QuantumMail V2

Admin + Member Onboarding • Extension Encryption Workflow

Use this URL everywhere

Platform + Server Base:
`https://quantummail-v2.onrender.com`

• Use it as **Server Base** in the extension login
• Use it to **Request Organization** / **Join Organization** on the home page

Before you start (60 seconds)

1. Install and enable the **QuantumMail** Chrome extension.
2. Make sure your organization request (or join request) is **approved**.
3. Login once in the extension - this **registers your device public key**.

Tip: Use the same browser profile for sending and decrypting links.

Key concept (important)

Decryption is tied to the device key used when the secure link was created. If you reinstall the extension, clear storage, or switch devices/browsers, older links may fail to decrypt. In that case, ask the sender to re-encrypt and share a fresh link.

Admin Setup

Use this section if you are creating a new org or approving members.

A) Create an Organization (first time)

1. Open `https://quantummail-v2.onrender.com`
2. Click **Request Organization**
3. Enter org details (Org name, Admin username/email, notes if required)
4. Submit the request and wait for approval/confirmation
5. Save your Org ID / Org name - you will use it in the extension login.

B) Login to Extension (Admin - registers device key)

1. Click the **QuantumMail** extension icon in your browser toolbar
2. Set **Server Base** to `https://quantummail-v2.onrender.com`
3. Enter **Org**, **Username**, and **Password**
4. Click **Login**
5. Confirm your status shows **Signed in** (or equivalent).

First login registers your public key for this device.

C) Approve Members (so they appear in Recipients list)

1. Ask the user to submit a **Join Organization** request from the home page
2. As Admin, open the org management section and find **Pending Requests**
3. Approve the user
4. Tell the user to **login to the extension once** (registers their public key)
5. After that, they will appear in **Recipients (within your org)**.

Member Setup + Daily Use

Use this section if you are joining an org and sending/receiving secure links.

1) Join an Organization (Member)

1. Open `https://quantummail-v2.onrender.com`
2. Click **Join Organization** (or Request Access)
3. Enter your **Org** and **Username** (and any required info)
4. Submit the request and wait for Admin approval
5. After approval, continue to step 2 (extension login).

2) Login to Extension (Member - registers device key)

1. Click the QuantumMail extension icon
2. Server Base: `https://quantummail-v2.onrender.com`
3. Enter **Org**, **Username**, **Password**
4. Click **Login**
5. Keep the extension signed in to decrypt links you receive.

3) Encrypt & Send a Secure Message (Sender)

1. Open Gmail (or your web email) and start composing a message
2. Highlight the **exact text** you want to protect
3. Open the extension and (optional) select recipients under **Recipients (within your org)**
4. Optional: add files under **Attachments** (stay under your total size limit)
5. Click **Encrypt Selected Text**
6. Your highlighted text is replaced with a secure QuantumMail link - send the email normally.

Recipient rule: If you do not pick recipients, it may default to **all org users**.

4) Decrypt a Secure Message (Receiver)

1. Open the email and click the QuantumMail secure link
2. If you see **Extension not detected**, enable/install the extension and refresh
3. If you see **Signed out**, open extension and login again
4. View decrypted content and download attachments (if included)

Troubleshooting

Issue	Fix
Decrypt failed: device key does not match	You switched devices/browsers or reinstalled/cleared storage. Ask sender to re-encrypt and send a new link.
Extension not detected	Install/enable extension, then refresh the page.
Recipients missing	User must be approved by Admin AND must login once to register a public key.
Signed out / session expired	Open the extension and login again.
Attachments too large	Reduce sizes or send fewer files to stay within the allowed total.

Best practices

Encrypt only what is sensitive (keys, credentials, private data). Verify recipients before encrypting. For reliable decrypting, use the same browser profile where you registered your device key.