিখ: ৬ ফাল্গুন ১৪৩২ বঙ্গাব্দ
১৯ ফেব্রুয়ারি ২০২৬ খ্রিস্টাব্দ

সদয় জ্ঞাতার্থে/জ্ঞাতার্থে (জ্যেষ্ঠতার ক্রমানুসারে নয়):

মহাপরিচালকের একান্ত সচিব, মহাপরিচালকের দপ্তর, খাদ্য অধিদপ্তর [মহাপরিচালক মহোদয়ের সদয় অবগতির জন্য]।



১৯-০২-২০২৬

মোঃ আনিসুর রহমান
প্রোগ্রামার

You are viewing an attached message. Actions are disabled.

Awareness on the Benefits of regular password change

Data Center <datacenter@bcc.gov.bd>

02/04/2026, 4:57 PM

Dear Valued Users,

To ensure the **security of your official email account** and protect it from unauthorized access, all users are advised to **change their email passwords regularly**.

Benefits of regular password change:

- Helps prevent **unauthorized access**
- Reduces the risk of **account compromise**
- Protects your account if a password is **accidentally exposed**
- Strengthens overall **email security**

Password best practices:

- Use a **strong and unique password**
- Avoid reusing previous passwords
- Do not share your password with anyone
- Change your password immediately if you suspect any unusual activity
- Ensure your password meets the following criteria:
 - Minimum of **8 characters**
 - Includes both **uppercase and lowercase letters** (A–Z, a–z)
 - Contains at least **one number** (0–9)
 - Includes **special characters** (e.g., !, @, #, \$, %, ^, &, *)

Enhance your account security by enabling Account Recovery:

Navigate to: *Login > Settings > Account Recovery > Add Recovery Email > Enter Verification Code from Recovery Email > Verified > Save*

Regular password updates and configuring account recovery are **simple but highly effective steps** to keep your account and official information secure.

If you need any assistance, please contact your **Email Support Team** or email us at datacenter@bcc.gov.bd.

Thank you for your cooperation.

Regards

National Data Center Operation Team
Bangladesh Computer Council (BCC)
Phone: +88 02 55006840

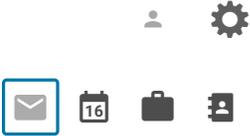
2 Attachments | [Download All](#)



2. Zimbra Passwor... .pdf
730.3 KB



2. Zimbra Passwor... .pdf
730.3 KB



mail

Inbox 41 ...

Drafts ...

Sent ...

Archive ...

Spam 9 ...

Trash ...

+ Add a folder

Tags +

User Guide
for
Self-Service Account Recovery of an Email Account

National Data Center
Bangladesh Computer Council (BCC)

Account Recovery:

1. In the Zimbra Web Client (Modern UI), go to **Settings > Accounts > Account Recovery** and enter a password recovery email address.

