THE CYBER TOOLCHAIN

NO. 088

Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED SEPTEMBER 28, 2026 · EVERY DAY

The daily firehose — everything the toolchain shipped today, already filtered.

▸ // HOW THIS ISSUE IS MADE SHOW

VIEW

ISSUE VIEW

scroll



SCROLL | EXPAND IN PLACE | PREVIEW PANE

INFORMATION DENSITY

everything



BRIEFED | EVERYTHING

Every tool in the issue, in full.

all 122 changes

Do you prefer **scroll**? 👍 👎

▸ // CONTENTS SHOW 20 tools

▾ // THE BRIEF HIDE

What stands out across today's releases, grouped by what it lets you do. Every tool named links to its entry below.

RESPOND

Work a phishing report and the endpoint activity behind it as one ident

vim ? help

Email threat telemetry flows into Elastic, quarantine runs as a SOAR action, and Attack Discovery correlates the mail signals with endpoint ones into ATT&CK-mapped incidents. That removes the usual pivot between a mail security console and the SIEM to answer whether the person who got the lure also clicked it.

Elastic Security Labs

GOVERN

Put a policy checkpoint between AI agents and the tools and data they touch

WitnessAI enforces an approved-tool list at the network layer for MCP, inspects traffic in both directions and logs it to one audit trail; Bedrock extends Agent DLP to the NVIDIA OpenShell sandbox boundary with blast-radius review before deployment. Agent tool calls have mostly been unlogged and ungoverned — this is the point where an org can answer which agent reached which system and with what data.

WitnessAI · Bedrock Security

IDENTIFY

Catch API attack surface growing before the release ships

Diff Mode compares discovered endpoints between git revisions and gates CI on the delta, with reports in multiple formats. Instead of re-running discovery and eyeballing a longer list, a reviewer sees exactly which routes this branch added — and full scans run roughly 1.75x faster.

noir

PROTECT

Allow a vetted GitHub Action without switching the control off

StepSecurity's low-score Action control now takes exemptions by name or owner across all versions, so one legitimately obscure but audited Action no longer forces teams to disable the gate repo-wide. Cloudsmith adds Nix binary cache push and substituter consumption plus Cargo and pnpm credential helpers, pulling those ecosystems behind the same private registry and auth path as the rest.

StepSecurity · Cloudsmith

OFFENSIVE SECURITY

◆ Exploitation & C2

Bugcrowd

Feedback ⓘ Request a Response Withdrawal (2026-09-28)

BLOG ↗ RANK

Bugcrowd is a crowdsourced security platform connecting organizations with ethical hackers to identify and report software vulnerabilities.

> Bugcrowd introduced a Response Withdrawal workflow for both researchers and customers, then extended it with dedicated tracking and filtering of withdrawn requests inside Security Inbox.

└──▷ **WHAT SHIPPED · 1 FEATURE** most completely described first ? what's the number?

01 **Response Withdrawal workflow and tracking** NEW 74

Researchers and customers can now retract a previously submitted response via the new Request a Response Withdrawal workflow, accessible under Researchers > Request a Response Withdrawal or Customers > Request a Response Withdrawal on a submission. Withdrawn Request a Response (RaR) submissions are automatically removed from active queues, surfaced via a dedicated Withdrawn requests to Customer filter in Security Inbox, and preserved as expandable items in the submission's Activity feed showing the researcher's stated withdrawal reason.

When a researcher needs to retract a previously submitted response on a submission.

> 📍 In the Bugcrowd platform, navigate to the relevant submission as a researcher, then go to Researchers › Request a Response Withdrawal and submit the withdrawal request.

When a customer needs to withdraw a response on a submission from their side of the platform.

> 📍 In the Bugcrowd platform, navigate to the relevant submission as a customer, then go to Customers › Request a Response Withdrawal and submit the withdrawal request.

Review all RaRs a researcher has withdrawn to audit outstanding response obligations and close out stale items.

> 📍 In Security Inbox, open the filters panel and select Withdrawn requests to Customer to list all withdrawn RaRs, then expand any entry in the submission's Activity feed to view the researcher's stated withdrawal reason.

— Names the exact filter, menu paths, and workflow but no API/config details.

Request a Response Withdrawal (2026-09-…

Request a Response Withdrawal (2026-09-28)

BLOG ↗ LATEST STABLE

Bugcrowd adds withdrawal tracking for Request a Response, with a dedicated `Withdrawn requests to Customer` filter in Security Inbox.

└──▷ HOW TO FIND IT

Review all RaRs a researcher has withdrawn to audit outstanding response obligations and close out stale items.

> 📍 In Security Inbox, open the filters panel and select `Withdrawn requests to Customer` to list all withdrawn RaRs, then expand any entry in the submission's Activity feed to view the researcher's stated withdrawal reason.

Filters withdrawn Request a Response (RaR) submissions via the `Withdrawn requests to Customer` filter in Security Inbox.

Automatically removes researcher-withdrawn RaRs from active queues and preserves them as expandable items in the submission's Activity feed with the withdrawal reason.

WAS THIS USEFUL? 👍 👎

Bugcrowd Researcher Platform

Feedback ⓘ

Request a Response Withdrawal (2026-09-28) BLOG ↗ RANK

Bugcrowd Researcher Platform crowdsources security vulnerability discovery by connecting organizations with ethical hackers and security researchers worldwide.

> Bugcrowd added self-service withdrawal for Request a Response (RaR) requests, letting researchers cancel open requests directly from the submission page.

└──▷ **WHAT SHIPPED · 1 FEATURE** most completely described first ? what's the number?

01 Self-service withdrawal for Request a Response (RaR) NEW

77

Researchers can now withdraw an open RaR request directly from the submission page at any time, which immediately frees the active account slot and cancels any review in progress. A confirmation email is sent and the withdrawal reason is logged in the submission's Activity feed. RaR limits are enforced at the submission level across both primary researchers and collaborators, with withdrawn requests permanently counting toward the 2-request-per-submission maximum.

Withdraw an open RaR request to reclaim your active slot before raising a new one on a different submission.

> 📍 1. Open the submission page for the report with an active RaR request. 2. Locate the open Request a Response entry. 3. Select Withdraw and provide a withdrawal reason. 4. Confirm — the slot is freed immediately and the reason is logged in the Activity feed.

— Names UI path, Activity feed, email, and 2-request limit; gives exact steps.

Request a Response Withdrawal (2026-09-…

Request a Response Withdrawal (2026-09-28) BLOG ↗ LATEST STABLE

Bugcrowd RaR gets self-service withdrawal: researchers can now cancel open requests directly from the submission page.

└──▷ **HOW TO FIND IT**

Withdraw an open RaR request to reclaim your active slot before raising a new one on a different submission.

> 📍 1. Open the submission page for the report with an active RaR request. 2. Locate the open Request a Response entry. 3. Select Withdraw and provide a withdrawal

reason. 4. Confirm — the slot is freed immediately and the reason is logged in the Activity feed.

Enables researchers to withdraw open Request a Response (RaR) requests directly from the submission page at any time, immediately freeing an active account slot and cancelling any review in progress.

Sends a confirmation email and logs the withdrawal reason in the submission's Activity feed when a RaR request is withdrawn.

Enforces RaR limits at the submission level across both primary researchers and collaborators, with withdrawn requests permanently counting toward the 2-request-per-submission maximum.

WAS THIS USEFUL?  

APPLICATION SECURITY

◆ SAST / SCA / Code Security

noir

Feedback ⓘ v1.4.0 NOTES ↗ RANK

Hunt every Endpoint in your code, expose Shadow APIs, map the Attack Surface.

> Noir's biggest addition this window is a full Diff Mode for tracking attack-surface drift across git revisions with CI gating and multi-format reports, alongside new DAST delivery integrations, a Tagger subsystem, and roughly 1.75x faster full scans.

└──▷ WHAT SHIPPED · 7 FEATURES most completely described first ? what's the number?

01 **Diff Mode for attack surface changes** NEW 98

Adds `--diff-ref <revision>` to `noir scan` to diff the current working tree's attack surface against any git revision (branch, tag, commit, or `HEAD~1`) without a second checkout, reporting added, removed, and changed endpoints and flagging lost authentication as `auth_removed`. `--fail-on` accepts comma-separated categories (`added`, `removed`, `changed`, `auth-removed`) and exits non-zero (exit code 3) on matches for CI gating; the GitHub Action exposes `diff_ref` and `fail_on` inputs. Output formats include `-f markdown-table` (count table plus separate added/removed/changed/lost-auth tables suitable for PR comments), `-f sarif` (added endpoints/params as notes, lost-auth endpoints as warnings), and `-f toml`, with any other `-f` value falling back to a text diff with a warning. Auth removal shows as `! auth tag removed` when run with `-T` / `--use-taggers`, and structured diff output exposes `auth_removed`, `params_added`, `params_removed`, `tags_added`, and `tags_removed` fields per endpoint.

Catch any route that dropped its auth requirement before merging — fail CI and write a markdown summary for the PR comment.

```
$ noir scan . --diff-ref origin/main --fail-on auth-removed,added
-f markdown-table -o diff.md
```

Block pushes locally if any endpoint silently loses its auth tag, using a git pre-push hook.

```
$ #!/bin/sh
exec noir scan . --diff-ref origin/main --fail-on auth-removed --
no-log
```

Scope the attack-surface diff to a single service in a monorepo and emit JSON for downstream processing.

```
$ noir scan ./services/billing --diff-ref origin/main -f json
```

Detect endpoints added, removed, or stripped of authentication since the last release tag — fail CI when any auth_removed finding is present.

```
$ noir scan . --diff-ref v1.3.1 --fail-on auth_removed
```

— Full mechanism, flags, formats and runnable commands given `v1.4.0`

02 **Multipart and XML request body generation** NEW 60

File upload params now emit multipart bodies in `curl`, `httpie`, `PowerShell`, `OAS2`, and `OAS3` output; XML params emit `application/xml` bodies in OAS and Postman output.

— Names formats affected but no command shown `v1.4.0`

THINNER COVERAGE BELOW

03 **Multi-threaded scanning performance** IMPROVED 50

Directory listing, file reads, passive-scan rules, and Go route parsing now run on worker threads in walk order, making default scans ~1.4x faster and full scans ~1.75x faster.

— Concrete speedup numbers but no action needed `v1.4.0`

04 **DAST pipeline and delivery integrations** NEW 45

Adds Gori as a supported DAST pipeline integration target alongside ZAP, Burp Suite, and Caido. A new Deliver subsystem pushes scan results directly to downstream tools including Burp Suite, ZAP, and Elasticsearch.

— Names targets but no config or command shown `product docs`

05 **Contributing technologies on merged endpoints** IMPROVED 45

Merged endpoints now carry every contributing technology in `details.technologies`.

— Names field but no usage example `v1.4.0`

06 **Tagger subsystem for endpoint context** NEW 40

Adds a Tagger subsystem that applies contextual tags to discovered endpoints; used, for example, to surface `auth` tag removal in diff output when scans run with `-T` / `--use-taggers`.

— Purpose stated but tagging rules unspecified `product docs`

07 **Express and gRPC route detection additions** IMPROVED 35

Adds support for Express routes registered through a forwarding helper and the field form of the gRPC `google.api.http` annotation.

— Names the patterns but no example or scope `v1.4.0`

`v1.4.0` NOTES ↗ LATEST STABLE

Noir v1.4.0 adds `--diff-ref` attack-surface diff mode with auth-removal detection, SARIF/markdown reports, and ~1.75x faster full scans.

└──▷ **GET THIS VERSION**

```
$ git clone --branch v1.4.0 https://github.com/owasp-noir/noir.git
# already have the repo? check out this version:
$ git checkout v1.4.0
```

└──▷ **TRY IT**

Detect endpoints added, removed, or stripped of authentication since the last release tag — fail CI when any auth_removed finding is present.

```
$ noir scan . --diff-ref v1.3.1 --fail-on auth_removed
```

Adds `--diff-ref` to diff the attack surface against a git revision, flagging changed endpoints and lost authentication as `auth_removed`; `--fail-on` exits with code 3 on matching findings, and the GitHub Action exposes `diff_ref` and `fail_on` inputs.

Diff mode renders markdown and SARIF diff reports for CI consumption.

Merged endpoints now carry every contributing technology in `details.technologies`.

File upload params now emit multipart bodies in curl, httpie, PowerShell, OAS2, and OAS3 output; XML params emit `application/xml` bodies in OAS and Postman output.

> Adds support for Express routes registered through a forwarding helper and the field form of the gRPC `google.api.http` annotation.
>
> +1 more

WAS THIS USEFUL? 👍 👎

Mend.io Mend SCA

Feedback ⓘ

Version 26.9.1 (27-September-2026) NOTES ↗ RANK

Traditional application security misses AI risk. Standalone AI security tools miss your code.

> Mend SCA added support for the Bun JavaScript package manager, extending dependency detection across the CLI and repository integrations.

└──▷ **WHAT SHIPPED · 1 FEATURE** most completely described first ? what's the number?

