

Testing & Evaluation Sheet	
Thunderbird	
1. Tool Overview	
Name:	Thunderbird
Category:	Email Clients
Purpose:	Open-source email application developed by Mozilla for managing multiple emails accounts with strong privacy, PGP encryption, OAuth2 support, and add-on extensibility.
Date Tested	4/23/25
Status:	Deployed <input checked="" type="checkbox"/> Operational - Actively running/maintained <input type="checkbox"/> In Testing - Currently being evaluated or piloted <input type="checkbox"/> Inactive/Deprecated - No longer maintained or functional
Deployment Architecture:	<input checked="" type="checkbox"/> A standalone software - Runs entirely locally (e.g., runs on computer and doesn't depend on external server) <input type="checkbox"/> A locally hosted service with separate server and client component - Run both backend/frontend yourself (e.g., backend could be on a local network, or self-hosted on cloud) <input checked="" type="checkbox"/> A service with a local client that's hosted by a third party - You install a client on your device, but it connects to and depends on a remote server (e.g., Signal: install app (client), but Signal's servers handle message relaying, etc.) Thunderbird application is a standalone software but email data is located on the remote email server (IMAP or POP3). <input type="checkbox"/> A service that is hosted by a third party but can also be self-hosted
Version:	137.0.2
2. Installation & Setup	
OS Compatibility	Windows, macOS, Linux, Android
Installation Manual:	Yes (manuals designed for each OS)
Installation Steps:	To install Thunderbird:

	<ol style="list-style-type: none"> 1. Visit the official Thunderbird website. 2. Download the installer for your operating system (Windows, macOS, or Linux). <ol style="list-style-type: none"> a. For Android, you can download Thunderbird straight from the Google Play Store (no further steps needed) 3. Once the download is complete, open the installer. 4. Follow the on-screen instructions to complete the installation of the Thunderbird application.
Mention if command-line setup or special configurations are needed	No command-line setup or configuration required for average users (command line options are available for advanced users such as system administrators or IT departments so they can install Thunderbird with preset configurations for users).
Common Installation Issues & Fixes:	Not many errors as Thunderbird generally installs smoothly, but issues may arise with configuration (like setting up encryption keys or connecting to email servers). Common fixes include verifying proxy settings or adjusting firewall permissions.
User Documentation:	Yes
Required Technical Knowledge	Intermediate (Intuitive email interface but requires learning a little bit on how to use encryption)

3. Testing & Evaluation

<u>Category</u>	<u>Details</u>	<u>Score</u>
Operational Functionality:	<p>Functionality</p> <ul style="list-style-type: none"> • Test Steps: Verify the tool's core features by using all major functions, tracking any failures or bugs. <p> <input type="checkbox"/> The tool is mostly non-functional with many broken features and bugs. <input type="checkbox"/> Several broken features or bugs <input type="checkbox"/> Minor bugs or issues <input type="checkbox"/> Mostly functional with few bugs or no bugs <input checked="" type="checkbox"/> Fully functional with no bugs </p> <p>Internet Dependence:</p> <ul style="list-style-type: none"> • Works offline for local mail (once emails are downloaded locally, you can read, search, and draft replies offline) • Full functionality requires internet connection (sending or receiving new emails) 	4.3

