

FactorSoft®

# Multi-Factor Authentication

To enhance data security and help protect against evolving cyber threats, we are introducing Multi-Factor Authentication (MFA) to the FactorSoft login and authentication process beginning April 6, 2026.

MFA is a security protocol that requires two or more independent methods of identity verification – such as your standard password plus a unique code sent to your mobile device or email address – before granting access to your account.

By moving beyond a single password, we are adding a critical layer of defense that ensures only authorized users can manage invoices and access sensitive funding information, providing you with greater peace of mind in every transaction.

## MFA Registration Process

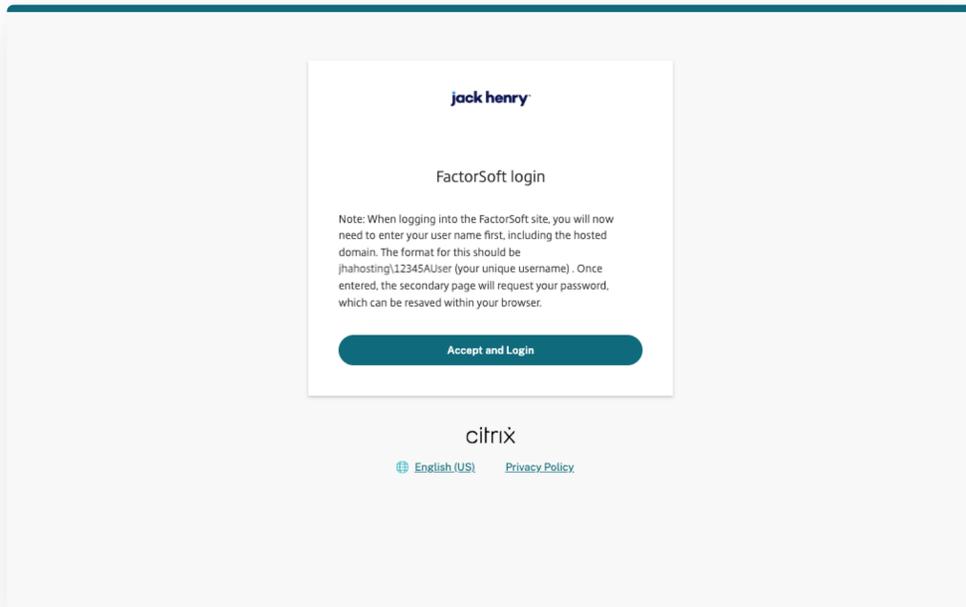
The first time you log into FactorSoft on or after April 6, 2026, you'll be required to set up multi-factor authentication, using one of the following methods:

- Google Authenticator™
- Microsoft® Authenticator
- Citrix® Authenticator

Here's a look at the initial registration experience.