01 **Bun package manager support** NEW 60

Mend CLI and Mend Repository Integrations now automatically detect and report direct and transitive dependencies for projects using `package.json` alongside `bun.lock` or `bun.lockb` files.

— Names exact files supported but no usage steps shown Version 26.9.1 (27-September-2026)

> Version 26.9.1 (27-September-2026) NOTES ↗ LATEST STABLE
>
> Mend SCA 26.9.1 adds Bun package manager support for automatic detection of direct and transitive JavaScript dependencies.

WAS THIS USEFUL? 👍 👎

Cloudsmith

Feedback ⓘ

CLI v1.21.0 to v1.26.0: Nix support, Cargo and pnpm credential helpers, and repository a

BLOG ↗ RANK

A fully-managed, enterprise-scale solution to control, secure, and distribute software packages and containers.

> Cloudsmith's CLI (v1.21–v1.26) adds Early Access Nix binary cache support with push, native substituter consumption and upstream management, alongside new Cargo and pnpm credential helpers and terminal-based repository GPG and access administration.

└──▷ **WHAT SHIPPED · 4 FEATURES** most completely described first ? what's the number?

01 **Nix binary cache support: push, consume and upstream management**

NEW 96

Cloudsmith adds Nix package support (Early Access) across CLI, API and web app. Packages are pushed with `cloudsmith push WORKSPACE/REPOSITORY STORE_HASH.nar --narinfo-file STORE_HASH.narinfo`, supporting optional narinfo sidecars and standard push flags `--tags`, `--republish`, and `--no-wait-for-sync`. Packages are served at `https://nix.cloudsmith.io/WORKSPACE/REPOSITORY` using the native Nix binary cache protocol with server-side ED25519 signing of every narinfo on read, and can be consumed by embedding a token in the substituter URL as `https://token:TOKEN@nix.cloudsmith.io/WORKSPACE/REPOSITORY`. Nix upstreams (e.g. to mirror a NixOS channel) are managed via `cloudsmith upstream create`, `list`, `update`, and `delete` subcommands driven by a JSON config file such as `nix-upstream.json`, supporting modes Cache and Proxy and auth modes including None, with a `--yes` flag on `cloudsmith upstream delete` for unattended removal.

Push a locally built NAR and its narinfo to Cloudsmith in one command so the package is immediately resolvable by Nix clients.

```
$ cloudsmith push myorg/mynixrepo abc123def456.nar --narinfo-file
abc123def456.narinfo --tags nix,ci
```

Point a Nix client at a private Cloudsmith binary cache so `nix-build` or `nix shell` can substitute store paths without rebuilding.

```ini
extra-substituters =
https://token:TOKEN@nix.cloudsmith.io/myorg/mynixrepo
```

Mirror a NixOS channel through Cloudsmith so consumers get cached upstream packages alongside your own, with a reusable JSON-driven workflow.

```
$ cloudsmith upstream create myorg/mynixrepo nix-upstream.json
```

— Full push/consume/manage workflow with exact commands, endpoints and flags

CLI v1.21.0 to v1.26.0: Nix support, Ca…

02 Cargo credential helper for private registries NEW

90

Adds the `cargo-credential-cloudsmith` credential helper, installable via `credential-helper`, which registers itself in `$CARGO_HOME/config.toml` (or `~/.cargo/config.toml`) under the `[registry]` `global-credential-providers` list and resolves Cloudsmith API keys, SSO tokens, and OIDC credentials automatically; requires Cargo 1.74+. Also supports the sparse Cargo registry protocol via `sparse+https://cargo.cloudsmith.io/WORKSPACE/REPOSITORY/` alongside the existing git-index endpoint.

Set up a private Cloudsmith Cargo registry using the credential helper so that existing Cloudsmith CLI credentials are used automatically — no token stored in Cargo config.

```
$ # 1. Add the registry (no token) in ~/.cargo/config.toml
# [registries]
# my-org-myrepo = { index =
"sparse+https://cargo.cloudsmith.io/my-org/my-repo/" }

# 2. Install the credential helper, discovering custom domains
for the workspace
credential-helper --workspace my-org
```

Register a Cloudsmith sparse Cargo registry for a private workspace without a hardcoded token, relying on the credential helper for auth.

```toml
[registries]
my-org-my-repo = { index =
"sparse+https://cargo.cloudsmith.io/my-org/my-repo/" }

[registry]
global-credential-providers = ["cargo:token", "cargo-credential-
cloudsmith"]
```

List or remove installed Cloudsmith credential helpers to audit or clean up a CI runner without disturbing crates.io authentication.

```
$ credential-helper list
credential-helper uninstall
```

— Names exact config keys, endpoint and version requirement

CLI v1.21.0 to v1.26.0: Nix support, Ca…

---

03 **pnpm credential helper for automatic authentication** NEW

90

Adds `pnpm-credential-cloudsmith`, a credential helper letting pnpm authenticate to Cloudsmith registries using the CLI credential chain (API key, SSO keyring token, or OIDC) via pnpm's `tokenHelper` setting in the user-level `.npmrc`. The installer writes a `//npm.cloudsmith.io/:tokenHelper=/path/to/pnpm-credential-cloudsmith` entry to the user-level `.npmrc` (target a non-default file with `NPM_CONFIG_USERCONFIG`). The `credential-helper pnpm` subcommand supports `-w` / `--workspace WORKSPACE` to discover custom Cloudsmith npm domains, plus `--domain HOSTNAME`, `--no-discover`, `--refresh`, `--dry-run`, and `--bin-dir DIRECTORY`; `credential-helper list` and `credential-helper uninstall pnpm` (with `--dry-run`) inspect or remove installed helpers.

Install the pnpm credential helper for a workspace so pnpm retrieves tokens automatically without storing them in plaintext.

```
$ credential-helper pnpm --workspace WORKSPACE
```

Preview what the uninstaller would remove before committing, to verify no unintended entries are touched.

```
$ credential-helper uninstall pnpm --dry-run
```

— Exact flags, config entry and env var given CLI v1.21.0 to v1.26.0: Nix support, Ca…

THINNER COVERAGE BELOW

04 Repository administration from the CLI terminal NEW

35

Enables GPG key management for repositories directly from the CLI, without using the web UI, and enables repository access-privilege administration from the CLI terminal.

— No commands or flags named, only prose description

CLI v1.21.0 to v1.26.0: Nix support, Ca…

└──▷ **ALSO FROM THESE RELEASES**

CLI v1.21.0 to v1.26.0: Nix support, Cargo and pnpm credential helpers, and repository

BLOG ↗ LATEST STABLE

Cloudsmith CLI v1.21–v1.26 adds Nix package push, Cargo and pnpm credential helpers, and terminal-based repo GPG/access management.

Adds Nix package support, enabling `cloudsmith push` for Nix packages.

Adds a Cargo credential helper so Rust projects authenticate to Cloudsmith repositories automatically.

Adds a pnpm credential helper so pnpm authenticates to Cloudsmith repositories automatically.

Enables GPG key management for repositories directly from the CLI, without using the web UI.

Enables repository access-privilege administration from the CLI terminal.

WAS THIS USEFUL?  

Mend.io Mend SAST

Feedback ⓘ

Version 26.9.1 (28-September-2026) NOTES ↗ RANK

Mend SAST is a static application security testing service that scans source code for vulnerabilities and helps teams prioritize remediation.

> Mend SAST 26.9.1 adds real-time console log streaming to CLI scans and automatically excludes macOS metadata files across all scan engines, while also extending JavaScript dependency detection to Bun.

└──▷ **WHAT SHIPPED · 3 FEATURES** most completely described first ? what's the number?

01 **Console log streaming for CLI scans** NEW 75

The `mend code` CLI now supports a `--print-to-console` flag that prints scan logs directly to stdout in real time, in addition to writing the existing log file, letting CI pipelines tail SAST scan progress without separately tailing the log file.

Stream scan logs to the console during CI runs so pipeline output captures real-time SAST progress without having to tail a separate log file.

```
$ mend code --print-to-console
```

Tail SAST scan progress live in a CI pipeline console without waiting for the log file to flush.

```
$ mend code --print-to-console
```

Tail SAST scan output in real time during CI runs without separately tailing the log file.

```
$ mend code --print-to-console
```

— Names exact flag and behaviour, runnable command given

Version 26.9.1 (28-September-2026)

02 **Automatic exclusion of macOS metadata files** IMPROVED 65

Default exclusions in `mend code` CLI scans now automatically ignore `/_MACOSX/..*` metadata files across all SAST scan engines, even when default exclusions are otherwise disabled.

— Names exact path pattern and scope, no user action needed

Version 26.9.1 (28-September-2026)

03 **Bun package manager support** NEW 60

Adds Bun package manager support for JavaScript projects, enabling automatic detection and reporting of direct and transitive dependencies when `package.json` is present alongside `bun.lock` or `bun.lockb` files.

— Names files and dependency scope but no CLI action shown product docs

Version 26.9.1 (28-September-2026) NOTES ↗ LATEST STABLE

Mend SAST 26.9.1 adds `--print-to-console` flag to `mend code` and auto-excludes macOS metadata files from all SAST scan engines.

└──▷ **TRY IT**

Stream scan logs to the console during CI runs so pipeline output captures real-time SAST progress without having to tail a separate log file.

```
$ mend code --print-to-console
```

Adds `--print-to-console` flag to `mend code` CLI scans, printing scan logs directly to stdout in real time in addition to the log file.

Default exclusions in `mend code` CLI scans now automatically ignore `/_MACOSX/..*` metadata files across all SAST scan engines, even when default exclusions are otherwise disabled.

WAS THIS USEFUL? 👍 👎

StepSecurity

Feedback ⓘ

Low Score Exemptions for Control Evaluation (2026-09-28) BLOG ↗ RANK

StepSecurity hardens CI/CD pipelines by detecting and preventing supply chain attacks through runtime security monitoring and vulnerability detection.

> StepSecurity added exemption support for the low-score Action control, letting teams whitelist vetted GitHub Actions by name or owner across all versions.

└──▷ **WHAT SHIPPED · 1 FEATURE** most completely described first ? what's the number?

01 **Low-score control exemptions in Control Evaluation** NEW

80

Adds exemption support for the 'Third-party GitHub Actions with high scores should be used' control, configurable under Settings > Control Evaluation in the Control options card. Actions can be exempted by exact name (e.g. `example-org/example-action`) or owner wildcard (e.g. `example-org/*`), and exemptions are version-independent — any version ref in an exemption entry is ignored, so the exemption covers every version of the Action.

Suppress low-score alerts for a vetted Action your team has reviewed, without needing to pin a specific version.

📍 In the StepSecurity console, go to Settings › Control Evaluation, open the Control options card for 'Third-party GitHub Actions with high scores should be used', and add `example-org/example-action` (or `example-org/*` to cover all Actions under that owner) to the exemptions list.

— Names exact UI path and config examples with clear mechanism.

Low Score Exemptions for Control Evalua…

Low Score Exemptions for Control Evaluation (2026-09-28) BLOG ↗ LATEST

STABLE

StepSecurity lets you exempt specific GitHub Actions from the low-score control by name or owner wildcard.

└──▷ **HOW TO FIND IT**

Suppress low-score alerts for a vetted Action your team has reviewed, without needing to pin a specific version.

📍 In the StepSecurity console, go to Settings › Control Evaluation, open the Control options card for 'Third-party GitHub Actions with high scores should be used', and add `example-org/example-action` (or `example-org/*` to cover all Actions under that owner) to the exemptions list.

Adds exemption support for the 'Third-party GitHub Actions with high scores should be used' control, configurable under Settings > Control Evaluation in the Control options card, allowing Actions to be exempted by exact name (e.g. `example-org/example-action`) or owner wildcard (e.g. `example-org/*`).

Exemptions are version-independent — any version ref in an exemption entry is ignored, so the exemption covers every version of the Action.

WAS THIS USEFUL? 👍 👎

Veracode

Feedback ⓘ Integration updates (2026-09-28) BLOG ↗

RANK

Veracode is a cloud-based application security platform that performs static, dynamic, and software composition analysis to identify vulnerabilities in code.

> Veracode expanded platform-driven management of its GitHub Workflow Integration—install, configure, and uninstall directly from the Veracode Platform, plus IaC/SCA/Static Analysis scheduling—while adding configuration and scheduling options to the Azure DevOps integration, extending findings filtering, authentication, and mitigation views across its IDE plugins, and adding pagination support to the Java API Wrapper.

└──▷ **WHAT SHIPPED · 11 FEATURES** most completely described first ? what's the number?

01 **Agent pool and branch scheduling config in Azure DevOps** NEW 85

Adds a custom agent pool name parameter to `veracode.yml` in Azure DevOps Workflow Integration v2.4.3 to specify which agent pool runs the pipeline, and adds support for scheduling `analysis_branch` scans in v2.3.10 so scheduled scans run against the branch set in `veracode.yml` instead of the default branch — together enabling scan scheduling for every organization where the Azure DevOps integration is installed.

— Names both config keys and their file, with versions Integration updates (2026-09-28)

02 **Pagination support in Java API Wrapper** IMPROVED 85

Adds page size support to the Platform Applications API (`/appsec/v1/applications`) in Java API Wrapper v26.3.19.0 to improve efficiency when retrieving large application lists, and introduces support for the paginated Sandbox REST API, enabling retrieval of sandbox lists using pagination.