	<ul style="list-style-type: none"> Basic sending/receiving mails works well on 2G/3G networks but syncing large mailboxes or initial setup/sync of an account will be slower. <p>Localization & Language Support</p> <ul style="list-style-type: none"> Supports around 63 languages including Chinese (Simplified & Traditional), Japanese, and Korean Community driven translations (translate and maintain user interface) <p>Mobile Accessibility</p> <ul style="list-style-type: none"> There is an official Thunderbird application for Android users on the Google Play store (new). Not accessible for iOS users but may be in the future. 	
Usability for Non-Technical Users	<p>Ease of Installation & Deployment</p> <ul style="list-style-type: none"> Downloading and installing is very easy and intuitive for users with limited steps — download the installer, run it, and follow a few quick steps like clicking 'Next' and 'Finish'. It's not exactly a one-click installation, but it's very close. Updates may not be real-time for every minor change, the documentation and guides are actively maintained and reliable for most users Installation took roughly 1 minute (Dell XPS 15 laptop). <p>User Onboarding Experience</p> <ul style="list-style-type: none"> There is documentation and forum posts on different questions new users can have when using the software. Wizard-based onboarding (user interface that leads a user through a sequence of small steps) A key topic often addressed is how to set up email accounts in Thunderbird — here's a helpful link: How to configure email accounts in Thunderbird <p>Technical Experience Level Required</p> <ul style="list-style-type: none"> Users with no programming experience can easily install and begin using the tool. The interface is user-friendly and visually appealing, making it accessible for non-technical users. Understanding how to set up end-to-end encryption and how it works may require more knowledge but overall very non-technical user friendly. 	4.0
Security & Privacy Strength	Encryption Standards	4.2

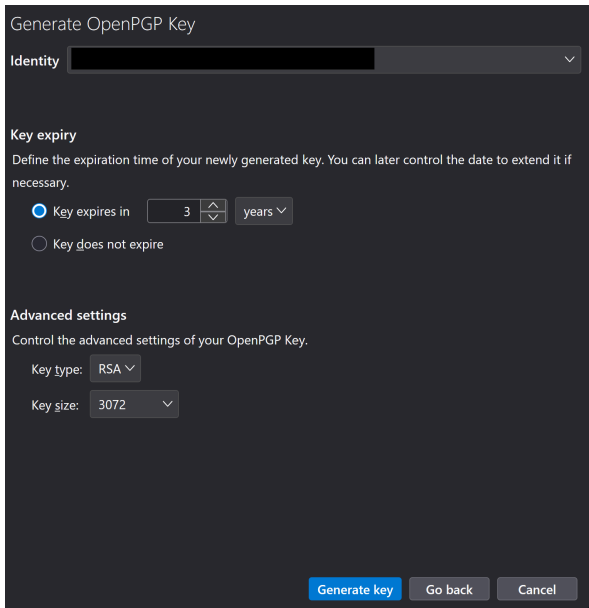
	<ul style="list-style-type: none"> ● OpenPGP (Pretty Good Privacy) encryption, which is used to encrypt emails and digitally sign messages for enhanced privacy and security. <ul style="list-style-type: none"> ○ AES-256: One of the algorithms used in OpenPGP ● Verified E2E encryption available in email compose settings ● Supports S/MIME (Secure/Multipurpose Internet Mail Extensions) for encrypting emails and verifying sender identity using public-private key pairs. ● TLS (Transport Layer Security): Encrypts the connection and ensures that emails are sent securely over the internet. This is commonly used for secure SMTP (sending emails) and IMAP/POP (receiving emails) connections. <p>Known Strength resilience</p> <ul style="list-style-type: none"> ● Thunderbird is quite resilient when properly configured as it supports end-to-end encryption. ● Offers strong authentication methods like OAuth2 and since it is open source, it benefits from public audits and the strong reputation of Mozilla Foundation. ● It is usable in regions with heavy censorship and surveillance but is not the greatest without additional steps. <ul style="list-style-type: none"> ○ Does not include built in censorship circumvention censorship and users would have to manually route traffic through VPN, Tor network, or another proxy. <p>Comparison with Known Standards</p> <ul style="list-style-type: none"> ● Against security/privacy standards like EFF's Secure Messaging Scorecard, EU GDPR principles, or NIST guidelines: <ul style="list-style-type: none"> ○ Thunderbird meets basic to strong standards for secure email clients but is not specialized for privacy. <p>Data Minimization</p> <ul style="list-style-type: none"> ● Thunderbird itself adheres to a minimal data collection policy. ● Without additional protections SMTP headers (sender, receiver, and date) are usually unencrypted. <p>Privacy Policy Accessibility and Clarity</p>	
--	---	--

