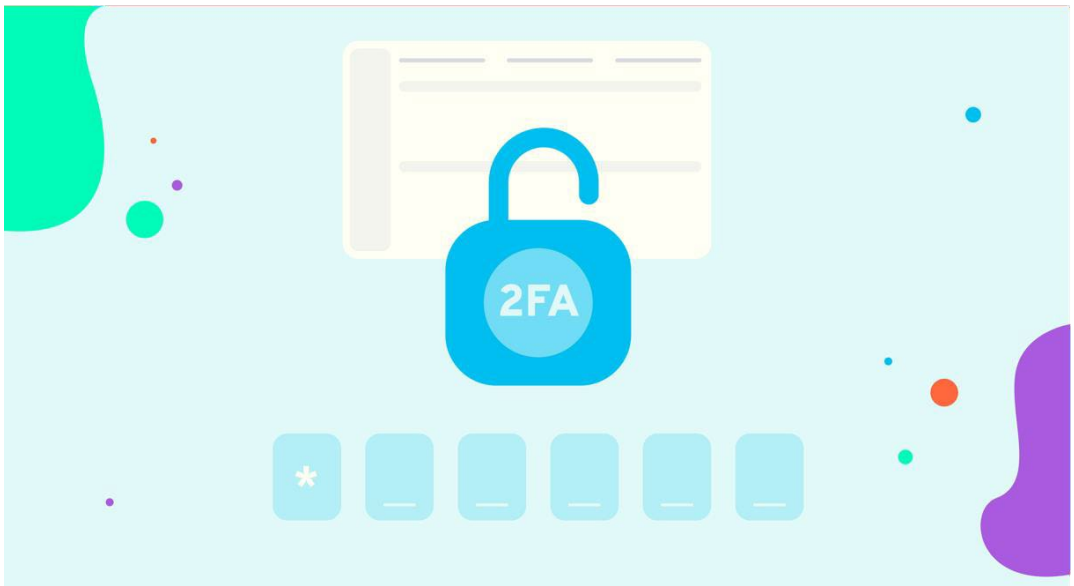
Two Factor Authentication

Pinnacle

Guide for Two–Factor Authentication

What is Two-factor Authentication (2FA)?

Two-factor Authentication (2FA) is an extra layer of security to protect critical information, like your online accounts. Every time you log into an account with a password and receive a verification code via email to verify your identity, you are using 2FA. It means that, in addition to your password, you need a second credential to confirm your identity before logging in.



How does Two-factor Authentication (2FA) work?

When users attempt to log into an account that uses 2FA, they first enter their username and password as usual. The system then generates a one-time code and sends it to the user's email. The user then enters the code in addition to their password to confirm their identity and gain access to the account.

This process makes it much more difficult for an unauthorized person to access the account, as they need both the password and the second factor. Using 2FA, organizations and individuals can increase the security of their sensitive information and help prevent data breaches and hacking attempts.

What are the benefits of implementing 2-factor Authentication?

1. Increased security: 2FA provides an extra layer of protection by requiring a second form of identification and a password. The secondary request makes it much more difficult for an unauthorized person to access the account.
2. Prevention of hacking attempts: 2FA helps prevent hacking attempts, as an attacker would need both the password and the second factor to access the account.

3. Easy to use: 2FA is easy to set up and use and does not require technical expertise.
4. Peace of mind: By using 2FA, individuals and organizations can know that their sensitive information is better protected.

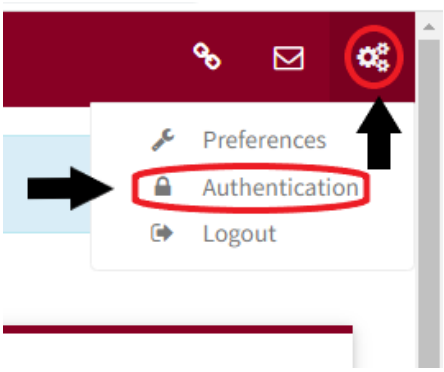
Overall, 2FA provides a simple and effective way to increase the security of online accounts and sensitive information.

How to activate Dnet 2-Factor Authentication on your account

Email Authentication:

To enable Email authentication:

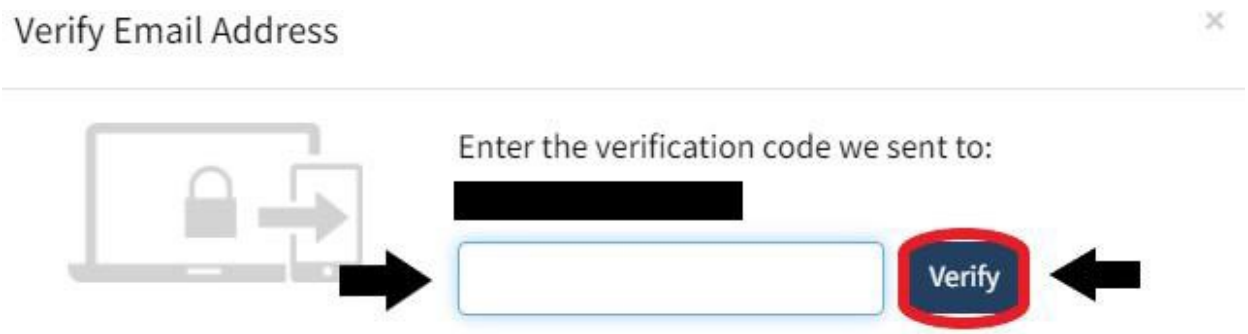
1. First, click on the gears icon on the upper right side of the dashboard and click on 'Authentication' from the drop-down menu.