— Names endpoint, wrapper version, and both surfaces Integration updates (2026-09-28)

03 **Findings filtering and grouping in VS Code** NEW 70

Adds a Current File filter to Static Scan Findings, scoping results to the file open in the editor, and adds an option to filter and group Static Scan Findings by file name with results grouped by severity per file, in Veracode Scan for VS Code v1.16.3.

— Names filters and version with clear UI path Integration updates (2026-09-28)

04 **Scan Scope setting in Visual Studio plugin** NEW 70

Adds a Scan Scope setting in Veracode Scan for Visual Studio v0.8.0 to scan either the full project directory or only the active solution.

— Names the setting, version, and two scan modes Integration updates (2026-09-28)

05 **Platform-managed GitHub Workflow Integration lifecycle** NEW 60

Enables installation, configuration, and credential updates for the GitHub Workflow Integration directly from the Veracode Platform, eliminating manual GitHub Marketplace steps, and adds a new workflow for uninstalling the Veracode app from GitHub organizations via the Platform.

— Describes before/after but only a UI path Integration updates (2026-09-28)

06 **Mitigated Findings section in VS Code policy view** NEW 60

Adds a Mitigated Findings section to the Flaws That Violate Policy view in Veracode Scan for VS Code v1.16.4, surfacing findings that have approved mitigations.

— Names the section, view, and version Integration updates (2026-09-28)

THINNER COVERAGE BELOW

07 **Scheduled scans for GitHub organizations** NEW 55

Enables scheduling of Static Analysis, SCA, and IaC scans directly from the Veracode Platform for every GitHub organization where the Workflow Integration is installed.

— Names scan types but only a Platform UI path Integration updates (2026-09-28)

08 **Region selection during VS Code OAuth authentication** NEW 55

Adds an option to change the region during OAuth authentication in Veracode Scan for VS Code v1.16.3, displaying the current or most recently used region below the Authentication screen.

— Names the screen and version, UI path only Integration updates (2026-09-28)

09 **Autopackaging for Apex, VB6, and Perl** NEW 50

Adds autopackaging support for Apex, VB6, and Perl in GitHub Workflow Integration v2.0.0.

— Names languages and version but no mechanism Integration updates (2026-09-28)

10 **Usage analytics across Veracode Scan plugins** NEW 50

Adds usage analytics to Veracode Scan for VS Code v1.16.0, Veracode Scan for JetBrains v1.8.0, and Veracode Scan for Visual Studio v0.8.0, providing insight into plugin adoption, feature usage, and scan activity.

— Passive telemetry, no reader action described Integration updates (2026-09-28)

11 **Veracode Fix for SCA in GitHub** NEW 10

Introduces Veracode Fix for SCA within GitHub, per the release summary; no further detail on scope or mechanism was provided in the source material.

— Summary-only mention with no supporting detail Integration updates (2026-09-28)

└──▷ **ALSO FROM THESE RELEASES**

Integration updates (2026-09-28) BLOG ↗ LATEST STABLE

Veracode integrations gain IaC policy param, Veracode Fix for SCA in GitHub, VS Code file filters, and new GitHub platform management.

└──▷ **USE IT**

Enforce a named policy on IaC scans in your GitHub workflow so failures are gated against your organisation's policy, not just the default.

veracode.yml

```
# veracode.yml
iac:
  policy: 'PCI-DSS Strict'
```

Adds support for custom predependency commands in the Veracode YAML file to prepare projects before scanning in GitHub Workflow Integration v2.1.3.

Adds a custom agent pool name parameter to `veracode.yml` in Azure DevOps Workflow Integration v2.4.3 to specify the agent pool for pipeline execution.

Adds support for scheduling `analysis_branch` scans in Azure DevOps Workflow Integration v2.3.10, so scheduled scans run against the specified branch instead of the default branch when `analysis_branch` is set in `veracode.yml`.

Enables scheduling of scans for every organization where the Azure DevOps Workflow Integration is installed, driven by `veracode.yml` configuration.

Adds a Current File filter to Static Scan Findings in Veracode Scan for VS Code v1.16.3, allowing findings to be scoped to the file open in the editor.

+13 more

WAS THIS USEFUL? 👍 👎

NETWORK SECURITY

◆ Network Analysis & Monitoring

Netcap

Feedback ⓘ v0.9.15 NOTES ↗ CODE ↗ RANK

A framework for secure and scalable network traffic analysis - https://netcap.io

> Netcap v0.9.15 introduces Roaring bitmap indexing across Community ID, certificate, fingerprint, and timeline facets, slashing filtered-count latency from ~2.6 ms to ~29 µs, alongside new correlation facets, vulnerability pivots, and a pinned Wireshark regression suite.

└──▷ **WHAT SHIPPED · 7 FEATURES** most completely described first ? what's the number?

01 **Certificate and timeline correlation facets** NEW 88

Certificate and timeline correlation facets are now indexed, including exact `host=<ip>` and repeatable `communityId=<value>` timeline facets with per-track postings, cursor pagination, nearest-event lookup, and duration overlap; the system falls back to exact scanning above a 32 MiB per-capture bitmap cap.

— Names exact query syntax and fallback threshold v0.9.15

02 **Wireshark sample corpus regression testing** NEW 75

NETCAP is now tested against a checksum-pinned Wireshark sample corpus of 22 representative pcap/pcapng captures, including all nine PROTOS robustness captures, run via `make test-wireshark`.

Run the pinned Wireshark sample corpus regression suite to validate all 22 pcap/pcapng captures after a build or config change.

```
$ make test-wireshark
```

— Runnable command with exact corpus size named v0.9.15

03 **Roaring bitmap indexes for filtered counts** NEW 68

Netcap now builds Roaring bitmap indexes for Community ID, certificate, fingerprint, and timeline facets, cutting filtered counts from ~2.6 ms to ~29 µs.

— Quantified before/after but no user-facing action named v0.9.15

THINNER COVERAGE BELOW

04 **Cross-UI Roaring index reuse via generation-checked snapshots**

IMPROVED 55

Roaring indexes for multi-ID records and fingerprints are now reused across the table, menu, and four charts in the web UI via generation-checked snapshots.

— Names UI surfaces but no exact navigation given v0.9.15

05 **Community ID bitmap prefiltering for audit streams** NEW 45

Audit streams are now prefiltered using Community ID bitmaps, enabling fast record selection without full-file scans.

— Explains mechanism but no exposed command or flag v0.9.15

06 **Vulnerability and exploit pivot indexing** NEW 30

Aggregated vulnerability and exploit pivots are now indexed in the web UI.

— Bare description, no mechanism or UI path given v0.9.15

07 **Database notices in archive paths** IMPROVED 23

Database notices are now included in every archive path.

— Thin one-line change with no further detail v0.9.15

v0.9.15 NOTES ↗ CODE ↗ LATEST STABLE

Netcap v0.9.15 adds Roaring bitmap indexes for Community ID, certificate, fingerprint, and timeline facets — cutting filtered counts from ~2.6 ms to ~29 µs.

└──▷ GET THIS VERSION

```
$ git clone --branch v0.9.15 https://github.com/dreadl0ck/netcap.git
# already have the repo? check out this version:
$ git checkout v0.9.15
```

└──▷ TRY IT

Run the pinned Wireshark sample corpus regression suite to validate all 22 pcap/pcapng captures after a build or config change.

```
$ make test-wireshark
```

Prefilters audit streams with Community ID bitmaps, enabling fast record selection without full-file scans.

Reuses Roaring indexes for multi-ID records and fingerprints across the table, menu, and four charts via generation-checked snapshots.

> Indexes certificate and timeline correlation facets, including exact `host=<ip>` and repeatable `communityId=<value>` timeline facets with per-track postings, cursor pagination, nearest-event lookup, and duration overlap; falls back to exact scanning above a 32 MiB per-capture bitmap cap.
>
> Indexes aggregated vulnerability and exploit pivots in the web UI.
>
> Includes database notices in every archive path.
>
> +1 more

WAS THIS USEFUL? 👍 👎

DETECTION & RESPONSE

◆ SIEM

Databricks

Feedback ⓘ

Horizontal scaling for Databricks Apps is now generally available (2026-09-29)

BLOG ↗ RANK

Databricks is a unified analytics platform for data engineering, data science, and machine learning built on Apache Spark.

> Databricks Apps gained general availability of horizontal scaling, letting a single app run across multiple instances behind one URL.

└──▷ **WHAT SHIPPED · 1 FEATURE** most completely described first ? what's the number?

01 **Horizontal scaling for Databricks Apps** NEW 50

Databricks Apps now supports running an app across multiple instances behind a single app URL, improving availability and concurrency. It includes zero-downtime deployments and best-effort session affinity, and is now generally available.

— Describes mechanism but no config keys or exact steps to enable it

Horizontal scaling for Databricks Apps …

> Horizontal scaling for Databricks Apps is now generally available (2026-09-29)
>
> BLOG ↗ LATEST STABLE
>
> Databricks Apps now supports horizontal scaling GA: multiple instances behind one URL with zero-downtime deployments and session affinity.

WAS THIS USEFUL? 👍 👎

Elastic Security Labs

Feedback ⓘ

Quarantined isn't contained: Agentic phishing response with Elastic and Sublime (2026-09

BLOG ↗ RANK

Power insights and outcomes with The Elasticsearch Platform. See into your data and find answers that matter with enterprise solutions designed to help you accelerate time to insight.

> Elastic Security shipped a native two-way Sublime Security integration for phishing response, pairing email threat telemetry ingestion with SOAR-driven quarantine actions and an Attack Discovery workflow that correlates email and endpoint signals into MITRE ATT&CK-mapped incidents.

└──▷ **WHAT SHIPPED · 4 FEATURES** most completely described first ? what's the number?

01 **Two-way SOAR response actions with Sublime** NEW 85

Elastic Workflows gains a two-way SOAR integration with Sublime Security, enabling response actions on the Sublime side — such as triggering a blast-radius quarantine using a SHA-256 hash from an Elastic Defend finding — without leaving Elastic.

After Elastic Defend identifies malware on a host, use a Workflow to pass the file's SHA-256 hash to Sublime Security and trigger a blast-radius quarantine that pulls the same message from every mailbox it reached.

> 📍 In Elastic Workflows, add a Sublime Security action step, select `Blast-radius quarantine`, and map the SHA-256 field from the Elastic Defend alert as the indicator input. Set the step to require analyst approval before execution.

— Concrete example gives exact steps to configure the action

Quarantined isn't contained: Agentic ph…

02 **Attack Discovery phishing correlation workflow** NEW 65

Attack Discovery's agentic workflow correlates Sublime Security email alerts with endpoint and other signals into unified, MITRE ATT&CK-mapped attack chains, querying raw logs and gathering supporting evidence before surfacing a prioritized incident to analysts.

.
.
.

— Describes mechanism and outputs but no navigation or command

Quarantined isn't contained: Agentic ph…

03 **Sublime Security email telemetry integration** NEW 60

Elastic Security adds a native Sublime Security integration that ingests email threat telemetry — including flagged message, detection rationale, targeted recipient, and Sublime action taken — into Elastic Security for correlation with endpoint, identity, and network signals.

.

— Names ingested fields but no config key or endpoint given

Quarantined isn't contained: Agentic ph…

THINNER COVERAGE BELOW

04 **Per-action autonomy configuration in Workflows** NEW

55

Elastic Workflows supports per-action configurable autonomy, letting teams set individual steps to run automatically or route through an analyst approval flow rather than applying a single automation policy across the whole system.

— Explains capability but no specific setting or UI path named

Quarantined isn't contained: Agentic ph…

Quarantined isn't contained: Agentic phishing response with Elastic and Sublime (2026-

BLOG ↗ LATEST STABLE

Elastic Security adds a native two-way Sublime Security integration, correlating email threat telemetry with endpoint, identity, and network signals and enabling SOAR-driven

└──▷ **HOW TO FIND IT**

After Elastic Defend identifies malware on a host, use a Workflow to pass the file's SHA-256 hash to Sublime Security and trigger a blast-radius quarantine that pulls the same message from every mailbox it reached.

📍 In Elastic Workflows, add a Sublime Security action step, select Blast-radius quarantine, and map the SHA-256 field from the Elastic Defend alert as the indicator input. Set the step to require analyst approval before execution.

Adds a native Sublime Security integration that ingests email threat telemetry (flagged message, detection rationale, targeted recipient, and Sublime action taken) into Elastic Security for correlation with endpoint, identity, and network signals.

Adds a two-way SOAR integration with Sublime Security inside Elastic Workflows, enabling response actions on the Sublime side — such as triggering a blast-radius quarantine using a SHA-256 hash from an Elastic Defend finding — without leaving Elastic.

Attack Discovery agentic workflow correlates Sublime Security email alerts with endpoint and other signals into unified, MITRE ATT&CK-mapped attack chains,

> querying raw logs and gathering supporting evidence before surfacing a prioritized incident to analysts.
>
> Elastic Workflows supports per-action configurable autonomy, letting teams set individual steps to run automatically or route through an analyst approval flow rather than applying a single automation policy across the whole system.