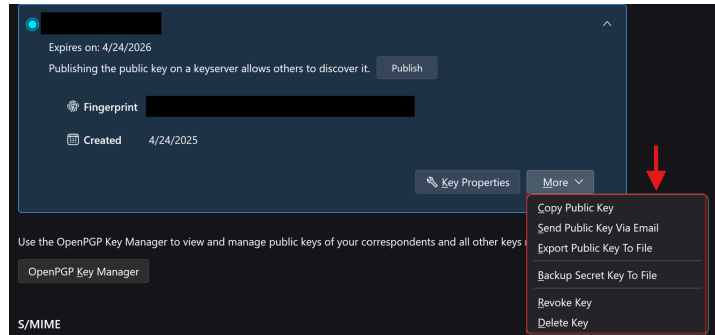
	<ul style="list-style-type: none"> Thunderbird collects very limited, mostly technical data (like version, OS); crash reports and telemetry are optional. No personal data is shared unless legally required. https://www.thunderbird.net/en-US/privacy/ 	
Maintenance/Sustainability	<p>Community support</p> <ul style="list-style-type: none"> It is easy to get help and ask questions on the official forums and Reddit communities. There is all well structured documentation and tutorials. https://support.mozilla.org/en-US/questions/thunderbird <p>Development active status</p> <ul style="list-style-type: none"> It is updated regularly with new monthly releases for users who want all available features and bug fixes monthly. Bug reports and feature requests are handled through Bugzilla and GitHub. <ul style="list-style-type: none"> Response times vary but important security issues are prioritized quickly. <p>Funding and Sponsorship</p> <ul style="list-style-type: none"> Primarily funded by the Mozilla Foundation (a non-profit organization). Sustainable through generous donations and small partnerships. Thunderbird is financially sustainable and has long term development plans. 	4.7
Performance / Effectiveness & Reliability	<p>Testing Environment Setup:</p> <ul style="list-style-type: none"> Device: Dell XPS 15 OS: Windows Network: 4G <p>User Experience Observations</p> <ul style="list-style-type: none"> The tool feels really smooth from an user standpoint. Thunderbird was quite responsive when being tested. There were minimal steps to download and they were very intuitive. <p>Speed & Responsiveness:</p> <ul style="list-style-type: none"> Minimal lag even with encrypted large email attachments. Slight delay when performing encryption or decryption on large messages, but this is typical for encryption processes. Very large email volumes: Thunderbird handles large mailboxes with several thousand emails efficiently, 	4.5

	<p>though searching or syncing large accounts may take a bit of time, especially if the account has complex filters or attachments.</p> <ul style="list-style-type: none"> Running through Tor network/VPNs: Can see noticeably slower email send time, more evident if email content is also encrypted. <p>Resource Usage:</p> <ul style="list-style-type: none"> Low resource usage during regular email tasks (e.g., reading, composing, and sending emails). RAM usage is typically low, even with many open emails (~50MB-100MB depending on the volume and complexity of attachments). CPU usage might increase when encrypting or decrypting messages, especially with large attachments, but it generally remains low. <p>Network Performance:</p> <ul style="list-style-type: none"> Online operations: Thunderbird is highly optimized for internet-based email protocols (IMAP/SMTP/POP3), with minimal network bandwidth usage unless large files are being downloaded/uploaded. Offline operations: Thunderbird is also partly functional offline, allowing for drafting, reading, and searching through previously downloaded emails without an active internet connection (can not send emails) <p>Reliability</p> <ul style="list-style-type: none"> Thunderbird is known for its stability and reliability as an open-source email client. Regularly performs security audits and has addressed vulnerabilities discovered by the community or security experts. Rarely fails under typical usage, and when it does, issues are often resolved quickly with frequent updates and community contributions. Thunderbird uses OpenPGP and S/MIME for email encryption (both are widely recognized as secure and reliable encryption standards). 	
<p>Deployment Considerations:</p>	<p>Open Source & Transparency:</p> <ul style="list-style-type: none"> Complete source code is available on GitHub. Anyone can audit, verify, and contribute to the repositories. 	

