

Top User Complaints and Gaps in the Cisco Duo Admin API

Background

The Cisco Duo Admin API (`/admin/v1`, `/admin/v2`, `/admin/v3` handlers, hosted at api-XXXXXXXX.duosecurity.com) provides programmatic CRUD access to users, phones, hardware tokens, admins, integrations/applications, policies, groups, and read access to authentication / administrator / telephony logs. It is bundled with Duo Essentials, Advantage, and Premier plans, uses HMAC-SHA1 signed Basic-Auth requests, and has official SDKs for Python, Java, Go, Node, Ruby, Perl, PHP and C#. Despite that surface area, recurring developer complaints across Cisco Community, the Duo Security Community, GitHub, Splunk/Sophos/Liongard partner docs, and Duo's own help-center cluster around a small set of structural issues that have persisted for years. [Duo Security Duo Security](#)

A Note on Sources

This report is built primarily from the **Cisco Community forums** (community.cisco.com, community.duo.com), **Duo's own documentation and KB articles** (duo.com/docs/*, help.duo.com), **GitHub issues** filed against the official `duo_client_python` SDK, the **Splunk answers community**, and **third-party integration vendor docs** (Sophos, Liongard, Edge Delta, Flexera, LogRhythm, Forcepoint) that publicly document Duo API workarounds. Direct hits on **Reddit (r/sysadmin, r/Cisco, r/networking)** and **Stack Overflow** were not retrievable within the research budget for this report; however, the Cisco/Duo community forums and GitHub repositories appear to be the primary venues where Duo Admin API users actually file complaints (Reddit Duo-API threads tend to redirect users back to these forums). Where I could not corroborate a Reddit/Stack Overflow source, I have relied on multiple corroborating sources from the venues above.

Executive Summary

While Duo has steadily expanded the API — most notably adding **Bulk Create Users** and a **Policy CRUD** endpoint set in 2023, plus higher-frequency directory sync in the D303 release — the recurring complaints are: **opaque/aggressive rate limiting (HTTP 429)**, **index-based pagination with race conditions**, **no bulk write endpoints beyond user creation**, **missing endpoints for several Admin Panel features (especially SSO/IdP configuration, full directory-sync trigger, parts of Trust Monitor)**, **official SDKs that lag the documented REST surface**, **weak documentation around request signing and v2 auth-log paging**, **fragile MSP/Accounts-API multi-tenant flows**, **hard object caps that return misleading HTTP 500s**, and **ongoing v1→v2→v3 migration churn**. Most of these are explicitly acknowledged in Duo's own documentation.

Top 10 Gaps & Limitations (Ranked by Frequency, then Recency)

1. Aggressive / opaque rate limiting (HTTP 429) far below documented thresholds — *very frequent, ongoing 2018–2026*

By far the most frequently raised complaint across every channel:

- A 2025 Cisco Community thread, "**Why Is My Duo Admin API Rate Limit Being Hit Despite Low Traffic?**", describes 30–50 calls/hour triggering 429s despite the documented 100/min limit. A respondent notes that Duo enforces additional silent per-key and per-IP throttling and recommends *"max 2/sec even if under 100/min"* and 500 ms pacing between sequential calls (community.cisco.com/t5/apis/why-is-my-duo-admin-api-rate-limit-being-hit-despite-low-traffic/td-p/5311520). [Cisco Community](#)
- GitHub issue **#240** in [duosecurity/duo_client_python](#) (Oct 2023, still open) — *"Received 429 Too Many Requests for auth logs even hitting the API in 6-7 minute intervals"* using the official client (github.com/duosecurity/duo_client_python/issues/240). [github](#)
- GitHub issue **#101** — *"What Causes 429 Too Many Requests Error?"* — and notes the Python package has no built-in retry method; the docs don't enumerate concrete per-endpoint limits (github.com/duosecurity/duo_client_python/issues/101). [GitHub](#)
- GitHub issue **#154** (Dec 2021, still open, filed by a Duo employee) — request to *"Increase `_MAX_BACKOFF_WAIT_SECS` seconds"* because the default backoff in the SDK is insufficient to recover from real-world 429 storms (github.com/duosecurity/duo_client_python/issues/154). [github](#)
- Sophos Central docs acknowledge the cross-integration interference problem: *"We have a 1 minute delay between paginated calls, but we've seen in the past that some customers used Duo credentials with other services (e.g., Splunk), and these services were 'stealing' the rate limit allowance"* (docs.sophos.com/central/customer/help/en-us/ManageYourProducts/ThreatAnalysisCenter/Integrations/Cisco/Duo/index.html). [Sophos](#)
- Duo's official **Rate Limits** doc admits three layered mechanisms (Per IP, Per AKEY+IP, Per AKEY) evaluated independently, but does **not** publish concrete numeric limits per Admin API endpoint — which is the root cause of the complaints (duo.com/docs/rate-limits). [Duo Security](#)

