

LiveU Applications Two-Factor Authentication (2FA)

Overview

LiveU Applications Two-Factor Authentication (2FA) adds a second layer of security, keeping your broadcasts, recordings, unit controls, and team access always protected. It ensures that only verified users can access your organization's LiveU Central environment.

2FA is not applicable to SSO-enabled inventories or OPS deployments.

LiveU 2FA uses a one-time code sent by email. No setup or mobile app is required - you only need a verified email address associated to your username and to enter the code when prompted at login.



Once a user's email address is verified, Two-Factor Authentication is enforced for that user. From that point forward, a six-digit verification code is required at login time.



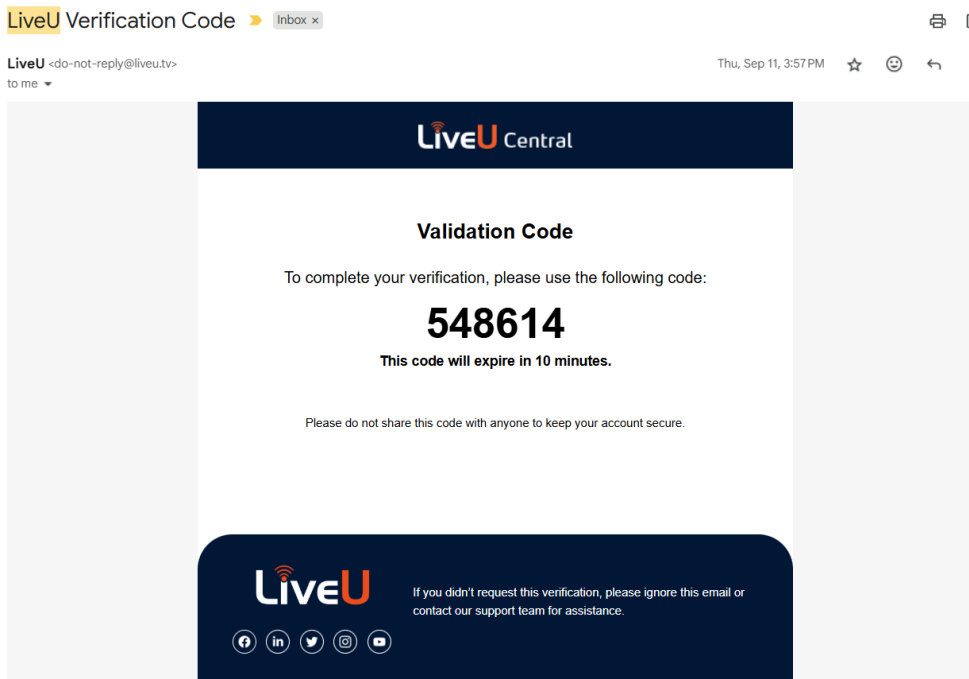
This security feature is enabled on all customer inventories, and will work for all users that verify their email, but is not yet mandatory, therefore users that do not verify their email can login successfully. LiveU plans to make 2FA mandatory for all users in the first months of 2026.

In this article we will cover:

- [How Two-Factor Authentication works](#)
- [How to verify one's email](#)
- [Administrator responsibilities](#)
- [Troubleshooting](#)
- [FAQs](#)

How Two-Factor Authentication works

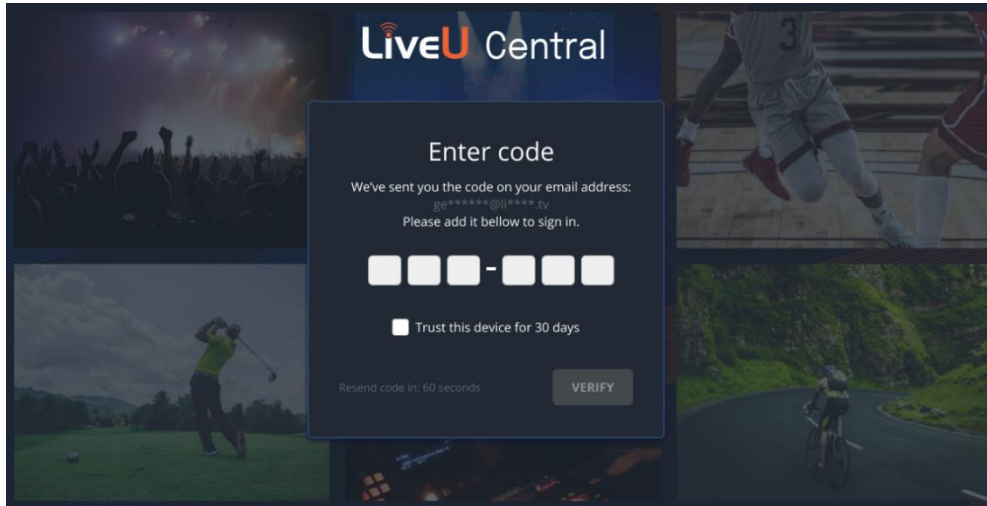
1. Sign in to any of the LiveU web application with your username and password.
2. After your email address is verified, you automatically receive a one-time six-digit verification code to your verified email address.



