IF you routinely login to www.csiesafe.com to access bank account statements/notices, please read on about new additional MFA security step.

IF you do not login to www.csiesafe.com, you can ignore this, though any future login to www.csiesafe.com will require the additional MFA security step.

IF you obtain your bank account statements/notices directly in your login to DSBconnect digital banking and no longer need access to www.csiesafe.com, respond with your name to online@dsbks.com and in Subject line enter: No More CSI

Dear CSIeSafe User, **May 7, 2026**

Your email address is associated with a checking/savings/CD/loan account(s) at Denison State Bank. This association may have been first set up 25 years ago when we first started providing account e-statements/notices.

Logging in to www.csiesafe.com still works and still allows you access to your registered bank account statements/notices. Up to now, you have been able to login at www.csiesafe.com with your Username (which is your email address) and your chosen password. Now, our provider CSI **will start requiring an additional multi-factor authentication step to further identify you as the valid user and to protect against unauthorized electronic access. The details and action needed by you are explained below.**

If you already use DSBconnect digital banking, we encourage you to instead opt-in your accounts to online statements/notices and no longer use the older CSIeSafe service. To opt-in to Digital Banking statements/notices, in your DSB login main menu, click Statements & Notices > Sign Up.

If you take no action, at your next login to www.csiesafe.com after May 7, you will be prompted. Then, for every login after then, an email verification will need to be sent to you before you are able to login and access the posted statements/notices.

Here is the overview of what the new MFA requirement on CSIeSafe:

(continued on next pages)

CSIeSafe is implementing Multi-Factor Authentication (MFA) to strengthen account security. MFA was previously optional and enabled on a per-user basis. With this update, MFA **will become mandatory for all CSIeSafe accounts**.

Why?

Protecting customers' sensitive information is a top priority for CSI teams. Banks, regulators, and examiners recognize MFA as a best practice for securing sensitive systems. It enhances security by requiring two or more distinct forms of verification to confirm a user's identity.

What to expect

All users logging in to CSIeSafe will be required to use MFA. During an initial transition period, users will be notified at login and prompted to enroll. They can choose to enroll or bypass the process temporarily. After the transition period ends, users will no longer be able to bypass the MFA enrollment. It will be required in order to access CSIeSafe.

When?

- Transition Period: **May 7, 2026, after 10:00 PM CT, through May 13, 2026, 10:00 PM CT**
  During this time, users will be prompted to enroll in MFA but may choose to bypass the process.
- Activation Date: **May 13, 2026, after 10:00 PM CT**
  MFA will be required for all users and must be completed to access CSIeSafe.

How it works

CSIeSafe will use an **authenticator app** and **email verification** to authenticate users.

Users will be prompted to enroll their CSIeSafe account with a **Time-Based One-Time Password (TOTP)** authenticator app (such as Google Authenticator or Microsoft Authenticator) link.

The TOTP process is a one-time enrollment step and does not need to be repeated unless the user's authenticator setup changes (e.g., changes devices, removes the authenticator app, resets the account).

Email verification will be used each time a user logs into CSIeSafe to authenticate the login and grant access to the site.

Detail Instructions for Multi-Factor Authentication for CSIeSafe:

User Experience: Transition Period

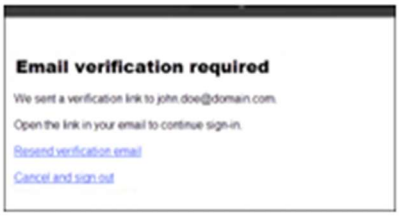
During the transition period, **May 7, 2026, after 10:00 PM CT, through May 13, 2026, 10:00 PM CT**, users will be presented with a TOTP setup screen when they log into CSIeSafe. From the screen, users can complete the MFA enrollment process or temporarily bypass it by clicking **"Skip for now**."

- Email verification will NOT be enforced during the transition period.
- After the transition period is complete, the "Skip for now" link will be removed. Users will no longer be able to bypass the TOTP Setup screen and must enroll in MFA in order to access CSIeSafe.

User Experience: Post Transition Period

Beginning **May 13, 2026, after 10:00 PM CT**, CSIeSafe will require **email verification** and completion of **Time-Based One-Time Password (TOTP)** enrollment for access.

- An **Email Verification** message will be displayed.



- Users must select the link provided in the email associated with their CSIeSafe account to continue.

After the user selects the email link, CSIeSafe will:

- Launch a new session.
- Automatically verify whether the user has completed **TOTP** enrollment in the background:
  - **If TOTP is already set up,** the user proceeds directly to the CSIeSafe home screen with no additional prompts.
  - **If TOTP is NOT set up,** the user is presented with the **TOTP setup screen** and must complete enrollment before accessing CSIeSafe.