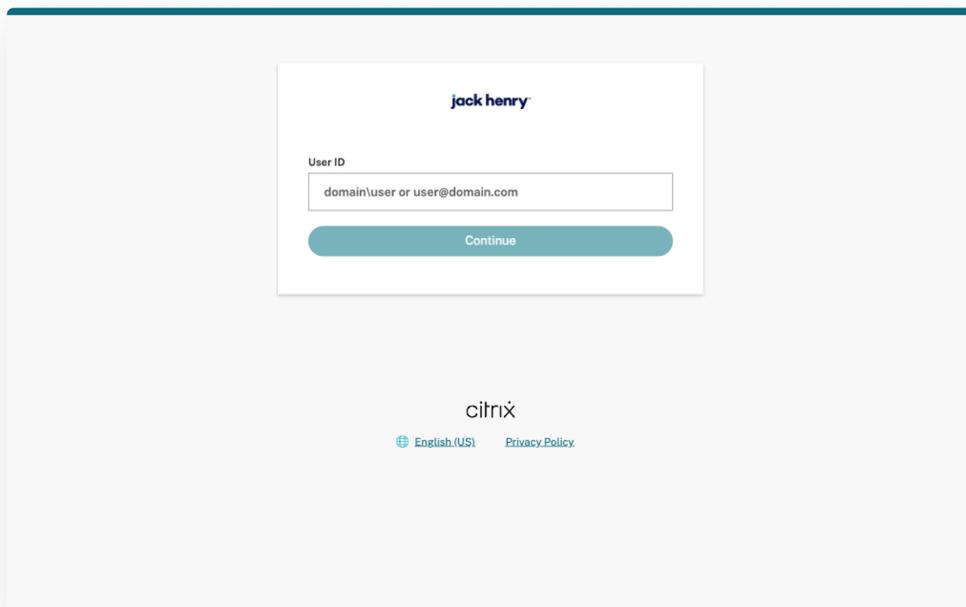
### Step 1

Open a web browser and navigate to <https://fshosting.jackhenry.com/>.



## Step 2

Enter the **domain** (jhahosting) with a slash, followed by your **user ID**, which is a number followed by your first initial and last name. A typical entry will look like this: jhahosting\123AUser.



### Step 3

At the next screen, enter your **username** again (it's the same as your user ID) and click Don't Have a Token?

The screenshot shows a login form for 'jack henry' on a Citrix portal. The form includes three input fields: 'Username' with the placeholder 'yourusername@youradress.com', 'Password' with the placeholder 'Enter password', and 'Password Token' with the placeholder 'Enter token'. A green circle highlights the text 'Don't have a token?' next to the Password Token field. Below the fields is a teal 'Sign In' button. At the bottom, the Citrix logo is displayed along with links for 'English (US)' and 'Privacy Policy'.

### Step 4

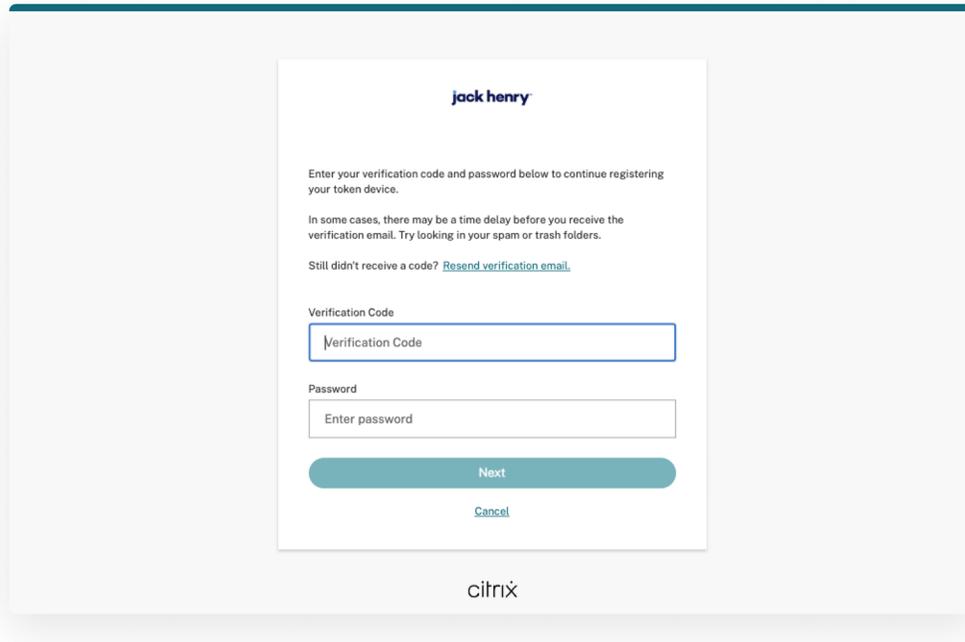
Once more, enter your username and click Next. The user ID should be entered using the following formats: jhahosting\123AUser or [123AUser@jhahosting.com](#).

The screenshot shows a registration form for 'jack henry' on a Citrix portal. The form includes a message: 'To register a token device, you first need to verify your identity. Enter your username below to send an email with a verification code.' Below this is a 'Username' input field containing '123AUser@jhahosting.com'. There are two buttons: a teal 'Next' button and a smaller 'Cancel' link below it. At the bottom, the Citrix logo is displayed along with links for 'English (US)' and 'Privacy Policy'.