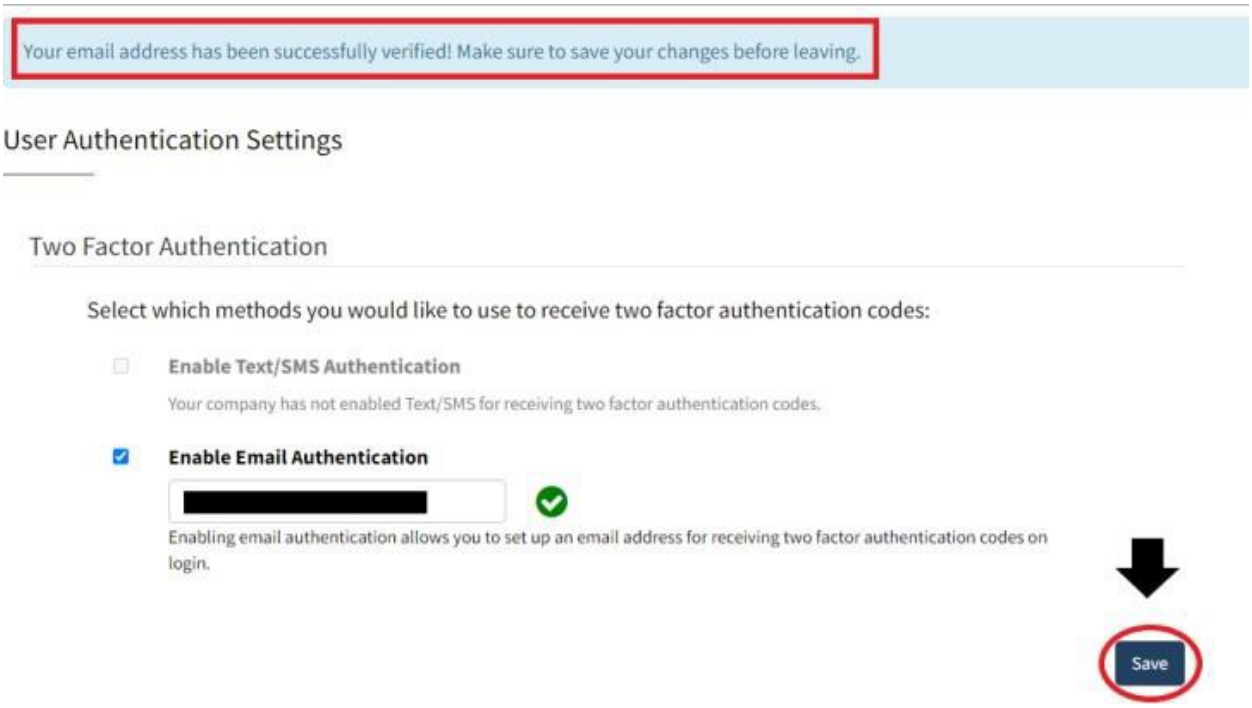
2. Next, mark the checkbox next to '**Enable Email Authentication'.**

3. Then, enter your email address in the box provided and select Verify.

4. A prompt will appear asking to verify your email address. When you click 'Verify', a system-generated, 6-digit code will be sent to the email address you input. To do this, enter the 6-digit code sent to your email and select 'Verify'.



5. Once completed, a message will indicate that your email was successfully verified. You may now click the 'Save' button on the bottom right corner to save your changes.



6. After saving your changes, the next time you sign in, you will be prompted first to enter your authentication code,

signing in with 2-Factor Authentication Enabled (Email)

1. After setting up your 2-Factor Authentication, the next time you sign in, you will receive a prompt for a verification code sent to your email, depending on which type of Authentication you currently have enabled. Enter your code in the field provided and select **Verify**. Once done, you will be logged into Dnet and can use it as you usually would.

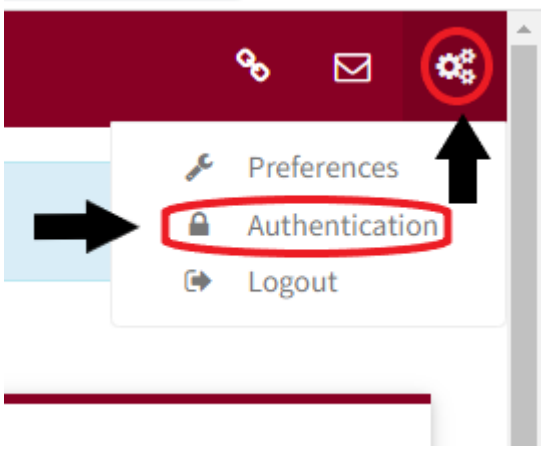
NOTE: If you don't want a prompt for this code every time you log in, and you are using a trusted device on which no one else will attempt to log in with your credentials, you can mark the checkbox to ***'Trust this device'.***

2. If you need to have your code resent, you can select the **'Re-send my code'** link, and you will receive another email with your code.

After you click the 'send my code via email' link, your verification code will be re-sent to your provided email address. Once received, enter your verification code into the field provided and select **'Verify'**.

Disabling 2-Factor Authentication for Your User

1. Suppose you no longer want to use 2-Factor Authentication. In that case, you can disable it from the **Authentication** settings by selecting the gears icon and choosing '**Authentication'** from the drop-down menu.



2. Next, Uncheck the box(es) next to the authentication type you wish to disable.