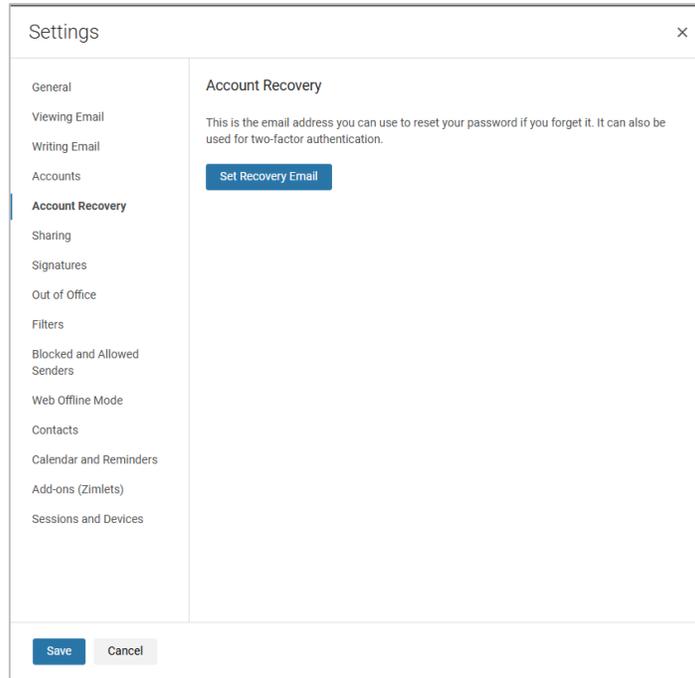


Figure 1. Account Recovery

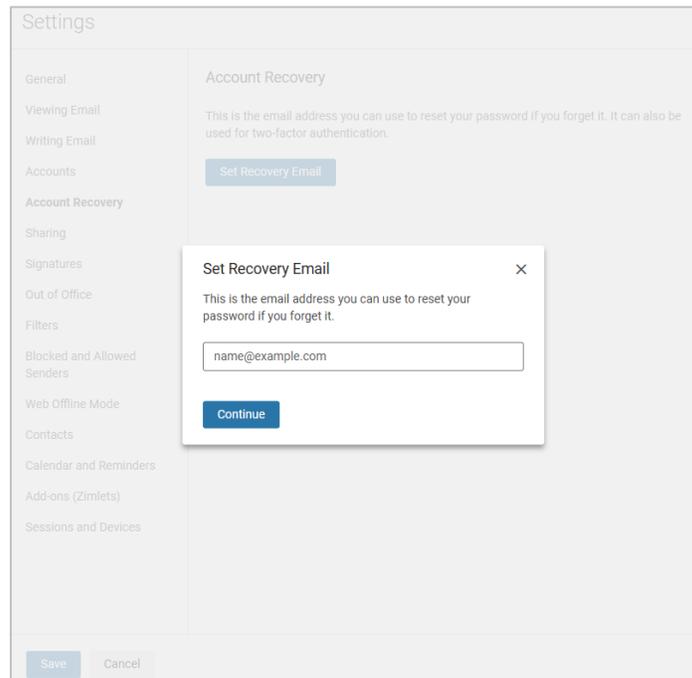


Figure 2. Recovery Email Setting

2. You will receive an email at that address with a **verification code**. Enter the verification code.

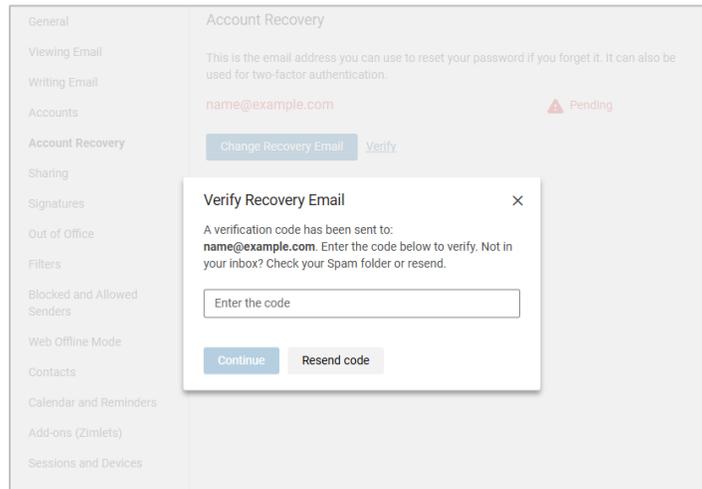


Figure 3. Verification Code Setting

3. Now, if you forget your password, then go to login URL and click on **Forgot Password**.

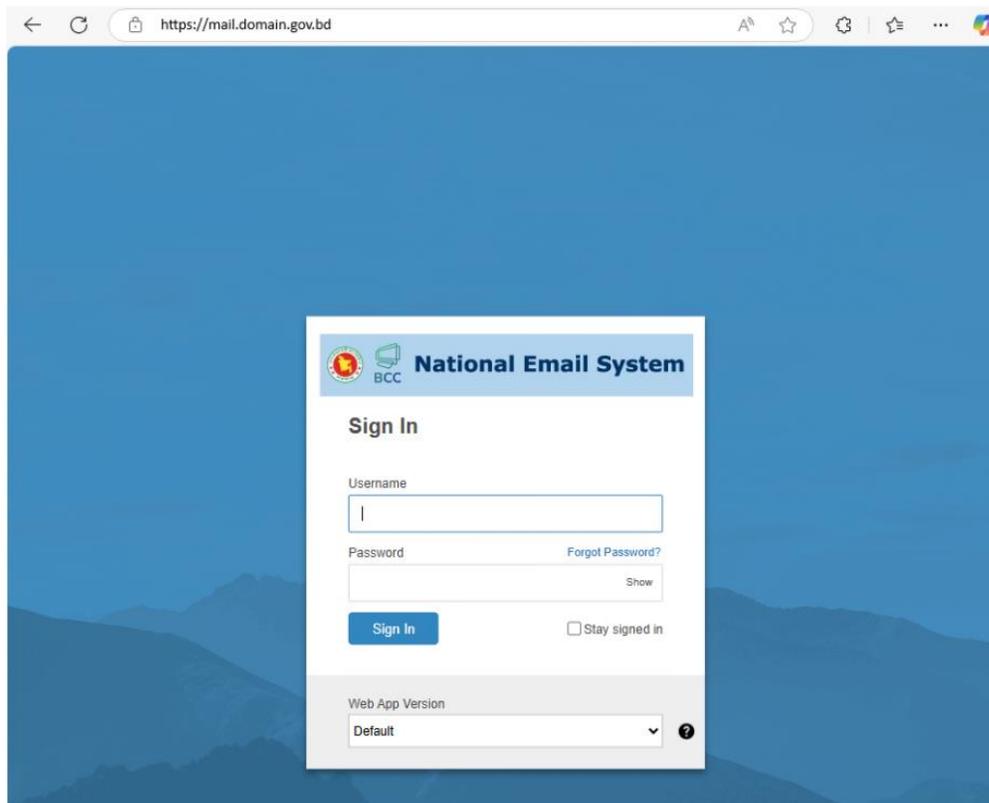


Figure 4. Login page of Email

4. Enter the **Full Email Address** of the account you are trying to recover, then click the "**Submit**" button.

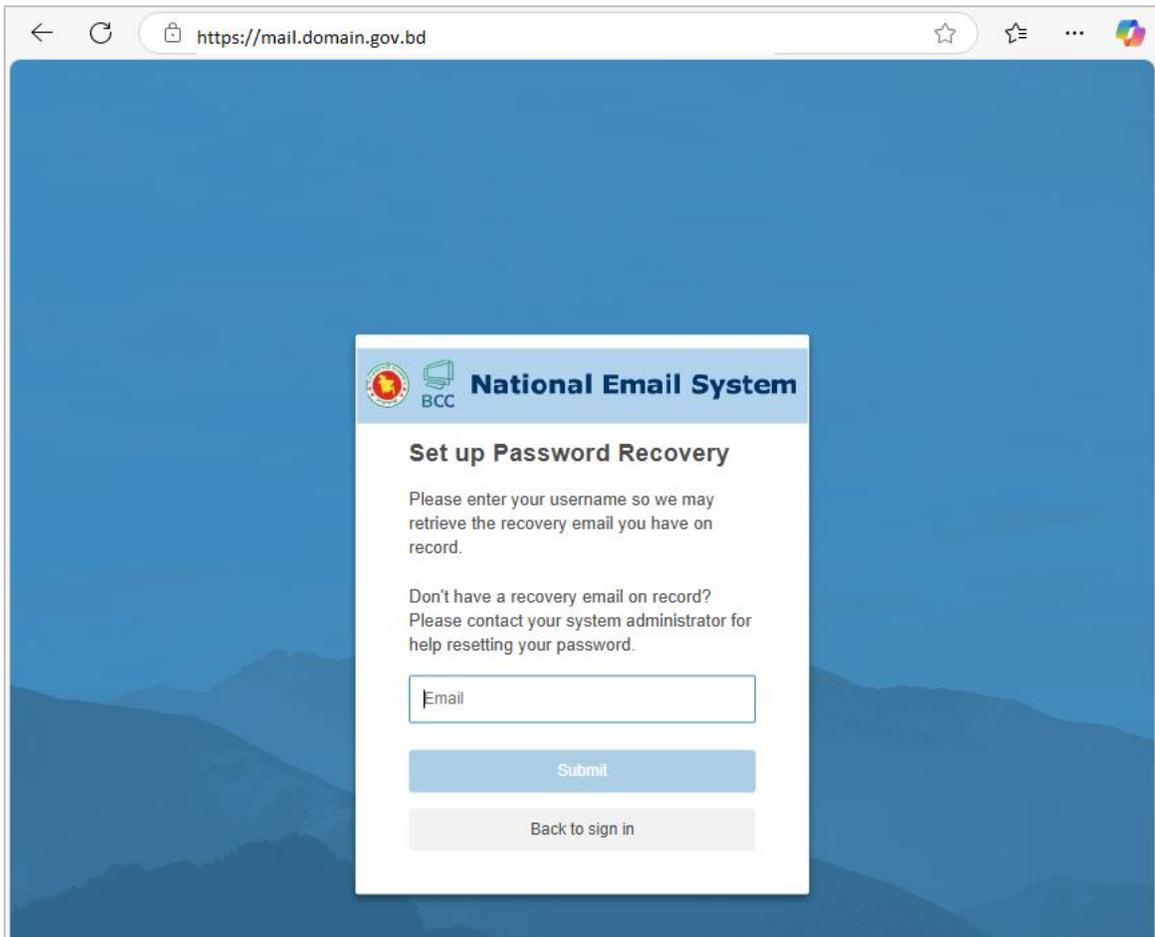


Figure 5. Password Recovery page of Email

