

Shared Responsibility Summary

[Version: 1 | Last modified: September 24, 2026]

Firefox Enterprise – On-Prem combines Mozilla-supplied software with customer-operated infrastructure. This summary describes the high-level operating boundary as a starting point for technical and governance review. Customers should assess how these boundaries apply in their specific context. Your contract and applicable support terms govern the services we provide.

Informational notice

This document is for informational purposes only. It is not intended to serve, and should not be construed, as legal advice. Customers are responsible for consulting their own legal advisors and privacy officers, as applicable, to understand their compliance obligations, including whether or not a DPIA is required for their use of Firefox Enterprise.

The model in one sentence

Mozilla provides Firefox Enterprise software, updates, documentation and entitled technical support. Your organization operates, secures and governs the On-Prem environment.

Mozilla's role

Mozilla is responsible for:

- providing Firefox Enterprise software, product documentation and product updates;
- addressing vulnerabilities and defects in Mozilla-supplied software;
- providing technical support in line with the support service you purchase; and
- supplying product information to support technical, privacy and security review.

Mozilla does not operate your On-Prem infrastructure or have access to the defined on-premises data categories. Some default browser connections to external services exist and should be assessed as part of your deployment design — see the Standard Active Connections section below and the External Connections and Telemetry Guide for details.

Your organization's role

Your organization is responsible for:

- designing, deploying, operating and hardening the environment;
- securing infrastructure, networks, databases, storage, backups and encryption;
- configuring browser policies, identity, access and integrations;
- managing users, administrators, retention, monitoring and SIEM exports;
- testing and applying updates under your own change-control process;
- responding to incidents in your environment; and
- meeting your own privacy, legal, employee-information and regulatory obligations.

Standard active connections

Firefox Enterprise – On-Prem is not air-gapped by default. The browser maintains a small number of outbound connections that customers should review and configure for their environment. These include:

- Software and security update service (if not disabled through the management console)
- Certificate validation and revocation checking (CRL/OCSP) (if not disabled via enterprise policy)
- Remote Settings (configuration distribution) (if not disabled through the management console)
- Safe Browsing / phishing protection (if not disabled via enterprise policy)
- Location services (if not disabled via enterprise policy)

As noted, each of these can be managed or disabled through the management console or via enterprise policy. Customers should review the External Connections and Telemetry Guide for the full list of connection categories and available controls, and confirm the effective configuration in their own environment.

Note: On-Prem deployment does not by itself mean that no data leaves your organization. Customers should assess each connection category in the context of their security and privacy requirements.

Working together

Mozilla can support your technical evaluation and help investigate a product issue. Your organization retains responsibility for decisions and actions within its environment, including deployment configuration, security operations and incident response.

Any access needed for support is controlled by your organization. Support-case information is limited to the information your organization chooses to share and is handled under the applicable support and data-processing terms.

Compliance and assurance

Firefox Enterprise can provide browser-layer controls and documentation that may support your security, privacy, and compliance assessment. Customers are responsible for determining how this information applies to their specific context and obligations.

Mozilla does not determine whether your organization is compliant with GDPR, NIS2, DORA, ISO 27001, SOC 2, or any other framework. Your organization remains responsible for its own compliance assessment and program.

Need more detail?

Contact fxenterprise@mozilla.com or use the Documentation Request Form from the Firefox Enterprise Trust Center page.