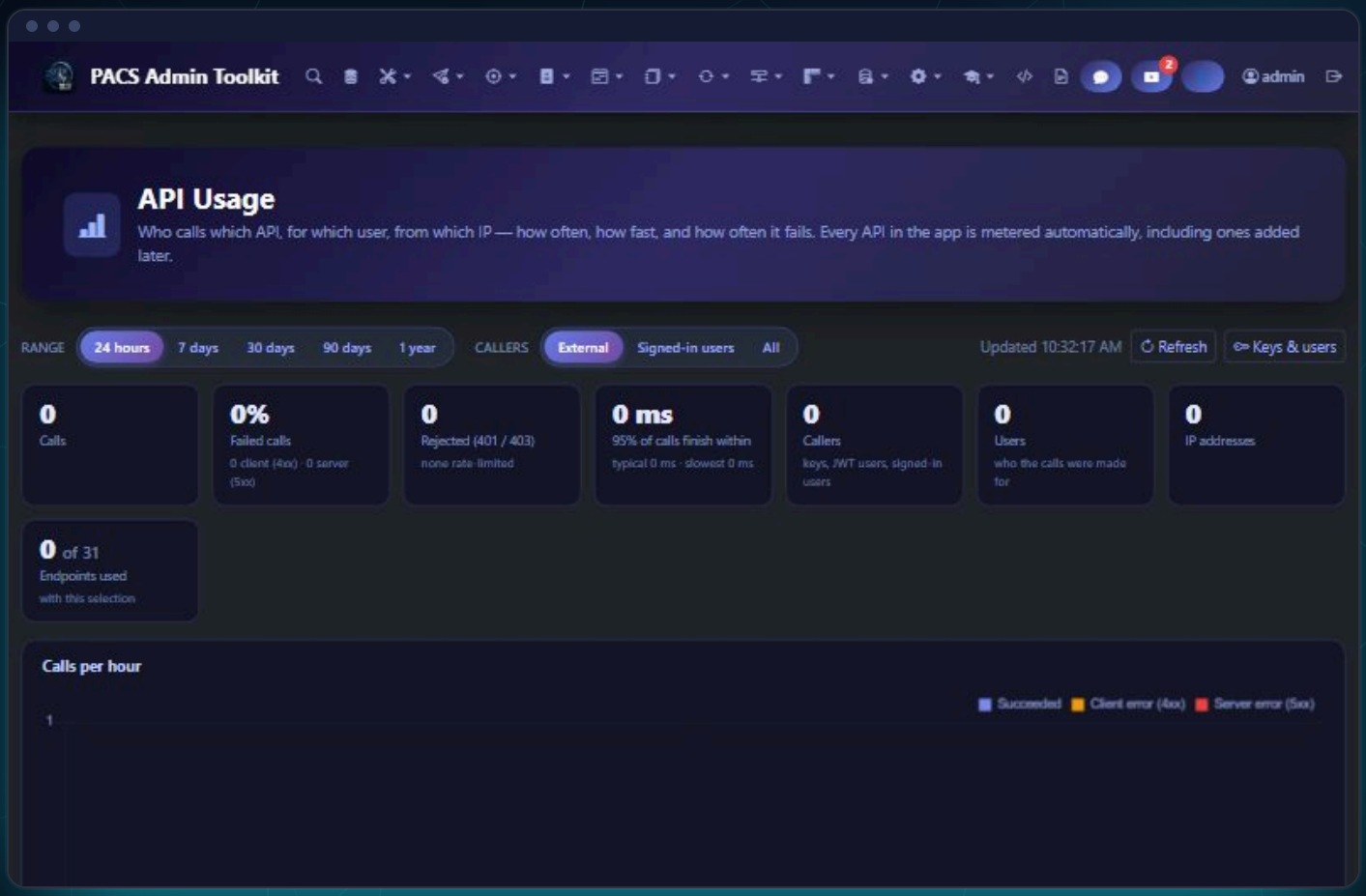
Platform & Integration | Leads with Trust

External API

Keys for every system that calls PATK, and a clear view of what each one actually does.



Application API keys and JWT API users let RIS, EHR, portals and scripts call PATK with their own credentials, roles and facility scope. API Usage meters every call by caller, user, endpoint and IP, and keeps the reason for every failure.

Every API
metered automatically, including ones added later

Shown once
each key's secret; only a hash is stored

30 days
of failure reasons kept for every failed call

Replaces: **API gateway or custom integration logging**

License module `API`

THE CHALLENGE

Why it matters

Every integration starts with a shared password in an email and ends with nobody sure which systems still use it. When an EHR launch or a portal call starts failing, the PACS team hears about it from users, then spends hours working out which caller, which endpoint and which error.

Most imaging tools leave API access to a single shared account and their logs to a text file. There is no way to say how much each system calls, from where, or for whom, and no way to limit an affiliate's system to its own data.