5. Click the **Request Code** button at the bottom of the box. This will send a code to your recovery email address. Like the verification code, this reset code is only valid for 10 minutes.

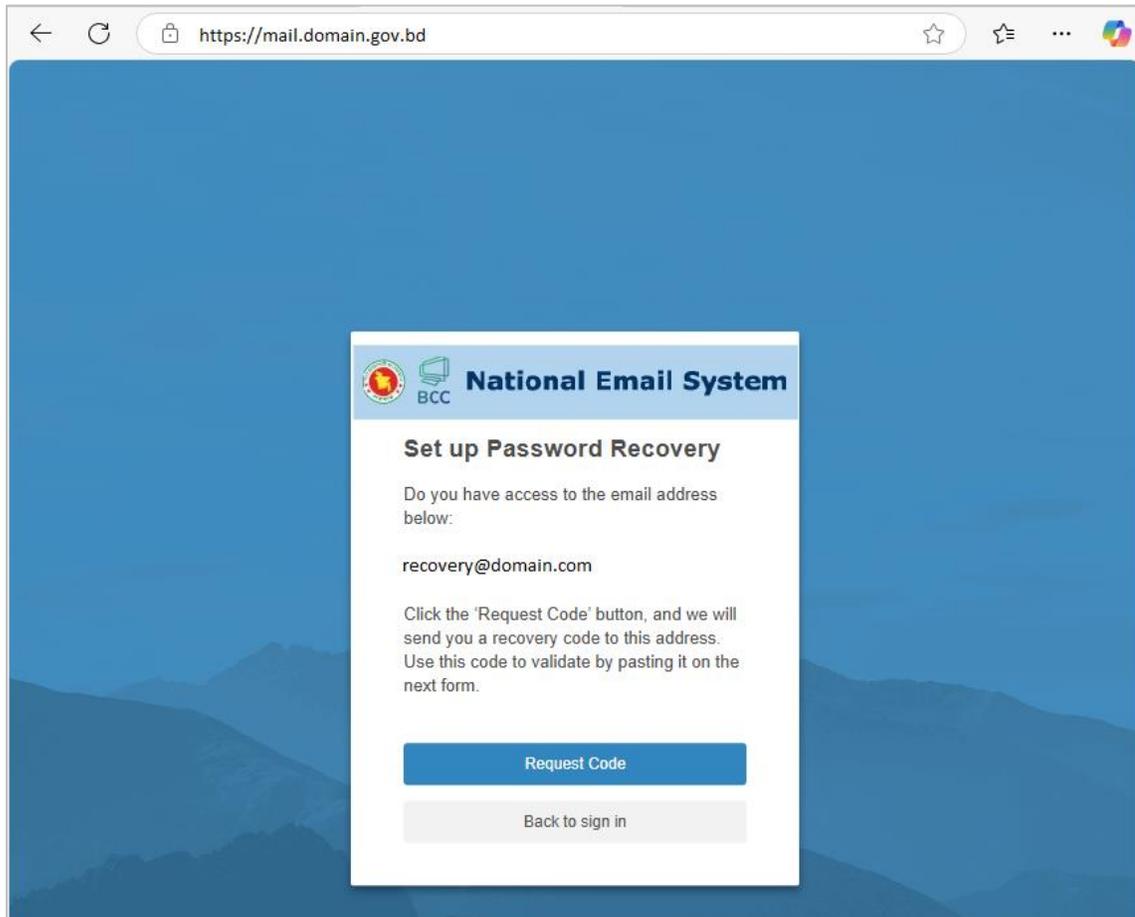


Figure 6. Request Code for Password Recovery of Email

6. Open that address mailbox and retrieve the reset code which you will enter on the Email recovery form. The email will look like this:



Figure 7. Sample email of Password recovery code

7. Go back to the Email recovery form, and enter the reset code within 10 minutes of clicking the **Request Code** button from the previous page. Then click the **Verify Code** button.