3. Enter the code on the login screen to complete sign-in.
Optionally, select **Trust this device for 30 days**. When selected, this browser will not require a 2FA code for the next 30 days.



Once a user's email address is verified, Two-Factor Authentication is enforced for that user. From that point forward, a six-digit verification code is required at login time.



Although 2FA brings a powerful improvement to your security level, higher security can be achieved using Single-Sign-On (SSO), as it helps you manage all users' access in sync with your Active Directory. Reach out to your LiveU representative for details.

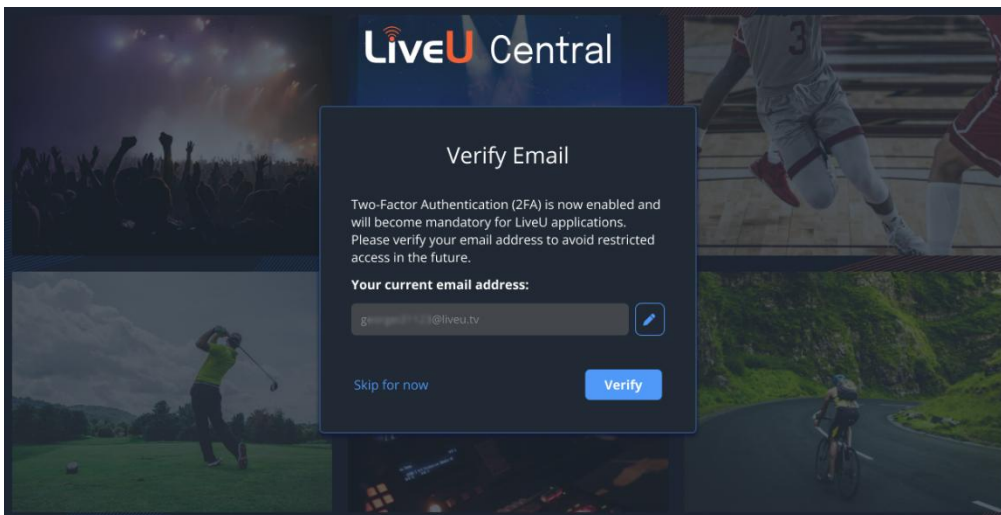
Verifying your email

Before you can use 2FA, your LiveU Central user account must have a verified email address. The verification ensures that 2FA codes reach you securely and without delay.

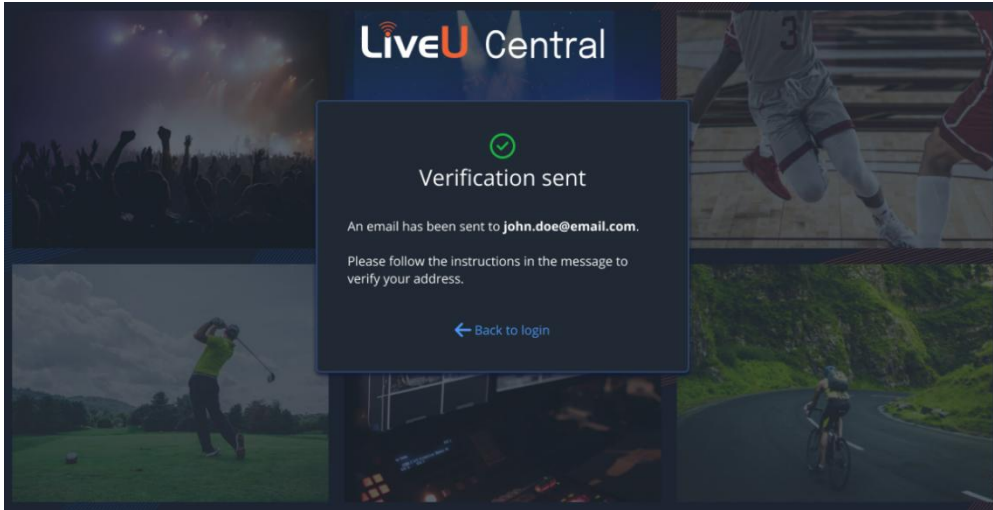


Once your email address is verified, Two-Factor Authentication will be enforced at login time, and you will be required to enter the six-digit code received by email.