The system will send an email to the address on file containing a one-time verification code.

## Step 5

Enter your one-time verification code and password, then click Next.



**jack henry**

Enter your verification code and password below to continue registering your token device.

In some cases, there may be a time delay before you receive the verification email. Try looking in your spam or trash folders.

Still didn't receive a code? [Resend verification email.](#)

Verification Code

Password

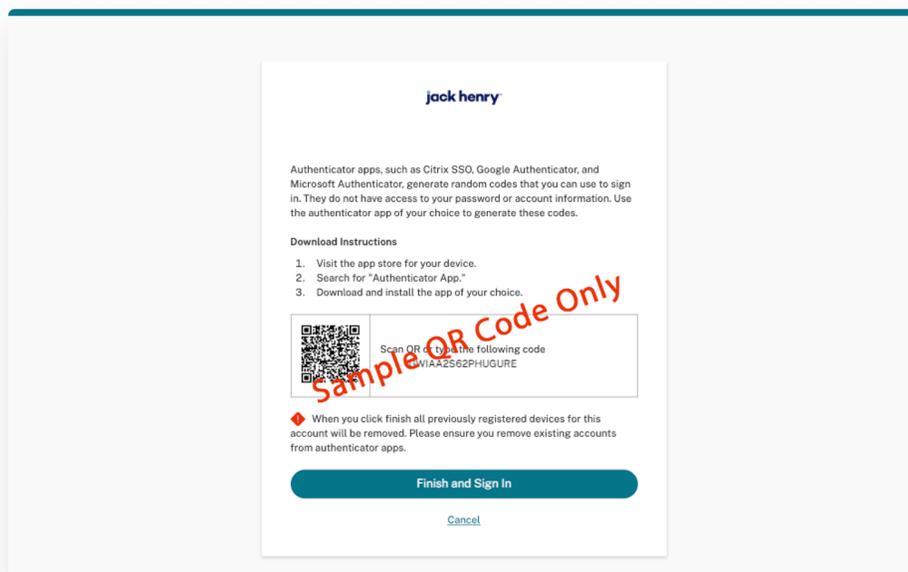
**Next**

[Cancel](#)

**citrix**

## Step 6

A screen will display with a QR code or numeric code you can use with the authenticator of your choice.



**jack henry**

Authenticator apps, such as Citrix SSO, Google Authenticator, and Microsoft Authenticator, generate random codes that you can use to sign in. They do not have access to your password or account information. Use the authenticator app of your choice to generate these codes.

**Download Instructions**

1. Visit the app store for your device.
2. Search for "Authenticator App."
3. Download and install the app of your choice.

Scan QR code by the following code  
VIAA2S6ZPHUGURE

**Sample QR Code Only**

◆ When you click finish all previously registered devices for this account will be removed. Please ensure you remove existing accounts from authenticator apps.

**Finish and Sign In**

[Cancel](#)

## Step 7

For existing FactorSoft users, that's it! You're good to go. From now on, you'll be asked to provide your MFA code every time you log in.

## Troubleshooting

While it's rare to encounter difficulties when adding MFA to your FactorSoft login, occasionally challenges arise. If you encounter any issues while adding MFA, please try these steps in order:

- 1. Clear your browser data:** Start by clearing the cookies and cache in your browser settings to ensure a fresh session.
- 2. Request a profile reset:** If that doesn't work, submit a ticket to the FactorSoft support team to have your device profile reset.
- 3. Request a password reset:** If the issue persists, update your FactorSoft support ticket to request a temporary password reset, which often clears registration hurdles.

Still stuck? If these steps don't solve the problem, please update your ticket as still unresolved. Our support team is standing by and ready to dive deeper into the technical details to get you logged in safely!

## stay safe out there

If you have questions about enabling MFA in FactorSoft, reach out to our team by opening a ticket in the [For Clients Portal](#) or by calling 800.299.4222.

For more information about Jack Henry, visit [jackhenry.com](https://jackhenry.com).