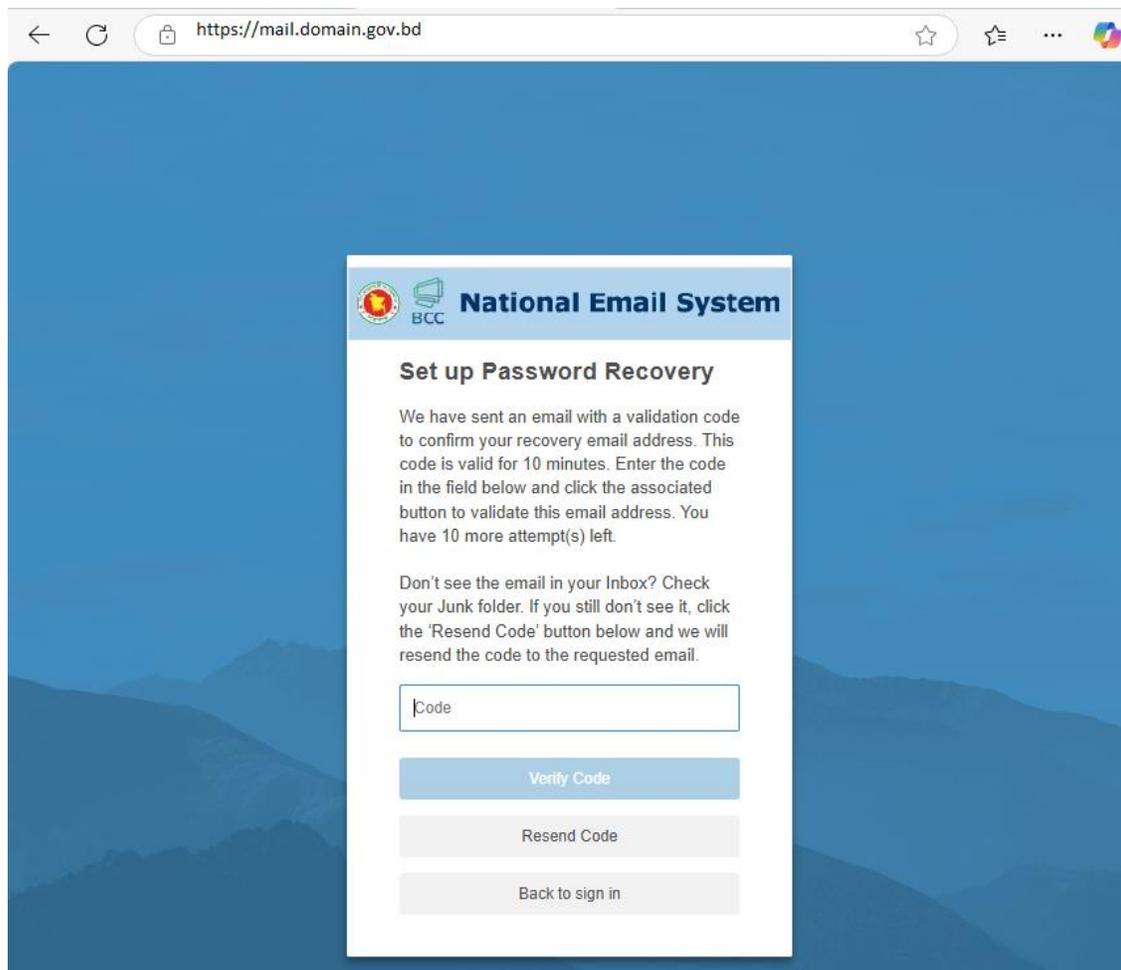


Figure 8. Email Recovery Form

8. Now, you can either choose to log into the web client directly, or you can choose to reset your password. We'll want to choose "**Reset Password**".