Impact: Multiple integrations sharing one tenant silently exhaust the global quota with no per-key visibility. Duo's de facto guidance (per the Sophos and Cisco threads) is *"create one API key per integration and add backoff."*

2. Pagination is index-based and prone to race conditions / missed or duplicated records — *frequent, ongoing since 2019*

- Duo Security Community thread "**Pagination bug in admin api?**" (community.duo.com/t/pagination-bug-in-admin-api/4242) explicitly describes the design flaw: *"When paging in the API, since things are index based, there are race conditions where records can be omitted or sent twice (if deletes or inserts happen while retrieving all)."* This is structural and unresolved. [Duo](#)
 - Splunk Community thread "**DUO API will enforce pagination on admin related A...**" documents Duo's 2019 forced migration to mandatory pagination, which broke many integrations including the official Splunk Add-on (answers.splunk.com/answers/717311/duo-api-will-enforce-pagination-on-admin-related-a.html). [Splunk](#)
 - Duo Help Center article "**Extending pagination capabilities in Duo Admin API**" (help.duo.com/s/article/4744) is Duo's own acknowledgment that customer integrations had to be reworked.
 - The Authentication Log v2 endpoint uses a *different* pagination scheme — a two-value `next_offset` of [`timestamp`, `txid`] — than every other endpoint, and the documentation incorrectly listed "allow multiple = No." Community thread "**Duo Admin API - admin/v2/logs/authentication**" (community.duo.com/t/duo-admin-api-admin-v2-logs-authentication/3836) — OP: *"The documentation around how to format the next_offset for this request is not detailed enough and there are no examples ... I would suggest reviewing this documentation for accuracy and adding a sample request."* [DuoDuo](#)
 - GitHub issue **#265** (Apr 2024, open) — *"next_offset pagination in auth logs"* — still actively confusing developers (github.com/duosecurity/duo_client_python/issues/265).
 - The legacy v1 groups endpoint **truncates results at the first 4,000 group members**, with no further paging — documented in duo.com/docs/adminapi-v1. Customers with large groups are forced onto v2. [Duo Security](#)
-

3. Lack of true bulk write operations (delete users, modify status, manage groups/devices, assign policies) — *frequent*

- The **only** documented bulk endpoint is **Bulk Create Users** (max 100 users/request at 50 calls/min) — recently added (duo.com/docs/adminapi). There is **no** bulk delete, bulk status change (active/disable/bypass), bulk group membership change, bulk phone delete, bulk token assignment, or bulk policy assignment. [Duo SecurityDuo Security](#)
- Bulk Create has the awkward "fail-the-batch" behavior: *"If one user fails to add, the entire operation fails"* — no per-row atomicity. [Duo SecurityDuo Security](#)
- Duo's own blog post "**Extended Policy Capabilities in Duo's API**" (May 2023) admits this gap on the roadmap: *"CRUD is only the beginning ... Our next step is to enhance applying policy via our API by enabling the ability to bulk apply policies, which will help further eliminate the manual labor of applying policies for multiple"*

groups or to multiple applications"

(duo.com/blog/extended-policy-capabilities-in-duo-api). As of mid-2026 the bulk-apply policy feature has not been confirmed shipped in the API docs. [Duo Security](#)

