THE CYBER TOOLCHAIN

NO. 107

# Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED OCTOBER 13, 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 94 changes

Do you prefer **scroll**? 👍 👎

▸ // CONTENTS SHOW 14 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.

Three unrelated things stand out. NETRESEC published Suricata rules and IOCs for AtlasRAT C2, so hunting starts today rather than after you se the protocol yourself. Veracode's SCA now flags outright

vim ? help

malicious packages, not just vulnerable ones. And nono pins executables by digest, so a swapped binary fails the policy instead of inheriting it.

DETECT

**Hunt AtlasRAT C2 on your own wire tonight**

Four Suricata rules plus IOCs, and a FlowCarp model updated to cover both known protocol variants — meaning the variant that changes its handshake no longer slips past a signature written for the first one. Teams get working detection without doing the malware analysis themselves.

NETRESEC

PROTECT

**Catch packages that are malicious, not merely vulnerable**

SCA scans now include malicious package detection alongside SBOM output, Poetry and Python 3.12 support. A CVE scanner says nothing about a typosquat or a hijacked maintainer release — that is a different failure mode, and it now surfaces in the same scan Python teams already run.

Veracode

PROTECT

**Stop a swapped binary from inheriting an approved command's permissions**

v0.80.0 pins executables by digest, signs AWS credentials per command, and gates macOS keychain access. A policy that allows a command by path trusts whatever is at that path today; digest pinning breaks that assumption, and per-command credential signing means a compromised tool cannot reach for the whole AWS session.

nono

IDENTIFY

**See which agent plugins and MCP servers developers actually installed**

Single-pane visibility into installed Claude Code plugins, MCP servers, skills and hooks across developer endpoints. Agent extensions arrive through developer-initiated installs with no procurement trail, so most teams currently cannot answer what is running — this is the inventory step before any policy on it is enforceable.

Backslash

## APPLICATION SECURITY

◆ SAST / SCA / Code Security

# GitHub

Feedback ⓘ

Code scanning AI Scan metrics in security overview (2026-10-13) BLOG ↗ RANK

GitHub is a web-based platform for version control and collaborative software development using Git repositories.

> GitHub added AI Scan metrics to the security overview's code scanning pages, giving teams visibility into autofix adoption and remediation rates alongside existing CodeQL metrics.

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

01 **AI Scan tab in security overview** NEW 75

The Code scanning on pull requests page (renamed from CodeQL pull requests) now has a dedicated AI Scan tab showing total findings, autofix suggestion coverage, remediation rate, and developer adoption of autofix across repositories, while existing CodeQL metrics move to their own CodeQL tab.

Review AI Scan effectiveness across your organization before deciding on a broader rollout.

> 📍 In Security Overview, go to Code scanning on pull requests › AI Scan tab, then filter by reporting period to see total findings, remediation rate, and how often developers applied autofix suggestions per repository.

— Names exact UI path and metrics shown, no API/flag given.

Code scanning AI Scan metrics in securi…

WAS THIS USEFUL? 👍 👎

# Veracode

Feedback ⓘ SCA updates (2026-10-12) BLOG ↗ RANK

Veracode is a cloud-based application security platform that scans software code, binaries, and dependencies to identify and help remediate security vulnerabilities throughout development.

> Veracode's SCA agent and upload scans gained new CLI flags, malicious package detection, SBOM support, Poetry and Python 3.12 compatibility, Unified Policy enforcement in two regions, deep-linking, and a full migration to new backend and download URLs.

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

## 01 --appname and --show-cli flags in SCA agent scans NEW

95

Adds `--appname` and `--show-cli` flags to the SCA agent scan command: `--appname` (Commercial region) links scan results to an application profile and requires OAuth or HMAC authentication, while `--show-cli`, used with `--json`, saves JSON output to a file while still displaying a human-readable CLI summary in the console, returning an error if used without `--json`.

Link an SCA agent scan to a named application profile for centralized visibility in the Veracode Platform.

```
$ srcclr scan . --appname 'MyApp' --json --show-cli
```

Save structured JSON scan output to a file while keeping a human-readable summary visible in CI console logs.

```
$ srcclr scan . --json results.json --show-cli
```

— Exact flags, requirements and runnable commands given SCA updates (2026-10-12)

## 02 SCA backend and download URL migration BREAKING

90

Changes default Veracode URLs for SCA: the Platform backend API URL for Commercial region scans moves to `https://sca-api.veracode.com` (from `https://api.sourceclear.io`), the European region API URL moves to `https://sca-api.veracode.eu` (from `https://platform-backend.analysiscenter.veracode.eu`), the US Federal region API URL moves to `https://sca-api.veracode.us` (from `https://platform-backend.analysiscenter.veracode.us`), and the SCA agent download URL moves

to `https://sca-downloads.veracode.com` (from `https://download.sourceclear.com`); all legacy URLs remain available for 12 months before retirement.

– All old and new URLs named with migration window SCA updates (2026-10-12)

03 **Unified Policy assignment for SCA agent workspaces** NEW

60

Adds Unified Policy assignment to SCA agent-based scan workspaces in the US Federal region and the European region, allowing policies to create issues and break builds based on defined criteria.

– Names regions and effect, lacks setup steps SCA updates (2026-10-12)

THINNER COVERAGE BELOW

04 **Poetry and Python 3.12 support in SCA scans** NEW 50

Adds support for Python projects using the Poetry package manager to both SCA agent-based scans and SCA Upload scans, and adds Python 3.12 environment support for SCA agent-based scans.

– Names package manager and Python version, no commands SCA updates (2026-10-12)

05 **Malicious package detection in SCA scans** NEW 40

Adds malicious package detection to SCA upload and agent-based scans, reporting malicious packages found in scanned libraries with no extra configuration or agent update required.

– Describes behavior but no config or output details SCA updates (2026-10-12)

06 **SBOM generation and scanning in SCA** NEW 40

Adds SBOM generation during SCA agent-based scans and SBOM file scanning support as part of SCA upload scans.

– No SBOM format or command specifics given SCA updates (2026-10-12)

07 **Deep-link redirect for SCA scan-results pages** NEW

40

Adds deep-link support for SCA pages: unauthenticated users opening a scan-results link are redirected to login and then back to the original page.

– Behavior described, no surface or config named SCA updates (2026-10-12)

└──▷ **BREAKING ON UPGRADE**

! The default SCA agent download URL changes from `https://download.sourceclear.com` to `https://sca-downloads.veracode.com`; scripts or pipelines that hardcode the old URL must be updated within 12 months before `https://download.sourceclear.com` is retired.

! The default Veracode Platform backend API URL for Commercial region SCA agent scans changes from `https://api.sourceclear.io` to `https://sca-api.veracode.com`; any configuration referencing the legacy SourceClear URL must be updated within 12 months.

! The default Veracode Platform backend API URLs for European region customers change from `https://platform-backend.analysiscenter.veracode.eu` to `https://sca-api.veracode.eu`, and for US Federal region customers from `https://platform-backend.analysiscenter.veracode.us` to `https://sca-api.veracode.us`; legacy URLs retire in 12 months.

---

WAS THIS USEFUL?  

