STAIRWELL

# Stairwell Windows Forwarder 1.6.6 Release Notes

Version: 1.6.6.5
Date: Dec 16, 2024

**New Features**

- The Windows forwarder will now report any associated Mark of the Web / Zone.Identifier data when sighting a file. This can be queried on the server via `object.origin == "WEB"` (FOR-83)
- The Windows forwarder now supports disabling the forwarder driver and running without any kernel presence. This mode results in limited visibility, but may be required in certain environments. When the driver is disabled, the forwarder will continue to sight process execution and DLL loads. However, file modifications are no longer visible.

  The driver status can be changed per-policy, via the `Enable Kernel Driver` checkbox. For auditing purposes, forwarders report their driver status (enabled or disabled), and this is visible on a forwarder's asset page. (FOR-406)
- The Windows forwarder now supports an optional daily backscan. This setting and the scan start time are configurable per-policy. For improved visibility in environments where the forwarder driver is disabled, we recommend enabling daily backscan. (FOR-480)
- The forwarder now sends alerts, audit logs, and telemetry to the server so that Stairwell can react more quickly to issues in the field. (FOR-384)
- As part of the telemetry effort, the forwarder now maintains a set of Windows Performance Counters, that can be viewed in Performance Monitor and similar. The counters are all grouped in the `StairwellForwarderCounters` category. (FOR-384)
- The environment variable `STAIRWELL_REGISTRATION_KEY` allows devices to be assigned a unique asset identifier, enabling each asset to be distinctly identified within an environment. Asset identifiers must be unique and comply with the company's naming standards. The Stairwell server ensures that devices with the same asset identifier are consistently assigned the same asset ID even after re-imaging. The Stairwell server ensures a one-to-one mapping between company-assigned tags and their corresponding Stairwell ASSET_ID (FOR-411)

STAIRWELL

- The forwarder installer has improved logic for handling the auth token and environment ID parameters, including fixing the case where the parameters are accidentally swapped. (FOR-106)

**Bug Fixes**

- The forwarder data folder was writable by regular users, leading to potential escalation of privilege & denial of service. The security on this folder has been tightened. (FOR-507)
- To reduce upload timeouts, the file upload timeout has been increased from 100 seconds to 300 seconds. (FOR-443)
- During backscan, file extensions specified in the policy could be excluded due to a bug in how the forwarder searched the policy. (FOR-408)
- In rare cases, the service could restart while uploading a file, due to a race condition. (FOR-442)
- In certain configurations, service shutdown could take up to a minute. The service now shuts down on the order of a few seconds. (FOR-471)
- Manually setting incorrect types for registry values (for example, a string instead of a DWORD) could cause the service to restart due to an exception. (FOR-371)
- Updating the forwarder or repairing the installation could sometimes require a reboot because of a race condition when stopping the service. We now wait for the service to stop before proceeding. (FOR-508)

**Thirdparty Components**

- .NET 6.0 is end-of-life as of November 12, 2024 though the forwarder will still use it if available. In our bundled installer, we have replaced .NET 6.0 with .NET 8.0.11 (FOR-466)
- We've updated the WiX Installer Toolset to 3.14.1 due to multiple vulnerabilities (FOR-500)

**Other Changes**

- Icons have been added to SwellService.exe so that the Stairwell icon appears in Task Manager and similar. (FOR-403)

**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 |
|---|---|---|
| af5cee61deac0990884a42375514e6a5a013c5054eb11abbf852d2666174ea13 | StairwellForwarderBundle-1.6.6.5.exe | https://downloads.stairwell.com/windows/1.6.6/StairwellForwarderBundle-1.6.6.5.exe |
| dc42001b88e58922c637f3a8ac7d26bfe30547b4e4e23638720741453dee7a5b | StairwellForwarder-1.6.6.5.exe | https://downloads.stairwell.com/windows/1.6.6/StairwellForwarder-1.6.6.5.exe |
| e32bbacdaa7ec07278fc607705df04c537b5687c633987d14c996306bc13e9dc | StairwellForwarderInternal-1.6.6.5.msi | https://downloads.stairwell.com/windows/1.6.6/StairwellForwarderInternal-1.6.6.5.msi |