WAS THIS USEFUL? 👍 👎

◆ Endpoint Security (EDR/XDR)

XFA

Feedback ⓘ

Require the antivirus products your organization uses (Beta) NOTES ↗ RANK

XFA is a framework for building and testing XML Forms Architecture documents with security and developer tooling capabilities.

> XFA's biggest addition this window is Beta support for requiring specific antivirus products per OS in device policy, alongside per-platform OS version policies, a new personal device-check view in the desktop app, and self-invite onboarding for organizations.

└──▷ WHAT SHIPPED · 4 FEATURES most completely described first ? what's the number?

01 **Self-invite for organization onboarding** NEW 80

Enables self-invite in Awareness settings (Beta) so users can join their organization by entering a work email and confirming with a one-time code, without waiting for an admin-sent invitation.

Allow employees to onboard themselves to XFA without waiting for an admin invitation, reducing friction for large rollouts.

> 📍 In the XFA admin console, go to Awareness settings and enable the self invite toggle (marked Beta).

— Names exact settings location and gives step-by-step enablement

Connect to your organization without wa…

02 **Require specific antivirus products in device policy** NEW 75

XFA Beta lets admins require specific antivirus products per OS in device policy: Windows (Microsoft Defender or any product registered with Windows Security Center) and Linux (ClamAV or Microsoft Defender for Endpoint), with suggestions drawn from the organization's device inventory. The device details view, sign-in verification screen, and risk emails now surface which antivirus product is required vs. detected so users understand why a check fails.

.

— Names OS-specific products and surfaces but only a policy screenshot, no config key

Require the antivirus products your org…

03 **Per-platform OS version requirement policies** NEW 65

XFA now supports per-platform OS version policies, letting admins set distinct warning or blocking thresholds for Windows, macOS, Linux, Android, iOS, and iPadOS independently. iPadOS now has its own dedicated policy, separate from iOS.

— Lists all six platforms but no exact policy field names

Choose OS requirements for each platform

04 **Personal security checks in desktop app** NEW 65

Adds a personal view in the XFA desktop app for checking your computer's security posture with or without being connected to an organization, including a setup wizard to guide initial configuration. Adds per-organization views showing which checks each organization requires, kept separate from personal checks, and lets users add personal checks alongside org-required ones with the ability to ignore individual personal findings independently of org requirements.

— Describes UI flow in detail but no command or API surface

Check your own computer, with or withou…

Require the antivirus products your organization uses (Beta) NOTES ↗

LATEST STABLE

XFA Beta lets you require specific antivirus products (Microsoft Defender, ClamAV, Windows Security Center partners) per OS in device policy.

Adds the ability to require specific antivirus products in device policy for Windows (Microsoft Defender or any product registered with Windows Security Center) and Linux (ClamAV or Microsoft Defender for Endpoint), with suggestions drawn from your device inventory.

Device details view, sign-in verification screen, and risk emails now surface which antivirus product is required vs. detected so users understand why a check fails.

Choose OS requirements for each platform NOTES ↗ STABLE

XFA now lets you set separate OS version requirements per platform — Windows, macOS, Linux, Android, iOS, and iPadOS each get their own policy.

Supports per-platform OS version policies, letting you set distinct warning or blocking thresholds for Windows, macOS, Linux, Android, iOS, and iPadOS independently.

Adds a dedicated OS version policy for iPadOS, separate from iOS.

Check your own computer, with or without an organization NOTES ↗ STABLE

XFA desktop app gains a personal security view for checking your own computer, with or without an org connection.

Adds a personal view in the desktop app for checking your computer's security posture without being connected to an organization.

Adds a setup wizard to guide users through initial configuration of personal device checks.

Adds per-organization views showing which checks each organization requires, kept separate from personal checks.

Enables adding personal checks alongside organization-required checks, with the ability to ignore individual personal findings independently of org requirements.

Connect to your organization without waiting for an invitation NOTES ↗

STABLE

XFA adds self-invite so users can join their org via email one-time code without waiting for an admin invitation.

└──▷ **HOW TO FIND IT**

Allow employees to onboard themselves to XFA without waiting for an admin invitation, reducing friction for large rollouts.

📍 In the XFA admin console, go to Awareness settings and enable the self invite toggle (marked Beta).

WAS THIS USEFUL? 👍 👎

EXPOSURE & VULNERABILITY MANAGEMENT

◆ Vulnerability Management

Edgescan

Feedback ⓘ Release Notes - 3rd Sep 2026 NOTES ↗ RANK

Edgescan is a vulnerability management platform that performs continuous web application and network security scanning and reporting.

> Edgescan's latest release adds the ability to clone global roles into specific organizations and refines the bulk asset scheduling workflow to reduce unnecessary confirmations.

└──▷ **WHAT SHIPPED · 2 FEATURES** most completely described first ? what's the number?

01 **Clone global role to an organization** NEW 50

Admins can clone a global role to a specific organization, scoping the same set of permissions to that organization rather than applying them globally.

— Explains what it does but no UI path or exact steps given Release Notes - 3rd Sep 2026

02 **Bulk asset scheduling confirmation refined** IMPROVED 40

The bulk asset workflow now only shows an assessment scheduling confirmation prompt when a user is actually setting or moving an assessment start date, reducing unnecessary confirmations.

— Describes behaviour change but no concrete UI location or steps

Release Notes - 3rd Sep 2026

> Release Notes - 3rd Sep 2026 NOTES ↗ LATEST STABLE
>
> Edgescan adds bulk asset scheduling improvements and global role cloning to organizations.
>
> Enables cloning a global role to a specific organization, scoping the same permissions to that organization.
>
> Improves bulk asset workflow so that assessment scheduling confirmation only appears when actually setting or moving an assessment start date.

WAS THIS USEFUL? 👍 👎

IDENTITY, ACCESS & DATA PROTECTION

◆ Identity & Access Management

JumpCloud

Feedback ⓘ Release Notes 2022 (2026-09-28) BLOG ↗

RANK

JumpCloud makes it simple to manage Windows, Apple, Linux, and Android devices and to deliver secure access with SSO, MFA, Zero Trust, RADIUS, and more.

> Across seven release-note updates, JumpCloud rounded out its platform with a full Password Vault (mobile app, Admin Portal, and browser autofill), Access Requests approval workflows, SaaS Management and License tracking, Device Monitoring and Alerting, and a wave of AI features (MCP Server, AI Commands Builder, Shadow AI Dashboard, Knowledge Base uploads), alongside expanded RADIUS, SSO, MDM policy, and Android management options — plus breaking changes to the systemusers reactivate endpoint and Dynamic Groups filter operators.

└──▷ **WHAT SHIPPED · 53 FEATURES** most completely described first ? what's the number?

01 Password Manager Desktop App feature and platform expansion

IMPROVED 90

The Password Manager Desktop App gained multi-select, item sorting, Download Logs, and Keyboard Shortcuts options; EU region selection on the activation/pairing page; raised item storage limits to 13,000 items with autofill enabled, up to 5,000 per shared folder, and up to 30,000 without autofill; a Move All items button in shared folders; an auto-lock schedule defaulting to 15 minutes (max 1,440 minutes) plus a separate Auto Lock setting that locks the app when the device locks; install/update via command template `v.2.0.0` on Windows and macOS after which users no longer need admin permissions; an ARM build for Apple M-series Macs with automatic build selection; an RPM build for Red Hat/Fedora Linux alongside the Debian build; admin creation/update of shared folders with user/group assignment; deletion of multiple folders at once; archiving with view/delete/restore; pagination at 100 items per page; a Copy button in Password History; shared folder events synced to Directory Insights; a What's New link under Settings > General; sorting by nickname; and an enhanced CSV export for the legacy Password Manager to support migration into JumpCloud Vault.

Select the EU region when activating a new Password Manager account on a desktop that must stay within EU data boundaries.

> 📍 On the desktop app activation page, select EU as your region before entering your activation code. For the browser extension, select EU on the pairing page before pairing.

— Names every flag, limit and setting shipped across two releases.

What's New: Password Manager Desktop Ap… | Release Notes 2024 (2026-09-28)

02 **Knowledge Base Uploads for AI Assistant** NEW 90

Adds Knowledge Base Uploads for AI Assistant, accepting PDF, TXT, DOCX, and MD files (10 MB max per file, 25 files max per org) into a private, org-scoped knowledge base so the assistant can answer questions about internal runbooks, SOPs, and policies, with source attribution in chat.

Upload an internal runbook so the AI Assistant can answer org-specific questions about incident response procedures.

> 📍 In the Admin Portal, navigate to AI Assistant › Knowledge Base and upload your runbook file (PDF, TXT, DOCX, or MD, up to 10 MB). The assistant will cite the source document in chat responses that draw from it.

— Exact file limits, formats, and a working upload walkthrough.

Release Notes 2026 (2026-09-28)

03 **systemusers reactivate endpoint migration** BREAKING 90

Replaces the deprecated `GET api/systemusers/reactivate/{id}` endpoint — which now returns a 404 error — with `POST https://console.jumpcloud.com/systemusers/reactivate/{id}` carrying `activation_email` in the request body; callers must migrate to the new endpoint.

Reactivate a user account after migrating off the deprecated GET endpoint — send the activation email via the new POST endpoint.

```
$ curl -s -X POST -H 'x-api-key: <api_key>' -H 'Content-Type: application/json' -d '{"activation_email": "user@example.com"}' 'https://console.jumpcloud.com/api/systemusers/reactivate/<id>'
```

— Exact old and new endpoints plus a runnable migration example.

Release Notes 2024 (2026-09-28)

04 **JumpCloud Password Vault launch** NEW 85

JumpCloud introduced Password Vault: the JumpCloud Protect mobile app can view, autofill, and launch credentials — including items in shared folders — from the same app used for Push and TOTP MFA; the Admin Portal lets admins enable the vault, assign access to users and user groups, create and share organizational credentials and websites, monitor password health from an Overview dashboard, and view audit logs in Directory Insights; and the JumpCloud Go browser extension adds autofill for non-SSO

website passwords and 2FA codes, secret viewing, and save-on-login/update/signup without requiring device registration.

— Names every surface — mobile app, Admin Portal, browser extension — and their functions.

Release Notes 2026 (2026-09-28)

05 **Dynamic Groups for devices and users** NEW 85

Adds Dynamic Groups for both devices and users, automating group membership via attribute-based rules with an optional review step before changes take effect; expands dynamic device group attributes with Vendor and Public IP Address, and adds Manager as a new dynamic user group attribute.

Add Vendor and Public IP Address attributes to a dynamic device group to automatically scope remote-access policies to devices on a known corporate network.

📍 In the Admin Portal, go to Device Groups › (select or create a Dynamic group) › Attribute Rules, add a rule for Vendor equals your hardware vendor and Public IP Address matches your egress IP range, then save.

— Names exact attributes and shows a configuration example.

Release Notes 2023 (2026-09-28)

06 **Client secret auth types for agent OAuth** NEW 85

Adds Client secret basic and Client secret post client authentication type options on an agent's Authentication tab so agent OAuth credentials match the exact method required by external platforms such as Amazon Bedrock AgentCore.

Configure an agent to use Client secret post so its OAuth token requests are compatible with Amazon Bedrock AgentCore.

📍 In the Admin Portal, open the agent record, select the Authentication tab, and under client authentication type choose Client secret post. Save the agent. JumpCloud will now send the client ID and secret in the request body when requesting a token.

— Names exact options and includes a runnable configuration example.

Release Notes 2026 (2026-09-28)

07 **API filter support for pipe characters** IMPROVED 85

Adds support for the pipe `|` character escaped with `\` inside `in` and `nin` filter operators on `GET /systemusers?filter=department:$in:Finance | Accounting|IT`, enabling pipe characters within search terms.

Query users whose department contains a pipe character (e.g. Finance | Accounting) alongside other departments using the `in` filter operator.

```
$ curl -s -H 'x-api-key: <api_key>'
'https://console.jumpcloud.com/api/systemusers?
filter=department:$in:Finance \| Accounting|IT'
```

— Names exact endpoint, operators and a runnable curl example.

Release Notes 2024 (2026-09-28)

---

08 **Android device management expansion** IMPROVED 80

Adds Android zero-touch enrollment for fully managed, dedicated, and company-owned Android devices with a work profile; makes Android EMM generally available for fully managed and dedicated devices with 7 new policies including Factory Reset Protection, Kiosk Mode, and System Updates; enables enrollment and management of company-owned and personal Android mobile devices via Android EMM with work profile support; and later adds policies for Display Settings, Autofill, Work Account authentication, Default App and Intent Handling, and enhanced Bluetooth Restrictions including outbound file-sharing control and personal-profile Bluetooth restrictions on company-owned devices with a work profile.

Enable Android zero-touch enrollment for corporate-owned devices so new hardware automatically enrolls into JumpCloud EMM without admin hands-on setup.

> 📍 In the Admin Portal, go to Device Management › Mobile Device Management › Android EMM, select your enrollment configuration, and enable Zero-Touch Enrollment for fully managed, dedicated, or company-owned work-profile devices.