> IN SHORT
>
> Application API keys and JWT API users let RIS, EHR, portals and scripts call PATK with their own credentials, roles and facility scope. API Usage meters every call by caller, user, endpoint and IP, and keeps the reason for every failure.

CAPABILITIES

What it does

- **Application API keys**
  Each calling system gets its own key, sent in the X-Api-Key header; the secret is shown once and only a hash is stored.
- **JWT API users**
  Systems that prefer a login exchange a username and password for a bearer token valid for 8 hours.
- **Roles and scope per caller**
  Each key or JWT user carries its own roles, and can be limited to chosen facilities or sites wherever Access Topology is enforced.
- **Full key lifecycle**
  Optional expiry dates, disable, rotate (the old secret stops at once) and revoke, with the record kept for history.
- **Usage, metered automatically**
  Every API in the app is counted by caller, the user the call was made for, endpoint and IP, including APIs added in later versions.
- **Answers, not just counts**
  Tiles show calls, failed share, rejected calls, the 95th-percentile response time, callers, users and IPs; charts show calls over time and the busiest hours.
- **Why a call failed**
  Each failed call keeps a short reason for 30 days: the server exception, the key or token rejection, or the error text the API answered; values that look like secrets are masked.
- **"Worth a look" signals**
  The usage page points out patterns that need attention, and one click filters the whole page to an endpoint, caller, user or IP.
- **A reference for integrators**
  API Details documents sign-in and the available endpoints and can be saved as a PDF.

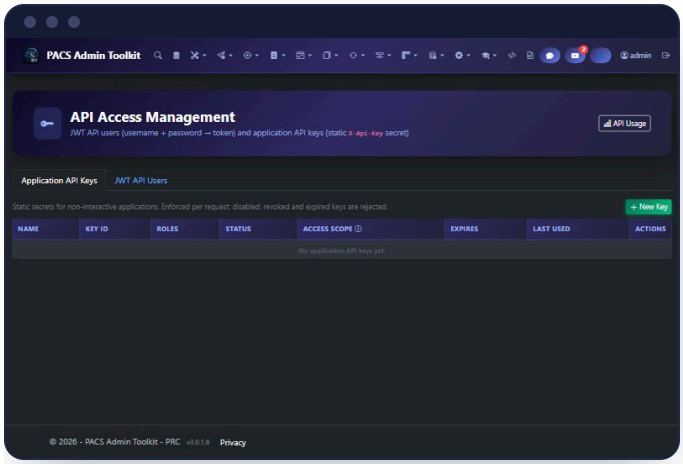
WORKFLOW

How it works

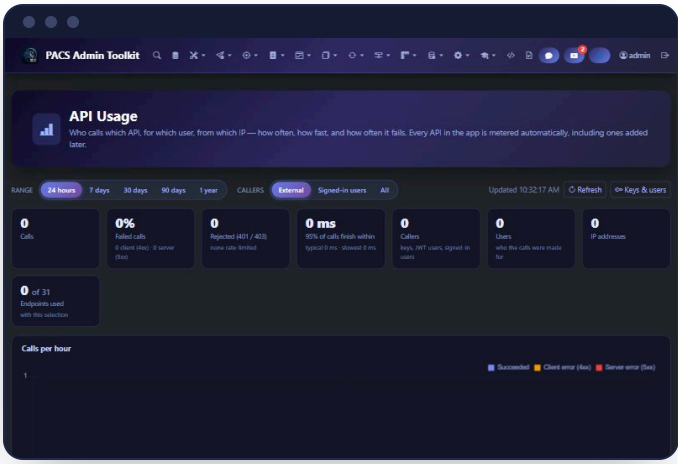
1. **Issue credentials**
   Create a key or JWT user for the calling system, with roles, expiry and scope.
2. **System calls**
   The RIS, EHR or portal sends its key or token with each request.
3. **Checked and scoped**
   PATK checks the credential and its roles, and limits records to its scope.
4. **Metered**
   Counts are written every 30 seconds and kept as hourly totals; failures keep their reason.
5. **Reviewed**
   API Usage shows who calls what, how fast and how often it fails.