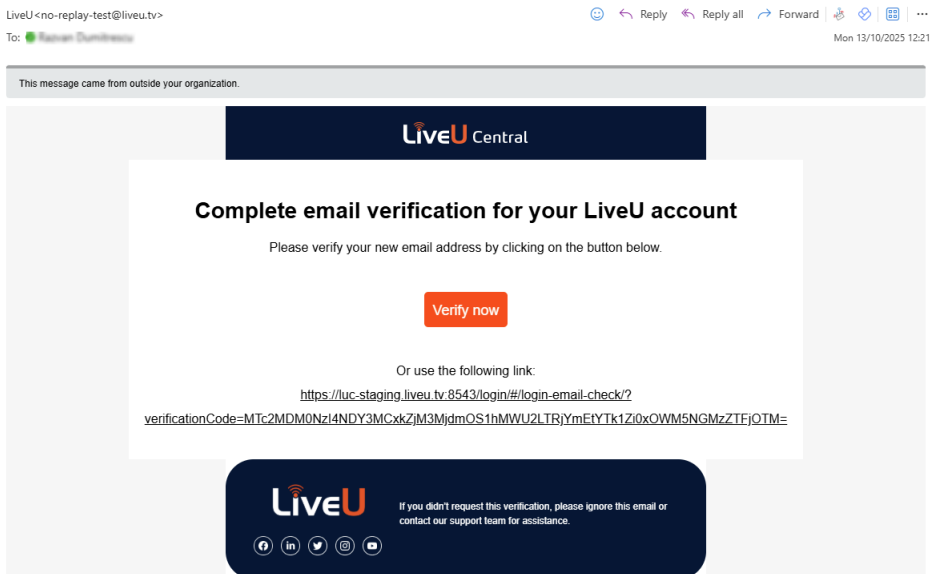
If your email address is not verified, you will be redirected to the **Verify Email** screen.

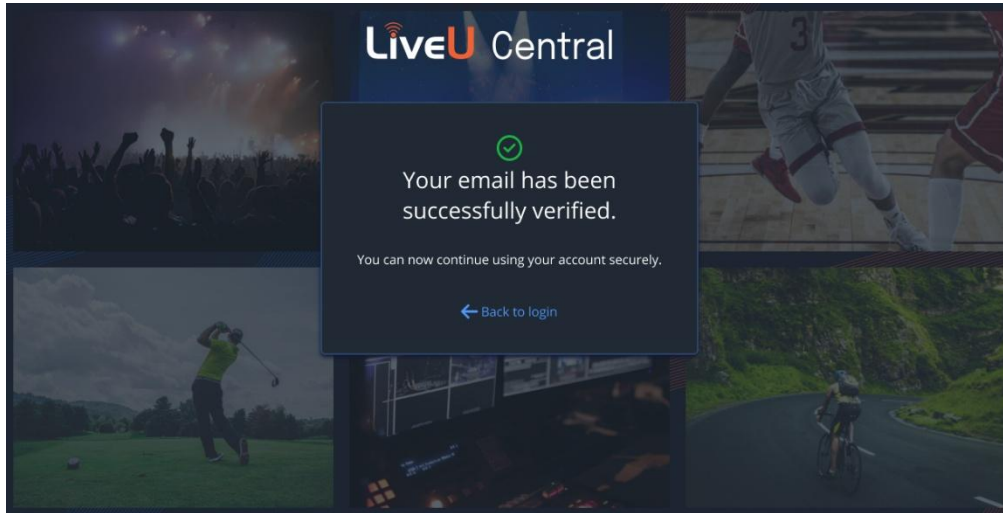


1. Check that your email address is correct (or click the pencil icon to edit it and then click Save), then click **Verify** to send yourself a verification email.
2. A confirmation message appears, indicating that the verification email was sent.



3. Open the verification message and follow the **Verify now** link to complete the process.

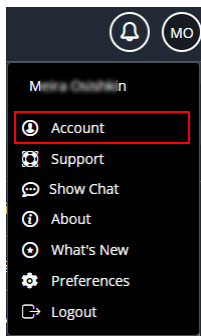




4. After verification, **click Back to login**. Two-Factor Authentication is now enforced, and you must enter the six-digit code at sign-in.

If you choose to postpone your email verification from the login screens by selecting **Skip for now**, you can verify it later from your Account Management menu.

1. Click your user initials at the top right and select **Account**.



2. Check that your email address is correct and click **Verify** to send yourself a verification email.

3. Open the verification message and follow the **Verify now** link to complete the process.

If you are unable to login or need to update your email, contact your **inventory administrator**. Admins can correct your email address and resend the verification message if necessary.

Administrator responsibilities

It is recommended that each inventory have at least one administrator. If your organization does not have an administrator user type, please reach out to your LiveU Sales Engineer / Technical Account Manager.

Admins can manage other user accounts of the inventory by:


- Updating or correcting a user’s email address.
- Triggering the verification email for another user when an address is changed.
- Assisting locked-out users by re-triggering their email verification link.
- Reminding users not to share accounts; each user should have a personal login and email for 2FA to function properly.
- Disabling 2FA for a specific user (if needed).