- Help Center articles **#2268** ("How do I permanently delete Duo users in bulk...") and **#2269** ("How do I immediately remove Duo users with Pending...") exist *because* customers must script per-user delete loops.
- A particularly dangerous behavioral gap: *"Users deleted by the API do not get moved into the Trash view as 'Pending Deletion' as they would if removed by directory sync, user deletion, or interactively from the Duo Admin Panel, and therefore are not available for restoration. Users deleted via the API are immediately and permanently removed from Duo"* (duo.com/docs/adminapi). The Admin Panel has soft-delete; the Admin API does not. [Duo Security](#)

4. Many Admin Panel features have no Admin API equivalent — *frequent, longstanding*

Items repeatedly cited as UI-only or only partially supported via the API:

- **SSO / SAML / OIDC application configuration:** The v1 modify-integration endpoint explicitly states *"This v1 API endpoint cannot modify Duo Single Sign-On applications"* (duo.com/docs/adminapi-v1). Configuring SSO sources, attribute mappings, claims, and authentication sources still requires the Admin Panel. [Duo Security](#)
- **Full directory sync trigger / scheduling:** The Cisco/Duo Community thread **"Directory Sync custom schedule"** (community.duo.com/t/directory-sync-custom-schedule/1648) has years of comments. One quote: *"I can't believe that this is still an outstanding issue for a security product. Every publicly traded company that is integrating into their directory is going to need this feature to be able to handle SOX audits."* The community workaround uses `/admin/v1/users/directorysync/[directory_key]/syncuser` in a loop — i.e., one user at a time. Duo only recently added "high-frequency automatic" sync in the D303 release; a true on-demand "Sync Now" API call for the whole directory remains absent. Duo's own KB article **#2224** is essentially a feature-request tracking page. [Duo + 3](#)
- **Trust Monitor risk events:** GitHub issue **#304** (Sep 2025, open) — *"Duo Trust monitor event accessibility 403 issue"* (github.com/duosecurity/duo_client_python/issues/304). The Trust Monitor surface is incomplete in the SDK and 403s are common.
- **Auth-summary / dashboard analytics endpoint:** GitHub issue **#268** (Jun 2024, open, tagged "good first issue") — *"add get auth summary endpoint to the admin object"* — the REST endpoint exists but the Python client doesn't expose it (github.com/duosecurity/duo_client_python/issues/268).
- **Universal Prompt / passport management:** only added to the Python client in **v5.5.0 (Mar 2026)**: *"Add 'supported browser' options to passport management api"*

method" (github.com/duosecurity/duo_client_python/releases). Customers on older clients hand-roll requests. [GitHub](#)

- **Filtering bypass / service accounts out of auth logs:** A Cisco Community post asks *"I have a service account set to bypass, and I'm not interested in its logs. Is there a way to exclude this account from the Authentication Logs when retrieving them via the Admin API?"* — no such filter parameter exists (community.cisco.com/t5/apis/bd-p/disc-duo-api). [Cisco Community](#)
-

5. Documentation quality — especially HMAC signing examples, PowerShell support, and v2/v3 examples — *very frequent complaint*

- Cisco Community thread **"Using Powershell to Access the Duo Admin API"** (community.duo.com/t/using-powershell-to-access-the-duo-admin-api/6941): *"The documentation is horrid and I don't want to go through the hassle of the module I found on GitHub ... I agree that the documentation is lacking."* There is no official PowerShell SDK. [Duo](#)
 - Cisco Community thread **"I can not replicate the basic auth header that the example shows"** (community.duo.com/t/i-can-not-replicate-the-basic-auth-header-that-the-example-shows/3223): *"This is very frustrating game of trial and error."* [Duo](#)
 - Cisco Community thread **"Authorization signature for API requests"** (community.duo.com/t/authorization-signature-for-api-requests/3877) — HTTP 401 / 40103 "Invalid signature" from literally following the docs. [Duo](#)
 - GitHub issue **#246** (Dec 2023) — *"Getting 40103 on making GET REST API calls"*: user followed the published doc verbatim but only the SDK worked; the canonical-string instructions are ambiguous about ports, certificates, and header ordering (github.com/duosecurity/duo_client_python/issues/246). [GitHub](#)
 - Cisco Community thread **"Create user using admin api"** (community.duo.com/t/create-user-using-admin-api/2931): *"I've poured through that documentation, but it doesn't give any examples of an http post."* [Duo](#)
-

