Blurrrer — Network Allowlist & SSL Inspection Guide

For IT and security administrators

Document version: 1.0 **| Last updated:** 2026-07-08

1. Product overview

Blurrrer is a browser-based screenshot sanitizer. Users drop screenshots into the app; OCR and pattern detection run entirely in the user's browser. No screenshot content is uploaded to Blurrrer servers. The app is hosted at **https://blurrrer.org**.

This guide is for network administrators who need to allow Blurrrer on corporate, school, or otherwise restricted networks that perform SSL/TLS inspection.

2. Why SSL inspection blocks Blurrrer

Blurrrer serves a valid TLS certificate issued by **Google Trust Services (GTS)** and uses HTTP Strict Transport Security (HSTS). When a network firewall decrypts and re-encrypts traffic, it replaces the real certificate with one signed by a local authority. Browsers that do not trust that local authority, or sites with HSTS, will display a security warning.

The warning is caused by the network, not by Blurrrer. The same behavior occurs for Gmail, banking sites, and other HSTS-enabled services.

3. Domains to allow / bypass SSL inspection

Add the following domains to your firewall/proxy bypass list, or to any SSL inspection exclusion list. All traffic is HTTPS on port 443.

Domain / host	Purpose	Protocol / port
`blurrrer.org`	Main web application and custom domain	HTTPS 443
`www.blurrrer.org`	WWW redirect to the main app	HTTPS 443
`secure-upload-shield.lovable.app`	Hosting platform fallback URL	HTTPS 443
`*.supabase.co`	Authentication and account backend (Lovable Cloud)	HTTPS 443
`ai.gateway.lovable.dev`	AI feature gateway	HTTPS 443

Optional first-run dependencies: The OCR engine loads static assets from **unpkg.com** and **tessdata.projectnaptha.com** on the first OCR run. These fetches do not carry user content.

4. Recommended SSL inspection handling

Option A — Bypass inspection (recommended): Add the domains above to your SSL inspection bypass list. This preserves end-to-end encryption and avoids certificate warnings.

Option B — Install your root CA on managed devices: If your policy requires inspecting all traffic, push your internal root CA certificate to all managed devices. Note that HSTS-enabled sites may still refuse custom certificates on some browsers.

5. Certificate details

Domain: blurrrer.org / www.blurrrer.org

Certificate authority: Google Trust Services (GTS)

HSTS: Enabled

Protocols: HTTPS 443, TLS 1.2 or higher

6. Verification steps

1. From an unrestricted network (e.g., mobile data), open https://blurrrer.org and confirm the app loads with a valid certificate.

2. Apply the allowlist/bypass rules above on the restricted network.

3. Clear the browser cache or restart the browser, then reload https://blurrrer.org.

4. If the warning persists, verify the browser trusts the network's root CA, or choose the bypass approach.

7. Contact

For support or to report an access issue, email **support@blurrrer.app**. Please include the network type (school, corporate, public), browser, and the exact error message.