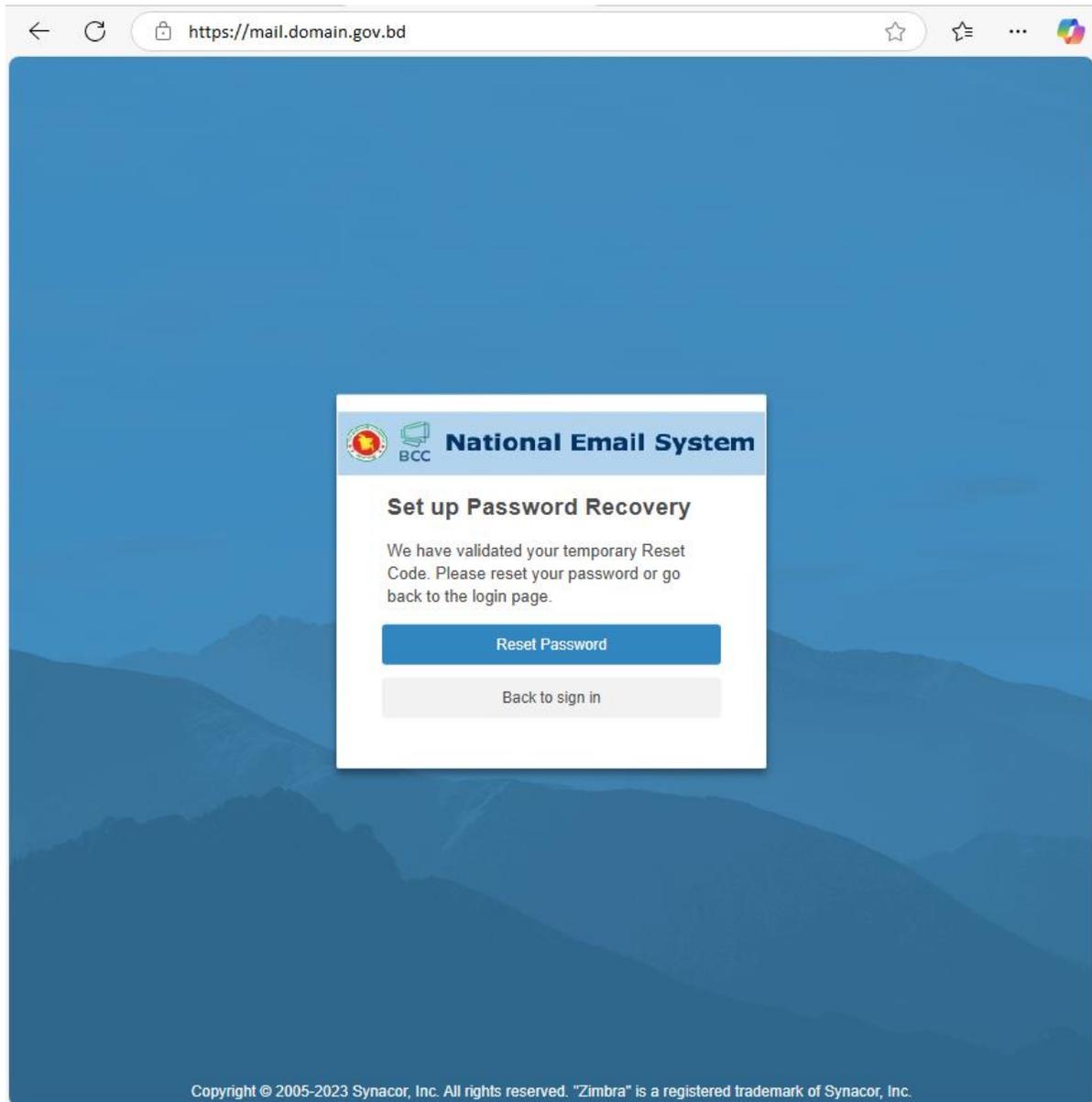
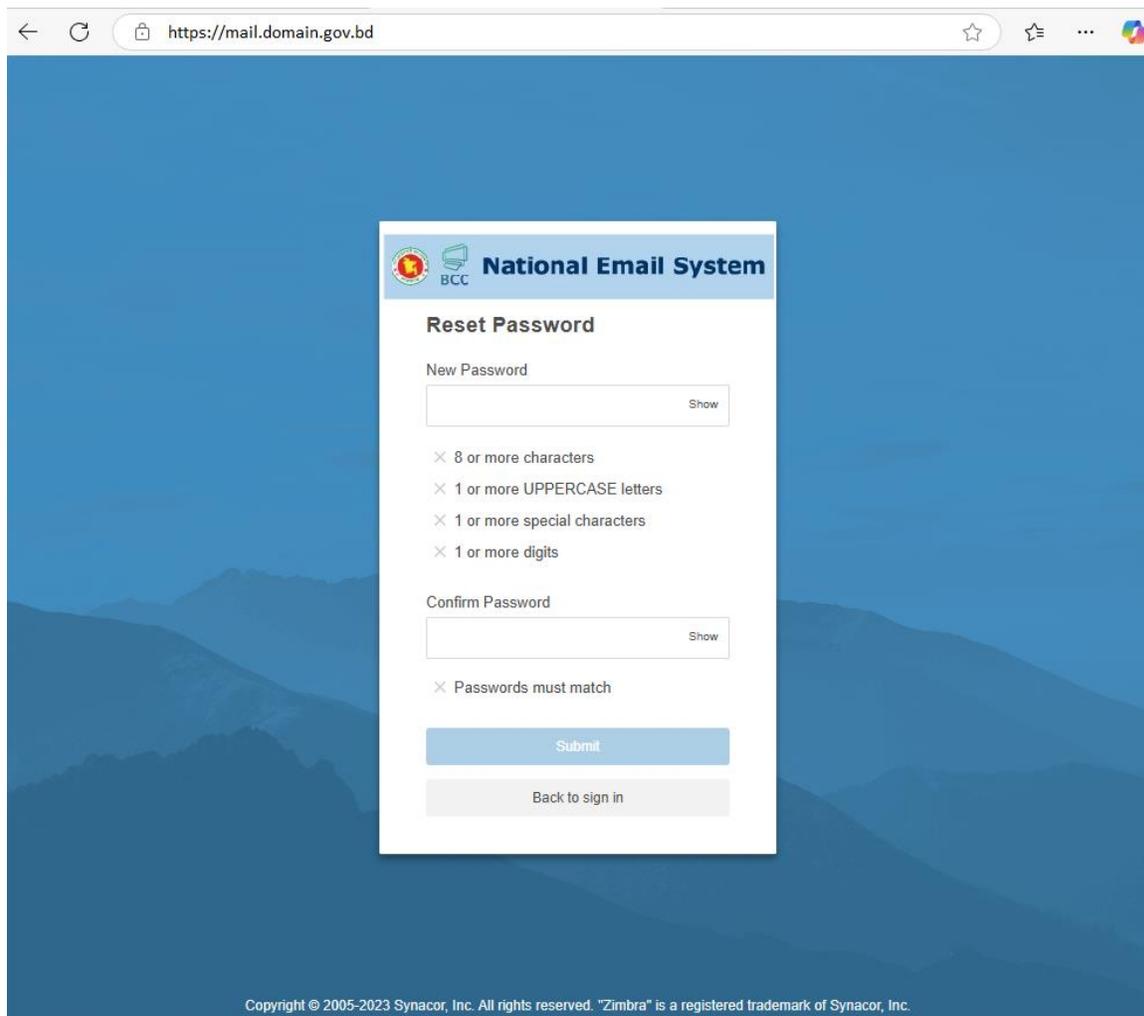


Figure 9. Password Recovery page of Email

9. At this point, you will be prompted to establish a new password.



The screenshot shows a web browser window with the address bar displaying "https://mail.domain.gov.bd". The main content area features a blue background with a mountain range. In the center, there is a white form titled "National Email System" with the BCC logo. The form is titled "Reset Password" and contains the following elements:

- A "New Password" input field with a "Show" button.
- Four validation rules, each with a red 'X' icon:
 - × 8 or more characters
 - × 1 or more UPPERCASE letters
 - × 1 or more special characters
 - × 1 or more digits
- A "Confirm Password" input field with a "Show" button.
- A validation rule: × Passwords must match
- A blue "Submit" button.
- A grey "Back to sign in" button.