— Names every policy category and enrollment mode across two releases.

Release Notes 2026 (2026-09-28) Release Notes 2023 (2026-09-28)

---

09 **Device Patch Report for Windows** NEW 80

Adds a Device Patch Report (Windows) in JumpCloud Reports with per-device KB installation status (Installed, Pending, Failed), an Admin Portal preview of up to 500 rows, and full CSV export.

— Names exact statuses, row limit and export format. Release Notes 2026 (2026-09-28)

---

10 **Asset Management expansion** NEW 80

Adds an Asset Manager role in the Admin Portal for scoped Asset Management access without broader Admin Portal permissions; an Invoice file-upload field under Purchase Details for uploading invoices or contracts to an asset record, with custom File Upload type fields also supported; a Disk Size field under Hardware Specifications; a Local Device Accounts section on the Asset Detail page for visibility into local users on a device; and asset cloning that auto-clears unique fields to prevent duplicate records.

Create a scoped Admin account for asset procurement teams without granting access to the broader Admin Portal.

> 📍 In the Admin Portal, go to Administrators › Roles, select `Asset Manager`, and assign it to the procurement team admin account.

— Names every field and role added, with a role-assignment example.

Release Notes 2025 (2026-09-28)

---

11 **Push Bombing Mitigation for JumpCloud Protect** NEW

80

Adds Push Bombing Mitigation to JumpCloud Protect, blocking more than one MFA push notification per resource within a 60-second window; configurable in MFA Configurations, with the blocked event logged in Directory Insights.

Configure Push Bombing Mitigation thresholds to balance security and usability for high-velocity login environments.

> 📍 In the Admin Portal, go to Security › MFA Configurations, locate `JumpCloud Protect Push Bombing Mitigation`, and adjust the maximum concurrent attempts limit or disable the feature for your organization.

— Exact threshold window and a configuration walkthrough. Release Notes 2023 (2026-09-28)

---

12 **RADIUS authentication methods: certificate-based and Azure AD** NEW

75

JumpCloud RADIUS gained certificate (passwordless) based authentication supporting certificates from any X.509 compliant certificate authority, and authentication via Azure AD credentials, letting organizations use Azure AD as the identity provider for RADIUS access.

Enable passwordless RADIUS authentication using an existing X.509 certificate authority — useful for orgs that already manage certificates and want to eliminate RADIUS passwords.

> 📍 In the Admin Portal, go to RADIUS › (select your RADIUS server) › Authentication, enable `Certificate Based Authentication`, then import your X.509 CA certificate under Certificate Authorities.

— Exact setup steps given for certificate auth via example.

Release Notes 2022 (2026-09-28)

---

13 **Default and bulk MFA enforcement for admins** IMPROVED

75

MFA is now enabled by default for all new admin accounts in the Admin Portal, and MSPs can enforce it in bulk via a Global MFA Requirement setting under Account > Settings in the Multi-Tenant Portal, applying to all MSP admins at once.

Enforce MFA for all MSP admins in the tenant from the Multi-Tenant Portal without touching individual accounts.

> 📍 In the Admin Portal, go to Account › Settings, locate Global MFA Requirement, and enable the setting to bulk-enforce MFA across all MSP administrators.

– Exact settings path given for bulk enforcement. Release Notes 2024 (2026-09-28) Release Notes 2023 (2026-09-28)

---

14 **Windows MDM policy framework and personalization policies** NEW 75

Introduces a Windows MDM policy framework using Configuration Service Providers (CSP) with six new policies — Windows Wi-Fi Configuration Policy, Windows VPN Policy, Install Certificate Policy, Bluetooth Configuration Policy, Control Policy Conflict, and Windows Notification Service — plus a policy to configure Simple Certificate Enrollment Protocol (SCEP) for Windows devices, and later adds three Windows Personalization policies: Taskbar Customization, Screen Saver Configuration, and Desktop and Lock Screen Settings.

– Enumerates all nine policies by exact name. Release Notes 2025 (2026-09-28) Release Notes 2024 (2026-09-28)

---

15 **Private Repository app management enhancements** IMPROVED 75

Private Repository now supports uploading and deploying IPA-based app packages to iOS and iPadOS devices, and gains in-place binary updates for existing applications via Update Version on the application's Details tab, including an install success exit code field for Windows EXE updates — eliminating the need to recreate the application or reassign devices.

– Names exact UI control and field for in-place updates. Release Notes 2026 (2026-09-28) Release Notes 2025 (2026-09-28)

---

16 **Dynamic Groups API operator change** BREAKING 75

Updates Dynamic Groups API `memberQuery` filters to use `$lte` and `$gte` operators in place of the deprecated `$le` and `$ge` operators, for alignment with other API list endpoints; existing requests using the old operators must be updated.

– Names exact deprecated and replacement operators. Release Notes 2024 (2026-09-28)

---

17 **SaaS Management and License tracking** IMPROVED 70

Launches SaaS Management to discover, track, categorize, warn, and block shadow-IT SaaS app usage via the JumpCloud Go browser extension, integrating with existing JumpCloud SSO apps and supporting manual licensing tracking; admins can manually add applications for tracking, warning, and blocking before automatic discovery; the JumpCloud Go requirement for discovering unmanaged applications is removed so the browser extension alone is sufficient; and SaaS License Management reaches general availability, automating license tracking and cost optimization via connectors.

— Covers full feature lifecycle but no exact console path.

Release Notes 2025 (2026-09-28) Release Notes 2024 (2026-09-28)

---

18 **JumpCloud Go passwordless authentication** IMPROVED 70

Introduces JumpCloud Go, enabling hardware-protected, phishing-resistant passwordless login to JumpCloud-protected web resources using Apple Touch ID or Windows Hello via a browser extension on managed macOS and Windows devices; strengthens it with user and device verification on every application session and sets it as the default MFA method for conditional access policies on SSO apps; adds a session-management section in User Portal > Security > Multi-Factor Authentication; and enables sessions to auto-refresh when a user logs in to or unlocks their managed device.

— Explains mechanism and session lifecycle, no exact command.

Release Notes 2024 (2026-09-28) Release Notes 2023 (2026-09-28)

---

19 **Remote Assist capabilities** IMPROVED 70

Introduces JumpCloud Remote Assist for free, unlimited remote desktop access on Windows and macOS devices, requiring JumpCloud Agent version 1.61.0 or later; adds user-account switching during sessions on Windows, a `Ctrl+Alt+Del` shortcut in the Session Options toolbar, and support for viewing and interacting with the Windows Server initial login screen including credential entry; ships as two separate architecture-specific packages — ARM64 for Apple Silicon and x86_64 for Intel — with automatic binary selection; and now automatically detects and terminates unresponsive agent instances when an admin initiates a connection.

— Traces the feature's evolution, lacks exact launch steps.

Release Notes 2024 (2026-09-28) Release Notes 2023 (2026-09-28) Release Notes 2022 (2026-09-28)

---

20 **macOS device software update scheduling** NEW 70

Adds single macOS device software update scheduling from the Admin Portal, including forced update and user delay/cancel flexibility options.

Block unintended macOS Ventura upgrades on your fleet before users trigger them via Apple's delta update mechanism.

> 📍 In the Admin Portal, go to Device Management › Policies › New Policy, select macOS, choose the `Delay or Block macOS Ventura` software management policy,

configure the deferral window, and bind it to the target device group.

— Example gives exact Admin Portal steps to bind an update policy.

Release Notes 2022 (2026-09-28)

21 **RSS feed subscriptions for release notes** NEW 70

Adds RSS feed subscriptions for JumpCloud Help Center content, including product release notes, agent release notes, and bug fix reports via Subscribe to Support RSS Feed , Subscribe to Release Notes and Bug Fixes RSS Feed , Subscribe to Agent Release Notes RSS Feed , and Subscribe to Bug Fixes RSS Feed options on the Release Notes and Bug Fixes page.

Subscribe your RSS reader to JumpCloud agent release notes so your team is automatically alerted when a new agent version ships.

📍 1. Navigate to the JumpCloud Release Notes and Bug Fixes page. 2. Click Subscribe to Agent Release Notes RSS Feed . 3. Copy the resulting RSS feed URL into your RSS reader (e.g., RSS Feed Reader extension in Chrome, or any browser with a built-in reader).

— Names every subscription option with a working setup walkthrough.

Subscribe to New Feature and Product Up…

22 **MFA factor, enrollment, and enforcement options** IMPROVED 65

JumpCloud expanded MFA options: TOTP is now a supported MFA factor for LDAP applications alongside JumpCloud Protect push; Duo Universal Prompt is supported; WebAuthn enrollment is split into separate credentials for Security Keys and Device authenticators; a User Group Exclusion lets excluded groups use TOTP only instead of Unified MFA Push; users can approve or deny JumpCloud Protect push notifications directly from the device lock screen via long-press (iOS) or notification expand (Android); and users can reset passwords from the User Portal when MFA is enforced but not yet enrolled.

— Lists six concrete MFA changes without deep mechanism on most.

Release Notes 2025 (2026-09-28) Release Notes 2023 (2026-09-28)

Release Notes 2022 (2026-09-28)

23 **MDM certificate and token status visibility** IMPROVED 65

Adds an MDM Upcoming Certificate Expirations homepage widget covering MDM, Apple VPP, and Automated Device Enrollment certificate lifecycles, later extended into an MDM Certificate & Token Status Board in the Admin Portal and Multi-Tenant Portal showing

expiration status for MDM, SSO, and AzureAD tokens and certificates, with an aggregate view for MSP admins across all tenant organizations.

— Describes scope well but no exact navigation path. Release Notes 2023 (2026-09-28) Release Notes 2022 (2026-09-28)

24 **Support portal and case management** IMPROVED 65

Adds a JumpCloud Case Portal for viewing and filtering support cases and ideas submitted by any administrator, and live chat support directly in the Admin Portal for Premium Support customers with automatic status recognition; later introduces a Customer Portal for tracking and managing support cases with sortable Last Modified Date, Account, and Requester columns, attachment uploads, and inline ticket editing, and lets MTP Admins access, view, and create support cases for all tenant organizations they manage.

— Names portal features and columns but no exact navigation.

Release Notes 2025 (2026-09-28) Release Notes 2022 (2026-09-28)

25 **MSP admin tooling in Multi-Tenant Portal** NEW 65

MSP Admins can create, save, and apply custom command templates across tenant organizations; a homepage widget shows aggregate reports across all tenant organizations from the last 24 hours with bulk export as JSON or CSV; admins can run ad hoc commands on devices from both the Multi-Tenant Portal and the Admin Portal with visibility into which commands are bound to specific devices; and new users and devices can be added directly from the Multi-Tenant Portal, with user/device list export and bulk actions on users.

— Lists every MTP capability added but no exact menu path.

Release Notes 2023 (2026-09-28) Release Notes 2022 (2026-09-28)

26 **JumpCloud App Catalog for Windows** NEW 65

Releases the JumpCloud App Catalog for Windows, supporting auto-updating installation of 1Password, Adobe Acrobat Reader DC, Chrome, Firefox, Google Drive, OneDrive, OpenVPN, Slack, Webex, and Zoom.

— Names every supported app; no exact enrollment steps. Release Notes 2024 (2026-09-28)

27 **Device Monitoring and Alerting** NEW 65

Introduces JumpCloud Device Monitoring and Alerting, enabling customizable alerts for device health (availability, software, uptime, disk, battery), policy/command/software management results, directory user-addition and privilege-elevation events, and command-execution monitoring across Windows, macOS, and Linux endpoints.

— Describes scope of alerting well, no setup path given. Release Notes 2024 (2026-09-28)

28 **Apple Compliance Dashboard** NEW 65

Adds an Apple Compliance Dashboard within Patch Management to track macOS, iOS, and iPadOS OS rollout progress against active update policies, with filtering by platform, release date, severity, and device status.

— Names filter dimensions but no navigation path given. Release Notes 2026 (2026-09-28)

29 **Password Manager admin controls and platform expansion**

IMPROVED 60

Admins can manage shared folder assignments and permissions for JumpCloud Password Manager from the Admin Portal, plus trigger manual per-folder sync from the desktop app; adds Cloud Backup as a secure fallback to minimize data loss; and adds a Password Manager Desktop App build for Linux (Debian/Ubuntu x86) with automatic updates.

— Names concrete admin controls but no exact menu path. Release Notes 2023 (2026-09-28)

30 **AppImage Linux build discontinued for Password Manager**

60

BREAKING

The `.appimage` Linux build of the Password Manager Desktop App is no longer supported as of v2.2.197 (April 18, 2024); Linux users must move to the supported Debian or RPM builds.

— Gives exact version and date but no migration command.

What's New: Password Manager Desktop Ap…

31 **Disk encryption device condition in Conditional Access Policies**

NEW 60

Adds disk encryption as a new device condition in Conditional Access Policies, checking FileVault on macOS, system drive encryption on Windows, and root disk encryption on Linux.

