

External Connections and Telemetry Guide

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

This guide describes browser connections, telemetry behaviour, and the administrator controls available in Firefox Enterprise – On-Prem. Use it to assess the default state of a deployment and the configuration options relevant to your environment. Customers are responsible for confirming the effective configuration in their own deployment.

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.

Start with the accurate boundary

Firefox Enterprise services run in the infrastructure you operate. Some browser connections to external services are active by default, however, and should be assessed as part of your deployment design.

On-Prem deployment does not by itself mean that no data leaves your organization, that there are no external connections, or that the deployment is fully air-gapped. Customers should review and configure each connection category for their environment.

Default browser connection categories

Firefox Enterprise may make browser connections related to:

Connection category	What it supports	How to assess it
Location services	Location-related browser functions.	Review enterprise policy and network configuration for your environment; can be disabled via policy.
Safe Browsing / phishing protection	Protection against known harmful sites.	Assess available configuration and the security impact of any restriction.
Search and search suggestions	Configured search functions and suggestions.	Review browser configuration and approved search-provider settings.
DNS-over-HTTPS	Browser DNS resolution.	Review enterprise policy and network controls alongside your DNS design.
Certificate validation	Certificate and connection validation.	Review network and trust configuration before limiting connections, as they may affect connection security.

Available controls differ by connection. Administrators should review enterprise policy, browser configuration and network controls together before and after deployment.

Remote Settings and isolation requirements

Remote Settings is a documented external dependency. The available deployment modes involve either retrieval of configuration data from a source repository or browser-client connections to a Mozilla-hosted endpoint.

Fully isolated operation is not a configuration Mozilla can confirm today. If isolation is a hard requirement, raise it during technical evaluation so the architecture and remaining dependencies can be assessed together. Customers are responsible for determining whether any deployment meets their specific isolation requirements.

Telemetry

No telemetry is sent to Mozilla in the On-Prem model.

Local telemetry collection within your infrastructure is enabled by default, and can be disabled entirely through enterprise policy. The current control is all-or-nothing: administrators can disable local telemetry collection rather than selectively filter individual metrics.

Customers should assess whether the default local telemetry collection is appropriate for their environment and configure accordingly.

Crash data

Full crash reports, including any memory-dump content, are collected on the customer's infrastructure and are submitted only when a user actively chooses to submit them. A separate crash ping is collected locally by default and is governed by the same enterprise policy used to disable telemetry.

Customers should assess whether crash reporting and telemetry collection are appropriate for their environment, then configure retention and access accordingly.

How to review and verify

- Confirm the effective configuration in your own environment.
- Review enterprise policies, network egress controls and applicable product documentation.
- Request the release-specific endpoint and configuration reference if you need a detailed technical assessment.

This guide describes the general connection categories and controls. The specific endpoints and policy details for your release should be confirmed against the release-specific documentation before deployment.

Need more detail?

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