6. Official SDKs (Python, Java, Go, etc.) lag the REST surface — *frequent, ongoing*

The [duosecurity/duo_client_python](https://github.com/duosecurity/duo_client_python) repo has ~149 stars and **11+ open issues** as of late 2025/2026. The Java SDK is on version 0.8.0 with similar coverage gaps:

- Issue **#303** (Jul 2025, open) — *"Not Working with Admin API v3 Endpoints"* (github.com/duosecurity/duo_client_python/issues/303). [GitHub](#)
- Issue **#254** (Feb 2024) — `get_secret_key` was documented in REST but absent from the Python SDK; only added after a community PR (github.com/duosecurity/duo_client_python/issues/254). [GitHub](#)
- Issue **#268** (Jun 2024) — auth-summary endpoint missing from the SDK.

- Issue **#222** (May 2023, open) — "Automatic proxy configuration" feature request. [github](#)
 - Issue **#153** (Dec 2021, open) — `auth_logs` request uses GET but doesn't check URI length limits, leading to silent failures on large parameter sets. [github](#)
 - Issue **#111** (Jul 2020, open) — `client.py` doesn't wrap underlying httplib exceptions; consumers see raw `BadStatusLine` and can't catch a defined exception type. [GitHub](#)
 - Issue **#178** (Aug 2022, open) — "Deprecated SSL protocol in `CertValidatingHTTPSConnection`". [github](#)
 - Issue **#155** (Dec 2021, open) — "Querying Authlog with a maxtime of > now-2 minutes may lead to inconsistent behavior" — i.e., the auth log has an undocumented ~2-minute consistency window. [github](#)
 - Issue **#46** — "Authenticated Proxies Support" — Duo's HTTPS connection helper historically didn't tunnel through authenticated corporate proxies (github.com/duosecurity/duo_client_python/issues/46). [GitHub](#)
 - The Java SDK (github.com/duosecurity/duo_client_java, v0.8.0) explicitly notes Accounts API "is not available with all Duo accounts" and has limited feature parity with the Python client. [GitHub](#)
-

7. MSP / Accounts API integration with Admin API is fragile (cross-deployment errors, no cross-tenant queries) — frequent for MSPs, ongoing

- Liongard's support article "**Duo Security | Error 400, Cross-deployment Admin API usage is not available**" documents a recurring HTTP 400 "Cross-deployment Admin API usage not available" for MSPs whose child tenants are in a different Duo deployment than the parent. The only fix is to file a Duo Support ticket to manually migrate the tenant on the backend (support.liongard.com/en/articles/8869100). Duo's docs confirm: "Cross-deployment Admin API usage through Accounts API is currently not available" (duo.com/docs/accountsapi). [LiongardLiongard](#)
- Cisco/Duo Community thread "**Duo Admin API - Groups/Tenants**" (community.duo.com/t/duo-admin-api-groups-tenants/9917) asks: "is it possible to query all groups across all tenants without creating separate/individual API application keys for each tenant?" — the answer is no; iterate per child account. [Duo](#)
- Several Accounts-API-with-Admin-API methods (edition management, telephony credits) are **gated behind a manual Duo Support ticket**: "These Admin API methods are not yet generally available with Accounts API. Please contact Duo Support to request access" (duo.com/docs/accountsapi). [Duo Security](#)
- Cisco's own **Duo API Playground** Postman workspace, hosted on Cisco Code Exchange (developer.cisco.com/codeexchange/github/repo/it-jonjon/Duo-API-Playground/), is explicitly "AS IS ... not officially supported by Cisco or Duo". Cisco felt the need to ship this community-maintained collection because the bare API is too cumbersome for routine MSP tasks like "retrieving bypassed users across child accounts." [ForcepointForcepoint](#)

8. Missing or limited filtering on log endpoints; latency windows; restricted retention — *frequent*

- The Authentication Log v2 endpoint has **no parameter to filter by `account_id`** (raised in community.duo.com/t/duo-admin-api-admin-v2-logs-authentication/3836), forcing MSPs to filter client-side after retrieval.
- No parameter to **exclude bypass or service accounts** from log queries (community.cisco.com/t5/apis/bd-p/disc-duo-api).
- The auth log has an undocumented ~2-minute eventual-consistency window (GitHub issue [#155](#)); querying very recent events returns inconsistent results.
- Third-party documentation indirectly acknowledges this. Edge Delta's integration guide (docs.edgedelta.com/http-pull-duo-admin-api/) and Sophos Central's guide both recommend specific intervals (5–10 minutes) and lookback windows (e.g., 360–720 seconds) precisely to work around log latency and rate-limit edge cases. [Edge Delta](#)