	<p>Cloud vs. Local Deployment:</p> <ul style="list-style-type: none"> Fully local and does not require cloud infrastructure. Emails are downloaded to personal computers unless using IMAP (stay on email provider's servers). <p>Dependencies:</p> <ul style="list-style-type: none"> Does not require Docker, Python, databases, or external databases to run. Dependencies for building Thunderbird form the source code are documented in the build instructions <p>Post-Deployment Maintenance</p> <ul style="list-style-type: none"> Regular auto-updates when installed normally. If self-built, maintenance requires occasionally rebuilds with updated dependencies. Forking the project is easy, but should be careful when rebranding due to Mozilla trademarks. <p>Merge/Sustainability:</p> <ul style="list-style-type: none"> Open to contributions to the original project. Small UI changes and tweaks are streamlined. Larger changes require coordination with Thunderbird developers. https://developer.thunderbird.net/thunderbird-development/fixing-a-bug 	
--	---	--

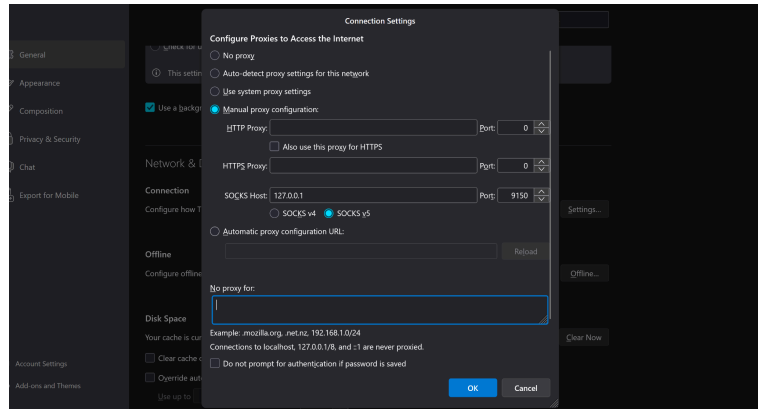
4. Testing Scenarios

<ul style="list-style-type: none"> Scenario 1 Encrypting Emails 	
---	--



-
- To create PGP key for encryption go to **Settings → Account Settings → [Your Email Account] → End-to-End Encryption**
- Here you can add or import existing keys and have some customization options (can leave them default).
- Once a key is imported or created, clicking the dropdown and clicking “More” provides ways to share this key (**ONLY EXPORT PUBLIC KEY**).
 - To send encrypted emails, **both you and the recipient** must have each other's **public keys**.
 - Public keys are **safe to share** with anyone. They allow others to encrypt messages **to** you, but **not** decrypt your messages.
- If you only send your public key → they can encrypt emails **to you**.
- If you both exchange keys → you both can **send and receive** encrypted emails.
- When drafting an email, a lock icon with the word Encrypt will be displayed which is how to encrypt emails.
- Thunderbird also uses S/MIME certificates (but OpenPGP is more common for private users)
 - **For Personal Use or Privacy:** OpenPGP is generally a better choice because it offers greater control over your keys and doesn't rely on centralized authorities.
 - **For Business or Enterprise Use:** S/MIME is often a better choice in business environments because it can integrate seamlessly with corporate email systems and relies on the trusted infrastructure of certificate authorities.

- **Scenario 2**
Set up Proxy Settings
to route traffic
through Tor network



- To route traffic through the Tor network to mask IP addresses, open **Settings** → **General** → **Network & Disk Space** → **Connection Settings**.
- Users can configure proxies to access the Internet and input information for the Tor Network.
 - Select Manual Proxy Configuration
 - Under SOCKS5 host, enter 127.0.0.1 (local Tor proxy)
 - Under SOCKS5 port, enter port number for Tor on your machine
 - Run Tor Browser.
 - Press **Windows + R**, type **resmon**, and press Enter to open Resource Monitor.
 - Go to the **Network** tab and look for **TCP Connections**.
 - Under Image or PID, find **tor.exe** and see which port it is connected to.
 - Make sure SOCKS v5 is selected.
 - Click OK.
- When you use the Tor network, it anonymizes your connection to the Microsoft SMTP server (or other email server). This means your real IP will not be visible to Microsoft. Instead, it will be the IP of the Tor exit node (which is randomly chosen and constantly changes).
- If you're trying to anonymize your identity fully, you would need to use alternative email services that do not require you to link a personal identity (such as a ProtonMail or Tutanota account), and avoid using services like Microsoft 365 that track your identity through your account credentials.
- **Your IP address will be anonymized** (it will appear as a Tor exit node's IP).