— Names exact per-OS checks but no policy setup steps. Release Notes 2022 (2026-09-28)

32 **Apple Account-Driven User Enrollment for BYOD** IMPROVED

60

Supports BYOD enrollments of iOS/iPadOS 18+ devices in MDM via Account-Driven User Enrollment (ADUE), now generally available, and adds Apple Business Manager as a new service discovery method for Account-driven Enrollment in Apple MDM.

— Names the enrollment mechanism and GA status, no walkthrough.

Release Notes 2025 (2026-09-28) Release Notes 2024 (2026-09-28)

33 **AI Gateway Dashboard** NEW 60

Adds a Dashboard tab to AI Gateway showing org-wide MCP server usage, tool call volume, error rates, summary cards, trend charts, and rankings for top servers, clients, and users with per-server drill-down.

— Names the tab and metrics shown, no interaction steps. Release Notes 2026 (2026-09-28)

THINNER COVERAGE BELOW

34 **New SSO protocol and integration support** NEW 55

JumpCloud added OpenID Connect (OIDC) Single Sign-On support for OIDC-capable web applications, a Deel SSO Connector for integrating with Deel, and an AWS Verified Access integration using JumpCloud Go, SAML, or OIDC SSO as a VPN-less access solution for remote employees.

— Names each integration but no configuration steps. Release Notes 2023 (2026-09-28) Release Notes 2022 (2026-09-28)

35 **New Apple MDM policies** NEW 55

Adds a Managed Login Items policy for macOS 13 Ventura to prevent users from disabling persistent software such as the JumpCloud Agent, and two new policies restricting Apple Intelligence features on iOS/iPadOS 18.1 and macOS 15.1 Sequoia devices.

— Names each policy but no configuration steps. Release Notes 2024 (2026-09-28) Release Notes 2022 (2026-09-28)

36 **Self-Service Account Provisioning** NEW 55

Adds Self-Service Account Provisioning, letting new users bind their account to JumpCloud-managed macOS and Windows devices directly from the login window, with wireless connectivity controls on the new macOS login window.

— Explains the flow but no step-by-step admin setup. Release Notes 2023 (2026-09-28)

37 **Agent Identities Public Preview** NEW 55

Adds Agent Identities (Public Preview) for non-human identity management of AI agents, providing OAuth-based authentication, group-based access control, ownership assignment, and full lifecycle revocation independent of employee user accounts.

— Explains capabilities but preview status limits actionability. Release Notes 2026 (2026-09-28)

38 **Shadow AI Dashboard** NEW 55

New Shadow AI Dashboard provides a dedicated UI for managing generative AI app usage, with visibility into AI adoption, usage by department, and most active users, including proactive approval and restriction controls.

— Describes dashboard scope, no navigation path given. Release Notes 2025 (2026-09-28)

39 **Patch management compliance reports** NEW 50

Adds an OS Patch Management Policy Report showing which policies are applied to each device and their current compliance status, and a Browser Patch Management Policy Report for compliance audit evidence of devices' current browser versions.

— Names both reports without detailing export or filters. Release Notes 2022 (2026-09-28)

40 **Portal UI usability additions** NEW 50

Splits the Applications area of the User Portal into All Applications and Favorites tabs, with per-app starring and a responsive search field on both; adds a Password Date column on the Admin Portal Users page showing when a user's password was last set; and adds a `⌘/Ctrl + K` keyboard shortcut in the Admin Portal for quick navigation and search.

— Names each UI element but no deeper mechanism. Release Notes 2024 (2026-09-28)

Release Notes 2023 (2026-09-28)

41 **Directory Insights filter granularity** IMPROVED 50

Splits the Directory Insights Application Name filter into Application Name, Application Display Name, and Application Display Label, and the Resource Name filter into Resource Name, Resource Display Name, and Resource Display Label.

— Names every new filter field, no usage guidance. Release Notes 2025 (2026-09-28)

42 **JumpCloud MCP Server general availability** NEW 50

JumpCloud MCP Server is now generally available, letting compatible AI tools and code editors interact with JumpCloud organizational data and administrative capabilities via the Model Context Protocol.

— States GA and protocol used, no connection instructions.

Release Notes 2025 (2026-09-28)

43 **AI Commands Builder general availability** NEW 50

JumpCloud AI Commands Builder is now generally available, enabling natural-language creation and refinement of commands for Windows, macOS, and Linux devices in the Admin Portal.

— Names the surface but no example prompt or command shown.

Release Notes 2025 (2026-09-28)

44 **Service Account for APIs** NEW 50

Introduces Service Account for APIs, allowing API service accounts not tied to individual Admin accounts for more secure and maintainable integrations.

— Names the feature but no creation steps. Release Notes 2025 (2026-09-28)

45 **JumpCloud Password Manager launch** NEW 45

JumpCloud introduced Password Manager with end-to-end encrypted local sync, a browser extension for auto-fill, secure password sharing, and password generation.

— Describes capability but gives no setup steps. Release Notes 2022 (2026-09-28)

46 **Faster reconnect for EAP connections** IMPROVED 45

Enables faster reconnect for EAP connections by allowing recently authenticated devices to skip the full security handshake using a cached session credential.

— Explains mechanism but no configuration control named. Release Notes 2025 (2026-09-28)

47 **Background Tools remote command line and file transfer** NEW 45

Adds remote command line and remote file transfer capabilities via Background Tools, allowing admins to access and troubleshoot end-user devices without interrupting their work.

— Describes capability without exact activation steps. Release Notes 2023 (2026-09-28)

48 **Universal browser patch management policy** NEW 40

Adds a universal browser patch management policy for Google Chrome across macOS, Windows, and Linux, managed from a single policy.

— Describes scope but no configuration path. Release Notes 2022 (2026-09-28)

49 **Identity-first two-screen login flow** NEW 40

Adds an identity-first (two-screen) login flow for the User Portal and SSO applications, with an option to remember the username.

— Names the change but gives no rollout or config detail. Release Notes 2022 (2026-09-28)

50 **Linux fleet management additions** NEW 40

Adds JumpCloud agent support for Linux Fedora 37, and a Linux Forbidden Services policy for removing unsupported or unnecessary service types from Linux fleets.

— Two small named additions with no further mechanism given.

Release Notes 2022 (2026-09-28)

51 **Custom Admin Roles general availability** NEW 40

Releases Custom Admin Roles for all direct organizations, enabling granular role customization based on specific admin responsibilities.

— States GA and purpose, no role-creation steps. Release Notes 2025 (2026-09-28)

52 **Active Directory Integration on 2022 Domain Controllers**

IMPROVED 35

Adds support for Active Directory Integration (ADI) on 2022 Domain Controllers and member servers without workarounds or decreased functionality.

— States compatibility but no setup guidance. Release Notes 2023 (2026-09-28)

53 **Source IP tracking for LDAP requests** NEW 25

Adds source IP tracking for incoming LDAP requests for enhanced security and traceability.

— Bare description, no mechanism or access path given. Release Notes 2025 (2026-09-28)

└──▷ **ALSO FROM THESE RELEASES**

Set the dormant application inactivity threshold so Access Risk flags re-access after 90 days of silence rather than on first access.

📍 In the Admin Portal, go to Access Risk › Configuration and set the dormant application threshold to your desired inactivity period (e.g., 90 days). Save the configuration. First-time access to a new app will no longer trigger an alert.

└──▷ **BREAKING ON UPGRADE**

! The `GET api/systemusers/reactivate/{id}` endpoint is deprecated and now returns a 404 error; all callers must migrate to `POST https://console.jumpcloud.com/systemusers/reactivate/{id}` with `activation_email` in the request body.

! Dynamic Groups API `memberQuery` filter operators `$le` and `$ge` are deprecated and replaced by `$lte` and `$gte`; existing API requests using the old operators must be updated.

! The `.appimage` Linux build is no longer supported as of v2.2.197 (April 18, 2024).

Release Notes 2022 (2026-09-28) BLOG ↗ STABLE

JumpCloud 2022 adds certificate-based RADIUS auth, TOTP for LDAP, Remote Assist, Password Manager, and new MSP command templates

└──▷ **HOW TO FIND IT**

Enable passwordless RADIUS authentication using an existing X.509 certificate authority — useful for orgs that already manage certificates and want to eliminate RADIUS passwords.

📍 In the Admin Portal, go to RADIUS › (select your RADIUS server) › Authentication, enable Certificate Based Authentication, then import your X.509 CA certificate under

Certificate Authorities.

Block unintended macOS Ventura upgrades on your fleet before users trigger them via Apple's delta update mechanism.

📍 In the Admin Portal, go to Device Management › Policies › New Policy, select macOS, choose the `Delay or Block macOS Ventura` software management policy, configure the deferral window, and bind it to the target device group.

Run a SentinelOne agent deployment across all managed endpoints by reusing a JumpCloud command, avoiding manual per-device installs.

📍 In the Admin Portal, go to Commands › New Command, select the target OS (macOS, Windows, or Linux), paste the SentinelOne Agent install script, and bind the command to the relevant device group to trigger installation.

Adds `Command After Agent Install` command type so admins can specify enrollment commands to run immediately after the JumpCloud agent is installed on new devices.

Adds `Running` column to the commands queue to distinguish commands waiting in the queue from commands that are actively running.

Adds certificate (passwordless) based authentication to JumpCloud RADIUS, supporting certificates from any X.509 compliant certificate authority.

Adds TOTP as a supported MFA factor for LDAP applications, in addition to JumpCloud Protect push notifications.

Adds disk encryption as a new device condition in Conditional Access Policies (FileVault on macOS, system drive encrypted on Windows, root disk encrypted on Linux).

+18 more

`Release Notes 2023 (2026-09-28)` `BLOG ↗` `STABLE`

JumpCloud 2023 adds passwordless Go SSO, Android zero-touch enrollment, dynamic groups, remote Background Tools, and self-service device provisioning.

└──▷ **HOW TO FIND IT**

Enable Android zero-touch enrollment for corporate-owned devices so new hardware automatically enrolls into JumpCloud EMM without admin hands-on setup.

📍 In the Admin Portal, go to Device Management › Mobile Device Management › Android EMM, select your enrollment configuration, and enable `Zero-Touch Enrollment` for fully managed, dedicated, or company-owned work-profile devices.

Configure Push Bombing Mitigation thresholds to balance security and usability for high-velocity login environments.

> 📍 In the Admin Portal, go to Security › MFA Configurations, locate `JumpCloud Protect Push Bombing Mitigation`, and adjust the maximum concurrent attempts limit or disable the feature for your organization.

Add Vendor and Public IP Address attributes to a dynamic device group to automatically scope remote-access policies to devices on a known corporate network.

> 📍 In the Admin Portal, go to Device Groups › (select or create a Dynamic group) › Attribute Rules, add a rule for `Vendor` equals your hardware vendor and `Public IP Address` matches your egress IP range, then save.

Adds `Password Date` as a viewable column on the Users page in Admin Portal, showing when a user's password was last set.

Strengthens JumpCloud Go SSO with user and device verification on every application session, and sets JumpCloud Go as the default MFA method for conditional access policies on SSO apps.

Adds support for Active Directory Integration (ADI) on 2022 DCs and member servers without workarounds or decreased functionality.

Adds a Deel SSO Connector for integrating JumpCloud with Deel.

Splits the Applications area of the User Portal into `All Applications` and `Favorites` tabs, with per-app starring and a responsive search field on both tabs.

`+23 more`

`Release Notes 2024 (2026-09-28)` `BLOG ↗` `STABLE`

JumpCloud 2024 adds Device Monitoring & Alerting, SaaS Management, Windows App Catalog, BYOD iOS 18 MDM, new CSP policies, and more.

`└──▷ TRY IT`

Query users whose department contains a pipe character (e.g. `Finance | Accounting`) alongside other departments using the `in` filter operator.

```
$ curl -s -H 'x-api-key: <api_key>'
'https://console.jumpcloud.com/api/systemusers?
filter=department:$in:Finance \| Accounting|IT'
```

Reactivate a user account after migrating off the deprecated GET endpoint — send the activation email via the new POST endpoint.

```
$ curl -s -X POST -H 'x-api-key: <api_key>' -H 'Content-Type:
application/json' -d '{"activation_email": "user@example.com"}'
'https://console.jumpcloud.com/api/systemusers/reactivate/<id>'
```

Enforce MFA for all MSP admins in the tenant from the Multi-Tenant Portal without touching individual accounts.

> 📍 In the Admin Portal, go to Account › Settings, locate `Global MFA Requirement`, and enable the setting to bulk-enforce MFA across all MSP administrators.

Adds `GET /systemusers?filter=department:$in:Finance | Accounting|IT` API filter support for the pipe `|` character escaped with `\` inside `in` and `nin` filter operators, enabling pipe characters within search terms.

Replaces the deprecated `GET api/systemusers/reactivate/{id}` endpoint with `POST https://console.jumpcloud.com/systemusers/reactivate/{id}` carrying `activation_email` in the request body.

Updates Dynamic Groups API `memberQuery` filters to use `$lte` and `$gte` operators in place of the deprecated `$le` and `$ge` operators for alignment with other API list endpoints.