◆ WAF, Bot & API Protection

# Levo

Feedback ⓘ October 13, 2026 NOTES ↗ RANK

Levo continuous API Security Assurance â observe, detect, and protect your APIs.

> Levo shipped a full create-validate-approve lifecycle for custom AI-authored tests, multi-GitHub-account support, bulk endpoint merging in the API Surface, a Beta Service Graph, and expanded authentication-bypass, form-encoded and unauthenticated-access test coverage — alongside a breaking change to the API Surface export format that requires integration updates.

└──▷ **WHAT SHIPPED · 13 FEATURES** most completely described first ? what's the number?

01 **Custom AI-authored test lifecycle** NEW 60

Introduces a full authoring lifecycle — create, validate, approve — for custom AI-authored tests, with every test run bound to the exact code a human reviewed.

– Full lifecycle and binding mechanism described, no UI path given October 6, 2026

THINNER COVERAGE BELOW

02 **API Surface export format changed** BREAKING 55

The API Surface export format has changed; integrations that read it must be updated before upgrading.

– Clear migration note but no new format details given October 6, 2026

03 **Expanded API security test coverage** NEW 50

Adds an authentication-bypass test for gateway path handling, and extends test coverage to form-encoded APIs and unauthenticated-access probes.

– Three new test types named, no config to enable them September 15, 2026 October 13, 2026

04 **Bulk merge for duplicate API endpoints** NEW 45

Adds bulk merge for duplicate API endpoints in the API Surface.

– Named feature area but no steps or UI path given October 6, 2026

05 **Beta Service Graph in API catalog** NEW 45

Introduces a Beta Service Graph in the API catalog for visualizing service relationships.

– Named feature with location, lacks further data detail September 15, 2026

06 **AI crawl and login improvements** IMPROVED 43

Improves AI-driven crawl efficiency by avoiding filter variants and focusing budget on real pages, and improves AI-guided login to verify successful sign-in before a scan continues.

— Mechanism described but no settings exposed October 13, 2026

07 **Bulk delete of test runs under RBAC** NEW 39

Adds bulk delete of test runs under role-based access control.

— Action and access model named, no role specifics given September 15, 2026

08 **Per-application API security test tuning** NEW 37

Adds per-application tuning of API security testing settings.

— Settings area named, no specific controls listed September 15, 2026

09 **Multi-GitHub-account support** NEW 33

Adds support for connecting multiple GitHub accounts to a single organization.

— No mechanism or UI path given for connecting accounts October 13, 2026

10 **Endpoint trace listing performance** IMPROVED 30

Improves endpoint trace listing load performance on large workspaces.

— Performance improvement without concrete figures October 13, 2026

11 **Cleaner OpenAPI specs for gateway imports** IMPROVED 30

Produces cleaner OpenAPI specs compatible with strict gateway imports.

— No detail on what changed in spec generation September 15, 2026

12 **AI-assisted triage for bulk vulnerabilities** NEW 25

Adds AI-assisted triage to bulk vulnerability selections.

— No detail on how AI triage works or where it's surfaced October 13, 2026

13 **Reduced on-prem health alert noise** IMPROVED 23

Reduces alert noise for on-prem component health alerts.

— No specifics on which alerts or thresholds changed September 15, 2026

NEW INTEGRATION WSO2 API Gateway integration

└──▷ BREAKING ON UPGRADE

! The API Surface export format has changed — integrations that read it must be updated before upgrading.

September 22, 2026 NOTES ↗ STABLE

Levo gains a full-screen Service Graph page, AI-assisted vulnerability triage, MFA support in DAST scans, and redesigned PDF reports.

Adds a dedicated full-screen page for the Service Graph.

Adds AI-assisted triage directly from the vulnerability view.

Adds second-factor (MFA) support for DAST scans.

Redesigns PDF reports for security testing results.

WAS THIS USEFUL? 👍 👎

## NETWORK SECURITY

◆ Network Analysis & Monitoring

# NETRESEC

Feedback ⓘ changelog · Oct 13, 2026 CHANGELOG ↗ RANK

Netresec is a network forensics, packet sniffers and IT security products. Download NetworkMiner and other free software for network security analysis.

> NETRESEC published four new Suricata detection rules and actionable IOCs for AtlasRAT C2 traffic, and updated its FlowCarp detection model to cover both known AtlasRAT protocol variants.

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

## 01 Suricata rules and IOCs for AtlasRAT C2 detection NEW

88

Adds four Suricata rules published to `https://github.com/Netresec/Suricata`: `sid:1471105` detects the AtlasRAT loader `SFuck` C2 check-in via byte pattern `|53 46 75 63 6b 00 00 00|` on `tcp-pkt`; `sid:1471106` detects the `BFuck` loader variant's C2 check-in via `|42 46 75 63 6b 00 00 00|` on `tcp-pkt`; `sid:1471107` detects the AtlasRAT TLS C2 handshake on TCP port 443; and `sid:1471108` detects AtlasRAT's self-signed X.509 certificate impersonating `update.microsoft.com`. Also documents JA3/JA3S fingerprints `e26606c572e55d499b0676e9095e3df8` / `f98a4985f829b6513fbeccf5b751b458` and certificate thumbprint `a66308a1fb09c8345228ca00335e633b2dabde53` as actionable IOCs.

— Names exact sids, byte patterns, hashes and repo; ready to deploy.

changelog-20261013-d9394e45

THINNER COVERAGE BELOW

## 02 FlowCarp detection model updated for AtlasRAT variants

IMPROVED

41

The FlowCarp detection model for `win.atlas_rat` was updated to cover both the older `SFuck` and newer `BFuck` C2 protocol variants.

— Names the model but gives no usage or config details. changelog-20261013-d9394e45

WAS THIS USEFUL? 👍 👎

◆ Firewalls & Network Defense

# Sophos Central Firewall

Feedback ⓘ

2026.41Released on October 13, 2026 NOTES ↗ RANK

Sophos Central Firewall is a cloud-managed network security platform that provides firewall protection, intrusion prevention, and threat monitoring for organizations' networks.

> Sophos Fusion adds an AI-powered Firewall Assistant for natural-language management and troubleshooting, and switches to instant configuration push for SFOS 23.0+ firewalls, replacing minute-by-minute polling.

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

01 **AI Firewall Assistant in Sophos Fusion** NEW 65

A new Firewall Assistant tab under Chat with an assistant in Sophos Fusion provides an AI-powered assistant for natural-language firewall management and troubleshooting, available for firewalls running SFOS 23.0 or later.

When you need to diagnose a firewall rule or troubleshoot connectivity without navigating deep menus, open the AI Assistant in Sophos Fusion.

> 📍 In Sophos Fusion, go to Chat with an assistant › Firewall Assistant tab, then type a natural-language query such as 'Why is traffic from 10.0.1.0/24 being dropped?'

— Names exact UI path and SFOS version, no deeper mechanism given

2026.41Released on October 13, 2026

THINNER COVERAGE BELOW

02 **Instant config push to firewalls** IMPROVED 50

Sophos Fusion now pushes configuration changes immediately to firewalls running SFOS 23.0 or later, replacing the previous pull-every-minute polling model.