At the bottom of the page, there is a copyright notice: "Copyright © 2005-2023 Synacor, Inc. All rights reserved. 'Zimbra' is a registered trademark of Synacor, Inc."

Figure 10. Set New Password

Note: Always create new secure passwords, never re-use passwords from other sites as they are likely compromised.

Once you have entered and confirmed your new password, click the "**Submit**" button to set it.

**User Guide
for
Two-Factor Authentication (2FA) of Email**

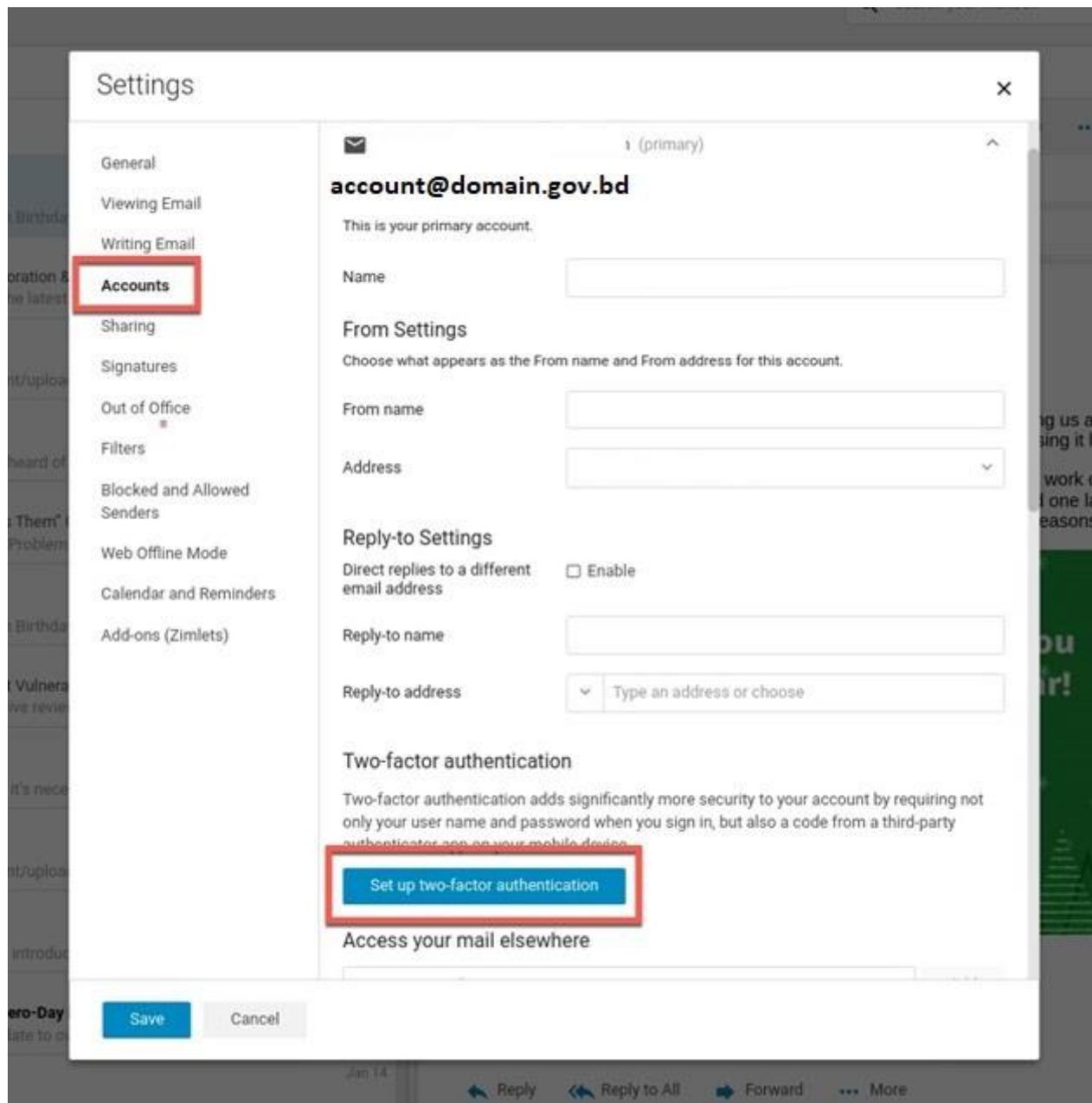
National Data Center
Bangladesh Computer Council (BCC)

Two-Factor Authentication (2FA)

With 2FA enabled, you use your password and a code generated on your smartphone to log into your Zimbra account.

Enabling 2FA is easy. You'll need access to your Email account and your smartphone to complete the 2FA setup.

1. In this system, click the gear menu.
2. Choose Settings > Accounts.
3. Select your account and click the Set up **two-factor authentication**.