Introduces JumpCloud Device Monitoring and Alerting, enabling customizable alerts for device health (availability, software, uptime, disk, battery), policy/command/software management results, directory user-addition and privilege-elevation events, and command-execution monitoring across Windows, macOS, and Linux endpoints.

Launches SaaS Management to discover, track, categorize, warn, and block shadow-IT SaaS app usage via the JumpCloud Go browser extension, with integration into existing JumpCloud SSO apps and manual licensing tracking.

+15 more

> └─▷ **BREAKING ON UPGRADE**
>
> ! The `GET api/systemusers/reactivate/{id}` endpoint is deprecated and now returns a 404 error; all callers must migrate to `POST https://console.jumpcloud.com/systemusers/reactivate/{id}` with `activation_email` in the request body.
>
> ! Dynamic Groups API `memberQuery` filter operators `$le` and `$ge` are deprecated and replaced by `$lte` and `$gte`; existing API requests using the old operators must be updated.

Release Notes 2025 (2026-09-28) BLOG ↗ STABLE

JumpCloud: Includes Authentication Methods References (AMR) claims in SAML assertions and OIDC ID tokens to provide per-login proof of MFA factors used (e.g., password + OTP), aligned with RFC 8176.

└──▷ **HOW TO FIND IT**

Route new Access Requests to your JIRA instance automatically so your team never misses an approval request.

> 📍 In the Admin Portal, go to Access Requests › Webhooks, add your JIRA webhook URL, and configure an approval flow assigning the relevant admin as approver — new requests will create JIRA tickets in real time.

Create a scoped Admin account for asset procurement teams without granting access to the broader Admin Portal.

> 📍 In the Admin Portal, go to Administrators › Roles, select `Asset Manager`, and assign it to the procurement team admin account.

New JumpCloud Access Requests feature enables configurable approval flows, with webhook integration to external ticketing systems such as JIRA for automatic ticket creation and real-time notifications.

Adds tracking of Access Request events in Directory Insights.

JumpCloud MCP Server is now GA, letting compatible AI tools and code editors interact with JumpCloud organizational data and administrative capabilities via the Model Context Protocol.

JumpCloud AI Commands Builder is now GA, enabling natural-language creation and refinement of commands for Windows, macOS, and Linux devices in the Admin Portal.

New Shadow AI Dashboard provides dedicated UI for managing generative AI app usage, with visibility into AI adoption, usage by department, and most active users — including proactive approval and restriction controls.

`+17 more`

`Release Notes 2026 (2026-09-28)` `BLOG ↗` `STABLE`

JumpCloud gains Password Vault, Patch Management dashboards, Agent Identities, Android policy expansion, and an AI Assistant knowledge base in 2026-09.

└──▷ **HOW TO FIND IT**

Set the dormant application inactivity threshold so Access Risk flags re-access after 90 days of silence rather than on first access.

📍 In the Admin Portal, go to Access Risk › Configuration and set the dormant application threshold to your desired inactivity period (e.g., 90 days). Save the configuration. First-time access to a new app will no longer trigger an alert.

Upload an internal runbook so the AI Assistant can answer org-specific questions about incident response procedures.

📍 In the Admin Portal, navigate to AI Assistant › Knowledge Base and upload your runbook file (PDF, TXT, DOCX, or MD, up to 10 MB). The assistant will cite the source document in chat responses that draw from it.

Configure an agent to use `Client secret post` so its OAuth token requests are compatible with Amazon Bedrock AgentCore.

📍 In the Admin Portal, open the agent record, select the Authentication tab, and under client authentication type choose `Client secret post`. Save the agent. JumpCloud will now send the client ID and secret in the request body when requesting a token.

Adds `Client secret basic` and `Client secret post` client authentication type options on an agent's `Authentication` tab so agent OAuth credentials match the exact method required by external platforms such as Amazon Bedrock AgentCore.

Adds Knowledge Base Uploads for AI Assistant, accepting PDF, TXT, DOCX, and MD files (10 MB max per file, 25 files max per org) into a private, org-scoped knowledge base so the assistant can answer questions about internal runbooks, SOPs, and policies, with source attribution in chat.

Adds a `Dashboard` tab to AI Gateway showing org-wide MCP server usage, tool call volume, error rates, summary cards, trend charts, and rankings for top servers, clients, and users with per-server drill-down.

Adds Device Patch Report (Windows) in JumpCloud Reports with per-device KB installation status (Installed, Pending, Failed), Admin Portal preview of up to 500 rows, and full CSV export.

Adds Password Vault to the JumpCloud Protect mobile app, enabling users to view, autofill, and launch credentials — including items in shared folders — from the same app used for Push and TOTP MFA.

+6 more

`Subscribe to New Feature and Product Update Announcements (2026-09-28)` `BLOG ↗`

`STABLE`

JumpCloud adds RSS feed subscriptions for release notes, agent updates, and bug fix announcements.

└──▷ **HOW TO FIND IT**

Subscribe your RSS reader to JumpCloud agent release notes so your team is automatically alerted when a new agent version ships.

📍 1. Navigate to the JumpCloud Release Notes and Bug Fixes page. 2. Click `Subscribe to Agent Release Notes RSS Feed`. 3. Copy the resulting RSS feed URL into your RSS reader (e.g., RSS Feed Reader extension in Chrome, or any browser with a built-in reader).

`What's New: Password Manager Desktop App (2026-09-28)` **BLOG ↗** **LATEST** **STABLE**

JumpCloud Password Manager Desktop App adds EU region support, raised storage limits, ARM macOS build, and shared folder admin controls.

└──▷ **HOW TO FIND IT**

Select the EU region when activating a new Password Manager account on a desktop that must stay within EU data boundaries.

📍 On the desktop app activation page, select `EU` as your region before entering your activation code. For the browser extension, select `EU` on the pairing page before pairing.

Adds EU region support; users can select their region on the activation page (desktop app) or pairing page (browser extension) before activating their account.

Raises item storage limits to 13,000 items with autofill enabled, up to 5,000 items per shared folder, and up to 30,000 items when autofill is not used.

Introduces a `Move All items` button in shared folders to move all items from a folder at once.

Introduces an auto-lock schedule with a default of 15 minutes of inactivity and a maximum of 1,440 minutes (24 hours).

Admins can install and update the Password Manager desktop app using the new command template v.2.0.0 on Windows and macOS devices, after which users no longer need admin permissions to perform updates.

`+12 more`

└──▷ **BREAKING ON UPGRADE**

! The `.appimage` Linux build is no longer supported as of v2.2.197 (April 18, 2024).

WAS THIS USEFUL? 👍 👎

◆ Data Security & DLP

Bedrock Security

Feedback ⓘ announced · Sep 28, 2026

PRESS ↗ RANK

More than DSPM: Bedrock's AI and data security platform unifies data, identity, and AI context so teams see real risk — not noise — without moving data.

> Bedrock Security extended its Agent DLP capability to NVIDIA OpenShell, giving AI agents data-aware policy enforcement at the sandbox boundary along with pre-deployment blast-radius visibility.

└──▷ **WHAT SHIPPED · 1 FEATURE** most completely described first ? what's the number?

01 Agent DLP extended to NVIDIA OpenShell agents NEW

78

Bedrock extends Agent DLP to NVIDIA OpenShell via OpenShell's Supervisor Middleware, evaluating each agent action against enterprise data policies and returning an allow/block decision enforced at the sandbox boundary. An observe-only mode records policy decisions without enforcing them so teams can validate coverage before turning on enforcement. At design time it exposes an agent's blast radius — what data its permissions can reach, what combinations that data forms, and where policy would be violated — for pre-deployment visibility. The same data policies apply across every tool invocation path an agent may use, including MCP tools, command-line invocations, and code the agent writes itself, from a single OpenShell control point, and data restrictions carry across table writes, tool handoffs, and agent-to-agent transfers based on the Metadata Lake knowledge graph rather than payload pattern matching, so restrictions travel with the data as it moves.

— Rich mechanism detail but no exact config key or command to invoke it

launch-20260928-00b820b2

> announced · Sep 28, 2026 PRESS ↗
>
> Bedrock Security extends Agent DLP to NVIDIA OpenShell, adding data-aware policy enforcement at the agent sandbox boundary.
>
> Extends Agent DLP to NVIDIA OpenShell via OpenShell's Supervisor Middleware, evaluating each agent action against enterprise data policies and returning an allow/block decision that OpenShell enforces at the sandbox boundary.
>
> Supports an observe-only mode that records policy decisions without enforcing them, letting teams validate coverage before turning on enforcement.
>
> At design time, exposes an agent's blast radius — what data its permissions can reach, what combinations that data forms, and where policy would be violated —

giving security teams pre-deployment visibility.

Applies the same data policies across every tool invocation path an agent may use — MCP tools, command-line invocations, and code the agent writes itself — from a single OpenShell control point.

Carries data restrictions across table writes, tool handoffs, and agent-to-agent transfers based on the Metadata Lake knowledge graph rather than payload pattern matching, so restrictions travel with the data as it moves.

WAS THIS USEFUL? 👍 👎

GOVERNANCE, RISK & COMPLIANCE

◆ Integrated & IT Risk Management

raviaxo RiskShard

Feedback ⓘ v0.11.1 NOTES ↗ RANK

Evidence-governed quantitative cyber risk — a trustworthy CLI and scenario engine where every number traces to a reviewed public source.

> RiskShard shipped a new doctor diagnostic that catches unreadable sources hiding on disk, and introduced per-anchor composition breakdown across figures, citations, and executive reports.

└──▷ **WHAT SHIPPED · 2 FEATURES** most completely described first ? what's the number?

01 **Per-anchor composition breakdown across reports and citations**

NEW 85

Adds `engine/composition.py` to partition each shard's per-event mean across its three anchors using the beta-PERT mean identity, exposing how much of a figure each anchor contributes. Surfaces this in three places — each explorer item, the executive report's How much to trust it section, and the citation, which now refuses to emit a figure without the breakdown. Publishes Finding 10 in `docs/FINDINGS.md`, showing anchor weighting by contribution diverges sharply from a raw count (three shards at 92%, 92%, and 98.8% measured on impact while drawing 100% of their frequency mean from an out-of-population source), and ships data pack `data_pack_releases/2026.08.23-v0.11.0.json` alongside.

— Names module, three surfaces, findings doc, and data pack path v0.11.0

02 **Doctor check for unreadable-but-held sources** NEW 70

Adds `engine.intake.blocked_but_held` diagnostic that cross-references every source the audit cannot read against extracted titles in the intake register, failing the doctor on any match where a document is on disk but not being read.

— Names the exact check and its mechanism, no usage example v0.11.1

v0.11.1 NOTES ↗ LATEST STABLE

Adds `engine.intake.blocked_but_held` check that fails the doctor when a source marked unreadable is found on disk

└──▷ **GET THIS VERSION**

```
$ git clone --branch v0.11.1
https://github.com/raviaxo/RiskShard.git
# already have the repo? check out this version:
$ git checkout v0.11.1
```

v0.11.0 NOTES ↗ STABLE

RiskShard v0.11.0 adds per-anchor composition breakdown to every figure, citation, and executive report section.

└──▷ **GET THIS VERSION**

```
$ git clone --branch v0.11.0
https://github.com/raviaxo/RiskShard.git
# already have the repo? check out this version:
$ git checkout v0.11.0
```

Adds `engine/composition.py` to partition each shard's per-event mean across its three anchors using the beta-PERT mean identity, exposing how much of a figure each anchor contributes.

Surfaces anchor composition in three places: each explorer item, the executive report's How much to trust it section, and the citation — which now refuses to emit a figure without the breakdown.

Publishes Finding 10 in `docs/FINDINGS.md`, showing that anchor weighting by contribution to the final figure diverges sharply from a raw count: three shards are 92%, 92%, and 98.8% measured on impact while drawing 100% of their frequency mean from an out-of-population source.

Ships data pack `data_pack_releases/2026.08.23-v0.11.0.json` alongside the engine update.

WAS THIS USEFUL? 👍 👎

GOVERN

◆ AI/LLM Security

ai-safe2-framework

Feedback ⓘ 2026-09-27_CLI_0.9.0

NOTES ↗ RANK

Ai-Safe2-Framework provides governance, risk, and compliance controls for securing agentic AI systems and non-human identities.

> AI SAFE² CLI 0.9.0 introduces a controlled, three-step workflow for running the six frozen Challenge 001 scenarios — pre-registration, bounded execution, and independent verification — backed by new sealed evidence schemas, evidence-manifest intake, and process-level safeguards.

└──▷ **WHAT SHIPPED · 6 FEATURES** most completely described first ? what's the number?

01 **Challenge 001 plan, execute, verify commands** NEW 95

Adds `safe2 challenge plan` to pre-register the evaluator, provider, treatment, execution limits, command-file identities, and optional system identity before any process runs; `safe2 challenge execute` to run the six frozen Challenge 001 scenarios as separate bounded process calls after explicit operator authorization via `--authorize-process-execution`; and `safe2 challenge verify-execution` to recheck the plan, source, normalized run, receipt, command-file digests, and optional identity binding without re-running the evaluator.