9. v1 endpoint deprecations and version fragmentation create migration churn — *recent, ongoing 2023–2026*

- Duo is in the middle of a multi-year v1→v2→v3 handler migration; some v1 endpoints have announced deprecation dates and *"will be limited or deprecated in the future"* (duo.com/docs/adminapi, duo.com/docs/adminapi-v1). [Duo Security + 2](#)
- Endpoints have inconsistent pagination semantics across versions (v2 auth logs use a 2-tuple `next_offset`; everything else uses an integer offset).
- A Cisco/Duo Community post on the APIs board reports: *"We are trying to figure out why calling `/admin/v1/integrations` via the official Golang API client works, but `/admin/v2/integrations` does not. Unfortunately, Duo support staff are struggling to help"* (community.cisco.com/t5/apis/bd-p/disc-duo-api). The official Go client lags v2 endpoints. [Cisco Community](#)
- GitHub issue [#303](#) (Jul 2025, open) — Python client *"Not Working with Admin API v3 Endpoints."*
- **CA bundle expiration on April 15, 2026:** A banner on the official Admin API docs warns *"Legacy clients could stop working at any time after April 15, 2026."* Multiple Python client releases in late 2025/early 2026 (5.4.x, 5.5.0) exist solely to *"Add support for new Duo certificate authorities"* (github.com/duosecurity/duo_client_python/releases). Customers on older SDKs face a hard-cutoff client-update burden. [Duo SecurityGitHub](#)

10. Hard object-count caps that surface as misleading "500 Internal Server Error" — *frequent, longstanding*

- Duo's own Rate Limits doc (duo.com/docs/rate-limits) admits that exceeding any of the one-to-many caps via the Admin API returns *"500 Internal Server Error – Unknown internal server error"* — not a proper 4xx validation error. The Admin Panel UI returns clear messages ("Cannot use phone for more than 100 users") while the API returns a generic 500. The documented caps include 100 phones/user, 100 users/phone, 100 groups/user, 100 OTP tokens/user, 100 U2F tokens/user, 100 WebAuthn credentials/user, 100 bypass codes/user, 100 groups per app, and 400 groups per LDAP/Azure directory sync. [Duo Security](#)[Duo Security](#)
- This is one of the more striking on-record acknowledgments that the API violates REST best practice; it is a frequent reason support tickets are misdiagnosed.

Recent (2023–2026) vs. Longstanding Issues

Issue	Era	Status
Pagination race conditions in indexed paging	2019–present	Longstanding, unresolved
Aggressive 429s well below documented limits	2019–present, fresh 2025 thread	Longstanding, unresolved
v1→v2/v3 migration churn; v2/v3 endpoint gaps in SDKs	2023–2026	Active migration
Policy CRUD endpoints via API	Added May 2023 — was a top complaint	Resolved (bulk-apply still pending)
Bulk Create Users endpoint	Added recently (100/req, 50 calls/min)	Partial — only create; no bulk delete/modify
Trust Monitor API gaps (Issue #304)	Sep 2025	Open

Admin API v3 not working in Python SDK (Issue #303)	Jul 2025	Open
Cross-deployment Accounts/Admin API failures	Ongoing through 2024 (Liongard article)	Workaround = support ticket
Directory Sync full trigger via API	Years of requests; partial fix in D303 release	Partial — full sync still UI/scheduler only
CA bundle rotation forcing client updates	2025–April 2026	Action required
SSO application config via API	Longstanding	Still missing for v1 modify-integration
Get-integration-secret-key in Python SDK	Feb 2024, community PR merged	Resolved in SDK
Universal Prompt / passport support in SDK	Added v5.5.0 (Mar 2026)	Recently resolved
Higher-frequency directory sync	D303 release	Recently resolved (partial)

Official Cisco/Duo Documentation Acknowledging Limitations

These are the explicit, on-record admissions in Duo's own documentation:

1. **duo.com/docs/rate-limits** — admits the API returns generic 500s when one-to-many caps are violated; admits multi-layer (Per IP / Per AKEY+IP / Per AKEY) silent throttling without publishing concrete per-endpoint numeric limits.