Checking User Verification status

Easily see if users in your organization are verified or not via the VERIFIED EMAIL column in the Users list (**MANAGE** tab > **Users**):

USER	FIRST NAME	LAST NAME	EMAIL	USER LABEL	USER TYPE	SSO	ODA	ACTIVE	VERIFIED EMAIL	
tbl@ingrat	Ingrat	Ingrat	tbl@yaho.oo		Ingest			✓		
Evana123	Evana	Prod	Evana123@liveu.tv		Regular			✓		
Evana23	Evana	Prod	Evana23@liveu.tv		Ingest			✓		
Evana45	Evana	Prod	Evana45@liveu.tv		Regular			✓	✓	
Evana67	Evana	Prod	Evana67@liveu.tv		Ingest			✓		

Updating a user's email address and/or triggering the verification email for them:

1. In the **MANAGE** tab, select **Users**.
The **MANAGE > Users** list is displayed.
2. In the row that you want to edit, click  to display the User Management window.

User Management

PROFILE

User: [5...@liveu.tv] **Email** [Verify Email](#)

PRIVACY

New Password: [] Confirm Password: []


First Name: [E...] Last Name: [P...]

User Type: [Regular] Reset Password: [Every 3 Months]

User Label: [] Active Enterprise

Disable 2FA Unit & License Activation Force users allocation to Auth0 inventories


[DELETE USER] [RESET PASSWORD] [CANCEL] [OK]

3. Click  next to the email address and modify it, then click **Save**.
4. Click **Verify Email**. A verification email is sent to the user.
5. Click **OK** to exit window.

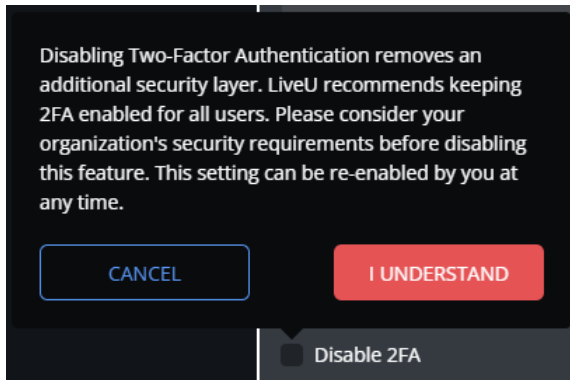
Disabling 2FA for a specific user



Disabling Two-Factor Authentication removes an additional security layer. LiveU recommends keeping 2FA enabled for all users. Please consider your organization's security requirements before disabling this feature. This setting can be re-enabled by you at any time.

1. In the **MANAGE** tab, select **Users**.
The MANAGE > Users list is displayed.
2. In the row that you want to edit, click  to display the User Management window.

3. Locate the **Disable 2FA** checkbox. Toggle the setting as needed:
 - **Unchecked** (default): 2FA is enabled for this user.
 - **Checked**: 2FA is disabled for this user.
4. Check the box to disable. Please read, make sure you understand the security implications and that you are allowed to take such a security decision within your organization. To confirm, press **I UNDERSTAND**.



5. Click **OK** to apply the changes and exit window.

Troubleshooting

Symptom	Cause	Fix
No 2FA email received	Incorrect or unverified email; message filtered to spam	Check spam/junk; verify your email under <i>Account</i> or ask your inventory admin to update and resend the verification.
“Invalid Code” message	The one-time code timed out or a new one was issued	Click Resend Code and use the latest verification code received via email.
Locked out after multiple attempts	Too many failed entries or outdated email	Ask your inventory admin to correct your email and trigger a new verification.
No 2FA prompt when using SSO	2FA does not apply to SSO-enabled inventories	Continue using your organization’s SSO login.
No 2FA prompt (no SSO)	2FA is disabled for the user	Ask your inventory admin to review the Disable 2FA setting in Manage > Users.

FAQs

- **Does 2FA work with SSO?**

No. Email-based 2FA is not applicable to SSO-enabled inventories.

- **How will I receive the code?**

By email only. Authenticator apps and SMS are not supported yet.



- **What if my email is wrong?**

Update it under *Account*, or have your inventory admin correct it from Manage > Users screen and trigger your verification email.

- **Can I skip 2FA after verifying my email?**

No. Once your email address is verified, entering the six-digit email code is required at every login (unless you checked the 'Trust this device for 30 days' checkbox).

- **Can I share a user account?**

Avoid shared or “group mailbox” accounts. Each user should have a personal login and email for reliable 2FA delivery.

- **What does “Trust this device for 30 days” mean?**

When selected, the current browser on the current device will not prompt for a 2FA code for the next 30 days. This does not apply to other browsers or devices you may be using with the same credentials.

- **Which LiveU applications support 2FA?**

LiveU Central, Matrix, Studio, Video Return, Ingest, Control+.