— States before/after behaviour but no config surface or metric

2026.41Released on October 13, 2026

WAS THIS USEFUL? 👍 👎

## DETECTION & RESPONSE

◆ SIEM

## Sumo Logic

Feedback ⓘ OpenAI Source (Collection) (2026-10-08)

BLOG ↗

Sumo Logic is a cloud-native machine data analytics platform that collects, searches, and analyzes logs and metrics for security monitoring, troubleshooting, and operational insights.

NEW INTEGRATION OpenAI source for Sumo Logic

WAS THIS USEFUL? 👍 👎

# EXPOSURE & VULNERABILITY MANAGEMENT

◆ Attack Surface & Exposure Management

## syzkaller

Feedback ⓘ changes since 2026-10-09 CODE ↗

syzkaller is an unsupervised coverage-guided kernel fuzzer

Adds `syzlang-vm-testing` agent skill and expands `GEMINI.md` with syzlang and seed authoring guidance for AI-assisted development.

└──▷ GET THIS VERSION

```
$ git clone --branch commits-2026-10-09
https://github.com/google/syzkaller.git
# already have the repo? check out this version:
$ git checkout commits-2026-10-09
```

Adds `syzlang-vm-testing` agent skill to guide LLM-based automated VM testing workflows.

NEW DETECTION netdevsim sysfs and debugfs interface descriptions

WAS THIS USEFUL? 👍 👎

◆ Identity & Access Management

# iDenfy

Feedback ⓘ snapshot-20261013 NOTES ↗ RANK

Explore iDenfy documentation for identity verification (KYC), business verification (KYB), AML screening, fraud prevention, and more.

> iDenfy's biggest addition this window is MCP connectivity letting AI assistants like Claude query iDenfy accounts under a consent screen, alongside free AML checks, SDK upgrades for bank card and Brazil CPF verification, a new Shopify age-estimation integration, and smaller KYC/KYB refinements.

└──▷ **WHAT SHIPPED · 10 FEATURES** most completely described first ? what's the number?

01 **MCP connectivity for AI assistants** NEW 80

Adds MCP connectivity so AI assistants (Claude and Claude Code) can access iDenfy accounts, with a consent screen that lets users control which data areas the assistant can view or edit.

Connect Claude to your iDenfy account over MCP to query verification data directly from an AI assistant.

> 📍 In Claude or Claude Code, add the iDenfy MCP server connection, then use the iDenfy consent screen to select which data areas (view or edit) the assistant is permitted to access.

— names mechanism, assistants, and consent control with setup steps snapshot-20261013

THINNER COVERAGE BELOW

02 **Free AML checks for unscreened accounts** NEW 55

Accounts without AML screening enabled can now run 10 complimentary AML checks directly from the dashboard.

— gives concrete number but no exact navigation path snapshot-20261013

03 **Bank card and Brazil CPF checks in SDKs** NEW 55

Adds bank card verification and Brazil CPF check support inside the iOS and Android SDKs, and extends the Brazil CPF check to also collect date of birth.

— names platforms and check types but no code snippet snapshot-20261013

04 **Shopify integration for age estimation** NEW 55

Adds a Shopify integration allowing merchants to sign up for and pay for age estimation directly within Shopify.

– names platform and product but no setup steps given snapshot-20261013

05 **Default KYC theme setting** NEW 55

A specific KYC theme can be set as the default so all new verification sessions start with it without per-session configuration, via the KYC Themes list in the dashboard.

Set a specific KYC theme as the default so all new verification sessions start with it without per-session configuration.

> 📍 In the iDenfy dashboard, open the KYC Themes list, select the desired theme, and enable Set as default for new sessions.

– only sourced from usage example, not mentioned in changelog bullets snapshot-20261013

06 **Marital name field in KYC responses** NEW 50

KYC responses now include a `marital name` field when an ID document contains a second surname.

– names the field and trigger condition but no usage example snapshot-20261013

07 **KYB update sharing and AI report registry lookup** NEW 40

Adds KYB update request sharing via link, and adds step-by-step registry lookup to KYB AI reports.

– two thin KYB additions named but not elaborated snapshot-20261013

08 **New-tab camera fallback for iFrame integrations** IMPROVED 40

Adds a new-tab camera fallback for iFrame integrations when the camera fails to load.

– describes trigger and fix but no further mechanism snapshot-20261013

09 **'Explore products' menu** NEW 35

Adds an Explore products menu showing products the account does not currently have.

– names UI element but no further detail on behavior snapshot-20261013

10 **European Accessibility Act compliance** NEW 10

iDenfy states compliance with the European Accessibility Act.

– mentioned only in summary with no further detail snapshot-20261013

WAS THIS USEFUL? 👍 👎

# JumpCloud

Feedback ⓘ Release Notes 2022 (2026-10-13) 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.

> JumpCloud's 2023–2026 releases introduced hardware-backed passwordless login (JumpCloud Go), expanded MDM across Windows, Apple and Android with new CSP and privacy policies plus unified patch-management dashboards, added AI-driven admin tooling (MCP Server, AI Commands Builder, Shadow AI Dashboard) and Access Requests, and overhauled admin role-based access control, alongside steady Password Manager desktop app upgrades.

└──▷ **WHAT SHIPPED · 40 FEATURES** most completely described first ? what's the number?

01 **MCP Server for admins and users** NEW 90

Introduces JumpCloud MCP Server (GA) to connect compatible AI tools and code editors to JumpCloud via the Model Context Protocol. Adds MCP Server for Users, enabled at `Settings > JumpCloud AI`, letting JumpCloud users connect AI clients to User Portal capabilities over OAuth; admins can review and revoke active sessions or set an automatic expiration window, and users can self-manage sessions at `Security > JumpCloud MCP` in the User Portal.

Connect an AI tool or code editor to JumpCloud via the MCP Server to query org data and run administrative actions directly from your development environment.

> 📍 In the Admin Portal, go to Get Started: JumpCloud MCP Server, generate your MCP Server credentials, then configure your AI tool or editor to connect to the JumpCloud MCP Server endpoint using those credentials.

Enable the MCP Server for Users so your team can perform User Portal tasks from AI clients, then verify active OAuth sessions are visible for audit.

> 📍 In the Admin Portal, go to Settings › JumpCloud AI and toggle on MCP Server for Users. To review or revoke active client sessions, stay on the same page. Users can view and revoke their own sessions at Security › JumpCloud MCP in the User Portal.

— Exact settings paths and steps for both admin and user sides.

Release Notes 2026 (2026-10-13) Release Notes 2025 (2026-10-13)

02 **JumpCloud Go passwordless authentication** NEW SUPPORTED PLATFORM

NEW 85

JumpCloud Go is a hardware-protected, phishing-resistant passwordless login method using Apple Touch ID and Windows Hello on managed macOS and Windows devices, verifying both user and device on every SSO session. Conditional access policies for SSO apps now default to JumpCloud Go as the MFA method, which may change the authentication flow for existing SSO app policies.

Enable JumpCloud Go as the required MFA method for an SSO application so every session is verified with a hardware-backed device authenticator.

