LOGZILLA DOCUMENTATION

Windows Event Forwarding (Windows Agent)

Forward Windows Event Log entries to LogZilla over HTTP and HTTPS using the LogZilla Windows Agent, with installation, access tokens, and failover servers

Receiving Data in LogZilla · Generated April 27, 2026 · logzilla.ai/docs/receiving-data/windows-event-forwarding

Windows Event Forwarding (Windows Agent)

Windows does not natively send syslog. The LogZilla Windows Agent forwards Windows Event Log entries to LogZilla over HTTP/HTTPS. The agent runs as a Windows service and requires a LogZilla access token.

Download

- Agent and README: logzilla/extras · winagent (https://github.com/logzilla/extras/tree/master/winagent)

Prerequisites

- Configuration tool `SyslogAgentConfig.exe` requires .NET Framework 4.7.2 or later.
- The service `SyslogAgent.exe` has no prerequisites.
- A LogZilla access token for authentication.

Installation and first run

Download and run the `.msi` installer from the GitHub repository.
The installer creates `C:\Program Files\LogZilla\SyslogAgent` and places the binaries and manual in that directory.
Launch the configuration tool `SyslogAgentConfig.exe` (run as Administrator).

Configuration summary

The configuration tool provides the following key settings. Refer to the README in the GitHub repository for full UI screenshots and field descriptions.

- Primary LogZilla Server
  - HTTP/HTTPS address of the LogZilla server, optionally including a port.
  - Example: `https://logzilla.example.com:8443`
- Primary / Secondary API Key
  - Use a LogZilla access token. Tokens can be created via the CLI; see Getting Started (https://www.logzilla.ai/docs/logzilla-api/getting-started).
- Secondary LogZilla Server
  - Optional HTTP/HTTPS address for dual-forwarding.
- Primary/Secondary Use TLS and Select Primary/Secondary Cert

    - When using HTTPS, select the `.pfx` certificate files as required. The configuration tool imports these into the agent directory.

- Event Logs
    - Choose which Windows Event Logs to forward.
- Look up Account IDs
    - Look up account names for logged user IDs; disable to reduce overhead.
- Ignore / Include Event IDs
    - Reduce volume by specifying event IDs to ignore or include.
- Catch-up / Only while running
    - Choose whether to send missed events after restarts (catch-up) or only send while the agent is running.
- Facility and Severity
    - Select default facility; set severity to Dynamic or Fixed.
- Extra Key/Values
    - Add custom key-value pairs to aid parsing in LogZilla rules.
- Max Batch Size / Max Batch Age
    - Control batching size and time; set batch size to 0 for immediate send.
- File Watcher (tail)
    - Optionally tail a text file and forward each new line as an event.
    - File Name: path to the file that will be tailed.
    - Program Name: value shown in LogZilla's `program` field for tailed events.
- Log Level and Log File Name
    - Configure agent logging for local diagnostics.

Delivery endpoint and authentication

The agent sends HTTP/HTTPS POST requests to LogZilla's HTTP Receiver at the `/incoming` path and uses a token for authentication.

- Example endpoint: `https://logzilla.example.com/incoming`
- Token header examples are documented in HTTP Event Receiver (https://www.logzilla.ai/docs/receiving-data/http-event-receiver).

Verification

- In LogZilla, verify events from the agent are visible. The default extra fields include:
  - `_source_type: windows_agent`
  - `log_type: eventlog` (or `file` when using File Watcher)
  - `event_id`, `event_log`
- For network-level checks and captures, see Syslog Troubleshooting (https://www.logzilla.ai/docs/administration/syslog-troubleshooting).
- For receiver endpoint reference and minimal tests, see HTTP Event Receiver (https://www.logzilla.ai/docs/receiving-data/http-event-receiver).

LogZilla Windows App

Install the "MS Windows" app from the LogZilla app store (Settings → App store) so messages from the agent are parsed and labeled appropriately.