4. Enter your email password.
5. Click Set up two-factor authentication.

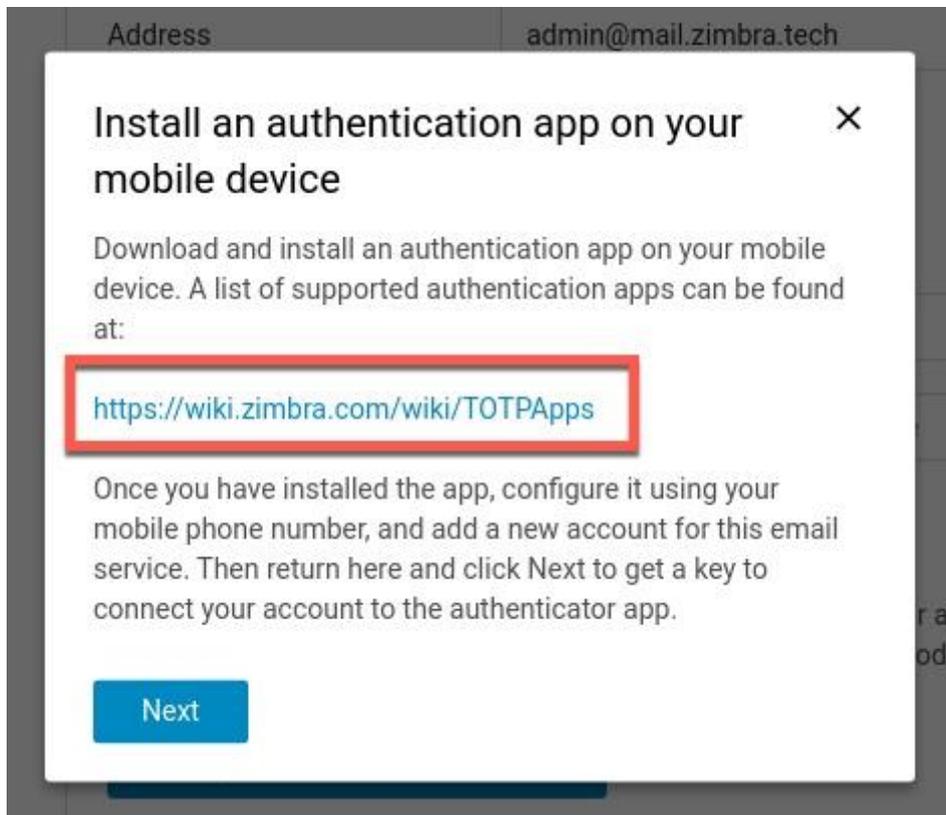
Two-factor authentication

Two-factor authentication adds significantly more security to your account by requiring not only your user name and password when you sign in, but also a code from a third-party authenticator app on your mobile device.

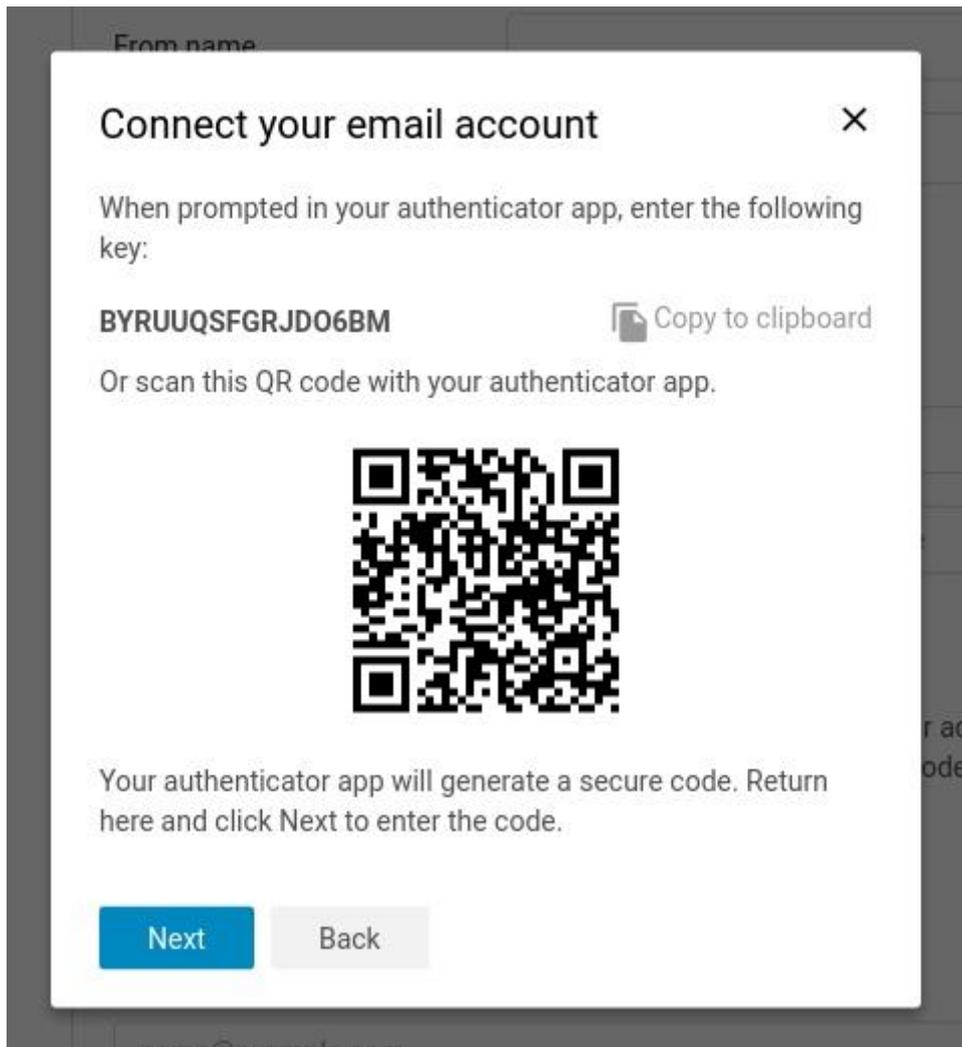
[Set up two-factor authentication](#)

The next steps require your smartphone.