> 📍 In the Admin Portal, go to SSO Applications › select your app › Conditional Access › set MFA Method to `JumpCloud Go`, then save.

— Mechanism and new default behavior both documented with a setup path.

Release Notes 2023 (2026-10-13)

---

03 **API filter pipe character escaping** IMPROVED 85

Adds pipe `|` escape support via backslash `\` in API `in` and `nin` filter operators, enabling pipe characters within search terms for requests like `GET /systemusers?filter=department:$in:Finance | Accounting|IT`.

Query users across departments that contain a pipe character in their name, using the new backslash escape in API filter expressions.

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

— Exact operator syntax with a runnable curl example. Release Notes 2024 (2026-10-13)

---

04 **Breaking API endpoint and filter operator changes** BREAKING 85

Replaces deprecated `GET api/systemusers/reactivate/{id}` with `POST https://console.jumpcloud.com/systemusers/reactivate/{id}` accepting an `activation_email` body field, with the old endpoint now returning a 404 error, and replaces deprecated `$ge` and `$le` Dynamic Groups `memberQuery` filter operators with `$gte` and `$lte` to align filter syntax across API list endpoints; any script, automation, or integration using the old endpoint or operators must be updated.

Migrate a reactivation script from the deprecated GET endpoint to the required POST endpoint.

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

— Both endpoints and field named, with a runnable migration example. Exact operator names given but no example request shown.

Release Notes 2024 (2026-10-13)

05 **Custom Admin Roles and granular RBAC scopes** UPDATED INTEGRATION NEW INTEGRATION BREAKING 85

Releases Custom Admin Roles for all direct organizations, enabling granular role tailoring based on specific responsibilities. Adds CRUD operations and No Access permission to the Identity Management and Application Management scopes; splits Identity Management and Directory and Groups Management into separate, independently assignable scopes; groups Directory Management and Group Management under a unified Directory and Groups Management permission; groups SaaS Applications and Asset Management under a unified SaaS and Asset Management permission; moves RADIUS Authentication under the Access Management scope; includes Application Templates within the Applications scope; and includes existing User Portal APIs and all User Portal operations within the Multi-Factor Authentication scope. The Policy Management scope is renamed to Access Management , System Management is renamed to Devices , and Authentication Policies is renamed to Conditional Access Policies and IP Lists ; Identity Management no longer bundles directory and group scopes, and JumpCloud Protect is not included in any scope and has no assignable permission.

— Every renamed and regrouped scope named verbatim.

Roles Based Access Release Notes 2025 (… Release Notes 2025 (2026-10-13)

06 **Patch Management dashboards** NEW 85

Adds unified Patch Management dashboards at Device Management > Patch Management — an Overview tab for cross-platform Windows and Apple compliance, a Windows KB-centric view with CSV and JSON export, and an Apple Compliance Dashboard tracking OS rollout progress against active update policies — alongside a new Device Patch Report (Windows) under JumpCloud Reports showing per-device KB patch status (Installed, Pending, Failed) with Admin Portal preview of up to 500 rows and full CSV download.

— Exact navigation path, export formats, and row limit given.

Release Notes 2026 (2026-10-13)

07 **Password Manager item and folder management improvements**

IMPROVED

80

Adds Password Manager Shared Folders management from the Admin Portal with manual per-folder sync from the Password Manager desktop application, letting admins create and update shared folders, view and assign users or user groups to any shared folder, use a Move All items button to move all items from a shared folder at once, and multi-select items in shared folders for bulk management (shared folder events are captured and synced with Directory Insights in the Admin Portal); scales item storage capacity to up to 30,000 items (without autofill) or 13,000 items (with autofill) and up to 5,000 items per shared folder, adds the ability to sort items by nicknames, and paginates the items list at 100 items per page; and adds multi-delete capability for folders, item archiving functionality letting users view, delete, and restore archived items, and a Copy button in the Password History area.

— Lists all admin shared-folder actions but no exact menu path. Exact capacity and pagination numbers given. Three small UI additions named; no step-by-step given.

What's New: Password Manager Desktop Ap… | Release Notes 2023 (2026-10-13)

---

08 **Push Bombing Mitigation** NEW

80

Adds Push Bombing Mitigation to JumpCloud Protect, blocking more than one push notification per resource within a sixty-second period, configurable in MFA Configurations.

Protect admin accounts against push bombing by reviewing or tightening the sixty-second concurrent push limit in MFA Configurations.

> 📍 In the Admin Portal, go to Security › MFA Configurations › JumpCloud Protect › Push Bombing Mitigation › adjust Maximum Concurrent Attempts or toggle off as needed.

— Exact threshold and configuration location, plus adjustment steps.

Release Notes 2023 (2026-10-13)

---

09 **Global MFA Requirement for MSP admins** NEW

80

Adds Global MFA Requirement setting under `Account > Settings` in the Multi-Tenant Portal, allowing admins with Billing to bulk-enforce MFA for all MSP admins.

Enable the Global MFA Requirement to enforce MFA across all MSP admins in bulk from the Multi-Tenant Portal.

> 📍 In the Admin Portal, go to Account › Settings, then enable the toggle under Global MFA Requirement.

— Exact menu path and a toggle action given. Release Notes 2024 (2026-10-13)

---

10 **Access Requests workflow** NEW

80

Launches JumpCloud Access Requests with configurable approval flows, request management in the Admin Portal and User Portal, Directory Insights tracking, and webhook integration with ticketing systems such as JIRA.

Set up Access Request webhooks to auto-create JIRA tickets whenever users submit an access request, enabling real-time ticketing without manual intervention.

> 📍 In the Admin Portal, go to Access Requests › Settings, add a webhook URL pointing to your JIRA instance, and configure the approval flow to assign the appropriate admins or users as approvers.

– Webhook integration and portal locations named with a setup path.

Release Notes 2025 (2026-10-13)

---

11 **Asset Visibility and Acknowledgement** NEW 80

Adds Asset Visibility and Asset Acknowledgement in User Portal, enabled at `Device Management > Asset Management > Settings and Fields > General Settings`; acknowledgement requests and responses are recorded in Asset History with email notifications.

– Exact enablement path and audit trail location given. Release Notes 2026 (2026-10-13)

---

12 **Apple MDM restriction and privacy policies** NEW 75

Adds two new JumpCloud MDM policies to restrict Apple Intelligence features on iOS/iPadOS 18.1 and macOS 15.1 Sequoia devices. Adds App Settings Privacy policies for Apple MDM: `User Level macOS App Settings Privacy` (macOS 27+, supervised Macs, assignable to users or user groups) and `Device Level iOS and iPadOS App Settings Privacy` (iOS/iPadOS 27+, supervised devices, assignable to devices or device groups), supporting permissions including Accessibility, Bluetooth, Camera, Dictation, Local Network, Location, and Microphone.

– Names policy titles, OS versions, and permission list. Release Notes 2026 (2026-10-13)

Release Notes 2024 (2026-10-13)

---

13 **SSO authentication event and token enhancements** NEW 75

Adds `sso_auth` event to logs for forced re-authentication, supporting `ForceAuthn="true"` in SAML and `prompt=login` in OIDC so the IdP honors step-up authentication requests from connected apps, and includes Authentication Methods References (AMR) claims in both SAML assertions and OIDC ID tokens, tagging logins with proof of factors used (e.g., password + OTP) for Zero Trust compliance.

