Log Collector - Check OS Version

Windows OS Version Compatibility Issues

Elastic Agent supports Windows Server versions (e.g., 2016+), Windows 10/11, but drops support for EOL versions like Windows 8 and Server 2012 from 7.17.19 onwards. It does not support 32-bit systems or ARM processors. Common issues arise from attempting installations on unsupported or EOL versions, leading to failures in enrollment, data collection, or security integrations like Elastic Defend (which requires Windows Security Center, absent on Servers).

Common Problems

- Installation or upgrades fail on EOL versions (e.g., Windows Server 2012R2), causing BSOD or rollback due to incompatibility checks.
- Elastic Defend not recognized or installable on Windows Server editions, as they lack Windows Security Center.
- Agent starts loops or stuck in updating state on Windows 10 with specific versions (e.g., 8.5.3 or during failed upgrades).
- No support for ARM processors, leading to installation errors on ARM-based Windows devices.
- Uninstall failures on Windows Server with newer versions (e.g., 9.1.4), leaving corrupted installations.
- Integration issues (e.g., Windows security events not processed) in certain agent versions like 9.1.4 or 8.19.4.

Symptoms

- BSOD or automatic rollback during upgrades on unsupported versions. (Rare case, happened on unsupported OS)
- Agent status stuck in "updating" or "unhealthy," with no data ingested.
- Errors like "unsupported OS" or "compatibility check failed" in installation logs.
- Service start loops or agent not running properly on older Windows 10 builds.
- Defend integration shows as unavailable or degraded on Servers.
- Uninstall errors leaving broken symlinks or processes.

Fixes

- Upgrade to a supported Windows version (e.g., Server 2016+ or Windows 10/11 non-ARM).

- For Defend, use non-Server editions or alternative integrations; avoid upgrades that trigger BSOD.
- Manually uninstall via command line (e.g., elastic-agent uninstall) and reinstall a compatible version.
- Update to latest agent versions (e.g., 9.1.4+ fixes for security events) and verify in Fleet.
- Check support matrix before install; use x86_64 hardware only.
- For start loops, restart service or downgrade/upgrade agent version.

***Sources**:*

Elastic Defend not recognized from Windows Server operating system - Elastic Security / Endpoint Security - Discuss the Elastic Stack

Elastic Defend on windows 2012R2 - Elastic Security - Discuss the Elastic Stack

Can't uninstall agent 9.1.4 on Windows server · Issue #10546 · elastic/elastic-agent

OSquery fails to run after upgrade from versions before v8.15.4 due to stricter extension permission checks · Issue #6792 · elastic/elastic-agent

Elastic Agent known issues | Elastic Agent

[Fleet] Agent gets stuck in the updating state if the upgrade action fails · Issue #2508 · elastic/elastic-agent

Elastic agent start loop - Security - Spiceworks Community

Upgrades that fail and are rolled back can break the elastic-agent command symlink · Issue #2264 · elastic/elastic-agent

Linux OS Version Compatibility Issues

Elastic Agent requires native Linux installs (no WSL), supports x86_64 and aarch64 (from 7.16+), but not 32-bit. Minimum distro versions include RHEL/CentOS 7+, Ubuntu 18.04+, with drops for EOL like CentOS 8, Debian 9/10 from 7.17.19/23. Issues often occur on unsupported distros or kernels, affecting installation, data collection, or integrations.

Common Problems

- No support for older distros like RHEL 5/6, CentOS 8, Debian 9/10, leading to install failures.
- WSL (Windows Subsystem for Linux) unsupported, causing agent to fail enrollment or run.
- Compatibility issues on EOL distros (e.g., CentOS/RHEL 7 dropped from 7.17.23, Users can still install older agent version), resulting in no updates or stability problems.
- OSquery or other integrations fail after upgrades on unsupported kernels/versions (e.g., post-8.15.4).
- Agent stuck in updating or unenrolled state on certain distros during version mismatches.
- No data collected on specific versions like 8.15.0 due to compatibility checks.

Symptoms

- Installation errors like "unsupported distribution" or "GO lang incompatibility."
- Agent shows "unhealthy" or "updating" indefinitely, with rollback logs.
- No metrics/logs ingested despite agent running.
- Unenrollment or duplicate processes after policy updates on mismatched versions.
- Stability issues post-EOL, like failed check-ins.

Fixes

- Migrate to supported distros (e.g., RHEL 7+ for older, or 8+ for full support).
- Use native Linux instead of WSL; install via package managers like yum/apt.
- Upgrade agent to versions that align with your distro (e.g., avoid post-7.17.23 on RHEL 7).
- Remove conflicting integrations (e.g., OSquery) before upgrade, then reinstall.
- Force unenroll/re-enroll in Fleet for stuck states.
- Check GO support for your distro; upgrade OS if near EOL.

Sources:

Agent support for OS windows server and red hat - Elastic Stack / Beats - Discuss the Elastic Stack

Elastic Agent support RHEL 6 - Elastic Stack / Elastic Agent - Discuss the Elastic Stack

8.7.0 and 8.6.2 agents get stuck in the updating state if the osquery.db file cannot be copied to the next version · Issue #2433 · elastic/elastic-agent

Elastic-Agents unexpectedly unenrolled after update to 8.16.x · Issue #6213 · elastic/elastic-agent

Some policy updates can cause duplicate Endpoint processes · Issue #2008 · elastic/elastic-agent

macOS OS Version Compatibility Issues

Elastic Agent supports macOS 11+ (Big Sur+), with x86_64 and aarch64 (M1/M2) from 8.2+. Drops support for EOL like 10.14/10.15 from 7.17.19. Issues are common on newer versions like Sequoia (support in progress) or Ventura, often involving SIP, extensions, or version-specific errors.

Common Problems

- Support for macOS Sequoia (15.x) in progress, but Elastic Defend installation may not be fully supported yet.
- Errors initializing version info or running on Ventura (13.x+), especially M1 chips.
- Dropped support for older macOS (10.14/10.15), causing install/upgrade failures.
- Network issues like external NIC blocked by agent in Monterey (12.x+).
- OSquery fails post-upgrade on versions before 8.15.4 due to checks.
- Agent stuck updating or unenrolled on version mismatches.

Symptoms

- Installation errors like "failed to fix permissions" on Ventura/M1.

- Agent degrades or shows unhealthy due to unsupported extensions on Sequoia.
- No data or logs ingested post-upgrade.
- Network connectivity loss after install on older macOS versions.
- Rollback logs or stuck "updating" status.
- Unenrollment after updates.

Fixes

- Upgrade to supported macOS (11+ for Intel, 8.2+ for M1/M2).
- For Sequoia, wait for official support or test Defend manually.
- Run as root (sudo elastic-agent run) for troubleshooting on Ventura+.
- Approve network extensions in System Settings for NIC issues.
- Uninstall OSquery before upgrade, then reinstall.
- Force policy reset or re-enroll for stuck states.

Sources:

macOS Sequoia (15.x) Support - Elastic Security - Discuss the Elastic Stack

Error initializing version information: reading package version from file....package.version: no such file or directory · Issue #3285 · elastic/elastic-agent

External NIC Blocked by Elastic Agent - Elastic Security / Endpoint Security - Discuss the Elastic Stack

[Fleet] Agent gets stuck in the updating state if the upgrade action fails · Issue #2508 · elastic/elastic-agent

Compatibility

Support Matrix | Elastic

Revision #5
Created 27 November 2025 09:09:13 by Richmond Abella
Updated 4 December 2025 02:08:28