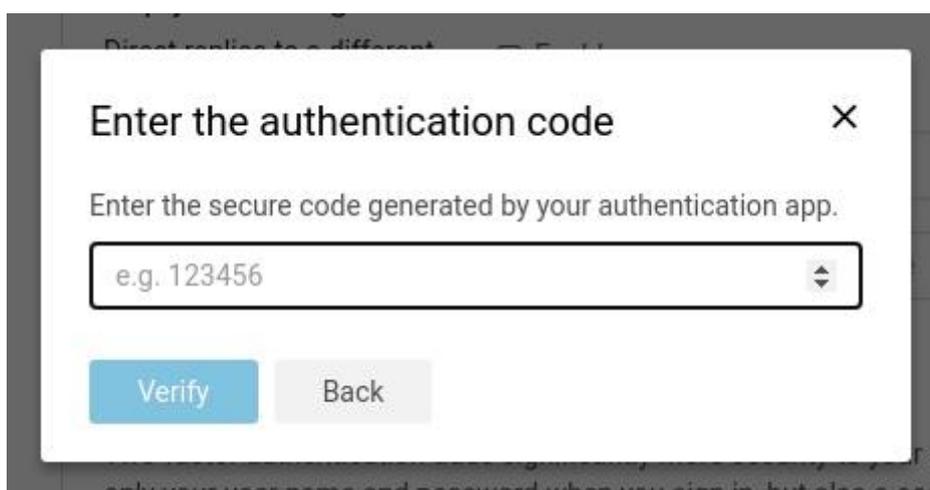
6. Click the URL to see the authentication applications available for your smartphone. Download the authentication application and install it on your smartphone. Click next.



7. Scan the code on the screen using the authentication app on your smart phone. Click Next.



8. Enter the code provided on your smartphone. Click Verify to complete 2FA setup.

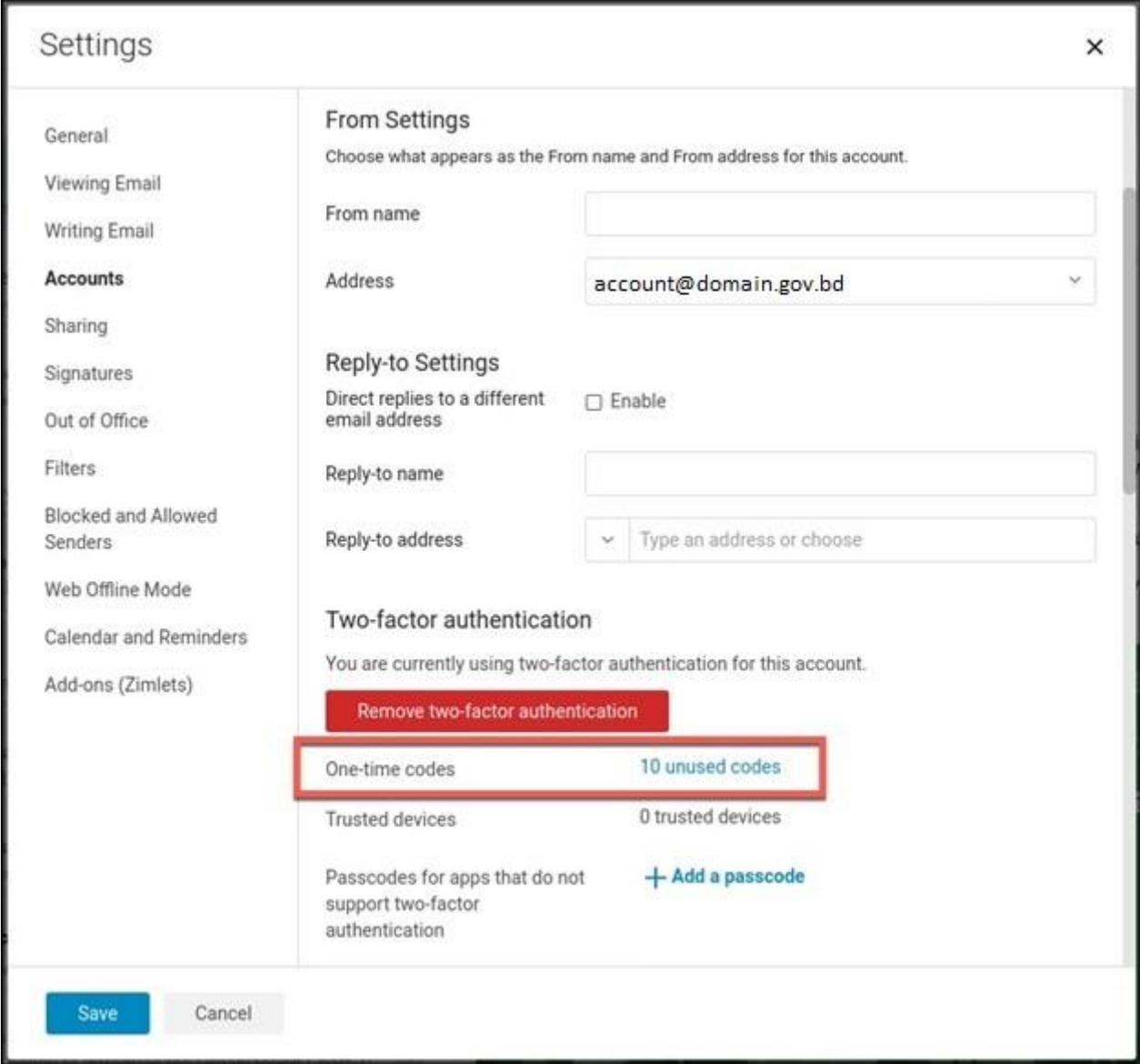


Success ... You enabled 2FA for your Zimbra account!

Now, when you log into your Email account, you will be prompted for a new code from the authentication app on your phone.

What if you don't have your phone, or what if your phone runs out of batteries?

You have 10 one-time codes to use if you don't have your phone available. Just click the **"10 unused codes"** link and print the 10 codes. Keep the codes handy, so they're available when you need them.



Note: If you don't see the **Set up two-factor authentication** option in your Email Preferences, your organization hasn't enabled the 2FA feature. Please contact your System Administrator or email service provider for more information.