– Exact protocol parameters named; no configuration steps given. Explains claim purpose; no configuration or endpoint given.

Release Notes 2025 (2026-10-13)

14 **Windows MDM CSP policy framework** NEW 70

Adds a new Windows MDM policy to configure Simple Certificate Enrollment Protocol via Create a Windows SCEP Profiles Policy, and introduces a Windows MDM CSP framework with six new policies: Windows Wi-Fi Configuration Policy, Windows VPN Policy, Install Certificate Policy, Bluetooth Configuration Policy, Control Policy Conflict (enabled by default), and Windows Notification Service (enabled by default).

— All seven policies named verbatim; no config walkthrough.

Release Notes 2024 (2026-10-13)

15 **Custom Risk Policies** NEW 70

Adds Custom Risk Policies (at Access Risk) to tailor risk detection for Admin Portal, User Portal, device, and SSO application logins — choose risk factors, adjust score contributions, assign to specific user groups or SSO apps, and set policy precedence over the Default Policy.

— Named location and configurable levers; no exact steps shown.

Release Notes 2026 (2026-10-13)

16 **Custom Messaging for User Portal** NEW 70

Adds Custom Messaging for the User Portal at `Settings > User Portal > Custom Messaging`, supporting login dialogs and announcement banners scoped by user group with configurable severity and publish controls.

— Exact settings path and message types named. Release Notes 2026 (2026-10-13)

17 **AI Assistant knowledge-base uploads** NEW 70

Adds internal knowledge-base uploads for AI Assistant: supports PDF, TXT, DOCX, and MD files (10 MB maximum per file, 25 files maximum per org), with source attribution in chat responses.

— Exact file formats and limits given; no upload steps shown.

Release Notes 2026 (2026-10-13)

18 **Support RSS feed subscriptions** NEW 70

Adds Subscribe to Support RSS Feed on the Release Notes and Bug Fixes page for any new Help Center content, Subscribe to Release Notes and Bug Fixes RSS Feed for product release notes, agent release notes, and bug fix reports, Subscribe to Agent Release Notes RSS Feed for agent-specific notes, and Subscribe to Bug Fixes RSS Feed for bug-fix-only notifications.

Subscribe to JumpCloud product and agent release notes via RSS so your team is automatically notified of new capabilities without checking the portal manually.

📍 1. Go to the JumpCloud Release Notes and Bug Fixes page. 2. Click Subscribe to Release Notes and Bug Fixes RSS Feed. 3. Open the RSS feed URL in your RSS

reader of choice (most browsers have built-in support; Chrome users can install RSS Feed Reader ).

— Each named feed option paired with a subscription walkthrough.

Subscribe to New Feature and Product Up…

19 **Dynamic Device and User Groups** NEW 65

Adds Dynamic Device Groups and Dynamic User Groups, allowing admins to automate group membership via attribute-based rules with an optional review step before changes take effect.

Automate Android device group membership so newly enrolled zero-touch devices with a specific vendor are added without manual intervention.

📍 In the Admin Portal, go to Device Groups › New Group › Enable Dynamic › Add Rule: Vendor equals <your_vendor_name>, then save.

— Exact UI steps given for creating a dynamic rule. Release Notes 2023 (2026-10-13)

20 **Device Monitoring and Alerting** NEW SUPPORTED PLATFORM NEW 65

Introduces JumpCloud Device Monitoring and Alerting with 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, supporting Windows, macOS, and Linux endpoints.

— Broad alert scope named; no setup steps given. Release Notes 2024 (2026-10-13)

21 **New platform builds: ARM macOS and RPM Linux** BREAKING 65

Adds a native ARM build for macOS devices with M1 and above silicon, available on the Downloads page, with automatic update to the ARM build when the chip is detected; adds an RPM build for Linux (x64 Red Hat distributions such as Fedora) with auto-update support, in addition to the existing Debian build. The `.appimage` Linux build is no longer supported as of April 18, 2024; users must migrate to the RPM or Debian build.

— Build targets and migration deadline both named.

What's New: Password Manager Desktop Ap…

22 **Auto-lock controls for Password Manager** NEW 65

Introduces an auto-lock schedule with a default of 15 minutes of inactivity and a configurable maximum of 1,440 minutes (24 hours), plus an Auto Lock setting that locks the Password Manager app when the device is locked.

— Exact default and maximum values given; no setting path shown.

What's New: Password Manager Desktop Ap…

23 **Admin install/update via command template v2.0.0** IMPROVED

65

Enables admins to install and update the Password Manager desktop app via a new command template v.2.0.0 on Windows and macOS, removing the need for users to have admin permissions for subsequent updates.

— Names the template version and its permission effect.

What's New: Password Manager Desktop Ap…

24 **Android MDM enrollment and policy expansion** NEW 60

Adds Android zero-touch enrollment support for fully managed, dedicated, and company-owned Android devices with a work profile, plus streamlined enrollment token creation; fully supports Android 15 in MDM; and adds new Android policies for display settings, autofill, work account authentication, default app and intent handling, and enhanced Bluetooth controls (including outbound Bluetooth file sharing and personal-profile Bluetooth restrictions on company-owned devices with a work profile).

— Enrollment types named but no setup walkthrough given. Names policy areas but no configuration path given.

Release Notes 2023 (2026-10-13) Release Notes 2026 (2026-10-13)

Release Notes 2024 (2026-10-13)

25 **Service Account for APIs** NEW 60

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

Create a service account for an API integration so credentials are not tied to an individual admin, reducing risk from staff turnover or account changes.

> 📍 In the Admin Portal, go to Service Account for APIs, create a new service account, assign the required API scopes, and generate an API key to use in your integration in place of a personal admin credential.

— Clear setup steps given despite a thin mechanism description.

Release Notes 2025 (2026-10-13)

THINNER COVERAGE BELOW

26 **User Portal Folders** NEW 55

Adds User Portal Folders at `All Applications > Folders`, letting end users organize assigned applications into private personal folders.

— Named navigation path for users to use directly. Release Notes 2026 (2026-10-13)

27 **Self-Service Account Provisioning** NEW 53

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

— Mechanism named; no admin configuration steps given. Release Notes 2023 (2026-10-13)

28 **MDM Certificate & Token Status Board** NEW 53

Adds MDM Certificate & Token Status Board showing upcoming expiration of MDM, SSO, and AzureAD tokens and certificates, with an aggregate view for MSP admins across all tenant organizations.

— Scope and data shown are specific; no navigation path given.

Release Notes 2023 (2026-10-13)

29 **Duo Universal Prompt support** BREAKING 50

Adds Duo Universal Prompt support for JumpCloud MFA. Duo is ending support for the traditional Duo two-factor prompt on March 30, 2024; organizations using the legacy Duo prompt with JumpCloud MFA must migrate to the Duo Universal Prompt.

