Stairwell Windows Forwarder 1.7.0 Release Notes

Version: 1.7.0.9
Date: May 19, 2025

This version includes all fixes and features from the 1.6.x stream, including customer hotfixes.

[1.6.8 Release Notes](#)

New Features

- When uninstalled, the forwarder now notifies the server. The asset view on the server shows that the forwarder has been uninstalled. (FOR-604)
- The Windows forwarder now sights Mach-O binaries, regardless of extension. (FOR-588)
- The Windows forwarder now sights ELF binaries, regardless of extension. (FOR-583)
- Diagnostics now contain additional CPU, disk, OS, and process information to help Stairwell troubleshoot customer issues. Calls to `wmic.exe` have been removed, since this component of the OS has been deprecated in Windows 11. (FOR-597)
- For troubleshooting purposes, the forwarder can now log all HTTP communication between the forwarder and the server. This is disabled by default, and can be enabled by setting the following registry value. The forwarder service needs to be restarted for this value to take effect. (FOR-631)

  Key: `HKEY_LOCAL_MACHINE\SOFTWARE\Stairwell\SwellService`
  Value: `TraceHttp`
  Type: `REG_DWORD`
  Supported Values: 0 - do not log HTTP traces, non-zero - log HTTP traces
  Default: 0
- New telemetry counters have been added to make it easier to troubleshoot customer issues (FOR-623)
  - Add new counters for file & process events dropped by the kernel driver before being reported. Events may be dropped under heavy load, or if the forwarder resource limits (CPU, disk, network) are too restrictive.
  - Add new counters to the backscan, to track the total number of files examined, as well as the number of files that are sighted.

○ Add new counters to track unreported file sightings and pending uploads.

Performance Enhancements and Tuning

- To ensure that the forwarder runs efficiently without impacting overall system performance, you can now fine-tune its resource usage, using the installation parameters below.

  These options provide flexibility to align the forwarder's behavior with your system's performance requirements. However, overly restricting the forwarder can result in missed sightings.

  ○ CPULIMIT - Limits the forwarder's CPU usage to the specified percentage. (FOR-594)
  ○ PROCESSPRIORITYCLASS - Adjusts the priority level of the forwarder process, relative to other processes on the system. (FOR-594)
  ○ NETLIMIT - Controls how much network bandwidth the forwarder can use. (FOR-615)
  ○ IOPRIORITY - Sets the priority for disk operations performed by the forwarder's hasher and uploader components. (FOR-598)
- By default, the forwarder now installs with the following resource limits. These limits can be overridden using installation parameters. (FOR-626, FOR-660)
  ○ Maximum CPU usage = 5%
  ○ Maximum network bandwidth = 50mbps
- Significantly improve the performance of the forwarder's in-memory file store, by adding indexes on frequently used data. (FOR-618, FOR-593)
- Improve kernel driver performance by ignoring uninteresting file IO, and delaying filename querying until required. (FOR-592, FOR-599)
- Improve backscan performance by reducing read sizes when looking for known content headers (FOR-591)
- The driver version data was fixed, as it previously caused some applications to display the driver description incorrectly (FOR-658)

Bug Fixes

- Improved handling of 503 HTTP codes. The forwarder now honors the retry-after header, if available. (FOR-581)
- Improved handling for renamed files, based on policy and content. (FOR-578)
- The forwarder uninstaller now has additional logic to delete the Stairwell data directory. Previously, the directory could sometimes be left behind. (FOR-515)
- The driver now normalizes all names before reporting them to the user mode service. Previously, a short path could be sent in some cases. (FOR-587, FOR-578)
- Performance counters are now persisted on service shutdown. (FOR-608)
- The driver now cleanly runs with driver verifier running. Previously, there was a race at startup that could result in a verifier warning. (FOR-571)
- Refactor hasher logic to avoid potential deadlocks. (FOR-574)

Thirdparty Components

- The forwarder bundled installer now includes the .NET Runtime version 8.0.15. (FOR-573)

Known Issues

- When the driver is disabled, the forwarder still attempts to sight files when they are executed. File sightings may be missed on volumes added after the forwarder starts, for example, on removable USB. In some cases, the OS provides the forwarder an unexpected path, and the forwarder skips the file. (FOR-521)
- We recommend installing to the default directory. If you install to a custom directory and upgrade, the upgraded version will be installed to the default directory (FOR-258)
- Updating from 1.4.x to this release is not supported. You can either update to 1.5.1 first (which requires a reboot to succeed) or you can manually uninstall 1.4.x and then install this release (FOR-357)

File Details

SHA256 Hash	File Name	URL
D71016117A31F3F5F5598D73EDDC1A30871F01D6186BB5F2466293B69835E66D	StairwellForwarderBundle-1.7.0.9.exe	https://downloads.stairwell.com/windows/1.7.0/StairwellForwarderBundle-1.7.0.9.exe
706CBA9711E5D04131CEB8B55637B47F7C04BD1F9628567338E4390D2DB8DD58	StairwellForwarder-1.7.0.9.exe	https://downloads.stairwell.com/windows/1.7.0/StairwellForwarder-1.7.0.9.exe
F2A203B8318BC835B3854C180CFB1DF93A3AE28C5C1E69FF1E9ED94267B2AC58	StairwellForwarderInternal-1.7.0.9.msi	https://downloads.stairwell.com/windows/1.7.0/StairwellForwarderInternal-1.7.0.9.msi