— Names every command and flag, forms a runnable three-step pipeline 2026-09-27_CLI_0.9.0

02 **Challenge execution plan and receipt schemas** NEW 75

Adds `safe2.challenge-execution-plan.v1`, a strict machine-readable pre-registration contract binding the executable, file arguments, provider declaration, treatment, and limits, and `safe2.challenge-execution-receipt.v1`, a sealed record of cross-artifact and per-episode evidence bindings including before-and-after SHA-256 digests for the executable and file arguments.

— Names both schema ids and exact fields, but no sample file shown 2026-09-27_CLI_0.9.0

03 **Controlled-executor example walkthrough** NEW 65

Adds a packaged controlled-executor example verifiable with `safe2 example verify challenge-controlled-executor` that demonstrates planning, execution, verification, reporting, and evidence-manifest intake end-to-end.

— Runnable verify command, but no output or transcript included 2026-09-27_CLI_0.9.0

04 **Bounded child-process execution safeguards** NEW 65

Enforces direct-child execution time limits and combined stdout/stderr byte limits, reduced child-process environment variables, no-overwrite artifact creation, and exact

regular-file resolution with symlink dereferencing before hashing.

— Concrete safeguards named, no configurable limit values given 2026-09-27_CLI_0.9.0

THINNER COVERAGE BELOW

05 **Explicit incomplete and conflict episode states** NEW

55

Surfaces incomplete and conflict episode states so invalid JSON, nonzero exits, timeouts, output limits, and contradicting evidence observations become explicitly visible rather than silently discarded.

— Describes behavior but gives no command to inspect these states 2026-09-27_CLI_0.9.0

06 **Evidence-manifest intake for challenge artifacts** NEW

50

Plans and execution receipts can now enter the existing AI SAFE² evidence inventory via `safe2 evidence manifest`.

— Names the intake command but not the manifest's structure 2026-09-27_CLI_0.9.0

2026-09-27_CLI_0.9.0 NOTES ↗ LATEST STABLE

AI SAFE² CLI 0.9.0 adds controlled Challenge 001 execution with pre-registration, independent grading, and sealed evidence receipts.

└──▷ GET THIS VERSION

```
$ git clone --branch 2026-09-27_CLI_0.9.0
https://github.com/CyberStrategyInstitute/ai-safe2-framework.git
# already have the repo? check out this version:
$ git checkout 2026-09-27_CLI_0.9.0
```

Adds `safe2 challenge plan` command to pre-register the evaluator, provider, treatment, execution limits, command-file identities, and optional system identity before any process runs.

Adds `safe2 challenge execute` command to run the six frozen Challenge 001 scenarios as separate bounded process calls after explicit operator authorization via `--authorize-process-execution`.

Adds `safe2 challenge verify-execution` command to recheck the plan, source, normalized run, receipt, command-file digests, and optional identity binding without re-running the evaluator.

Adds `safe2.challenge-execution-plan.v1` schema providing a strict, machine-readable pre-registration contract binding the executable, file arguments, provider

declaration, treatment, and limits.

Adds `safe2.challenge-execution-receipt.v1` schema providing a sealed record of cross-artifact and per-episode evidence bindings, including before-and-after SHA-256 digests for the executable and file arguments.

+4 more

WAS THIS USEFUL? 👍 👎

WitnessAI

Feedback ⓘ

MCP authentication and authorization: OAuth for AI agents (2026-09-28) BLOG ↗

RANK

WitnessAI sits in the network path and monitors, controls and protects employee, application and agent AI activity.

> WitnessAI's latest release adds a full stack of MCP agent governance controls, from network-level approved-tool enforcement and cross-platform agent visibility to bidirectional content inspection, unified audit trails, and intent-based enforcement decisions.

└──▷ **WHAT SHIPPED · 5 FEATURES** most completely described first ? what's the number?

01 Bidirectional content inspection via Protect runtime APIs

NEW 65

The Protect module's runtime APIs now evaluate agent inputs before processing and responses before delivery, with malicious prompt detection validated in production across more than 100 LLMs.

— Names APIs and scope, no exact endpoint given MCP authentication and authorization: O…

02 MCP server and tool visibility in Observe module NEW

60

The Observe module gains MCP server and tool visibility by identifying agentic sessions through inspection of tool advertisements in traffic payloads, covering Claude Desktop, VS Code with AI extensions, and local agents built on LangChain, LlamaIndex, CrewAI, and custom code.

— Lists many named platforms but no direct user action

MCP authentication and authorization: O…

THINNER COVERAGE BELOW

03 Approved-tool enforcement for MCP via Agentic Control NEW

55

An organization-wide approved-tool list for MCP servers and tools is enforced at the network level before agent calls execute, spanning IDE, chat, and agent surfaces via the Agentic Control module.

— Names enforcement point and module but no config surface

MCP authentication and authorization: O…

04 Intent-based ML classification for Control enforcement NEW

50

Intent-based machine learning classification of conversational context now drives Control module enforcement decisions: allow, warn, block, or route to an approved internal model.

— Names decision options but not classification mechanism detail

MCP authentication and authorization: O…

05 **Unified audit trails for agent and human identity** NEW

30

Audit trails now correlate agent actions and blocked tool calls to the triggering human identity, covering both agent and employee activity routed through the platform.

— Describes outcome only, no mechanism or interface named

MCP authentication and authorization: O…

MCP authentication and authorization: OAuth for AI agents (2026-09-28) BLOG ↗

LATEST STABLE

WitnessAI adds MCP server/tool discovery, approved-tool enforcement, and bidirectional content inspection for enterprise AI agent governance.

Adds an organization-wide approved-tool list for MCP servers and tools, enforced at the network level before agent calls execute across IDE, chat, and agent surfaces via Agentic Control.

Adds MCP server and tool visibility through the Observe module, identifying agentic sessions by inspecting tool advertisements in traffic payloads across Claude Desktop, VS Code with AI extensions, and local agents built on LangChain, LlamaIndex, CrewAI, and custom code.

Adds bidirectional content inspection via the Protect module's runtime APIs, evaluating agent inputs before processing and responses before delivery, with malicious prompt detection validated in production across more than 100 LLMs.

Adds unified audit trails that correlate agent actions and blocked tool calls to a triggering human identity, covering both agent and employee activity routed through the platform.

Supports intent-based machine learning classification of conversational context to drive Control module enforcement decisions: allow, warn, block, or route to an approved internal model.

WAS THIS USEFUL? 👍 👎

Mend.io Mend AI

Feedback ⓘ (27-September-2026) NOTES ↗

RANK

Traditional application security misses AI risk. Standalone AI security tools miss your code.

> This window's shipments span Mend's CLI SAST scanner, its Renovate dependency updater, and Mend AI's triage workflow, with per-finding triage control the most consequential change for security teams.

└──▷ **WHAT SHIPPED · 3 FEATURES** most completely described first ? what's the number?

01 CLI logging and scan exclusions in mend code IMPROVED

75

The `mend code` CLI SAST scan gains a `--print-to-console` flag that streams scan logs directly to stdout in addition to the log file, useful for real-time visibility in CI pipelines. Default exclusions across all SAST scan engines now automatically ignore `/_MACOSX/..*` metadata files, preventing macOS system files from interfering with the TreeSitter parser on Windows.

Tail SAST scan output in CI pipelines without having to locate the log file — useful for real-time visibility in pipeline runners.

```
$ mend code --print-to-console
```

— Names exact flag and exclusion pattern with a runnable command product docs

02 Renovate versioning scheme improvements IMPROVED

65

Mend Renovate adds a `gomod` versioning scheme so Renovate can version-match Go module dependencies and query pseudo-versions, applies the downgrade guard across every versioning scheme (not just select ones) to prevent accidental downgrades in any package manager, and extends Poetry versioning to accept PEP 440 specifiers instead of relying on a lookup special case.

— Names three concrete versioning schemes and their behaviour but no config example

product docs

THINNER COVERAGE BELOW

03 Finding-level Suppress and Review triage in Mend AI IMPROVED

40

Suppress and Review triage actions now extend to the individual finding level, enabling security teams to triage specific findings within an entity independently rather than only being able to act on the entity as a whole.

— Describes the behaviour change but no UI path or API surface named (27-September-2026)

> (27-September-2026) NOTES ↗ LATEST STABLE
>
> Mend AI extends Suppress and Review triage actions to the individual finding level for more precise control.

WAS THIS USEFUL? 👍 👎

PLATFORMS & UTILITIES

◆ General Utilities & Libraries

goshs

Feedback ⓘ v2.1.7 NOTES ↗ RANK

Feature-rich single-binary file server for red teamers and developers. HTTP/S · WebDAV · FTP/SFTP · SMB · LDAP/S · NTLM hash capture · DNS/SMTP callbacks · TLS · Auth · Share links.

> goshs v2.1.7 closes several access-control gaps by enforcing per-folder `.goshs` ACLs across every non-HTTP protocol, hardening brute-force lockout and case-insensitive filtering, and adding folder upload to the web UI — with a breaking change to how malformed `.goshs` files are handled.

└──▷ **WHAT SHIPPED · 5 FEATURES** most completely described first ? what's the number?

01 **Cross-protocol ACL enforcement via ProtocolACL** NEW — 73

Introduces `httpserver.ProtocolACL`, a fail-closed enforcer that wires per-folder `.goshs` ACL checks into every SFTP, FTP, TFTP and SMB read, write, list, rename, and handle-creation path — folders protected or blocked over HTTP are now denied outright on all protocols.

— Names mechanism and all four protocols covered. v2.1.7

02 **Fail-closed .goshs ACL resolution** BREAKING — 72

The `.goshs` ACL resolver now fails closed: an unreadable, unparsable, or non-regular `.goshs` entry (including a dangling symlink or a directory named `.goshs`) denies everything in the subtree rather than silently dropping inherited auth and block lists; `?mkdir` and uploads refuse any `.goshs` path component. Setups that inadvertently had a `.goshs` directory will lose access to those paths on upgrade.

— Documents exact breaking condition and affected surfaces, `?mkdir` named. v2.1.7

03 **Folder upload in web UI** NEW — 61

Whole directory trees, including subdirectories, can now be dragged, dropped, or selected for upload through the web UI with structure preserved server-side; `..` path components and `.goshs` path segments are refused.

— UI action described but no exact navigation path given. v2.1.7

THINNER COVERAGE BELOW

04 **Case-insensitive block-list matching** IMPROVED — 56

Extends all block-list and never-serve enforcement points across HTTP, WebDAV, SFTP and directory listing filters to compare names case-insensitively, closing bypasses on Windows and macOS filesystems.

— Explains scope and fixed bypass but no config surface. v2.1.7

05 **Brute-force lockout counter hardening** IMPROVED 56

Each per-IP attempt is now counted inside the same locked section as the credential check, preventing concurrent requests from resetting the counter and bypassing the 5-failure lockout window.

— Names the 5-failure threshold and mechanism, no config to tune. v2.1.7

└──▷ **BREAKING ON UPGRADE**

! Any `.goshs` entry that is a directory, dangling symlink, or otherwise non-regular file now causes the ACL resolver to deny all access to that subtree instead of returning an empty ACL. Setups that inadvertently had a `.goshs` directory will lose access to those paths on upgrade.

v2.1.7 NOTES ↗ LATEST STABLE

goshs v2.1.7 enforces per-folder `.goshs` ACLs across SFTP/FTP/TFTP/SMB via `ProtocolACL` and adds folder upload to the web UI.

└──▷ **GET THIS VERSION**

```
$ git clone --branch v2.1.7 https://github.com/goshs-labs/goshs.git
# already have the repo? check out this version:
$ git checkout v2.1.7
```

Introduces `httpserver.ProtocolACL`, a fail-closed enforcer that wires per-folder `.goshs` ACL checks into every SFTP, FTP, TFTP and SMB read, write, list, rename, and handle-creation path — folders protected or blocked over HTTP are now denied outright on all protocols.

Adds folder upload to the web UI: whole directory trees (including subdirectories) can be dragged, dropped, or selected for upload with structure preserved server-side; `..` path components and `.goshs` path segments are refused.

Extends all block-list and never-serve enforcement points across HTTP, WebDAV, SFTP and directory listing filters to compare names case-insensitively, closing bypasses on Windows and macOS filesystems.

Hardens the brute-force lockout so each per-IP attempt is counted inside the same locked section as the credential check, preventing concurrent requests from resetting the counter and bypassing the 5-failure lockout window.

Makes the `.goshs` ACL resolver fail closed: an unreadable, unparsable, or non-regular `.goshs` entry (including a dangling symlink or a directory named `.goshs`) now denies everything in the subtree rather than silently dropping inherited auth and block lists; `?mkdir` and uploads refuse any `.goshs` path component.

└──▷ **BREAKING ON UPGRADE**

! Any `.goshs` entry that is a directory, dangling symlink, or otherwise non-regular file now causes the ACL resolver to deny all access to that subtree instead of returning an empty ACL. Setups that inadvertently had a `.goshs` directory will lose access to those paths on upgrade.

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

The Cyber Toolchain · curated daily · September 28, 2026
Releases & features from the open-source and commercial cyber tools that practitioners actually run.

▷ Subscribe | Feedback on this issue