Authenticator App: Time-Based One-Time Password (TOTP)

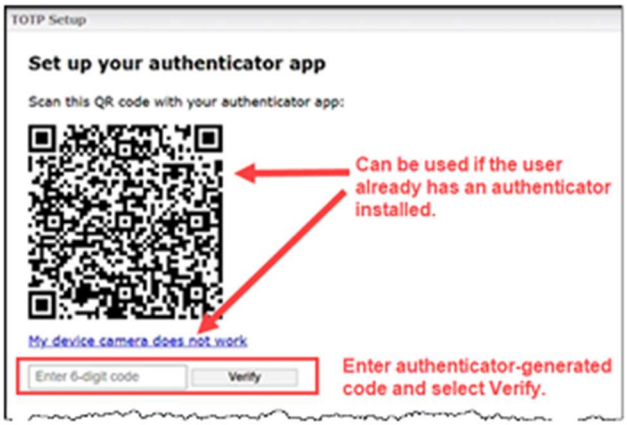
During the initial MFA enrollment process, users will be prompted to enroll their CSIeSafe account with a TOTP authenticator app (such as Google Authenticator or Microsoft Authenticator).

The TOTP process is a one-time enrollment step and does not need to be repeated unless the user's authenticator setup changes (e.g., changes devices, removes the authenticator app, resets the account).

How it works

If the user already has an authenticator app installed on their mobile device, they will:

1. Scan the provided QR code or click the "My device camera does not work" link for a URL instead.
2. Enter the temporary code (typically valid for 30–60 seconds) generated by their authenticator app on the TOTP Setup screen and select **Verify**.
3. After verification, the user is granted access and returned to CSIeSafe.



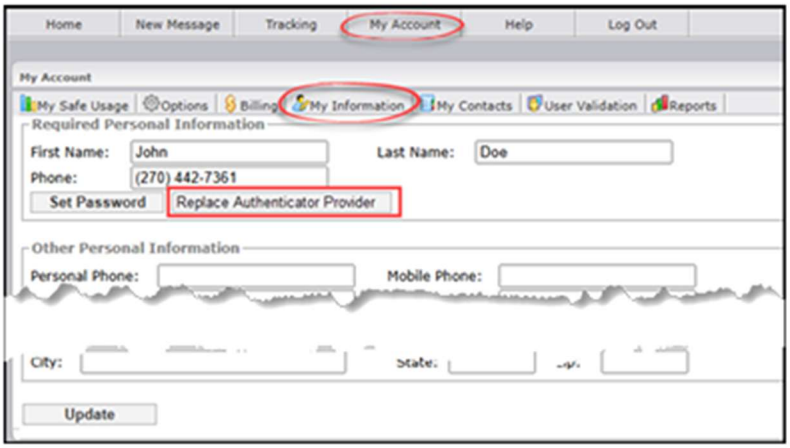
If the user does NOT have an authenticator app installed on their mobile device, they will need to:

1. Download an authenticator from their device's app store.
2. Scan the provided QR code or click the "My device camera does not work" link for a URL instead.
3. Enter the temporary code (typically valid for 30–60 seconds) generated by their authenticator app on the TOTP Setup screen and select Verify.
4. After verification, the user is granted access and returned to CSIeSafe.

For convenience, a download QR code and link will be provided for the Google and Microsoft Authenticator apps on the TOTP Setup screen.

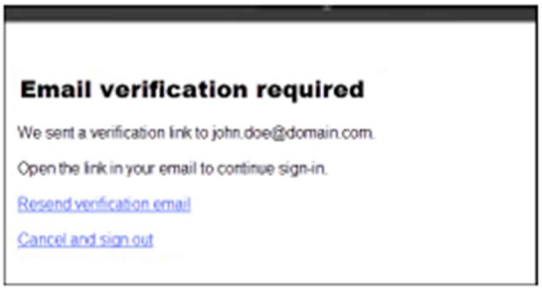
Update Authenticator in CSIeSafe

If needed, users can update the authenticator used for **CSIeSafe** under **My Account > My Information > Replace Authenticator Provider**. The user is then prompted to complete the TOTP setup process again using the new authenticator.



Email Verification

Beginning on the activation date and going forward, CSIeSafe will use email verification to authenticate users each time they log in.



The user must select the link provided in the email associated with their CSIeSafe account to complete the login process. The link is only valid for the current session and cannot be reused.

Expired CSIeSafe Password

If the user's CSIeSafe password has expired, an email verification link will be sent to the email address associated with the CSIeSafe account. After the user selects the link,

- CSIeSafe checks the account for TOTP enrollment.
- If not enrolled, the user must complete TOTP enrollment.
- If TOTP enrollment is already complete, the user proceeds with the standard password reset process.

Forgotten CSIeSafe Password

If the user does not remember their CSIeSafe password, they should select **Forgot Password** just as they would today. After selecting Forgot Password,

- CSIeSafe checks the account for TOTP enrollment.
- If not enrolled, the user must complete TOTP enrollment.
- If TOTP enrollment is already complete, the user enters the authenticator-generated code to continue with the password reset process.

Matt Taylor
Senior Vice President/Digital and Marketing
DENISON STATE BANK
Member FDIC/Equal Housing Lender

Office: 421 New York Ave, PO Box 71, Holton, KS 66436
Work: 785-364-3131 ext 1138
Cell: 785-364-7760
Email: MTaylor@dsbks.com Web: www.dsbks.com Facebook: www.facebook.com/DenisonStateBank