— Clear migration deadline; no migration steps given. Release Notes 2023 (2026-10-13)

30 **AI Commands Builder** NEW 50

Adds AI Commands Builder (GA) inside the Admin Portal to generate and refine commands for Windows, macOS, and Linux devices using plain-English prompts.

— Supported platforms named; no walkthrough given. Release Notes 2025 (2026-10-13)

31 **Custom Banned Password List** NEW 50

Adds Custom Banned Password List to Password Policies, letting organization admins block specific words, terms, and phrases from user passwords.

— Names the policy and its purpose; no configuration steps given.

Release Notes 2026 (2026-10-13)

32 **EU region support for Password Manager** NEW 50

Supports EU region for Password Manager; users select their region on the activation page (desktop) or pairing page (browser extension) before activating their account.

— Names where to select region but no further config detail.

What's New: Password Manager Desktop Ap…

33 **New SSO integrations: AWS Verified Access and Deel** NEW 48

Adds an AWS Verified Access integration using JumpCloud Go, SAML, or OIDC SSO as a VPN-less remote-access solution, and a Deel SSO Connector integration with JumpCloud.

— Names both integrations and the auth methods used. Release Notes 2023 (2026-10-13)

34 **BYOD iOS enrollment via Account-Driven User Enrollment** NEW 48

Supports BYOD enrollments of iOS/iPadOS 18+ devices in MDM via Account-Driven User Enrollment (ADUE), now in general availability.

— Mechanism and version named; no enrollment steps given. Release Notes 2024 (2026-10-13)

35 **Shadow AI Dashboard** NEW 48

Introduces the Shadow AI Dashboard under the renamed JumpCloud AI & SaaS Management for dedicated visibility into generative AI shadow IT, adoption, department usage, and most-active users.

— Names dashboard data points; no navigation path given. Release Notes 2025 (2026-10-13)

36 **Remote Assist Background Tools** NEW 43

Adds Remote Assist Background Tools enabling admins to use a remote command line and remote file transfer to access and troubleshoot end-user devices without disrupting the user's work.

— Describes capability but omits usage steps. Release Notes 2023 (2026-10-13)

37 **Asset Manager admin role** NEW 43

Adds a new Asset Manager role in the Admin Portal granting dedicated access to Asset Management without broader Admin Portal permissions.

— Named role and scope limit; no assignment steps given. Release Notes 2025 (2026-10-13)

38 **IPA file support in Private Repository** NEW 35

Adds IPA file support to the JumpCloud Private Repository for uploading and deploying iOS and iPadOS app packages.

— One-line format addition with no deployment steps. Release Notes 2025 (2026-10-13)

39 **MFA enabled by default for new admin accounts** BREAKING 30

MFA is now enabled by default for all new admin accounts — new admins will be required to complete a second factor on every Admin Portal login.

— States the default change but no opt-out or config path.

Release Notes 2023 (2026-10-13)

40 **Cloud Backup for Password Manager** NEW 15

Adds Cloud Backup for JumpCloud Password Manager providing a secure fallback to minimize data loss risk.

— Only a one-line description, no mechanism given. Release Notes 2023 (2026-10-13)

NEW INTEGRATION SentinelOne integration via JumpCloud Commands

└──▷ ALSO FROM THESE RELEASES

└──▷ BREAKING ON UPGRADE

! MFA is now enabled by default for all new admin accounts — new admins will be required to complete a second factor on every Admin Portal login.

! Conditional access policies for SSO apps now default to JumpCloud Go as the MFA method, which may change the authentication flow for existing SSO app policies.

! Duo is ending support for the traditional Duo two-factor prompt on March 30, 2024; organizations using the legacy Duo prompt with JumpCloud MFA must migrate to the Duo Universal Prompt.

! The `GET api/systemusers/reactivate/{id}` endpoint is deprecated and now returns a 404 error; replace with `POST https://console.jumpcloud.com/systemusers/reactivate/{id}` with `activation_email` in the request body in any script, automation, or integration.

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

! The Policy Management scope is renamed to Access Management.

! The System Management scope is renamed to Devices.

! The Authentication Policies scope is renamed to Conditional Access Policies and IP Lists.

! Identity Management no longer bundles directory and group scopes — Directory and Groups Management is now a separate scope requiring its own permission assignment.

! `JumpCloud Protect` is not included in any scope and has no assignable permission.

! The `.appimage` Linux build is no longer supported as of April 18, 2024; users must migrate to the RPM or Debian build.

Release Notes 2022 (2026-10-13) BLOG ↗ STABLE

JumpCloud 2022 adds certificate-based RADIUS auth, TOTP for LDAP MFA, OIDC SSO, Password Manager, Remote Assist, new device policies, and MSP command templates.

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

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

Adds OpenID Connect (OIDC) Single Sign-On for OIDC-capable web applications.

Adds the `Command After Agent Install` command type for automated enrollment scripting on new devices.

Adds a `Running` column to the commands queue.

+16 more

WAS THIS USEFUL? 👍 👎

## GOVERNANCE, RISK & COMPLIANCE

◆ Continuous Control Monitoring (CCM)

### RegScale

Feedback ⓘ CLI 6.52.0 (2026-10-13) BLOG ↗

RegScale is a compliance automation platform that helps organizations manage security controls, risk, and regulatory frameworks such as NIST, FedRAMP, and SOC 2.

JCAM SSP import now logs the RegScale security plan ID and a creation count per run summary.

NEW INTEGRATION Acunetix XML scan import

UPDATED INTEGRATION CrowdStrike Spotlight sync known-exploit data

WAS THIS USEFUL? 👍 👎

## GOVERN

◆ AI/LLM Security

# Docker Sandboxes

Feedback ⓘ v0.48.0 NOTES ↗ RANK

Docker Sandboxes run AI coding agents in isolated environments on your machine or on Docker-managed cloud infrastructure

> Docker Sandboxes v0.48.0 ships a unified `--format` output system, managed SSH targets for Codex and Claude Desktop, v3 kit capabilities, and a large set of breaking CLI and JSON-schema changes across sandbox, template, policy, ports, and volume commands.

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

## 01 Unified `--format` output system

BREAKING

90

`sbx diagnose` gains `--format table`, `--format json`, `--format yaml`, and `--format github-issue`, replacing the old `--output` / `-o` flag, and `sbx prune --dry-run` gains `--format json` / `--format yaml` for structured dry-run output. `--format json` / `--format yaml` are now mutually exclusive with `--json` and `-q` (even `--json --format json` is rejected), and unsupported `--format` values now fail at flag-parse time instead of silently falling back to human-readable output.

