PROVEIT DATASHEET
by rubycat

VISA DE SÉCURITÉ
Ref. 05/2023 - Validity 06/2026

An IS security policy includes **traceability** and **control of control of privileged access**

Your IT equipment contains **sensitive data** or **applications** that need to be protected to ensure business continuity and the long-term future of your company, as well as **compliance with standards and regulations** (ISO 27007, GDPR, DORA, NIS 1 & 2 ...) and **ANSSI* recommendations**.

« Administrators are distinct from other users by the permissions and privileges they need to carry out the administrative actions that fall within the scope of their duties. »

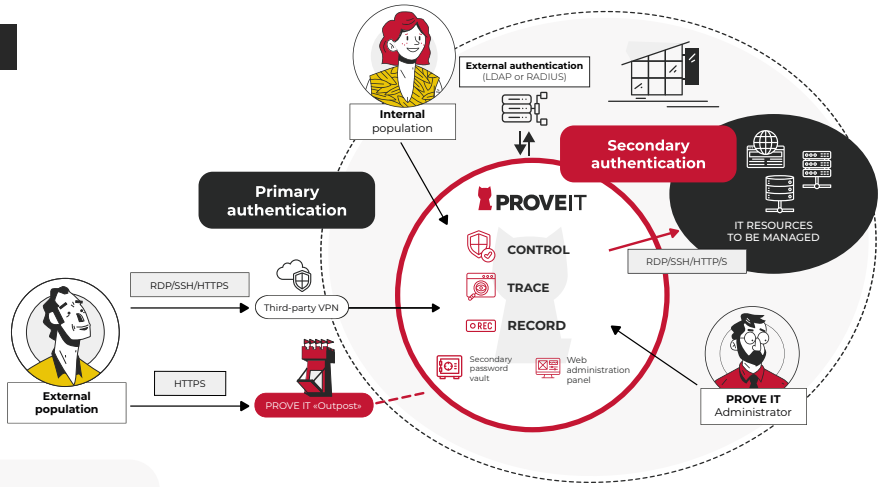
(see ANSSI Guide to secure administration of IS based on AD)

« Administration actions entail, among other things, traceability and confidentiality requirements. »

(see ANSSI Guide to secure IS administration: R25 & Chapter 13)

Topology diagram - All-In-One PAM

- **Controlled** and **secured** exposure to the Internet
- **Centralized authentication** and **single point of access** for administration of the IS
- Federating portal for **industrialized access management of privileged users**
- Enhanced access security with **MFA** and **secure privileged accounts**
- Reduction in **incident response time**



Licensing

The **PROVE IT license** is based on **the maximum number of simultaneous open sessions to IT resources**. The number of users and resources declared is unlimited.

Purchasing methods

There are **2 purchasing methods** available :

- **Perpetual license** + additional maintenance contract
- **Subscription** : fixed-term license with software maintenance included.

Partners

To support you, we have a **network of certified integrator partners** around the world.

Certifications & qualifications

- **Security VISA** - CSPN by ANSSI *(Ref. 2023/05 - Valid June 2026)*
- **Label France Cybersecurity**
- **Cybersecurity Label Made in Europe**
- **Used by French armies forces**

Compliance : regulations, recommandations, standards

PROVE IT is a strong element in your compliance :

RDPR - ISO 27001 - ANSSI* - NIS1 & NIS2 - TISAX - DORA - PCI-DSS...

Documentation and support

Dedicated editor support in France - The maintenance contract includes the provision of minor and major updates, as well as a vulnerability watch.

Rubycat editor maintenance : corrective, preventive, evolutionary and regulatory.

English and French documentation available directly within the solution.

PROVE IT COMES IN 3 RANGES :

	STANDARD	ADVANCED	CLUSTER
Strong and centralized authentication	✓	✓	✓
Role-based access control to resources (RBAC)	✓	✓	✓
Internal / external connections and administration operations logging	✓	✓	✓
Secure vault for managing sensitive accounts	✓	✓	✓
Recording and archiving sessions	✓	✓	✓
Real-time supervision Reviewing for analysis and corrective action	✓	✓	✓
Advanced event notifications	✓	✓	✓
Configurable retention policy	✓	✓	✓
Profile-based administrative permissions segmentation : auditors / operators / administrators	✗	✓	✓
REST API to ease common administration operations	✗	✓	✓
Delegated Authentication via RADIUS	✗	✓	✓
More than 50 simultaneous sessions	✗	✗	✓
Improved resilience	✗	✗	✓
Disaster Recovery assured thanks to an active/passive architecture with manual failover	Option	Option	Option

*French National Cyber Security Agency

Technical specifications

POC
Free evaluation license on request
Environment
VMWare ESXi 5+
Microsoft Hyper-V 2008+
QEMU/KVM/Nutanix/Proxmox
Delivery and deployment
Virtual Appliance - Installation of an ISO image based on Ubuntu 24.04 LTS, including all PROVE IT components.
Cloud hosting - provision of a cloud-init file
Provision of prerequisites for VM sizing Example : 10 sessions = 4CPU, 3GB RAM, 110Go storage space for 60 days retention
Installation in less than an hour
Intercepting proxy
Compatibility with offline environments
Agent-free / non-invasive
Management on several network interfaces possible
Available in STANDALONE *(STANDARD / ADVANCED) or CLUSTER* versions
Possibility of automating provisioning on the command line - ANSIBLE
Secure internet exposure
Using third-party VPN
Using PROVE IT «Outpost» (HTTPS web fronted) : no sensitive information exposed on the Internet thanks to a diode architecture. Only authenticated data flows through the PROVE IT «Outpost».