2. **duo.com/docs/adminapi-v1** — admits the v1 groups endpoint truncates at 4,000 members; admits v1 modify-integration cannot modify Duo SSO applications and returns secret keys in plain text; warns *"There is no way to restore an integration deleted in error with Admin API."* [Duo Security](#)
 3. **duo.com/docs/adminapi** — admits API-deleted users skip the Trash and cannot be restored; admits the Bulk Create endpoint fails entirely if even one user is invalid; admits v1/v2 handlers will be limited or deprecated in the future.
 4. **duo.com/docs/accountsapi** — admits *"Cross-deployment Admin API usage through Accounts API is currently not available"* and that certain methods (edition management, telephony credits) require manual Duo Support enablement.
 5. **help.duo.com/s/article/4744** — *"Extending pagination capabilities in Duo Admin API"* — the paging-breakage notice.
 6. **help.duo.com/s/article/2224** — Duo's directory-sync-schedule feature-request tracking article (referenced from community.duo.com/t/directory-sync-custom-schedule/1648).
 7. **help.duo.com/s/article/2268** and **help.duo.com/s/article/2269** — workaround KB articles that exist precisely because there is no bulk delete endpoint.
 8. **help.duo.com/s/article/5774** — *"Can I create policies or manage Duo's policy engine via API?"* — itself reflective of the longstanding gap before Policy CRUD was added.
 9. **duo.com/blog/extended-policy-capabilities-in-duo-api** (May 2023) — admits that before this release, policy management was not available via API at all, and lists bulk-apply policy as a **future** roadmap item.
 10. **duo.com Admin API page banner (2026)** — Action Required: April 15, 2026 Duo CA Bundle Expiration; *"Legacy clients could stop working at any time after April 15, 2026"* (KB article 9451). [Duo Security + 2](#)
-

How the Community Works Around the Gaps

Across the threads surveyed, the common workarounds are:

- **One API key per integration**, rotated monthly, to isolate rate-limit allowances — recommended in community.cisco.com/t5/apis/why-is-my-duo-admin-api-rate-limit-being-hit-despite-low-traffic/td-p/5311520 and reflected in Sophos' integration design. [Cisco Community](#)
- **Hard-coded 500 ms request pacing + exponential backoff** even when below the documented 100/min limit.
- **Looping single-object endpoints** in scripts to approximate bulk delete/disable/sync operations.
- **Iterating the single-user directory-sync endpoint** to approximate an on-demand AD/Azure full sync.
- **Community Postman collections** (notably it-jonjon/Duo-API-Playground on Cisco Code Exchange, unsupported) to compensate for the lack of an official MSP-friendly toolkit.

- **Pulling logs with a 2-minute floor** on `maxtime` to avoid the undocumented consistency-window bug (Issue #155).
 - **Filing Duo Support tickets** to enable gated Accounts-API methods or to migrate child tenants between deployments.
 - **Hand-rolling HMAC signatures in PowerShell** because Duo ships no official PowerShell SDK; community PowerShell helper functions are widely shared (community.duo.com/t/using-powershell-to-access-the-duo-admin-api/6941). [Duo](#)
-

Bottom Line

The Duo Admin API is functional and steadily improving — Policy CRUD endpoints (2023), Bulk Create Users, the single-user directory-sync trigger, v3 handler rollouts, and Universal Prompt/passport SDK support (2024–2026) all addressed long-running pain points. But the **most-cited 2026 complaints remain familiar**: opaque rate limiting, brittle index-based pagination, missing endpoints for SSO/IdP configuration and several Admin Panel actions, lack of bulk write operations beyond user creation, documentation that lags the API itself (especially HMAC signing and v2 auth-log paging), SDKs that don't expose every documented REST capability, fragile MSP/Accounts API cross-deployment behavior, and hard object caps that masquerade as HTTP 500s. Duo's own documentation, KB articles, and blog posts explicitly acknowledge most of these gaps, which suggests they are known to the product team rather than disputed — they simply remain on the roadmap.