Parse sandbox names from `sbx ls` JSON in a script after the output structure changed from a wrapped object to a bare array.

```
$ sbx ls --format json | jq '.[].name'
```

— Named flags, formats, and a runnable example make this fully actionable. v0.48.0

## 02 Structured JSON/YAML output schema overhaul

BREAKING

90

Structured output changes across commands: `sbx ls --json` replaces the top-level `{"sandboxes": [...]}` object with a bare array, uses `snake_case` fields, RFC 3339 timestamps for `created_at` / `last_used_at`, and adds `detached`; `sbx template ls --json` replaces `{"images": [...]}` with a bare array; `sbx mcp ls --json` locally replaces `{"gateway": {...}, "servers": [...]}` with a bare server array carrying `gateway` per row; `sbx policy log` replaces `allowed_hosts` / `blocked_hosts` (and cloud camelCase fields) with `{updated_at, allowed: [...], blocked: [...]}` entries containing `sandbox_id`, `host`, `proxy_type`, `rule`, `reason`, `count`, `first_seen`, `last_seen`; `sbx --cloud policy ls` fields move from camelCase to `snake_case`; `sbx ports` cloud rows rename `port` to `sandbox_port` while local rows use `host_ip`, `host_port`,

`sandbox_port`, `protocol`; `sbx ports --publish` / `--unpublish` locally emit result rows with `action: published` / `action: unpublished` and send warnings to stderr; cloud `volume create`, `volume ls`, `volume inspect` move from PascalCase (`ID`, `Name`, `CreatedAt`) to `snake_case` (`id`, `name`, `created_at`), with `volume inspect` now defaulting to a human-readable view (use `--format json` for JSON); and `sbx rm`, `sbx stop`, `sbx template rm`, `sbx volume rm` now return an array of result objects with `action`, `resource`, `name`, and optional `id` / `error`, with lowercase action strings.

— Every affected command and field named with exact before/after schema. v0.48.0

---

03 **CLI flag standardization around --force and friends** BREAKING

80

Several short-lived flags are renamed and now rejected: `--detached` on `sbx run` / `sbx env run` becomes `--detach` / `-d`; `--quiet` / `-q` on `sbx create` becomes `--no-progress` (suppressing progress while still printing the creation summary); `--env` on `sbx secret ls` / `sbx secret rm` becomes `--env-name`; `--yes` / `-y` on `sbx logout` becomes `--force` / `-f`; `--auto-approve` / `-y` on `sbx env plan`, `sbx env create`, and `sbx env run` becomes `--force` / `-f`; `-d` on `sbx template save` becomes `--description`; and `--quiet` / `-q` on `sbx policy log` is removed with no replacement.

— Every renamed flag and its command named, but no combined example. v0.48.0

---

04 **Managed SSH setup for Codex and Claude Desktop** NEW

75

`sbx setup ssh --auto-create` on macOS and Windows registers Docker Sandbox connections in Codex and Claude Desktop, creating a dedicated sandbox on first use.

Register a dedicated Codex and Claude Desktop sandbox on macOS or Windows so AI coding agents connect via SSH without a host workspace mounted.

```
$ sbx setup ssh --auto-create
```

— Exact command, platforms, and behaviour given with a runnable example. v0.48.0

---

05 **MCP server unload without agent restart** NEW

75

`sbx mcp unload NAME --sandbox SANDBOX` detaches a loaded MCP server from a running sandbox without restarting the sandbox's agent.

Detach a loaded MCP server from a running sandbox without restarting its agent — useful when swapping MCP configurations mid-session.

```
$ sbx mcp unload my-server --sandbox my-sandbox
```

— Exact subcommand and flags with a runnable example. v0.48.0

06 **V3 kit capabilities and startup commands** NEW 75

`sbx kit add` now supports kits with startup commands that run after the kit is added and on each subsequent sandbox start. V3 kits add support for capability groups, `kit.env` references, bundled agent skills, and the `ssh-agent@1` and `git-identity@1` capabilities. `sbx kit validate` now rejects kits whose credentials route the same host, identifying the conflicting services.

— Names every kit surface and mechanism but gives no runnable example. v0.48.0

07 **Cloud always-on timeout control extended** IMPROVED 60

`--ttl` and `--on-timeout restart` are now supported on `sbx move --to cloud` and `sbx --cloud env create`, extending always-on timeout control beyond the existing `sbx --cloud create` support.

— Named flags and commands but no usage example given. v0.48.0

08 **Non-interactive and confirmation behavior changes** BREAKING 60

Confirmation prompts now require terminal input — piping an answer (e.g. `echo y | sbx secret set ...`) no longer confirms; use `--force` / `-f` instead. Declining a confirmation now returns a non-zero exit status consistently for removal, reset, and prune operations. Read-only invocations and runs with `--force` no longer start an interactive sign-in flow, so authentication must be completed before running automation. Without a terminal, `sbx diagnose --upload` saves the diagnostic bundle but skips uploading and exits 0, and `sbx create` / `sbx run` fail if the workspace directory does not exist (printing a `mkdir -p` hint). Ctrl-D at a selection or free-text prompt now cancels instead of accepting the default.

— Describes several behavior changes with commands named but no single example. v0.48.0

THINNER COVERAGE BELOW

09 **SBX_AGENT environment variable in sandboxes** NEW 50

A new `SBX_AGENT` environment variable is exposed inside sandbox containers, surfacing the provisioned agent's name for use by kit hooks and scripts.

— Names the variable and purpose but no example of use. v0.48.0

10 **SSH-agent forwarding for Windows OpenSSH and 1Password** IMPROVED 40

SSH-agent forwarding now supports Windows OpenSSH and 1Password agents when `SSH_AUTH_SOCK` is not set.

— Names the agents and env var but no setup steps. v0.48.0

---

11 **Sandbox-scoped secret overrides** IMPROVED 35

Sandbox-scoped custom secrets can now override global secrets that share the same environment variable name.

— States the behaviour but no mechanism, flag, or example. v0.48.0

└──▷ **BREAKING ON UPGRADE**

! `--detached` on `sbx run` and `sbx env run` is rejected; replace with `--detach` or `-d`.

! `--yes` / `-y` on `sbx logout` is rejected; replace with `--force` or `-f`.

! `--auto-approve` / `-y` on `sbx env plan`, `sbx env create`, and `sbx env run` is rejected; replace with `--force` or `-f`.

! `--quiet` / `-q` on `sbx create` is rejected; replace with `--no-progress`.

! `-d` (short for description) on `sbx template save` is rejected; replace with `--description`.

! `--output` / `-o` on `sbx diagnose` is rejected; replace with `--format table`, `--format json`, `--format yaml`, or `--format github-issue`.

! `--env` on `sbx secret ls` and `sbx secret rm` is rejected; replace with `--env-name`.

! `--quiet` / `-q` on `sbx policy log` is removed with no replacement.

! `--format`, `--json`, and `-q` are mutually exclusive; even `--json --format json` is rejected.

! Unsupported `--format` values now fail at flag-parse time instead of falling back to human-readable output.

! `sbx ls --json` output changes: the top-level object `{"sandboxes": [...]}` is replaced by a bare array; update filters from `.sandboxes[].name` to `.[].name`. Fields are now `snake_case`, `created_at` and `last_used_at` use RFC 3339 timestamps, and rows include `detached`.

! `sbx template ls --json` output changes: top-level `{"images": [...]}` is replaced by a bare array for local and cloud sandboxes.

! `sbx mcp ls --json` locally: top-level `{"gateway": {...}, "servers": [...]}` is replaced by a bare server array; each row carries `gateway`.

! `sbx policy log` output changes: local `allowed_hosts` / `blocked_hosts` and cloud camelCase fields are replaced by `{updated_at, allowed: [...], blocked: [...]}` with entries containing `sandbox_id`, `host`, `proxy_type`, `rule`, `reason`, `count`, `first_seen`, and `last_seen`.