Compatible utilities
Minimum RDP version : v8
Minimum SSH version : v2
Minimum web browser version : Chrome 103, Edge 103, Firefox 100
Examples of compatible utilities (non-exhaustive list) · MRemote NG · MobaXterm · Putty · Remmina · Web portals - as RDWeb (Microsoft) · MSTSC
Backup and migration
Automatic locally on VM
Backup import/export capability
Migration script available for upgrading from STANDARD and ADVANCED to CLUSTER versions
Solution lifecycle
Regular updates available · Minors : approximately every 2 months · Major : approximately every 24 months
Documentation : administration, user and installation guides, integration manuals - included in WebAdmin - updated with each release

Contact us for any other configuration

Features

General

Authentication modes on the PAM solution and towards target devices
Local directory (proveit - internal)
Compatible directories: AD, AzureAD, OpenLDAP, LDAPS - Synchronous / Asynchronous
· Multi-factors : interfacing with third-party RADIUS solutions (TrustBuilder / STA / DUO / PrivacyIDEA / Forti. . .) (ADVANCED version) · Multi-factors : Integrated WebAuthn - strong authentication using passkey for web portals (FIDO2 compatible, Windows Hello, smartphone, etc.)
Integrated and configurable fail2ban (number of attempts over a period of time)
Kerberos / Protected Users / Restricted Admin (RDP) compatibility
Authentication mode to targets : (secondary auth.) · Propagation of primary credentials · Using secrets from the vault (SSH key or login / password) · LAPS 2015 for RDP resources · Manual entry by the user
Domains
Management of multiple authentication scenarios
Session management : inactivity timeout, limited number of sessions per use - per domains
License
In increments of 5 sessions
Burst token allows you to unlock the number of license sessions with a single click
User path
Kiosk access - display available resources
Direct access (traceability preserved): · Direct connection to the identified resource · Machine to machine connection
Accès Web : SSH / RDP / HTTPS
Cluster
High resilience
Load balancing – more than 50 sessions
Hosting on the same LAN
Password vault
Protected via PASSPHRASE or SECRET SHARING (key sharing)
1 container per secret
CHACHA20-POLY1305 encryption
API Admin (ADVANCED version)
Automate common administration tasks
Mass import of target resources (using CSV template)

PAM - Managing and controlling privileged access

Access control (RBAC - Role Based Access Control)
Made up of users, services and time filters
Time-based access filters : date interval - date - frequency - times
Access policy toggleable with a single click
WebAdmin in HTTPS - platform administration
ADVANCED version - PROVE IT profile-based administrative permissions segmentation
Session control
Optional session recording
Dissuasion - recording warning message - customizable

SSH : · Allow X11, SCP, SFTP, PIY, SHELL, command execution, record SHELL · session keystrokes · Direct/inverse port forwarding for all non-native protocols (e.g. VNC, SQL, Telnet ...)
RDP : · Allow disk redirection, use of clipboard, dynamic channels, console mode · NLA · Force Restricted Admin mode
HTTP/S : native HTML5
Any other protocol via jump server or SSH tunneling
Web portal
Supports HTTPS, RDP and SSH service access
MFA via RADIUS+ native or WebAuthn integration
IP filters
Tracing and blocking of suspicious accesses (mainly bots and DDoS)
Enhanced protection of legitimate users (CSP, OCSP Stapling)
Encryption
SSH encryption protocol: aes256-ctr,aesl92-ctr,aesl28-ctr
RDP encryption protocol : TLSv1.2-1.3 / ECDHE-ECDSA-AES256-GCMSHA384: ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCMSHA256: ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHERSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA
HTTPS encryption protocol: : TLSv1.2-1.3 / ECDHE-ECDSA-AES128-GCMSHA256: ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCMSHA384: ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305

Auditability - Visibility of actions taken

Logging / Traceability and real-time visibility
Real-time user session supervision
On the fly user session termination
Search by machine name, protocol, authentication date...
SSH, RDP and HTTP/S session logging
Watch in the browser or download recordings locally
Video : average 1.5 MB/minute/active session
Configurable retention time for recordings and logs
Logs
User : authentication, other events...
PROVE IT administrator : authentication, actions performed on the WebAdmin
Notifications via SMTP (email) or Syslog
Alert with granular configuration *E.g. : successful connection of a user to a particular service*
System alerts - threshold exceeded, number of sessions, storage volume, etc.
SNMP
Ubuntu MIB

rubycat control & trace

RUBYCAT is a French software publisher specializing in traceability and access control for information systems.
We bring you our expertise in cybersecurity and securing access to help you find an easy solution to a major problem : the lack of visibility over the actions carried out by privileged accounts on your information systems.

RUBYCAT - Le Luthétium, 3 Square du Chêne Germain, 35510 Cesson-Sévigné (FRANCE)
Telephone : + 33 (0)2 99 30 21 11 – sales@rubycat.eu – www.rubycat.eu