IN THE PRODUCT

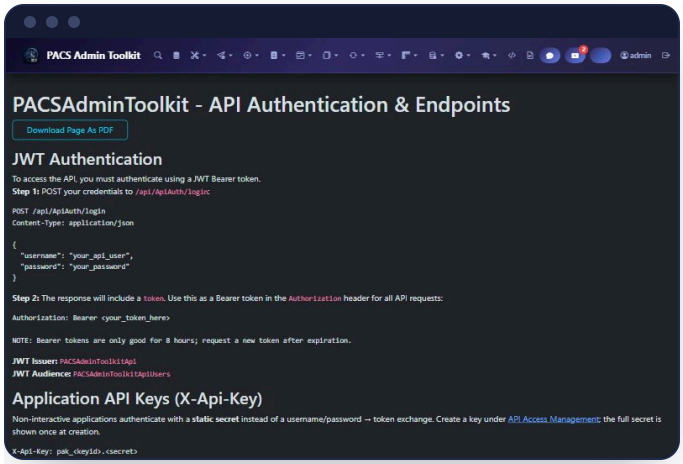
See it in action



API User Management: keys and JWT users with roles, expiry and scope



API Usage: calls, failures, response times and callers at a glance



API Details, the reference to hand to an integrator

USE CASES

Where it pays off

EHR context launch of prior studies

CHALLENGE	Clinicians open priors from the EHR, and the integration team needs its own credential that can be rotated without breaking other systems.
WITH PATK	The EHR gets an application key with the priors role (the launch itself needs the Priors Fetch toolset); API Usage shows its launches per day and any failures.
OUTCOME	**One credential per system, rotated on a schedule, with launch volume and errors visible instead of reported by users.**

Affiliate imaging centre portal

CHALLENGE	An affiliated imaging centre's portal calls PATK, but must only ever reach that centre's data.
WITH PATK	Its key gets scope rows for the centre's facility; wherever access is enforced, the key sees only those records.
OUTCOME	**The affiliate integrates directly, with no risk of reaching another facility's patients and an audit of everything it called.**

One metered entry point for a multi-site radiology group

CHALLENGE	A multi-site radiology group has several systems that need imaging functions, and didn't want each one wired separately to the PACS with its own credentials and no shared view of traffic.
WITH PATK	The group uses PATK's External API as a passthrough: each system calls PATK with its own key, and PATK handles the imaging side.
OUTCOME	**Every system's traffic shows up on one usage page, by caller and endpoint, and access can be changed or revoked per system without touching the others.**

"The integration stopped working"

CHALLENGE	A vendor reports intermittent failures after an upgrade on their side, and nobody can tell which calls fail.
WITH PATK	API Usage filtered to the vendor's caller shows the failed calls grouped by status and reason, the endpoint and the IP they came from.
OUTCOME	**The cause (an expired key, a validation error, a wrong endpoint) is clear in minutes and the conversation with the vendor starts with evidence.**

3T

Trust · Truth · Transform

Trust

Secrets are shown once and stored as hashes, each caller has its own roles and facility scope, rotation stops the old secret immediately, and API calls are audited.

Truth

See every caller, user, endpoint and IP, the failure rate and response times, and the exact reason each call failed over the last 30 days.

Transform

Integrations are issued, rotated and diagnosed from one page, instead of shared passwords, log-file searches and calls with the vendor.

VALUE MODEL

What it can be worth

An example department with four systems calling PATK (EHR, RIS, portal and scripts).

Systems calling PATK APIs	4
Integration incidents per year, hours saved on each with failure reasons by caller	24 x 2 hours (48)
Key onboarding and rotation tasks per year, hours saved on each	8 x 2 hours (16)
Monthly usage reports for governance or billing, hours saved on each	12 x 3 hours (36)
Blended integration and PACS administrator cost per hour	$65
Separate API metering or gateway subscription avoided per year	$10,000

$16,500

Estimated yearly value

Illustrative example. Your volumes, staffing and costs will differ; we will build this model with your own numbers.

DIFFERENTIATORS

Why it stands out

- **Metering is built in**
  Every endpoint is counted without configuration, where an add-on gateway or custom logging has to be set up per API.
- **Failures explained**
  The reason is kept with each failed call, so diagnosis does not depend on searching server log files.
- **Scoped to facilities**
  Keys follow the same facility and site model as people when Access Topology is licensed, rather than all-or-nothing access.
- **Part of the same platform**
  Keys, usage, audit and the APIs themselves live in one product with one support contract.

SPECIFICATIONS

At a glance

Credentials	Application API keys (X-Api-Key), JWT API users (bearer token, 8 hours)
Controls	Roles per caller, facility / site scope, expiry, disable, rotate, revoke
Usage	Calls, failed and rejected calls, 95th-percentile response time, callers, users, IPs, endpoints
Detail	Calls over time, busiest hours, endpoint / caller / user / IP tabs, recent errors with reasons (30 days)
Documentation	API Details reference, saveable as PDF
Licensing	API calls usage meter

See External API with your own data

Ask for a guided demo or a trial license. PACS Admin Toolkit installs on your own Windows server in under an hour, and every module comes with step-by-step guides and in-app guided tours.

sales@3tconsults.com | support@3tconsults.com | +1 (612) 564-9194 | www.3tconsults.com

Not a medical device. PACS Admin Toolkit is not FDA-cleared or CE-marked and is not intended for primary diagnosis. It manages imaging and reporting data and workflows around the clinical systems that do.

Other product and company names may be trademarks of their respective owners. Screenshots show sample data. Value models are illustrative estimates, not guarantees. © 2026 3T Consults and Coaching.