	<ul style="list-style-type: none"> • Your identity is still tied to your Microsoft account (email address and authentication details), so Microsoft can still track and identify you by your login credentials.
<h2>5. Insights & Recommendations</h2>	
Key Findings	<p>Strengths:</p> <ul style="list-style-type: none"> • End-to-End Encryption (E2EE): Thunderbird supports OpenPGP and S/MIME encryption, enabling secure communication, ensuring privacy, and protecting against interception. • No Telemetry by Default: Thunderbird collects minimal data about users, and this is opt-in, ensuring privacy without compromising functionality. • Active Community Support: Thunderbird benefits from contributions and assistance from a global community of developers and users. • Integrate VPNs and Tor Network: Users can manually integrate VPNs or relay traffic through the Tor network to increase privacy. <p>Weaknesses:</p> <ul style="list-style-type: none"> • No Built-in Circumvention of Censorship: Thunderbird does not have “built in” support for tools like VPNs, Tor, or other censorship circumvention methods. • Setup for E2EE: It requires some experimentation and a solid understanding of encryption keys to fully understand how the encryption process works and to effectively use it. • Less Integration with Cloud Services: Thunderbird does not integrate as seamlessly with cloud storage solutions like Gmail, Outlook, etc., compared to native webmail services.
Suggested Improvements	<p>Built-in Censorship Circumvention: Suggest integrating VPN support or Tor directly into Thunderbird. This would improve security and also make it easier to use for non-technical users in censorship-heavy regions.</p> <p>Streamline End-to-End Encryption Setup: Create a more thorough guide of how to use the end-to-end encryption similar to Scenario 1.</p> <p>Mobile App: Developing a fully functional iOS version of Thunderbird would expand the user base who can access secure email services.</p>

	<p>Better Cloud Integration: Can potentially integrate with cloud services like Google Drive, Dropbox, or something similar to enhance Thunderbird's usability and collaboration features.</p>
Alternative Tools:	ProtonMail, TutaNota, Mailpile
License	Mozilla Public License 2.0 (MPL-2.0)
Cost/Resource Implications	<p>Total Cost of Ownership:</p> <ul style="list-style-type: none"> • Free to use and does not charge for basic usage. There are no premium tiers or paid features. • There are no additional fees for maintenance or updates. • Thunderbird is easy to install and maintain, especially for users on standard platforms like Windows and Linux. However, setting up encryption (OpenPGP or S/MIME) might require some extra time.
Why is this useful to civil societies in authoritarian environments?	<p>Thunderbird is useful to civil societies in authoritarian environments due to the end-to-end encryption of emails. Utilizing OpenPGP and S/MIME encryption, Thunderbird can ensure that emails remain unreadable even if intercepted by government authorities.</p> <p>For example, let's say an activist in Taiwan, who is working on a cross-border human rights campaign, needs to communicate with people inside China. China is known for its extensive digital surveillance and censorship, including the Great Firewall, which blocks many secure communication tools.</p> <p>The activist can use Thunderbird with OpenPGP encryption to send confidential emails regarding protests, fundraising, and international support. The emails are encrypted so even if they are intercepted by Chinese authorities, they cannot be read.</p> <p>However, since many encrypted email services are blocked in China, the activist can configure Thunderbird to work with Tor or VPNs, ensuring that their emails are routed through a secure, anonymous network. This bypasses the firewall, allowing the activist to continue communicating securely despite censorship.</p> <p>Thunderbird's encryption and ability to bypass firewalls allow the activist to maintain privacy, safety, and secure communication with allies inside China, avoiding detection by the authorities.</p>

	<p>Note: If Thunderbird's official website is blocked, you can download it from trusted alternative mirrors, use VPN or Tor to access the site, or download the source code from GitHub and compile it manually.</p>
--	--