

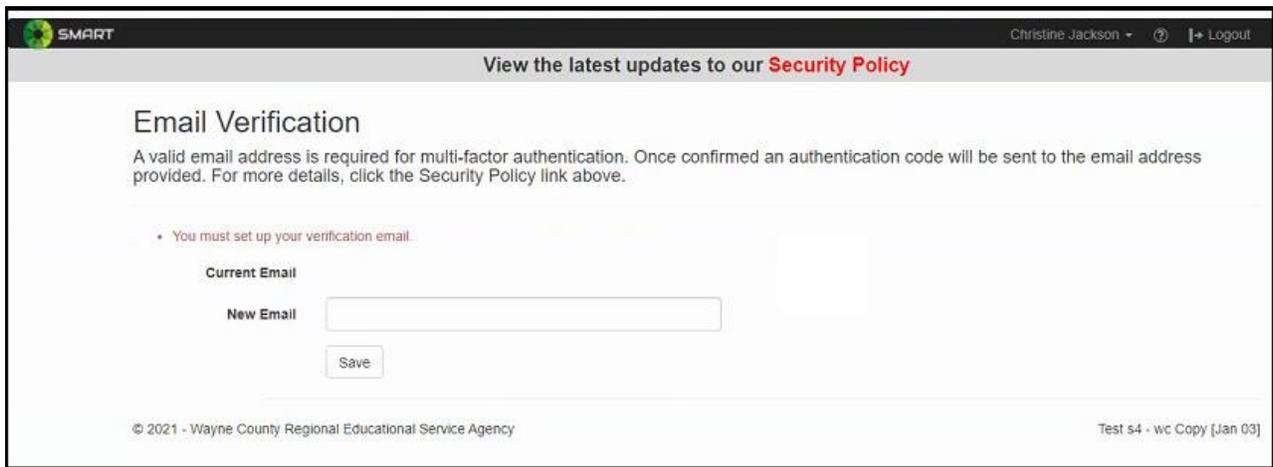
Steps for Authenticating

Why Am I Being Prompted to Authenticate?

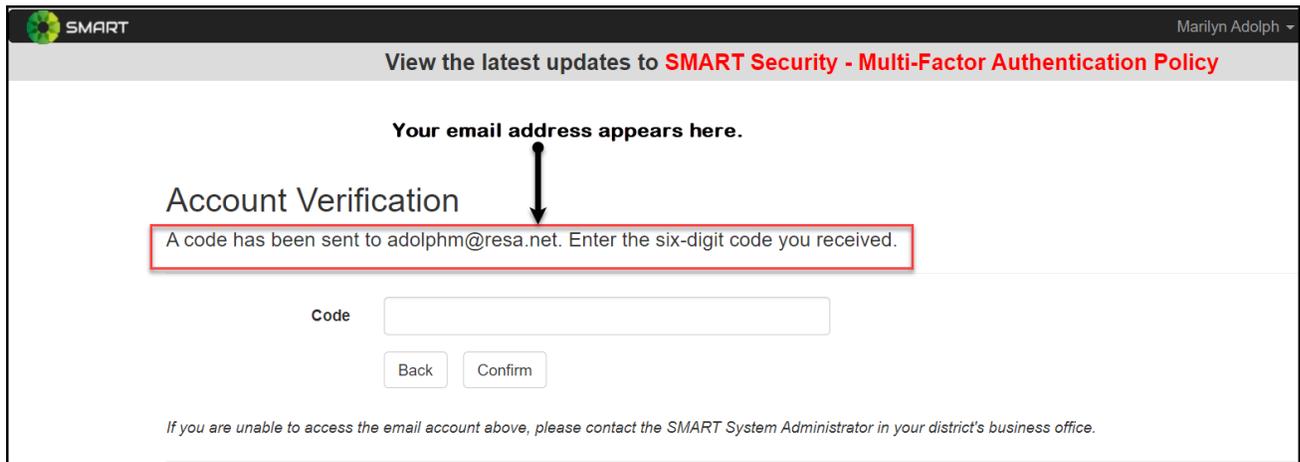
Beginning 7/1/21, Wayne RESA implemented Multi-Factor Authentication in SMART. For more details about what is Multi-Factor Authentication click [here](#). **If you would like to watch a video on how to authenticate in SMART, click [here](#).**

How Do You Authenticate?

1. Go to **smart.resa.net**. The first time you authenticate, SMART will ask you to set up a verification email. Enter your email address in the **New Email field** and click the **Save** button. The email address may be a personal or work email address. A verification code will be sent to the email address you entered.

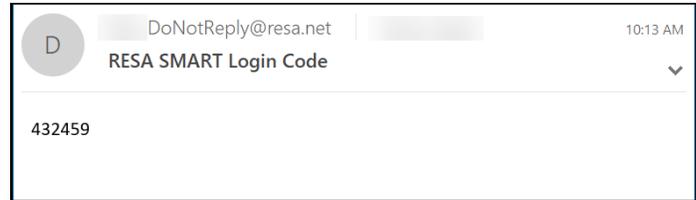


2. The next prompt will appear asking for the verification code. This prompt displays the email address entered on the previous screen. **If this address is not correct, see [Question 3](#) for more assistance.**