! `sbx --cloud policy ls` field names change from camelCase to `snake_case`.

! `sbx ports` cloud rows rename `port` to `sandbox_port`; local rows use `host_ip`, `host_port`, `sandbox_port`, and `protocol`.

! `sbx ports --publish` / `--unpublish` locally: structured formats now emit result rows with `action: published` or `action: unpublished`; warnings go to stderr.

! Cloud `volume create`, `volume ls`, and `volume inspect` field names change from PascalCase (`ID`, `Name`, `CreatedAt`) to `snake_case` (`id`, `name`, `created_at`). `volume inspect` now defaults to a human-readable details view; use `--format json` for JSON.

! `sbx rm`, `sbx stop`, `sbx template rm`, `sbx volume rm` structured output now returns an array of result objects with `action`, `resource`, `name`, and optional `id` and `error`; actions are lowercase strings.

! Confirmation prompts require terminal input; piping an answer (e.g. `echo y | sbx secret set ...`) no longer confirms the operation — use `--force` / `-f` instead.

! Declining a confirmation now returns a non-zero exit status consistently for removal, reset, and prune operations.

! Read-only invocations and runs with `--force` no longer start an interactive sign-in flow; authentication must be completed before running automation.

! Without a terminal, `sbx diagnose --upload` saves the diagnostic bundle but skips uploading and exits with status 0 — a zero exit no longer guarantees an upload occurred.

! Without a terminal, `sbx create` and `sbx run` fail if the workspace directory does not exist (a `mkdir -p` hint is printed).

! Ctrl-D at a selection or free-text prompt now cancels instead of accepting the default.

---

WAS THIS USEFUL? 👍 👎

## NoLabs nono

Feedback ⓘ v0.80.0 NOTES ↗ CODE ↗ RANK

The nono runtime runs AI agents in isolated environments with policy-controlled filesystem, network, and credential access.

> nono v0.80.0 strengthens its command-policy sandbox with executable-digest pinning, per-command AWS credential signing, and macOS keychain access grants.

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

01 **SHA-256 executable pinning for commands** NEW 86

Adds a `sha256` field to `CommandPolicyConfig` in the command-policy config to pin a command to its expected SHA-256 executable digest, blocking substituted or tampered binaries. A policy can specify both `executable` path and `sha256` digest, e.g. pinning `gh` to `/usr/local/bin/gh` with a specific hash.

Pin a sandboxed tool to its exact binary so a supply-chain swap or path-hijack is caught before execution.

json

```
{
  "command_policies": {
    "commands": {
      "gh": {
        "executable": "/usr/local/bin/gh",
        "sha256":
"e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
"
      }
    }
  }
}
```

— Names exact config field and shows runnable example v0.80.0

02 **Per-command AWS SigV4 auth in sandbox** NEW 77

Adds `aws_auth` field (type `AwsAuthConfig`) to `CommandCredentialConfig` in the command-policy config, enabling per-command AWS SigV4 signing in tool-sandbox scoped-proxy routes. The child process sees only dummy keys while real credentials are resolved host-side.

— Names config field and mechanism, no runnable example v0.80.0

03 **macOS keychain_access grant for commands** NEW 62

Adds a command-level `keychain_access` grant for macOS, letting profiles permit a specific sandboxed command to access the macOS Keychain without widening the entire session sandbox.

— Names the grant and scope, lacks config example v0.80.0

---

WAS THIS USEFUL? 👍 👎

## Backslash

Feedback ⓘ

Claude Code mods: What they are, and what you should be aware of - Backslash (2026-10-12)

BLOG ↗ RANK

Backslash detects and prioritizes reachable vulnerabilities in cloud-native application code and dependencies.

> Backslash published guidance on Claude Code agent mod risks and highlighted its single-pane visibility into installed agent plugins, MCP servers, skills, and hooks across developer endpoints.

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

01 **Visibility into Claude Code plugins, MCP servers, and hooks**

NEW 55

Backslash provides a single-pane view across developer endpoints showing every installed agent plugin, MCP server, skill, and hook — including those that auto-load from `~/.claude/skills/` with no install step — alongside what each can reach and which carry risk.

— States capability and scope but no UI path, limits, or mechanism detail.

Claude Code mods: What they are, and wh…

└──▷ **ALSO FROM THESE RELEASES**

Inspect a mod before installing it to see which events it hooks and which Claude Code functions it calls.

```
$ claude plugin validate ./my-mod-folder
```

Lock a managed team environment so only company-approved mods can run — preventing unknown third-party mods from loading.

```yaml
allowManagedModsOnly: true
```

List all installed plugins (including auto-loading ones in ~/.claude/skills/) to audit what is active in the current environment.

```
$ claude plugin list
```

WAS THIS USEFUL? 👍 👎

## INFRASTRUCTURE

◆ Internet Services

# Cloudflare

Feedback ⓘ

Workers, BYOIP, Bots - Workers subrequests now preserve context for BYOIP destinations (

BLOG ↗ RANK

Cloudflare is a connectivity cloud platform delivering internet security, performance, and developer infrastructure services.

> Cloudflare shipped persistent browser sessions for the Agents SDK, real-time MCP event streaming for Workers Issues, sub-part RUM metrics for Core Web Vitals, and fixed Workers subrequests to BYOIP destinations so Bot Management evaluates the original client connection.

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

01 **BYOIP subrequest context preserved for Bot Management**

IMPROVED 85

Workers subrequests to Cloudflare-proxied BYOIP destinations now preserve the `CF-Worker` header and `cf.worker.upstream_zone` field, ensuring consistent security rule evaluation across same-zone and cross-zone subrequests. Bot Management fields on destination zones — including bot scores, verified bot status, and JA3/JA4 fingerprints — now reflect the original end-user connection rather than the internal Cloudflare-to-Cloudflare connection.

— Names exact header, field, and fingerprint types affected

Workers, BYOIP, Bots - Workers subreque…

02 **Persistent browser sessions in Agents SDK** NEW 60

Adds `browserTool` to the Agents SDK — a persistent browser that retains tabs and logins between turns, with adapters for Pi Durable, AI SDK, and TanStack AI.

— Names the SDK tool and adapters, no usage example given product docs

03 **Sub-part RUM metrics for LCP, INP, and connection time**

IMPROVED 60

Real User Monitoring in Cloudflare Web Analytics now breaks LCP and INP into sub-part metrics and splits connection time into TCP and TLS, surfaced in the dashboard and via the GraphQL Analytics API.

— Names metrics and API surface, screenshots show dashboard view product docs

THINNER COVERAGE BELOW

04 **MCP event streaming for Workers Issues** NEW 50

The Cloudflare API MCP server now streams Workers Issues as MCP events, enabling MCP clients to subscribe and receive each new issue in real time.

— Describes mechanism but no endpoint or event schema named `product docs`

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

The Cyber Toolchain · curated daily · October 13, 2026
Releases & features from the open-source and commercial cyber tools that practitioners actually run.

▷ Subscribe | Feedback on this issue