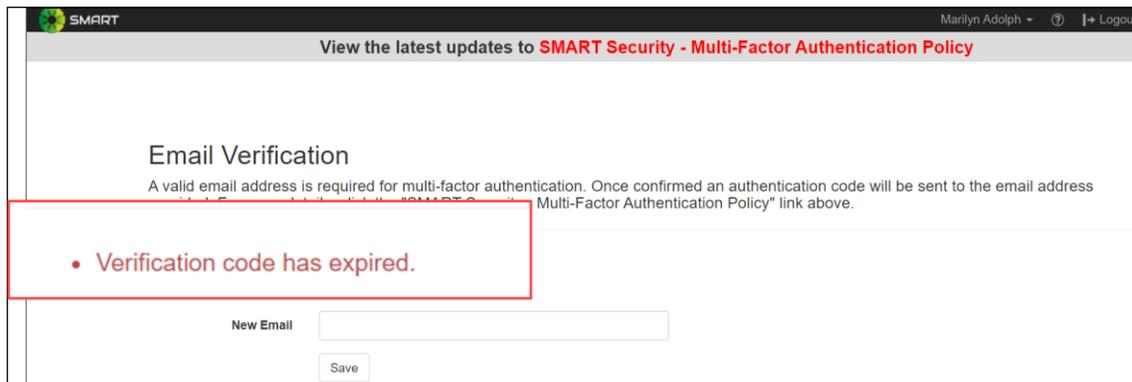


Steps for Authenticating

- Go to your email used to authenticate. Look for an email from donotreply@resa.net in your inbox. The email message will look similar to the image below.



- Enter the code from your email in the **Code field** and click the **Confirm** button. Once confirmed, you will be successfully logged into SMART.
- The authentication code expires after 3 minutes.** If you don't enter the code within 3 minutes, you will receive an error message, **Verification code has expired**. You will need to start the process over by entering your email address.



Steps for Authenticating

How Often Do I Authenticate?

You will only be prompted to authenticate once per day per Internet browser and/or device.

The next time you authenticate, SMART will display a prompt asking you to authenticate. A masked version of the email address is included in the message. The code will be sent to the email address displayed. ***If you no longer have access to this email address or don't recognize the email address, please see [Question 3](#) for assistance.***

Questions & Answers

Question 1: What if I enter the wrong email address when authenticating for the first time?

Answer: You can change the email address by clicking the **Back** button below the **Code** field and entering a new email address. See image below.

Steps for Authenticating

Question 2: What if I accidentally close the browser tab/window before entering the authentication code?

Answer: Go back to smart.resa.net. Since you have not completed authentication, SMART will prompt you again to enter an email address.

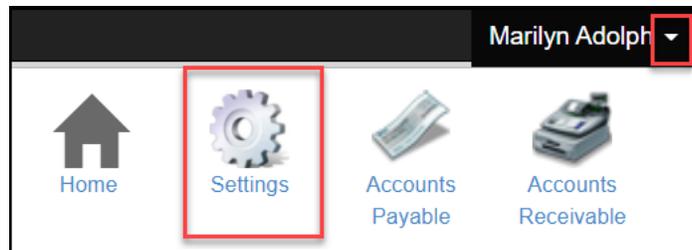
Question 3: What if I no longer have access to the email address I used previously?

Answer: Contact your SMART Security Administrator, they can provide you with the email address on file for Multi-Factor Authentication (MFA) and change the email address if necessary. If you aren't sure who the SMART Security Administrator is in your district, contact your district's business office for guidance.

Question 4: Can I change the email address used for authentication?

Answer: Yes, you have the ability to change the email address used for authentication. Follow the steps below after logging into smart.resa.net.

1. Follow the authentication steps if prompted.
2. Next, go to the menu and select **Settings**.



3. Click the link labeled **Change your email**.

Edit Profile

Change your account settings.

Password: [\[Change your password\]](#)
Security Question: [\[Update Security Question\]](#)
Email: [\[Change your email\]](#)

Steps for Authenticating

4. Enter a **new email address** and click the **Save** button.

Email Verification

A valid email address is required for multi-factor authentication. Once confirmed an authentication code will be sent to the email address provided. For more details, click the "SMART Security - Multi-Factor Authentication Policy" link above.

Current Email adolphm@resa.net

New Email

5. SMART will need to authenticate using the new email address. Follow the steps to authenticate.

Account Verification

A code has been sent to marilynmvick@gmail.com. Enter the six-digit code you received.

new email address

Code

If you are unable to access the email account above, please contact the SMART System Administrator in your district's business office.

6. A message displays confirming your email address has been changed.

Edit Profile

Your email has been changed.

Change your account settings.

Password: [\[Change your password\]](#)
Security Question: [\[Update Security Question\]](#)
Email: [\[Change your email\]](#)

What is MFA (Multi-Factor Authentication)?

What is MFA?

Multi-Factor Authentication (MFA) is an authentication method that requires the user to provide multiple pieces of verification information to access a resource, such as an online web application like SMART or MISTAR. Rather than just asking for a username and password, MFA requires one or more additional pieces of verification information, which decreases the likelihood of a successful cybersecurity attack.

Why MFA?

There has been a surge in global cybersecurity incidents over the last two years. Education is among the most affected sectors. In turn insurance coverage has become more limited and expensive plus there is a need to implement additional controls to limit the risks. Those controls include staff training, incident response planning, secured backups and enhanced user authentication strategies like Multi-Factor Authentication (MFA). Therefore, we are accelerating the implementation of MFA for our consortium applications, Smart & MISTAR-Q, to protect the data we are hosting in our data center.

How Will This Change Affect You?

Beginning July 1, you will be required to authenticate when accessing Web SMART (smart.resa.net). For this first phase of security enhancements, Web SMART will be using MFA with email. After the security updates have been deployed to the production environment, for Web SMART, users will be required to provide a valid email address (work or personal) for authentication purposes.
